

DDOS PROTECTION & MITIGATION MARKET

GLOBAL FORECAST TO 2031

BY SOLUTION TYPE (NETWORK TRAFFIC ANALYZERS, BOTNET DETECTION & MANAGEMENT), APPLICATION AREA (NETWORK & IP, WEB APPLICATIONS & API, DNS INFRASTRUCTURE), VERTICAL (BFSI, ENERGY & UTILITIES)

MarketsandMarkets™ is the world's largest revenue impact company, serving over 7500 customers. 80% of top 2000 companies globally rely on us for identifying new high growth and niche revenue opportunities. In the face of constant technology innovation and market disruption, we help organizations plan and operationalize their future revenue mix decisions by identifying over 30,000 high growth opportunities ranging from \$1B to \$500B across 90+ industry trends and markets. Organizations choose MarketsandMarkets™ to stay ahead of the curve and accelerate their revenue decisions and implementations by 6 – 12 months, giving them a unique, first-mover advantage. Our revenue impact methodology provides quantified and actionable insights on converged, granular and connected market ecosystems that result from disruptive technologies and high-growth markets. We provide an extended lens on not only what will impact our client's revenue but also what will impact their clients' revenues, continually uncovering latent opportunities.

We work across all major B2B industries with C-level executives in functions such as Strategy, Marketing, Sales, R&D, Product, and M&A. MarketsandMarkets™ brings exclusive high-growth markets intelligence generated by over 850 SMEs and analysts along with its proprietary Revenue Impact platform (KnowledgeStore).

Copyright © 2026 MarketsandMarkets™

All Rights Reserved. This document contains highly confidential information and is the sole property of MarketsandMarkets™. No part of it shall be circulated, copied, quoted, or otherwise reproduced without the prior written approval of MarketsandMarkets™.

TABLE OF CONTENTS

1	INTRODUCTION.....	47
1.1	STUDY OBJECTIVES.....	47
1.2	MARKET DEFINITION.....	47
1.3	STUDY SCOPE AND SEGMENTATION.....	48
1.3.1	MARKET SEGMENTATION AND REGIONS COVERED	48
1.3.2	INCLUSIONS & EXCLUSIONS	49
1.3.3	YEARS CONSIDERED	50
1.4	CURRENCY CONSIDERED	50
1.5	STAKEHOLDERS	51
1.6	SUMMARY OF CHANGES.....	51
2	EXECUTIVE SUMMARY.....	52
2.1	KEY INSIGHTS AND MARKET HIGHLIGHTS.....	52
2.2	KEY MARKET PARTICIPANTS: MAPPING OF STRATEGIC DEVELOPMENTS	53
2.3	DISRUPTIONS SHAPING MARKET	54
2.4	HIGH-GROWTH SEGMENTS	55
2.5	SNAPSHOT: GLOBAL MARKET SIZE, GROWTH RATE, AND FORECAST	56
3	PREMIUM INSIGHTS	57
3.1	ATTRACTIVE OPPORTUNITIES FOR PLAYERS IN DDOS PROTECTION & MITIGATION MARKET	57
3.2	DDOS PROTECTION & MITIGATION MARKET, BY OFFERING	58
3.3	DDOS PROTECTION & MITIGATION MARKET, BY SOLUTION	58
3.4	DDOS PROTECTION & MITIGATION MARKET, BY SOLUTION TYPE	59
3.5	DDOS PROTECTION & MITIGATION MARKET, BY SERVICE.....	59
3.6	DDOS PROTECTION & MITIGATION MARKET, BY APPLICATION AREA.....	60
3.7	DDOS PROTECTION & MITIGATION MARKET, BY VERTICAL	60
3.8	DDOS PROTECTION & MITIGATION MARKET, BY REGION.....	61
4	MARKET OVERVIEW.....	62
4.1	INTRODUCTION	62
4.2	MARKET DYNAMICS.....	62
4.2.1	DRIVERS	63
4.2.1.1	Rising frequency and complexity of DDoS attacks.....	63
4.2.1.2	Proliferation of IoT botnets and DDoS-for-hire services	63
4.2.1.3	Growing dependence on internet-facing applications, APIs, cloud services, and digital infrastructure	64
4.2.1.4	Increasing targeting of critical infrastructure through geopolitical and hacktivist-driven DDoS campaigns.....	64

4.2.2	RESTRAINTS.....	64
4.2.2.1	Limited integration across multi-vendor environments.....	64
4.2.2.2	Regulatory and data sovereignty constraints	65
4.2.3	OPPORTUNITIES.....	65
4.2.3.1	Growing adoption of AI-driven and autonomous DDoS detection and mitigation	65
4.2.3.2	Expansion of DDoS protection for APIs, AI applications, and cloud-native workloads	65
4.2.3.3	Increasing demand for integrated, hybrid, and managed DDoS protection	66
4.2.4	CHALLENGES	66
4.2.4.1	Lack of skilled cybersecurity professionals	66
4.2.4.2	Cost and complexity of solutions.....	66
4.3	UNMET NEEDS AND WHITE SPACES	67
4.4	INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES.....	68
4.4.1	INTERCONNECTED MARKETS.....	68
4.4.2	CROSS-SECTOR OPPORTUNITIES.....	69
4.5	STRATEGIC MOVES BY TIER-1/2/3 PLAYERS.....	70
4.5.1	CROSS-TIER STRATEGIC PATTERNS	71
4.5.2	STRATEGIC TRENDS	72
4.5.2.1	AI-Driven and Autonomous DDoS Detection and Mitigation	73
4.5.2.2	Increasing Focus on Application, API, and DNS Protection	73
4.5.2.3	Shift Toward Cloud-Native and Hybrid DDoS Protection	73
5	INDUSTRY TRENDS	74
5.1	PORTER'S FIVE FORCES ANALYSIS	74
5.1.1	THREAT OF NEW ENTRANTS	75
5.1.2	THREAT OF SUBSTITUTES.....	75
5.1.3	BARGAINING POWER OF SUPPLIERS	76
5.1.4	BARGAINING POWER OF BUYERS	76
5.1.5	INTENSITY OF COMPETITIVE RIVALRY	76
5.2	MACROECONOMICS INDICATORS.....	76
5.2.1	INTRODUCTION	76
5.2.2	GDP TRENDS AND FORECAST	77
5.2.3	TRENDS IN GLOBAL DDOS PROTECTION & MITIGATION INDUSTRY	78
5.3	VALUE CHAIN ANALYSIS	79
5.3.1	TRAFFIC MONITORING & ANALYSIS.....	79
5.3.2	DDOS PROTECTION SOLUTIONS.....	80
5.3.3	SYSTEM INTEGRATION & DEPLOYMENT.....	80
5.3.4	MANAGED SERVICES & DISTRIBUTION	80
5.3.5	END USERS.....	80
5.4	ECOSYSTEM ANALYSIS	81

5.5	PRICING ANALYSIS	82
5.5.1	AVERAGE SELLING PRICE TREND OF KEY PLAYERS, BY OFFERING, 2025.....	82
5.5.2	INDICATIVE PRICING ANALYSIS OF DDOS PROTECTION AND MITIGATION, BY OFFERING, 2025.....	83
5.6	KEY CONFERENCES AND EVENTS	84
5.7	TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS	84
5.8	INVESTMENT AND FUNDING SCENARIO.....	85
5.9	CASE STUDY ANALYSIS.....	85
5.9.1	NEXUSGUARD EMPOWERED IRIX AND SAINS TO OVERCOME DDOS THREATS	85
5.9.2	XTEL COMMUNICATIONS CHOSE NETSCOUT TO IMPROVE VISIBILITY INTO NETWORK TRAFFIC	86
5.9.3	PENTELEDATA SELECTED RADWARE'S AMS FOR TECHNICAL INTEGRATION WITH KENTIK TECHNOLOGIES	86
5.9.4	CNI CHOSE CORERO TO PROTECT ITS CUSTOMERS FROM DDOS ATTACKS.....	87
5.10	DDOS PREVENTION TECHNIQUES.....	88
5.11	IMPACT OF 2025 US TARIFF – DDOS PROTECTION AND MITIGATION MARKET	88
5.11.1	INTRODUCTION	88
5.11.2	KEY TARIFF RATES	89
5.11.3	PRICE IMPACT ANALYSIS.....	91
5.11.4	IMPACT ON COUNTRY/REGION.....	92
5.11.4.1	North America	92
5.11.4.2	Europe	93
5.11.4.3	Asia Pacific	94
5.11.5	IMPACT ON END-USE INDUSTRIES.....	95
6	TECHNOLOGICAL ADVANCEMENTS, AI-DRIVEN IMPACT, PATENTS, INNOVATIONS, AND FUTURE APPLICATIONS	96
6.1	TECHNOLOGY ANALYSIS	96
6.1.1	KEY EMERGING TECHNOLOGIES	96
6.1.1.1	Traffic filtering.....	96
6.1.1.2	Rate limiting	96
6.1.1.3	Web application firewall (WAF).....	96
6.1.2	COMPLEMENTARY TECHNOLOGIES.....	97
6.1.2.1	Artificial intelligence (AI).....	97
6.1.2.2	Machine learning (ML).....	97
6.1.3	ADJACENT TECHNOLOGIES	97
6.1.3.1	Load balancers.....	97
6.1.3.2	Content delivery networks (CDNs)	98

6.2	TECHNOLOGY ROADMAP	98
6.2.1	SHORT-TERM (2026–2027) FOUNDATION & CLOUD-BASED PROTECTION	98
6.2.2	MID-TERM (2027–2030) INTELLIGENT AUTOMATION & UNIFIED DDOS PROTECTION	98
6.2.3	LONG-TERM (2030–2035+) AUTONOMOUS, ADAPTIVE & AI-DRIVEN DDOS DEFENSE	99
6.3	PATENT ANALYSIS	99
6.4	FUTURE APPLICATIONS.....	102
6.4.1	AUTONOMOUS AND AI-DRIVEN DDOS PROTECTION	102
6.4.2	APPLICATION-LAYER AND API-BASED DDOS PROTECTION	103
6.4.3	ADAPTIVE MULTI-LAYER AND MULTI-VECTOR DDOS MITIGATION.....	103
6.4.4	CLOUD, EDGE AND MULTI-CLOUD DDOS RESILIENCE.....	103
6.4.5	IOT AND BOTNET-BASED DDOS PROTECTION	104
6.5	IMPACT OF AI/GEN AI ON DDOS PROTECTION AND MITIGATION MARKET	104
6.5.1	BEST PRACTICES IN DDOS PROTECTION & MITIGATION MARKET	105
6.5.2	CASE STUDIES OF AI IMPLEMENTATION IN DDOS PROTECTION & MITIGATION MARKET	106
6.5.3	INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS	107
6.5.4	CLIENTS' READINESS TO ADOPT GENERATIVE AI IN DDOS PROTECTION & MITIGATION MARKET	107
6.6	SUCCESS STORIES AND REAL-WORLD APPLICATIONS.....	108
6.6.1	CLOUDFLARE: DDOS PROTECTION FOR A GLOBAL RETAILER	108
6.6.2	NETSCOUT: DDOS PROTECTION FOR A GLOBAL MANUFACTURER	108
7	REGULATORY LANDSCAPE	109
7.1	REGULATORY LANDSCAPE	109
7.1.1	REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	109
7.1.2	INDUSTRY STANDARDS	113
8	CUSTOMER LANDSCAPE AND BUYER BEHAVIOR.....	115
8.1	DECISION-MAKING PROCESS.....	115
8.2	BUYER STAKEHOLDERS AND BUYING EVALUATION CRITERIA	116
8.2.1	KEY STAKEHOLDERS IN BUYING PROCESS.....	116
8.2.2	BUYING CRITERIA.....	116
8.2.3	ADOPTION BARRIERS AND INTERNAL CHALLENGES	117
8.3	UNMET NEEDS IN VARIOUS END-USE INDUSTRIES	118
8.3.1	REVENUE POTENTIAL.....	119
8.3.2	COST DYNAMICS.....	120
8.3.3	MARGIN OPPORTUNITIES IN KEY APPLICATIONS	120

9	DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING.....	122
9.1	INTRODUCTION	123
9.1.1	OFFERING: DDOS PROTECTION AND MITIGATION MARKET DRIVERS	123
9.2	SOLUTIONS	124
9.2.1	HARDWARE.....	126
9.2.1.1	Firewalls	127
9.2.1.1.1	Hardware firewalls filter and block malicious traffic to enable efficient server access for legitimate requests	127
9.2.1.2	Intrusion Detection and Prevention Systems (IDPS)	127
9.2.1.2.1	IDPS prevents DDoS attacks by continuously monitoring network traffic and actively blocking malicious requests.....	127
9.2.1.3	Load Balancers	127
9.2.1.3.1	Load balancers protect against DDoS attacks by distributing traffic across multiple servers.....	127
9.2.1.4	Other hardware	127
9.2.2	SOFTWARE/PLATFORMS	128
9.2.2.1	Global rise in IoT devices to drive market.....	128
9.3	SERVICES	129
9.3.1	PROFESSIONAL SERVICES	131
9.3.1.1	Design and implementation.....	133
9.3.1.1.1	Increase in need to improve network performance and reliability	133
9.3.1.2	Consulting and advisory.....	134
9.3.1.2.1	Growing concerns for cybersecurity and adoption of advanced technologies	134
9.3.1.3	Training and education	135
9.3.1.3.1	Rising need for training and creating awareness of DDoS attacks	135
9.3.1.4	Support and maintenance	136
9.3.1.4.1	Rising need for support for technical issues and guidance.....	136
9.3.1.5	DDoS testing and validation	137
9.3.1.5.1	Identify vulnerabilities and evaluate the effectiveness, capacity, and responsiveness of existing DDoS mitigation mechanisms	137
9.3.2	MANAGED SERVICES	138
9.3.2.1	Need to increase business efficiency and operations	138
10	DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE	139
10.1	INTRODUCTION	140
10.1.1	SOLUTION TYPE: DDOS PROTECTION AND MITIGATION MARKET DRIVERS	140
10.2	NETWORK TRAFFIC ANALYZERS	141
10.2.1	NETWORK LAYER ATTACKS TO INCREASE ADOPTION OF DDOS PROTECTION SOLUTIONS.....	141

10.3	THREAT MITIGATION SYSTEMS	142
10.3.1	RISE IN LAYER 7 ATTACKS TO INCREASE DEMAND FOR DDOS PROTECTION AND MITIGATION SOLUTIONS	142
10.4	BOTNET DETECTION & MANAGEMENT	143
10.4.1	EVOLVING DISRUPTIVE TECHNOLOGIES AND EASY AVAILABILITY OF CLOUD-BASED APPLICATIONS TO DRIVE MARKET	143
10.5	OTHER SOLUTION TYPES	144
11	DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA	146
11.1	INTRODUCTION	147
11.1.1	APPLICATION AREA: DDOS PROTECTION AND MITIGATION MARKET DRIVERS	147
11.2	NETWORK & IP INFRASTRUCTURE.....	148
11.2.1	INCREASING NEED FOR HIGH-CAPACITY, ALWAYS-ON PROTECTION CAPABLE OF ABSORBING AND FILTERING MALICIOUS TRAFFIC	148
11.3	WEB APPLICATIONS & APIS	149
11.3.1	RISING NEED TO MITIGATE DDOS ATTACKS AND MAINTAIN PROTECTION	149
11.4	DNS INFRASTRUCTURE.....	150
11.4.1	INCREASING DEPENDENCE ON ONLINE APPLICATIONS AND DISTRIBUTED DIGITAL INFRASTRUCTURE IS DRIVING MARKET	150
12	DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE	152
12.1	INTRODUCTION	153
12.1.1	DEPLOYMENT MODE: DDOS PROTECTION AND MITIGATION MARKET DRIVERS.....	153
12.2	ON-PREMISES.....	154
12.2.1	ON-PREMISE SERVICES PROVIDE FULL CONTROL OF DEPLOYED SOLUTIONS TO IT STAFF	154
12.3	CLOUD	155
12.3.1	CLOUD DEPLOYMENT HELPS MANAGE DNS, REROUTE TRAFFIC, AND SAFEGUARD WEBSITE TRAFFIC.....	155
12.4	HYBRID	156
12.4.1	ENABLE ORGANIZATIONS TO DISTRIBUTE PROTECTION ACCORDING TO THE CHARACTERISTICS AND SCALE OF THEIR INFRASTRUCTURE.....	156
13	DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE	158
13.1	INTRODUCTION	159
13.1.1	ORGANIZATION SIZE: DDOS PROTECTION AND MITIGATION MARKET DRIVERS	159
13.2	LARGE ENTERPRISES.....	160
13.2.1	INCREASING SEVERITY OF DDOS DAMAGE CAUSED BY SINGLE ATTACK TO DRIVE MARKET.....	160
13.3	SMALL & MEDIUM-SIZED ENTERPRISES	161
13.3.1	GROWING NEED TO MITIGATE SECURITY ATTACKS TO ENHANCE MARKET GROWTH	161

14	DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL.....	163
14.1	INTRODUCTION	164
14.1.1	VERTICAL: DDOS PROTECTION AND MITIGATION MARKET DRIVERS	164
14.2	BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI)	166
14.2.1	FRAGILE DATA CENTER SECURITY AND RISK OF CLOUD STORAGE DATA LEAKS TO DRIVE MARKET	166
14.3	GOVERNMENT & DEFENSE.....	167
14.3.1	INCREASING NEED FOR DDOS PROTECTION AND MITIGATION SOLUTIONS AND SERVICES TO HELP MARKET GROWTH	167
14.4	MANUFACTURING	168
14.4.1	EVOLVING VOLUMETRIC DDOS ATTACKS ON MANUFACTURING PROCESSES TO CONTRIBUTE TO MARKET GROWTH.....	168
14.5	ENERGY & UTILITIES	169
14.5.1	INCREASING ADOPTION OF SMART SYSTEMS AND APPLICATIONS TO DRIVE MARKET.....	169
14.6	IT AND ITES	170
14.6.1	RISE OF ADVANCED TECHNOLOGIES TO FUEL MARKET	170
14.7	TELECOMMUNICATIONS	171
14.7.1	RISE IN NUMBER OF WEB AND MOBILE APPLICATIONS TO FUEL MARKET	171
14.8	HEALTHCARE.....	172
14.8.1	REGULATORY NORMS TO INCREASE DEPLOYMENT OF DDOS PROTECTION AND MITIGATION SOLUTIONS	172
14.9	EDUCATION	173
14.9.1	NEED FOR CONFIDENTIALITY, INTEGRITY, AND EASY AVAILABILITY OF DATA AND RESOURCES TO AUGMENT MARKET GROWTH	173
14.10	RETAIL	174
14.10.1	GROWING CYBERATTACKS AND DATA THEFT TO INCREASE ADOPTION OF DDOS PROTECTION AND MITIGATION SOLUTIONS	174
14.11	OTHER VERTICALS	175
15	DDOS PROTECTION AND MITIGATION MARKET, BY REGION	177
15.1	INTRODUCTION	178
15.2	NORTH AMERICA	179
15.2.1	US	185
15.2.1.1	Presence of major vendors in US driving market growth	185
15.2.2	CANADA.....	190
15.2.2.1	Rapid technological advancements and increasing DDoS attacks on network infrastructure to drive market.....	190

15.3	EUROPE	196
15.3.1	UK	202
15.3.1.1	Increasing demand for monitoring solutions among SMEs to drive market	202
15.3.2	GERMANY	207
15.3.2.1	Increasing investments in DDoS protection and mitigation solutions to drive market	207
15.3.3	FRANCE	212
15.3.3.1	Market is driven by the growing exposure of critical sectors to cyber threats	212
15.3.4	ITALY	217
15.3.4.1	The market is driven by increasing cyber threats in critical infrastructure	217
15.3.5	REST OF EUROPE	222
15.4	ASIA PACIFIC	227
15.4.1	CHINA	234
15.4.1.1	Development of cybersecurity safeguard system to fuel market	234
15.4.2	JAPAN	239
15.4.2.1	Stringent laws and regulations for cybersecurity to drive market	239
15.4.3	INDIA	244
15.4.3.1	Increasing DDoS attacks leading to adoption of DDoS protection and mitigation solutions	244
15.4.4	REST OF ASIA PACIFIC	249
15.5	MIDDLE EAST & AFRICA	254
15.5.1	GCC	259
15.5.1.1	KSA	265
15.5.1.1.1	Increasing investments in mitigation and growth in number of startups to drive market	265
15.5.1.2	UAE	270
15.5.1.2.1	Growing reliance on cloud-based applications to boost market	270
15.5.1.3	Rest of GCC	275
15.5.2	SOUTH AFRICA	280
15.5.2.1	Government initiatives and substantial foreign investments to drive market	280
15.5.3	REST OF MIDDLE EAST & AFRICA	285
15.6	LATIN AMERICA	290
15.6.1	BRAZIL	296
15.6.1.1	Increasing focus on establishing effective cybersecurity strategies to drive market	296
15.6.2	MEXICO	301
15.6.2.1	Rising adoption of cloud-based services to drive market	301
15.6.3	REST OF LATIN AMERICA	306

16	COMPETITIVE LANDSCAPE	312
16.1	INTRODUCTION	312
16.2	KEY PLAYER STRATEGIES/RIGHT TO WIN, 2022–2025	312
16.3	REVENUE ANALYSIS, 2021–2025.....	314
16.4	MARKET SHARE ANALYSIS, 2025	314
16.5	BRAND COMPARISON	318
16.6	COMPANY VALUATION AND FINANCIAL METRICS, 2025	319
16.6.1	COMPANY VALUATION	319
16.6.2	FINANCIAL METRICS	319
16.7	COMPANY EVALUATION MATRIX: KEY PLAYERS, 2025.....	319
16.7.1	STARS.....	320
16.7.2	EMERGING LEADERS.....	320
16.7.3	PERVASIVE PLAYERS.....	320
16.7.4	PARTICIPANTS	320
16.7.5	COMPANY FOOTPRINT: KEY PLAYERS, 2025.....	322
16.7.5.1	Company footprint.....	322
16.7.5.2	Regional footprint	323
16.7.5.3	Offering footprint.....	324
16.7.5.4	Vertical footprint	325
16.8	COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2025.....	326
16.8.1	PROGRESSIVE COMPANIES.....	326
16.8.2	RESPONSIVE COMPANIES	326
16.8.3	DYNAMIC COMPANIES	327
16.8.4	STARTING BLOCKS	327
16.8.5	COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2025	328
16.8.5.1	Detailed list of key startups/SMEs	328
16.8.5.2	Competitive benchmarking of key startups/SMEs	329
16.9	COMPETITIVE SCENARIO & TRENDS.....	329
16.9.1	PRODUCT LAUNCHES & ENHANCEMENTS.....	329
16.9.2	DEALS.....	332
16.9.3	EXPANSIONS.....	333
17	COMPANY PROFILES.....	334
17.1	KEY PLAYERS.....	334
17.1.1	AKAMAI	334
17.1.1.1	Business overview	334
17.1.1.2	Products/Solutions/Services offered.....	335
17.1.1.3	Recent developments.....	336
17.1.1.3.1	Product launches & enhancements	336
17.1.1.3.2	Deals.....	337
17.1.1.4	MnM view.....	337
17.1.1.4.1	Right to win.....	337

17.1.1.4.2	Strategic choices	337
17.1.1.4.3	Weaknesses and competitive threats	337
17.1.2	CLOUDFLARE	338
17.1.2.1	Business overview	338
17.1.2.2	Products/Solutions/Services offered	339
17.1.2.3	Recent developments	340
17.1.2.3.1	Product launches & enhancements	340
17.1.2.3.2	Deals	341
17.1.2.4	MnM view	341
17.1.2.4.1	Key strengths	341
17.1.2.4.2	Strategic choices	341
17.1.2.4.3	Weaknesses and competitive threats	341
17.1.3	RADWARE	342
17.1.3.1	Business overview	342
17.1.3.2	Products/Solutions/Services offered	343
17.1.3.3	Recent developments	344
17.1.3.3.1	Product launches & enhancements	344
17.1.3.3.2	Deals	345
17.1.3.4	MnM view	346
17.1.3.4.1	Right to win	346
17.1.3.4.2	Strategic choices	346
17.1.3.4.3	Weaknesses and competitive threats	346
17.1.4	FORTINET	347
17.1.4.1	Business overview	347
17.1.4.2	Products/Solutions/Services offered	348
17.1.4.3	Recent developments	349
17.1.4.3.1	Product launches & enhancements	349
17.1.4.4	MnM view	349
17.1.4.4.1	Key strengths	349
17.1.4.4.2	Strategic choices	349
17.1.4.4.3	Weaknesses and competitive threats	349
17.1.5	NETSCOUT	350
17.1.5.1	Business overview	350
17.1.5.2	Products/Solutions/Services offered	351
17.1.5.3	Recent developments	352
17.1.5.3.1	Product launches & enhancements	352
17.1.5.3.2	Expansions	352
17.1.5.4	MnM view	353
17.1.5.4.1	Right to win	353
17.1.5.4.2	Strategic choices	353
17.1.5.4.3	Weaknesses and competitive threats	353

17.1.6	NEXUSGUARD	354
17.1.6.1	Business overview	354
17.1.6.2	Products/Solutions/Services offered.....	354
17.1.6.3	Recent developments	355
17.1.6.3.1	Product launches & enhancements	355
17.1.6.3.2	Deals.....	356
17.1.7	HUAWEI	357
17.1.7.1	Business overview	357
17.1.7.2	Products/Solutions/Services offered.....	358
17.1.7.3	Recent developments	359
17.1.7.3.1	Product launches & enhancements	359
17.1.8	LINK11	360
17.1.8.1	Business overview	360
17.1.8.2	Products/Solutions/Services offered.....	360
17.1.8.3	Recent developments	361
17.1.8.3.1	Product launches & enhancements	361
17.1.8.3.2	Deals.....	362
17.1.9	THALES (IMPERVA)	363
17.1.9.1	Business overview	363
17.1.9.2	Products/Solutions/Services offered.....	364
17.1.9.3	Recent developments	365
17.1.9.3.1	Product launches & enhancements	365
17.1.10	BT.....	366
17.1.10.1	Business overview	366
17.1.10.2	Products/Solutions/Services offered.....	367
17.1.11	A10 NETWORKS	368
17.1.11.1	Business overview	368
17.1.11.2	Products/Solutions/Services offered.....	369
17.1.11.3	Recent developments	370
17.1.11.3.1	Product launches & enhancements	370
17.1.11.3.2	Deals.....	370
17.1.12	NSFOCUS	371
17.1.12.1	Business overview	371
17.1.12.2	Products/Solutions/Services offered.....	371
17.1.13	MICROSOFT	373
17.1.13.1	Business overview	373
17.1.13.2	Products/Solutions/Services offered.....	374
17.1.13.3	Recent developments	375
17.1.13.3.1	Product launches & enhancements	375

17.1.14	F5.....	376
17.1.14.1	Business overview	376
17.1.14.2	Products/Solutions/Services offered.....	377
17.1.14.3	Recent developments	378
17.1.14.3.1	Product launches & enhancements	378
17.1.14.3.2	Deals.....	379
17.1.15	ALIBABA CLOUD.....	380
17.1.15.1	Business overview	380
17.1.15.2	Products/Solutions/Services offered.....	381
17.1.15.3	Recent developments	382
17.1.15.3.1	Product launches & enhancements	382
17.1.16	CORERO	384
17.1.16.1	Business Overview	384
17.1.16.2	Products/Solutions/Services offered.....	385
17.1.16.3	Recent developments	386
17.1.16.3.1	Product launches & enhancements	386
17.1.16.3.2	Deals.....	387
17.1.17	AWS.....	389
17.1.17.1	Business Overview	389
17.1.17.2	Products/Solutions/Services offered.....	390
17.1.17.3	Recent developments	391
17.1.17.3.1	Product launches & enhancements	391
17.2	OTHER KEY PLAYERS.....	392
17.2.1	FASTLY.....	392
17.2.2	ALLOT	393
17.2.3	STRATACORE	394
17.2.4	SUCURI (GODADDY)	395
17.2.5	LUMEN TECHNOLOGIES.....	396
17.2.6	SECEON.....	397
17.2.7	HALTDOS	398
17.2.8	DDOS-GUARD	399
17.2.9	INDUSFACE.....	400
17.2.10	MLYTICS	401
17.2.11	RIOREY	402
17.2.12	PHOENIXNAP	402
17.2.13	XCITIUM.....	403
17.2.14	MAZEBOLT	404
17.2.15	QRATOR LABS.....	405
17.2.16	GCORE.....	406

18	RESEARCH METHODOLOGY.....	407
18.1	RESEARCH DATA	407
18.1.1	SECONDARY DATA.....	408
18.1.2	PRIMARY DATA.....	408
18.1.2.1	Breakup of primary profiles.....	409
18.1.2.2	Key industry insights.....	409
18.2	DATA TRIANGULATION	410
18.3	MARKET SIZE ESTIMATION	410
18.3.1	TOP-DOWN APPROACH.....	411
18.3.2	BOTTOM-UP APPROACH	411
18.4	MARKET FORECAST	414
18.5	RESEARCH ASSUMPTIONS	416
18.6	RESEARCH LIMITATIONS.....	417
19	APPENDIX.....	418
19.1	DISCUSSION GUIDE	418
19.2	KNOWLEDGESTORE: MARKETSandMARKETS' SUBSCRIPTION PORTAL.....	422
19.3	CUSTOMIZATION OPTIONS.....	424
19.4	RELATED REPORTS	424
19.5	AUTHOR DETAILS.....	425

LIST OF TABLES

TABLE 1	INCLUSIONS & EXCLUSIONS	49
TABLE 2	USD EXCHANGE RATES, 2021–2025	50
TABLE 3	UNMET NEEDS AND WHITE SPACES IN DDOS PROTECTION AND MITIGATION MARKET	67
TABLE 4	STRATEGIC MOVES BY PLAYERS IN DDOS PROTECTION & MITIGATION MARKET	71
TABLE 5	CROSS-TIER STRATEGIC PATTERNS OF VENDORS	72
TABLE 6	IMPACT OF PORTER'S FIVE FORCES ON DDOS PROTECTION AND MITIGATION MARKET	74
TABLE 7	GDP PERCENTAGE CHANGE, BY KEY COUNTRY, 2021–2030	77
TABLE 8	ROLE OF COMPANIES IN ECOSYSTEM	81
TABLE 9	AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2025	83
TABLE 10	INDICATIVE PRICING ANALYSIS OF DDOS PROTECTION AND MITIGATION, BY OFFERING, 2025	83
TABLE 11	DDOS PROTECTION AND MITIGATION MARKET: LIST OF KEY CONFERENCES AND EVENTS, 2026–2027	84
TABLE 12	KEY TARIFF RATES	89
TABLE 13	EXPECTED CHANGE IN PRICES AND LIKELY IMPACT ON END-USE MARKET DUE TO TARIFF IMPACT	92
TABLE 14	LIST OF TOP PATENTS IN DDOS PROTECTION & MITIGATION MARKET, 2024–2026	100
TABLE 15	TOP USE CASES AND MARKET POTENTIAL	105
TABLE 16	BEST PRACTICES: COMPANIES IMPLEMENTING USE CASES	105
TABLE 17	DDOS PROTECTION & MITIGATION MARKET: CASE STUDIES RELATED TO GEN AI IMPLEMENTATION	106
TABLE 18	INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS	107
TABLE 19	NORTH AMERICA: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	109
TABLE 20	EUROPE: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	110
TABLE 21	ASIA PACIFIC: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	111
TABLE 22	REST OF THE WORLD: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	112
TABLE 23	GLOBAL INDUSTRY STANDARDS IN DDOS PROTECTION & MITIGATION MARKET	113
TABLE 24	INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS (%)	116
TABLE 25	KEY BUYING CRITERIA FOR TOP THREE VERTICALS	117
TABLE 26	UNMET NEEDS IN DDOS PROTECTION & MITIGATION MARKET, BY END-USE INDUSTRY	119
TABLE 27	DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	124
TABLE 28	DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	124
TABLE 29	DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	125
TABLE 30	DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	125

TABLE 31	DDOS PROTECTION AND MITIGATION SOLUTIONS MARKET, BY REGION, 2020–2025 (USD MILLION)	125
TABLE 32	DDOS PROTECTION AND MITIGATION SOLUTIONS MARKET, BY REGION, 2026–2031 (USD MILLION)	125
TABLE 33	DDOS PROTECTION AND MITIGATION HARDWARE MARKET, BY REGION, 2020–2025 (USD MILLION)	126
TABLE 34	DDOS PROTECTION AND MITIGATION HARDWARE MARKET, BY REGION, 2026–2031 (USD MILLION)	126
TABLE 35	DDOS PROTECTION AND MITIGATION SOFTWARE/PLATFORMS MARKET, BY REGION, 2020–2025 (USD MILLION)	128
TABLE 36	DDOS PROTECTION AND MITIGATION SOFTWARE/PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)	129
TABLE 37	DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	130
TABLE 38	DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	130
TABLE 39	DDOS PROTECTION AND MITIGATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	130
TABLE 40	DDOS PROTECTION AND MITIGATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	130
TABLE 41	DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	131
TABLE 42	DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	132
TABLE 43	DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY TYPE, 2020–2025 (USD MILLION)	132
TABLE 44	DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY TYPE, 2026–2031 (USD MILLION)	132
TABLE 45	DDOS PROTECTION AND MITIGATION DESIGN AND IMPLEMENTATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	133
TABLE 46	DDOS PROTECTION AND MITIGATION DESIGN AND IMPLEMENTATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	133
TABLE 47	DDOS PROTECTION AND MITIGATION CONSULTING AND ADVISORY SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	134
TABLE 48	DDOS PROTECTION AND MITIGATION CONSULTING AND ADVISORY SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	134
TABLE 49	DDOS PROTECTION AND MITIGATION TRAINING AND EDUCATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	135
TABLE 50	DDOS PROTECTION AND MITIGATION TRAINING AND EDUCATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	135
TABLE 51	DDOS PROTECTION AND MITIGATION SUPPORT AND MAINTENANCE SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	136
TABLE 52	DDOS PROTECTION AND MITIGATION SUPPORT AND MAINTENANCE SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	136
TABLE 53	DDOS PROTECTION AND MITIGATION DDOS TESTING AND VALIDATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	137
TABLE 54	DDOS PROTECTION AND MITIGATION DDOS TESTING AND VALIDATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	137
TABLE 55	DDOS PROTECTION AND MITIGATION MANAGED SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)	138
TABLE 56	DDOS PROTECTION AND MITIGATION MANAGED SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)	138

TABLE 57	DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	141
TABLE 58	DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	141
TABLE 59	DDOS PROTECTION AND MITIGATION NETWORK TRAFFIC ANALYZERS MARKET, BY REGION, 2020–2025 (USD MILLION)	142
TABLE 60	DDOS PROTECTION AND MITIGATION NETWORK TRAFFIC ANALYZERS MARKET, BY REGION, 2026–2031 (USD MILLION)	142
TABLE 61	DDOS PROTECTION AND MITIGATION THREAT MITIGATION SYSTEMS MARKET, BY REGION, 2020–2025 (USD MILLION)	143
TABLE 62	DDOS PROTECTION AND MITIGATION THREAT MITIGATION SYSTEMS MARKET, BY REGION, 2026–2031 (USD MILLION)	143
TABLE 63	DDOS PROTECTION AND MITIGATION BOTNET DETECTION & MANAGEMENT MARKET, BY REGION, 2020–2025 (USD MILLION)	144
TABLE 64	DDOS PROTECTION AND MITIGATION BOTNET DETECTION & MANAGEMENT MARKET, BY REGION, 2026–2031 (USD MILLION)	144
TABLE 65	OTHER DDOS PROTECTION AND MITIGATION SOLUTION TYPES MARKET, BY REGION, 2020–2025 (USD MILLION)	145
TABLE 66	OTHER DDOS PROTECTION AND MITIGATION SOLUTION TYPES MARKET, BY REGION, 2026–2031 (USD MILLION)	145
TABLE 67	DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	148
TABLE 68	DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	148
TABLE 69	DDOS PROTECTION AND MITIGATION MARKET IN NETWORK & IP INFRASTRUCTURE, BY REGION, 2020–2025 (USD MILLION)	149
TABLE 70	DDOS PROTECTION AND MITIGATION MARKET IN NETWORK & IP INFRASTRUCTURE, BY REGION, 2026–2031 (USD MILLION)	149
TABLE 71	DDOS PROTECTION AND MITIGATION MARKET IN WEB APPLICATIONS & APIS, BY REGION, 2020–2025 (USD MILLION)	150
TABLE 72	DDOS PROTECTION AND MITIGATION MARKET IN WEB APPLICATIONS & APIS, BY REGION, 2026–2031 (USD MILLION)	150
TABLE 73	DDOS PROTECTION AND MITIGATION MARKET IN DNS INFRASTRUCTURE, BY REGION, 2020–2025 (USD MILLION)	151
TABLE 74	DDOS PROTECTION AND MITIGATION MARKET IN DNS INFRASTRUCTURE, BY REGION, 2026–2031 (USD MILLION)	151
TABLE 75	DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	154
TABLE 76	DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	154
TABLE 77	ON-PREMISE DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)	154
TABLE 78	ON-PREMISE DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2026–2031 (USD MILLION)	155
TABLE 79	CLOUD-BASED DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)	155
TABLE 80	CLOUD-BASED DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2026–2031 (USD MILLION)	156
TABLE 81	HYBRID DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)	156
TABLE 82	HYBRID DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2026–2031 (USD MILLION)	157

TABLE 83	DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	159
TABLE 84	DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	160
TABLE 85	DDOS PROTECTION AND MITIGATION MARKET FOR LARGE ENTERPRISES, BY REGION, 2020–2025 (USD MILLION)	160
TABLE 86	DDOS PROTECTION AND MITIGATION MARKET FOR LARGE ENTERPRISES, BY REGION, 2026–2031 (USD MILLION)	161
TABLE 87	DDOS PROTECTION AND MITIGATION MARKET FOR SMALL & MEDIUM-SIZED ENTERPRISES, BY REGION, 2020–2025 (USD MILLION)	162
TABLE 88	DDOS PROTECTION AND MITIGATION MARKET FOR SMALL & MEDIUM-SIZED ENTERPRISES, BY REGION, 2026–2031 (USD MILLION)	162
TABLE 89	DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	165
TABLE 90	DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	166
TABLE 91	DDOS PROTECTION AND MITIGATION MARKET IN BFSI, BY REGION, 2020–2025 (USD MILLION)	166
TABLE 92	DDOS PROTECTION AND MITIGATION MARKET IN BFSI, BY REGION, 2026–2031 (USD MILLION)	167
TABLE 93	DDOS PROTECTION AND MITIGATION MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2020–2025 (USD MILLION)	167
TABLE 94	DDOS PROTECTION AND MITIGATION MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2026–2031 (USD MILLION)	168
TABLE 95	DDOS PROTECTION AND MITIGATION MARKET IN MANUFACTURING, BY REGION, 2020–2025 (USD MILLION)	168
TABLE 96	DDOS PROTECTION AND MITIGATION MARKET IN MANUFACTURING, BY REGION, 2026–2031 (USD MILLION)	169
TABLE 97	DDOS PROTECTION AND MITIGATION MARKET IN ENERGY AND UTILITIES, BY REGION, 2020–2025 (USD MILLION)	169
TABLE 98	DDOS PROTECTION AND MITIGATION MARKET IN ENERGY AND UTILITIES, BY REGION, 2026–2031 (USD MILLION)	170
TABLE 99	DDOS PROTECTION AND MITIGATION MARKET IN IT AND ITES, BY REGION, 2020–2025 (USD MILLION)	170
TABLE 100	DDOS PROTECTION AND MITIGATION MARKET IN IT AND ITES, BY REGION, 2026–2031 (USD MILLION)	171
TABLE 101	DDOS PROTECTION AND MITIGATION MARKET IN TELECOMMUNICATIONS, BY REGION, 2020–2025 (USD MILLION)	171
TABLE 102	DDOS PROTECTION AND MITIGATION MARKET IN TELECOMMUNICATIONS, BY REGION, 2026–2031 (USD MILLION)	172
TABLE 103	DDOS PROTECTION AND MITIGATION MARKET IN HEALTHCARE, BY REGION, 2020–2025 (USD MILLION)	172
TABLE 104	DDOS PROTECTION AND MITIGATION MARKET IN HEALTHCARE, BY REGION, 2026–2031 (USD MILLION)	173
TABLE 105	DDOS PROTECTION AND MITIGATION MARKET IN EDUCATION, BY REGION, 2020–2025 (USD MILLION)	173
TABLE 106	DDOS PROTECTION AND MITIGATION MARKET IN EDUCATION, BY REGION, 2026–2031 (USD MILLION)	174
TABLE 107	DDOS PROTECTION AND MITIGATION MARKET IN RETAIL, BY REGION, 2020–2025 (USD MILLION)	174
TABLE 108	DDOS PROTECTION AND MITIGATION MARKET IN RETAIL, BY REGION, 2026–2031 (USD MILLION)	175

TABLE 109	DDOS PROTECTION AND MITIGATION MARKET IN OTHER VERTICALS, BY REGION, 2020–2025 (USD MILLION)	175
TABLE 110	DDOS PROTECTION AND MITIGATION MARKET IN OTHER VERTICALS, BY REGION, 2026–2031 (USD MILLION)	176
TABLE 111	DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)	178
TABLE 112	DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2026–2031 (USD MILLION)	179
TABLE 113	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	180
TABLE 114	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	180
TABLE 115	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	181
TABLE 116	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	181
TABLE 117	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	181
TABLE 118	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	181
TABLE 119	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	182
TABLE 120	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	182
TABLE 121	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	182
TABLE 122	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	183
TABLE 123	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	183
TABLE 124	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	183
TABLE 125	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	183
TABLE 126	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	184
TABLE 127	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	184
TABLE 128	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	184
TABLE 129	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	184
TABLE 130	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	185
TABLE 131	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)	185
TABLE 132	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	185
TABLE 133	US: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	186
TABLE 134	US: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	186

TABLE 135	US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	186
TABLE 136	US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	186
TABLE 137	US: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	187
TABLE 138	US: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	187
TABLE 139	US: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	187
TABLE 140	US: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	187
TABLE 141	US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	188
TABLE 142	US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	188
TABLE 143	US: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	188
TABLE 144	US: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	188
TABLE 145	US: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	189
TABLE 146	US: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	189
TABLE 147	US: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	189
TABLE 148	US: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	189
TABLE 149	US: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	190
TABLE 150	US: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	190
TABLE 151	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	191
TABLE 152	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	191
TABLE 153	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	191
TABLE 154	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	192
TABLE 155	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	192
TABLE 156	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	192
TABLE 157	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	192
TABLE 158	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	193
TABLE 159	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	193
TABLE 160	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	193

TABLE 161	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	194
TABLE 162	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	194
TABLE 163	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	194
TABLE 164	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	194
TABLE 165	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	195
TABLE 166	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	195
TABLE 167	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	195
TABLE 168	CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	196
TABLE 169	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	196
TABLE 170	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	197
TABLE 171	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	197
TABLE 172	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	197
TABLE 173	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	197
TABLE 174	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	197
TABLE 175	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	198
TABLE 176	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	198
TABLE 177	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	198
TABLE 178	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	199
TABLE 179	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	199
TABLE 180	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	199
TABLE 181	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	199
TABLE 182	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	200
TABLE 183	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	200
TABLE 184	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	200
TABLE 185	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	200
TABLE 186	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	201

TABLE 187	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)	201
TABLE 188	EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	201
TABLE 189	UK: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	202
TABLE 190	UK: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	202
TABLE 191	UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	202
TABLE 192	UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	203
TABLE 193	UK: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	203
TABLE 194	UK: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	203
TABLE 195	UK: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	203
TABLE 196	UK: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	204
TABLE 197	UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	204
TABLE 198	UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	204
TABLE 199	UK: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	205
TABLE 200	UK: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	205
TABLE 201	UK: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	205
TABLE 202	UK: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	205
TABLE 203	UK: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	206
TABLE 204	UK: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	206
TABLE 205	UK: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	206
TABLE 206	UK: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	207
TABLE 207	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	207
TABLE 208	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	207
TABLE 209	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	208
TABLE 210	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	208
TABLE 211	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	208
TABLE 212	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	208

TABLE 213	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	209
TABLE 214	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	209
TABLE 215	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	209
TABLE 216	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	210
TABLE 217	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	210
TABLE 218	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	210
TABLE 219	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	210
TABLE 220	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	211
TABLE 221	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	211
TABLE 222	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	211
TABLE 223	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	211
TABLE 224	GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	212
TABLE 225	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	212
TABLE 226	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	213
TABLE 227	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	213
TABLE 228	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	213
TABLE 229	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	213
TABLE 230	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	213
TABLE 231	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	214
TABLE 232	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	214
TABLE 233	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	214
TABLE 234	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	215
TABLE 235	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	215
TABLE 236	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	215
TABLE 237	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	215
TABLE 238	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	216

TABLE 239	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	216
TABLE 240	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	216
TABLE 241	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	216
TABLE 242	FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	217
TABLE 243	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	217
TABLE 244	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	218
TABLE 245	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	218
TABLE 246	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	218
TABLE 247	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	218
TABLE 248	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	218
TABLE 249	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	219
TABLE 250	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	219
TABLE 251	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	219
TABLE 252	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	220
TABLE 253	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	220
TABLE 254	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	220
TABLE 255	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	220
TABLE 256	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	221
TABLE 257	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	221
TABLE 258	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	221
TABLE 259	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	221
TABLE 260	ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	222
TABLE 261	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	222
TABLE 262	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	222
TABLE 263	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	223
TABLE 264	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	223

TABLE 265	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	223
TABLE 266	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	223
TABLE 267	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	224
TABLE 268	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	224
TABLE 269	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	224
TABLE 270	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	225
TABLE 271	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	225
TABLE 272	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	225
TABLE 273	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	225
TABLE 274	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	226
TABLE 275	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	226
TABLE 276	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	226
TABLE 277	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	226
TABLE 278	REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	227
TABLE 279	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	228
TABLE 280	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	228
TABLE 281	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	229
TABLE 282	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	229
TABLE 283	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	229
TABLE 284	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	229
TABLE 285	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	230
TABLE 286	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	230
TABLE 287	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	230
TABLE 288	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	231
TABLE 289	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	231
TABLE 290	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	231

TABLE 291	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	231
TABLE 292	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	232
TABLE 293	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	232
TABLE 294	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	232
TABLE 295	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	232
TABLE 296	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	233
TABLE 297	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)	233
TABLE 298	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	233
TABLE 299	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	234
TABLE 300	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	234
TABLE 301	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	234
TABLE 302	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	235
TABLE 303	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	235
TABLE 304	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	235
TABLE 305	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	235
TABLE 306	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	236
TABLE 307	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	236
TABLE 308	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	236
TABLE 309	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	237
TABLE 310	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	237
TABLE 311	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	237
TABLE 312	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	237
TABLE 313	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	238
TABLE 314	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	238
TABLE 315	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	238
TABLE 316	CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	239

TABLE 317	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	239
TABLE 318	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	240
TABLE 319	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	240
TABLE 320	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	240
TABLE 321	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	240
TABLE 322	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	240
TABLE 323	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	241
TABLE 324	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	241
TABLE 325	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	241
TABLE 326	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	242
TABLE 327	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	242
TABLE 328	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	242
TABLE 329	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	242
TABLE 330	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	243
TABLE 331	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	243
TABLE 332	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	243
TABLE 333	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	243
TABLE 334	JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	244
TABLE 335	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	244
TABLE 336	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	245
TABLE 337	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	245
TABLE 338	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	245
TABLE 339	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	245
TABLE 340	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	245
TABLE 341	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	246
TABLE 342	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	246

TABLE 343	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	246
TABLE 344	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	247
TABLE 345	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	247
TABLE 346	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	247
TABLE 347	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	247
TABLE 348	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	248
TABLE 349	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	248
TABLE 350	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	248
TABLE 351	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	248
TABLE 352	INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	249
TABLE 353	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	249
TABLE 354	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	249
TABLE 355	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	250
TABLE 356	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	250
TABLE 357	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	250
TABLE 358	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	250
TABLE 359	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	251
TABLE 360	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	251
TABLE 361	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	251
TABLE 362	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	252
TABLE 363	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	252
TABLE 364	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	252
TABLE 365	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	252
TABLE 366	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	253
TABLE 367	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	253
TABLE 368	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	253

TABLE 369	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	253
TABLE 370	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	254
TABLE 371	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	254
TABLE 372	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	255
TABLE 373	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	255
TABLE 374	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	255
TABLE 375	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	255
TABLE 376	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	255
TABLE 377	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	256
TABLE 378	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	256
TABLE 379	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	256
TABLE 380	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	257
TABLE 381	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	257
TABLE 382	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	257
TABLE 383	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	257
TABLE 384	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	258
TABLE 385	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	258
TABLE 386	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	258
TABLE 387	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	258
TABLE 388	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	259
TABLE 389	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)	259
TABLE 390	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	259
TABLE 391	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	260
TABLE 392	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	260
TABLE 393	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	260
TABLE 394	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	260

TABLE 395	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	261
TABLE 396	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	261
TABLE 397	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	261
TABLE 398	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	261
TABLE 399	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	262
TABLE 400	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	262
TABLE 401	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	262
TABLE 402	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	262
TABLE 403	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	263
TABLE 404	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	263
TABLE 405	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	263
TABLE 406	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	263
TABLE 407	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	264
TABLE 408	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	264
TABLE 409	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)	265
TABLE 410	GCC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	265
TABLE 411	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	265
TABLE 412	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	266
TABLE 413	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	266
TABLE 414	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	266
TABLE 415	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	266
TABLE 416	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	266
TABLE 417	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	267
TABLE 418	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	267
TABLE 419	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	267
TABLE 420	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	268

TABLE 421	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	268
TABLE 422	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	268
TABLE 423	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	268
TABLE 424	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	269
TABLE 425	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	269
TABLE 426	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	269
TABLE 427	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	269
TABLE 428	KSA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	270
TABLE 429	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	270
TABLE 430	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	271
TABLE 431	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	271
TABLE 432	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	271
TABLE 433	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	271
TABLE 434	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	271
TABLE 435	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	272
TABLE 436	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	272
TABLE 437	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	272
TABLE 438	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	273
TABLE 439	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	273
TABLE 440	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	273
TABLE 441	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	273
TABLE 442	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	274
TABLE 443	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	274
TABLE 444	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	274
TABLE 445	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	274
TABLE 446	UAE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	275

TABLE 447	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	275
TABLE 448	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	275
TABLE 449	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	276
TABLE 450	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	276
TABLE 451	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	276
TABLE 452	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	276
TABLE 453	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	277
TABLE 454	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	277
TABLE 455	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	277
TABLE 456	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	278
TABLE 457	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	278
TABLE 458	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	278
TABLE 459	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	278
TABLE 460	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	279
TABLE 461	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	279
TABLE 462	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	279
TABLE 463	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	279
TABLE 464	REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	280
TABLE 465	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	280
TABLE 466	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	281
TABLE 467	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	281
TABLE 468	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	281
TABLE 469	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	281
TABLE 470	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	281
TABLE 471	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	282
TABLE 472	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	282

TABLE 473	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	282
TABLE 474	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	283
TABLE 475	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	283
TABLE 476	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	283
TABLE 477	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	283
TABLE 478	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	284
TABLE 479	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	284
TABLE 480	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	284
TABLE 481	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	284
TABLE 482	SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	285
TABLE 483	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	285
TABLE 484	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	285
TABLE 485	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	286
TABLE 486	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	286
TABLE 487	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	286
TABLE 488	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	286
TABLE 489	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	287
TABLE 490	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	287
TABLE 491	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	287
TABLE 492	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	288
TABLE 493	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	288
TABLE 494	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	288
TABLE 495	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	288
TABLE 496	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	289
TABLE 497	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	289
TABLE 498	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	289

TABLE 499	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	289
TABLE 500	REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	290
TABLE 501	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	290
TABLE 502	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	291
TABLE 503	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	291
TABLE 504	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	291
TABLE 505	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	291
TABLE 506	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	291
TABLE 507	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	292
TABLE 508	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	292
TABLE 509	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	292
TABLE 510	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	293
TABLE 511	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	293
TABLE 512	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	293
TABLE 513	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	293
TABLE 514	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	294
TABLE 515	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	294
TABLE 516	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	294
TABLE 517	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	294
TABLE 518	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	295
TABLE 519	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)	295
TABLE 520	LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)	295
TABLE 521	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	296
TABLE 522	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	296
TABLE 523	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	296
TABLE 524	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	297

TABLE 525	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	297
TABLE 526	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	297
TABLE 527	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	297
TABLE 528	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	298
TABLE 529	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	298
TABLE 530	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	298
TABLE 531	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	299
TABLE 532	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	299
TABLE 533	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	299
TABLE 534	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	299
TABLE 535	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	300
TABLE 536	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	300
TABLE 537	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	300
TABLE 538	BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	301
TABLE 539	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	301
TABLE 540	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	301
TABLE 541	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	302
TABLE 542	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	302
TABLE 543	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	302
TABLE 544	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	302
TABLE 545	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	303
TABLE 546	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	303
TABLE 547	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	303
TABLE 548	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	304
TABLE 549	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	304
TABLE 550	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	304

TABLE 551	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	304
TABLE 552	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	305
TABLE 553	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	305
TABLE 554	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	305
TABLE 555	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	305
TABLE 556	MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	306
TABLE 557	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)	306
TABLE 558	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)	307
TABLE 559	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)	307
TABLE 560	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)	307
TABLE 561	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)	307
TABLE 562	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)	307
TABLE 563	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)	308
TABLE 564	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)	308
TABLE 565	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)	308
TABLE 566	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)	309
TABLE 567	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)	309
TABLE 568	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)	309
TABLE 569	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)	309
TABLE 570	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)	310
TABLE 571	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)	310
TABLE 572	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)	310
TABLE 573	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)	310
TABLE 574	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)	311
TABLE 575	DDOS PROTECTION AND MITIGATION MARKET: OVERVIEW OF STRATEGIES DEPLOYED BY KEY PLAYERS	312
TABLE 576	DDOS PROTECTION AND MITIGATION MARKET: DEGREE OF COMPETITION, 2025	315

TABLE 577	DDOS PROTECTION AND MITIGATION MARKET: REGIONAL FOOTPRINT, 2025	323
TABLE 578	DDOS PROTECTION AND MITIGATION MARKET: OFFERING FOOTPRINT, 2025	324
TABLE 579	DDOS PROTECTION AND MITIGATION MARKET: VERTICAL FOOTPRINT, 2025	325
TABLE 580	DDOS PROTECTION AND MITIGATION MARKET: KEY STARTUPS/SMES, 2025	328
TABLE 581	DDOS PROTECTION AND MITIGATION MARKET: COMPETITIVE BENCHMARKING OF KEY STARTUPS/SMES, 2025	329
TABLE 582	DDOS PROTECTION AND MITIGATION MARKET: PRODUCT LAUNCHES AND ENHANCEMENTS, JANUARY 2024–AUGUST 2026	329
TABLE 583	DDOS PROTECTION AND MITIGATION MARKET: DEALS, JANUARY 2024–AUGUST 2026	332
TABLE 584	DDOS PROTECTION AND MITIGATION MARKET: EXPANSIONS, JANUARY 2024–AUGUST 2026	333
TABLE 585	AKAMAI: COMPANY OVERVIEW	334
TABLE 586	AKAMAI: PRODUCTS/SOLUTIONS/SERVICES OFFERED	335
TABLE 587	AKAMAI: PRODUCT LAUNCHES & ENHANCEMENTS	336
TABLE 588	AKAMAI: DEALS	337
TABLE 589	CLOUDFLARE: COMPANY OVERVIEW	338
TABLE 590	CLOUDFLARE: PRODUCTS/SOLUTIONS/SERVICES OFFERED	339
TABLE 591	CLOUDFLARE: PRODUCT LAUNCHES & ENHANCEMENTS	340
TABLE 592	CLOUDFLARE: DEALS	341
TABLE 593	RADWARE: COMPANY OVERVIEW	342
TABLE 594	RADWARE: PRODUCTS/SOLUTIONS/SERVICES OFFERED	343
TABLE 595	RADWARE: PRODUCT LAUNCHES & ENHANCEMENTS	344
TABLE 596	RADWARE: DEALS	345
TABLE 597	FORTINET: COMPANY OVERVIEW	347
TABLE 598	FORTINET: PRODUCTS/SOLUTIONS/SERVICES OFFERED	348
TABLE 599	FORTINET: PRODUCT LAUNCHES & ENHANCEMENTS	349
TABLE 600	NETSCOUT: COMPANY OVERVIEW	350
TABLE 601	NETSCOUT: PRODUCTS/SOLUTIONS/SERVICES OFFERED	351
TABLE 602	NETSCOUT: PRODUCT LAUNCHES & ENHANCEMENTS	352
TABLE 603	NETSCOUT: EXPANSIONS	352
TABLE 604	NEXUSGUARD: COMPANY OVERVIEW	354
TABLE 605	NEXUSGUARD: PRODUCTS/SOLUTIONS/SERVICES OFFERED	354
TABLE 606	NEXUSGUARD: PRODUCT LAUNCHES & ENHANCEMENTS	355
TABLE 607	NEXUSGUARD: DEALS	356
TABLE 608	HUAWEI: COMPANY OVERVIEW	357
TABLE 609	HUAWEI: PRODUCTS/SOLUTIONS/SERVICES OFFERED	358
TABLE 610	HUAWEI: PRODUCT LAUNCHES & ENHANCEMENTS	359
TABLE 611	LINK11: COMPANY OVERVIEW	360
TABLE 612	LINK11: PRODUCTS/SOLUTIONS/SERVICES OFFERED	360
TABLE 613	LINK11: PRODUCT LAUNCHES & ENHANCEMENTS	361
TABLE 614	LINK11: DEALS	362
TABLE 615	THALES (IMPERVA): COMPANY OVERVIEW	363
TABLE 616	THALES (IMPERVA): PRODUCTS/SOLUTIONS/SERVICES OFFERED	364
TABLE 617	THALES (IMPERVA): PRODUCT LAUNCHES & ENHANCEMENTS	365

TABLE 618	BT: COMPANY OVERVIEW	366
TABLE 619	BT: PRODUCTS/SOLUTIONS/SERVICES OFFERED	367
TABLE 620	A10 NETWORKS: COMPANY OVERVIEW	368
TABLE 621	A10 NETWORKS: PRODUCTS/SOLUTIONS/SERVICES OFFERED	369
TABLE 622	A10 NETWORKS: PRODUCT LAUNCHES & ENHANCEMENTS	370
TABLE 623	A10 NETWORKS: DEALS	370
TABLE 624	NSFOCUS: COMPANY OVERVIEW	371
TABLE 625	NSFOCUS: PRODUCTS/SOLUTIONS/SERVICES OFFERED	371
TABLE 626	MICROSOFT: COMPANY OVERVIEW	373
TABLE 627	MICROSOFT: PRODUCTS/SOLUTIONS/SERVICES OFFERED	374
TABLE 628	MICROSOFT: PRODUCT LAUNCHES & ENHANCEMENTS	375
TABLE 629	F5: COMPANY OVERVIEW	376
TABLE 630	F5: PRODUCTS/SOLUTIONS/SERVICES OFFERED	377
TABLE 631	F5: PRODUCT LAUNCHES & ENHANCEMENTS	378
TABLE 632	F5: DEALS	379
TABLE 633	ALIBABA CLOUD: COMPANY OVERVIEW	380
TABLE 634	ALIBABA CLOUD: PRODUCTS/SOLUTIONS/SERVICES OFFERED	381
TABLE 635	ALIBABA CLOUD: PRODUCT LAUNCHES & ENHANCEMENTS	382
TABLE 636	CORERO NETWORK SECURITY: COMPANY OVERVIEW	384
TABLE 637	CORERO: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS	385
TABLE 638	CORERO: PRODUCT LAUNCHES & ENHANCEMENTS	386
TABLE 639	CORERO: DEALS	387
TABLE 640	AWS: COMPANY OVERVIEW	389
TABLE 641	AWS: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS	390
TABLE 642	AWS: PRODUCT LAUNCHES & ENHANCEMENTS	391
TABLE 643	FACTOR ANALYSIS	414

LIST OF FIGURES

FIGURE 1	DDOS PROTECTION & MITIGATION MARKET SEGMENTATION	48
FIGURE 2	STUDY YEARS CONSIDERED	50
FIGURE 3	MARKET SCENARIO	52
FIGURE 4	GLOBAL DDOS PROTECTION AND MITIGATION MARKET, 2020–2031 (USD MILLION)	53
FIGURE 5	MAJOR STRATEGIES ADOPTED BY KEY PLAYERS IN DDOS PROTECTION AND MITIGATION MARKET, 2025	53
FIGURE 6	DISRUPTIVE TRENDS INFLUENCING GROWTH OF DDOS PROTECTION AND MITIGATION MARKET	54
FIGURE 7	HIGH-GROWTH SEGMENTS IN DDOS PROTECTION AND MITIGATION MARKET, 2025	55
FIGURE 8	ASIA PACIFIC TO REGISTER HIGHEST GROWTH DURING FORECAST PERIOD	56
FIGURE 9	GROWTH IN FREQUENCY OF LARGE-SCALE DDOS ATTACKS AND RISING ADOPTION OF CLOUD-BASED MITIGATION SERVICES DRIVE MARKET	57
FIGURE 10	SERVICES SEGMENT TO ACCOUNT FOR LARGER MARKET SHARE DURING FORECAST PERIOD	58
FIGURE 11	SOFTWARE/PLATFORMS SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD	58
FIGURE 12	NETWORK TRAFFIC ANALYZERS SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD	59
FIGURE 13	PROFESSIONAL SERVICES SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD	59
FIGURE 14	NETWORK & IP INFRASTRUCTURE SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD	60
FIGURE 15	BFSI SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD	60
FIGURE 16	ASIA PACIFIC TO EMERGE AS BEST MARKET FOR INVESTMENT IN NEXT FIVE YEARS	61
FIGURE 17	DDOS PROTECTION AND MITIGATION MARKET: DRIVERS, RESTRAINTS, OPPORTUNITIES, AND CHALLENGES	63
FIGURE 18	DDOS PROTECTION AND MITIGATION MARKET: PORTER'S FIVE FORCES ANALYSIS	75
FIGURE 19	DDOS PROTECTION AND MITIGATION MARKET: VALUE CHAIN ANALYSIS	79
FIGURE 20	DDOS PROTECTION AND MITIGATION MARKET: ECOSYSTEM ANALYSIS	81
FIGURE 21	AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2025 (USD)	82
FIGURE 22	TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS	84
FIGURE 23	INVESTMENT AND FUNDING SCENARIO, 2025	85
FIGURE 24	NUMBER OF PATENTS GRANTED FOR DDOS PROTECTION & MITIGATION MARKET, 2017–2026	100
FIGURE 25	FUTURE APPLICATIONS OF DDOS PROTECTION & MITIGATION	102
FIGURE 26	DDOS PROTECTION & MITIGATION MARKET: DECISION-MAKING FACTORS	115
FIGURE 27	INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS	116
FIGURE 28	KEY BUYING CRITERIA FOR TOP THREE VERTICALS	116
FIGURE 29	ADOPTION BARRIERS AND INTERNAL CHALLENGES	118
FIGURE 30	SERVICES SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD	123
FIGURE 31	SOFTWARE/PLATFORMS SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD	124

FIGURE 32	MANAGED SERVICES SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD	129
FIGURE 33	CONSULTING & ADVISORY SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD	131
FIGURE 34	BOTNET DETECTION & MANAGEMENT SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD	140
FIGURE 35	WEB APPLICATIONS AND APIS SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD	147
FIGURE 36	CLOUD SEGMENT TO RECORD FASTER GROWTH DURING FORECAST PERIOD	153
FIGURE 37	SMES SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD	159
FIGURE 38	BFSI SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD	165
FIGURE 39	NORTH AMERICA TO LEAD MARKET FROM 2026 TO 2031	178
FIGURE 40	NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET SNAPSHOT	180
FIGURE 41	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET SNAPSHOT	228
FIGURE 42	DDOS PROTECTION AND MITIGATION MARKET: REVENUE ANALYSIS OF FIVE KEY PLAYERS, 2021–2025	314
FIGURE 43	SHARE ANALYSIS OF LEADING COMPANIES IN DDOS PROTECTION AND MITIGATION MARKET, 2025	315
FIGURE 44	DDOS PROTECTION AND MITIGATION MARKET: COMPARISON OF VENDOR BRANDS	318
FIGURE 45	COMPANY VALUATION, 2025 (USD BILLION)	319
FIGURE 46	FINANCIAL METRICS, 2025	319
FIGURE 47	DDOS PROTECTION AND MITIGATION MARKET: COMPANY EVALUATION MATRIX (KEY PLAYERS), 2025	321
FIGURE 48	DDOS PROTECTION AND MITIGATION MARKET: COMPANY FOOTPRINT, 2025	322
FIGURE 49	DDOS PROTECTION AND MITIGATION MARKET: COMPANY EVALUATION MATRIX (STARTUPS/SMES), 2025	327
FIGURE 50	AKAMAI: COMPANY SNAPSHOT	335
FIGURE 51	CLOUDFLARE: COMPANY SNAPSHOT	339
FIGURE 52	RADWARE: COMPANY SNAPSHOT	343
FIGURE 53	FORTINET: COMPANY SNAPSHOT	348
FIGURE 54	NETSCOUT: COMPANY SNAPSHOT	351
FIGURE 55	HUAWEI: COMPANY SNAPSHOT	358
FIGURE 56	THALES (IMPERVA): COMPANY SNAPSHOT	364
FIGURE 57	BT: COMPANY SNAPSHOT	367
FIGURE 58	A10 NETWORKS: COMPANY SNAPSHOT	369
FIGURE 59	MICROSOFT: COMPANY SNAPSHOT	374
FIGURE 60	F5: COMPANY SNAPSHOT	377
FIGURE 61	ALIBABA CLOUD: COMPANY SNAPSHOT	381
FIGURE 62	CORERO: COMPANY SNAPSHOT	385
FIGURE 63	AWS: COMPANY SNAPSHOT	390
FIGURE 64	DDOS PROTECTION & MITIGATION MARKET: RESEARCH DESIGN	407
FIGURE 65	BREAKUP OF PRIMARY PROFILES, BY COMPANY TYPE, DESIGNATION, AND REGION	409
FIGURE 66	KEY INSIGHTS FROM INDUSTRY EXPERTS	409
FIGURE 67	DATA TRIANGULATION	410
FIGURE 68	APPROACH 1 (SUPPLY SIDE): REVENUE OF VENDORS IN DDOS PROTECTION & MITIGATION MARKET	411

FIGURE 69	APPROACH 2 (DEMAND SIDE): DDOS PROTECTION & MITIGATION MARKET	412
FIGURE 70	TECHNOLOGY/PRODUCT ROADMAP	412
FIGURE 71	DDOS PROTECTION & MITIGATION MARKET ESTIMATION: RESEARCH FLOW	413
FIGURE 72	APPROACH 2: BOTTOM-UP (DEMAND SIDE) - PLATFORMS/SOLUTIONS/ SERVICES	414

LIST OF ABBREVIATIONS

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
AICPA	American Institute of CPAs
APIs	Application Programming Interfaces
APPI	Act on the Protection of Personal Information
AWS	Amazon Web Services
BFSI	Banking, Financial Services, and Insurance
BI	Business Intelligence
BUs	Business Units
CCPA	California Consumer Privacy Act
CDN	Content Delivery Network
CEOs	Chief Executive Officers
CERL	Computer Education Research Laboratory
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CSP	Customer Security Program
CTO	Chief Technology Officer
DDoS	Distributed Denial of Service
DIA	Dedicated Internet Access
DNS	Domain Name System
DoS	Denial of Service
DSL	Data Security Law
ECC-Net	European Consumer Centers Network
ENISA	European Union Agency for Network and Information Security
FAQs	Frequently Asked Questions
FFIEC	Federal Financial Institutions Examination Council

FISMA	Federal Information Security and Management Act
FTC	Federal Trade Commission
FY	Financial year
GCA	Global Cybersecurity Agenda
GDPR	General Data Protection Regulation
GLB	GRAMM-LEACH-BLILEY
GWP	Gross World Product
HBAD	Host Behavior Anomaly Detection (
HIPAA	Health Insurance Portability and Accountability ACT
HLEG	High Level Experts Group
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IEC	Israel Electric Corporation
IMF	International Monetary Fund
IMS	Information Management System
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
IRS	Internal Revenue Service
ISPs	Internet Service Providers
ISVs	Independent Software Vendors
IT	Information Technology
ITU	International Telecommunications Union
KSA	Kingdom of Saudi Arabia
MD	Managing Director
ML	Machine Learning
MSS	Managed Security Services
MSSPs	Managed Security Service Providers
MTCS	Multi-tier Cloud Security
NBAD	Network Behavior Anomaly Detection
NCCIC	National Cybersecurity and Communications Integration Center

NFV	Network Functions Virtualization
NTP	Network Time Protocol
OECD	Economic Cooperation and Development
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
OTM	Open Threat Management
PCI-DSS	Payment Card Industry - Data Security Standard
PHI	Protected health information
PIPL	Personal Information Protection Law
PoS	Point of Sale
PPP	Purchasing Power Parity
R&D	Research and Development
RDDoS	Ransom Distributed Denial of Service
SaaS	Software-as-a-Service
SDN	Software-defined Networking
SEC	Securities and Exchange Commission
SECaaS	Security-as-a-Service
SEIM	Security Information and Event Management
SME	Small and Medium-sized Enterprise
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SOX	SARBANES-OXLEY
SQL	Structured Query Language
SSDP	Simple Service Discovery Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCS	Tata Consultancy Services
TMS	Threat Mitigation System
UAE	United Arab Emirates
USB	Universal Serial Bus
USD	United States Dollar

VAR	Value-added Reseller
VoIP	Voices over Internet Protocol
VP	Vice President
VR	Virtual Reality
WAF	Web Application Firewall
XMLRPC	eXtensible Markup Language Remote Procedure Call

1 INTRODUCTION

1.1 STUDY OBJECTIVES

- To define, describe, and forecast the distributed denial of service (DDoS) protection & mitigation market by offering, solution type, application area, deployment mode, organization size, vertical, and region
- To forecast the size of the market segments with respect to five main regions: North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa
- To provide detailed information about the major factors (drivers, opportunities, threats, and challenges) influencing the growth of the DDoS protection & mitigation market
- To study the complete value chain and related industry segments and perform a value chain analysis of the DDoS protection & mitigation market landscape
- To analyze the industry trends, pricing data, patents, and innovations related to the DDoS protection & mitigation market
- To analyze the opportunities for stakeholders by identifying the high-growth segments of the DDoS protection & mitigation market
- To profile the key players in the market and comprehensively analyze their market share/ranking and core competencies
- To track and analyze the competitive developments, such as mergers and acquisitions, product launches and developments, partnerships, agreements, collaborations, business expansions, and research & development (R&D) activities

1.2 MARKET DEFINITION

DDoS (distributed denial of service) protection & mitigation refers to measures designed to defend against and minimize the impact of DDoS attacks, where multiple compromised systems flood a target with traffic, rendering it unavailable. These solutions monitor network traffic to detect abnormal spikes, filter malicious requests, and reroute or block traffic before it overwhelms the target infrastructure. Key techniques include traffic scrubbing, rate limiting, bot filtering, and real-time traffic analysis. DDoS mitigation services often employ hardware, software, and services to ensure seamless business operations and maintain the availability, performance, and integrity of online resources.

1.3 STUDY SCOPE AND SEGMENTATION

This study analyzes the global DDoS protection & mitigation market from 2020, based on contemporary market trends and developments, and its potential growth from 2026 to 2031. It provides detailed market trends, vendors' market shares, market sizes, forecasts, and analysis of the key players in the market.

1.3.1 MARKET SEGMENTATION AND REGIONS COVERED

FIGURE 1 DDOS PROTECTION & MITIGATION MARKET SEGMENTATION



Note: Other hardware includes scrubbing devices, rate limiters, anti-DDoS gateways.

Other solution types include orchestration & management and threat intelligence.

Other verticals include oil and gas, media and entertainment, transportation and logistics, and travel and hospitality.

Rest of Europe includes the Netherlands, the Czech Republic, Ireland, and other countries.

Rest of Asia Pacific includes South Korea, Taiwan, Hong Kong, and other countries.

Rest of Middle East & Africa includes Iraq, Turkey, and other countries.

Rest of Latin America includes Argentina, Chile, Peru, and other countries.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

1.3.2 INCLUSIONS & EXCLUSIONS

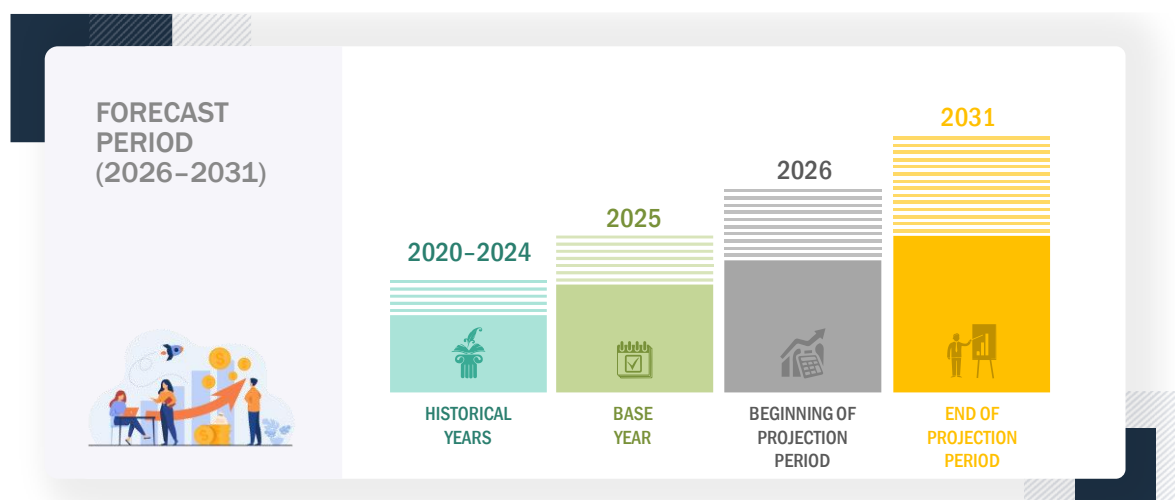
TABLE 1 INCLUSIONS & EXCLUSIONS

CATEGORY	INCLUSION	EXCLUSION
Offering	- Hardware solutions, software/platforms, and services are included. - Hardware includes firewalls, intrusion detection & prevention systems, load balancers, scrubbing devices, rate limiters, and anti-DDoS gateways. - Software/platforms include DDoS-specific solutions. - Services include professional and managed DDoS services.	General-purpose networking hardware such as routers, switches, and access points without dedicated DDoS protection functionality; standalone cybersecurity software without DDoS protection/mitigation capabilities; general IT consulting, network management, and cybersecurity services not related to DDoS protection.
Solution Type	Network traffic analyzers, threat mitigation systems, botnet detection & management, and other solution types, including DDoS orchestration & management and DDoS-related threat intelligence.	Standalone SIEM platforms, standalone SOAR platforms, generic network monitoring tools, general-purpose anomaly detection tools, standalone threat intelligence platforms, generic vulnerability management solutions, and general cybersecurity orchestration tools without DDoS-specific functionality.
Application Area	Network & IP infrastructure, web applications & APIs, and DNS infrastructure are included where DDoS protection & mitigation are applied.	Endpoint security, email security, mobile security, database security, identity & access security, and data security are excluded when DDoS protection is not the primary application. General cloud security is excluded unless it specifically provides DDoS protection for cloud infrastructure, applications, or APIs.
Deployment Mode	On-premises, cloud, and hybrid deployment modes are included.	Offline/air-gapped deployments without Internet-facing or DDoS protection requirements are excluded.
Organization Size	Large enterprises and SMEs are included.	Individual consumers/home users and consumer-grade personal Internet protection are excluded.
Vertical	BFSI, government & defense, healthcare, IT & ITeS, telecommunications, manufacturing, energy & utilities, retail, education, and other verticals are included.	- Residential/consumer users and non-organizational use cases are excluded. - An in-depth analysis of each vertical related to a particular country or region
Region	North America, Europe, Asia Pacific (APAC), Middle East & Africa (MEA), and Latin America are included. Country-level analysis can cover the major markets within each region based on DDoS protection adoption and market relevance.	- A separate analysis of countries in the rest of Europe, Asia Pacific, the Middle East & Africa, and Latin America - Analysis of local markets and cities

Source: Secondary Research and MarketsandMarkets Analysis

1.3.3 YEARS CONSIDERED

FIGURE 2 STUDY YEARS CONSIDERED



- The forecast period is 2026 to 2031.
- The financial year considered for most company profiles is 2025. The previous year's data was considered if the data was unavailable for specific companies' base years.
- The period considered for studying the competitive landscape ranges from January 2024 to August 2026.

1.4 CURRENCY CONSIDERED

- The currency used in the report is US dollars, with the market size indicated in USD million/billion.
- ISO 4217 codes depict currency names; the market size is represented using USD.
- The market has been studied in terms of USD million, with specific values provided in USD billion. The denomination is based on the size of the values, enabling uniform accommodation of these values within the tables, figures, or segments.
- The data has been taken from companies' annual reports reporting their revenues in USD.
- For companies that reported their revenue in other currencies, the average annual currency conversion rate used for that particular year has been taken from the US IRS to convert to US dollar values.

TABLE 2 USD EXCHANGE RATES, 2021-2025

Currency	2021	2022	2023	2024	2025
Euro (EUR)	1.13	1.06	1.10	1.09	1.17
Indian Rupee (INR)	0.013	0.012	0.012	0.012	0.012
Great British Pound (GBP)	1.34	1.20	1.27	1.25	1.34
Canadian Dollar (CAD)	0.78	0.73	0.75	0.75	0.73
Japanese Yen (JPY)	0.008	0.007	0.007	0.007	0.007

Source: Oanda.com

1.5 STAKEHOLDERS

- DDoS protection & mitigation hardware vendors
- DDoS protection & mitigation software vendors
- DDoS protection & mitigation service providers
- Defense organizations
- Government agencies
- Independent software vendors (ISVs)
- Consulting firms
- System integrators
- Value-added resellers (VARs)
- Information technology (IT) security agencies
- Managed security service providers (MSSPs)
- Internet service providers (ISPs)

1.6 SUMMARY OF CHANGES

- The study includes qualitative data for historical years from 2020 to 2024, the base year 2025, and the forecast period (2026 to 2031).
- Financial information/product portfolio of players: The report includes the players' financial information, product information, and recent developments from January 2024 to August 2026 for each listed company.
- Market developments of profiled players: The report covers market developments between January 2024 and August 2026.
- The study includes a market ecosystem, value chain analysis, pricing analysis, patent analysis, strategic moves by tier 1, tier 2, and tier 3 players, interconnected markets and cross-sector opportunities, macroeconomic outlook, the impact of AI/Gen AI, trends/disruptions impacting customers' businesses, decision-making process, key stakeholders in the buying process, and the study also highlights major conferences and events scheduled for 2026-2027.
- The study includes competitive landscape analysis, market share/ranking, micro-quadrants for key players and SME/startup players, key player strategies, competitive scenarios and trends, revenue share analysis, and coverage of emerging/new players, their product offerings, and recent developments.
- The study comprises detailed industry-specific use cases across multiple sectors.

2 EXECUTIVE SUMMARY

2.1 KEY INSIGHTS AND MARKET HIGHLIGHTS

The DDoS protection and mitigation market continues to expand rapidly as increasing digitalization, IoT adoption, cloud computing, and online service usage heighten enterprise exposure to large-scale distributed denial-of-service attacks. With attackers leveraging automation, AI, and botnets to launch more sophisticated volumetric and application-layer DDoS assaults, organizations across BFSI, ecommerce, IT, gaming, government, and telecom sectors face growing risks that demand advanced real-time detection and mitigation. Modern attacks, including massive volumetric floods, DNS amplification, NTP amplification, SYN floods, HTTP floods, and bot-based stealth attacks, now frequently reach terabit-level intensity; for example, Google Cloud mitigated a record-breaking 398 million RPS attack in 2023, while Microsoft handled multiple events exceeding 1 Tbps. The rise of DDoS-for-hire services and AI-driven attack automation has further lowered the barrier to launching disruptive campaigns, making resilient cloud-based scrubbing, zero-trust architectures, and AI-enhanced mitigation essential for business continuity. Leading vendors such as NETSCOUT, Radware, Cloudflare, Nexusguard, and Akamai continue advancing adaptive defense mechanisms designed to anticipate, absorb, and neutralize attacks before service disruption occurs. As organizations adopt hybrid and multi-cloud environments, DDoS protection is shifting into a strategic cybersecurity priority, with the market expected to maintain strong global growth supported by heightened awareness, evolving compliance requirements, and the rising demand for uninterrupted digital services.

FIGURE 3 MARKET SCENARIO

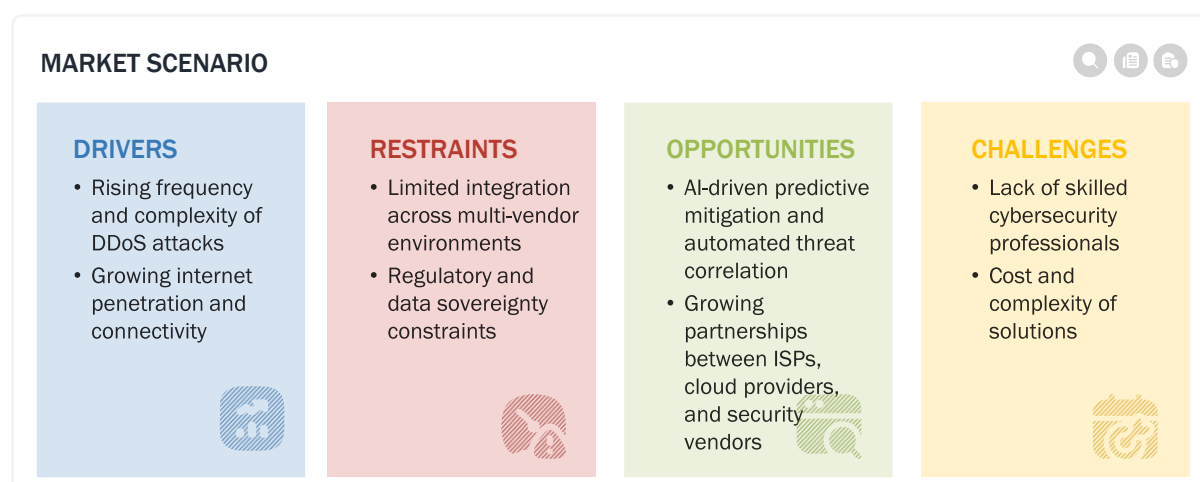
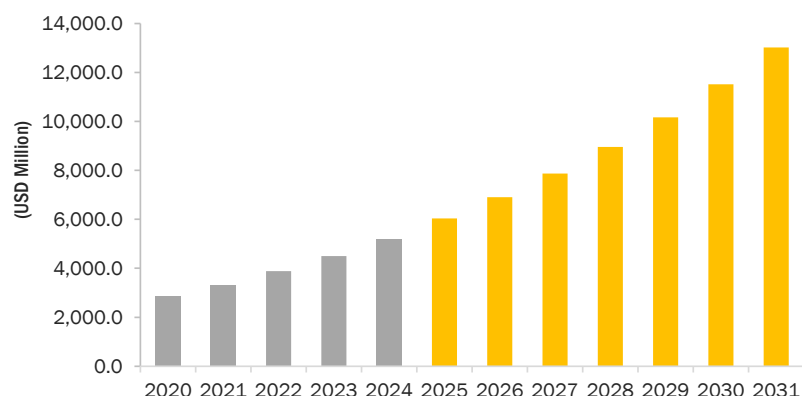


FIGURE 4 GLOBAL DDOS PROTECTION AND MITIGATION MARKET, 2020–2031 (USD MILLION)



13.5%

The global DDoS protection and mitigation market is driven by the rising frequency of large-scale cyberattacks, the rapid digitalization of enterprises, and the increasing need for real-time, automated defenses to secure critical online services across cloud, IoT, and multi-cloud environments.

The global DDoS protection and mitigation market is projected to grow steadily from USD 6,897.7 million in 2026 to USD 13,014.3 million by 2031, supported by a strong 13.5% CAGR. This growth is driven by the increasing frequency and scale of cyberattacks, rapid digitalization across industries, and the rising dependence on cloud, IoT, and multi-cloud environments. As enterprises face higher risks of service outages and downtime, the need for real-time, automated, and scalable DDoS protection solutions continues to intensify, resulting in consistent market expansion throughout the forecast period.

2.2 KEY MARKET PARTICIPANTS: MAPPING OF STRATEGIC DEVELOPMENTS

FIGURE 5 MAJOR STRATEGIES ADOPTED BY KEY PLAYERS IN DDOS PROTECTION AND MITIGATION MARKET, 2025

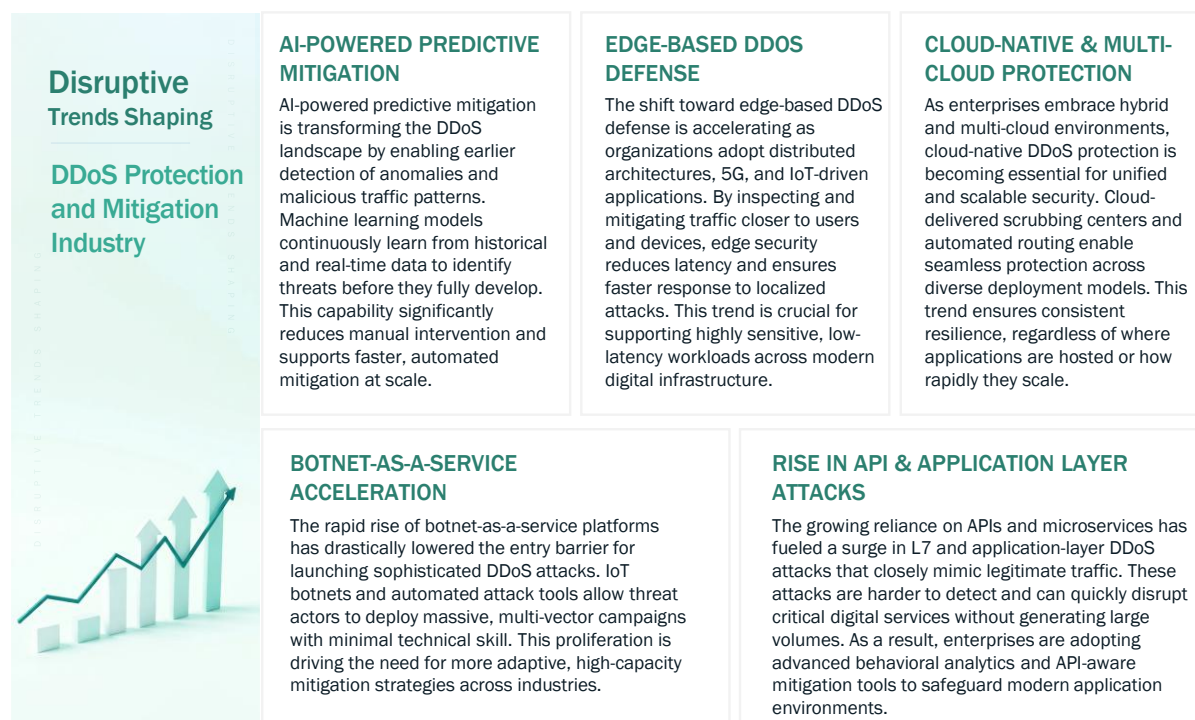
COMPANY	NETSCOUT	Akamai	radware	FORTINET	CLOUDFLARE	NEXUSGUARD
Product Launches	●	●	●	●	●	●
Mergers & Acquisitions	●	●	●	●	●	●
Partnerships, Agreements, Collaborations, and Joint Ventures	●	●	●	●	●	●
Expansions	●	●	●	●	●	●
IMPACT ● EXCELLENT ● GOOD ● FAIR ● POOR						

Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

The DDoS protection and mitigation market is consolidated, with the top five players holding a combined market share of 25–30%. The top players have strong geographical presence, a high focus on innovation and research, and adopt a mix of business strategies. The major strategies adopted by major players are expansions, mergers & acquisitions, and agreements & partnerships. Companies in the market are focused on enhancing strong footholds in their home regions and are exploring geographic diversification alternatives to grow their businesses and expand their presence in the DDoS protection and mitigation industry.

2.3 DISRUPTIONS SHAPING MARKET

FIGURE 6 DISRUPTIVE TRENDS INFLUENCING GROWTH OF DDOS PROTECTION AND MITIGATION MARKET

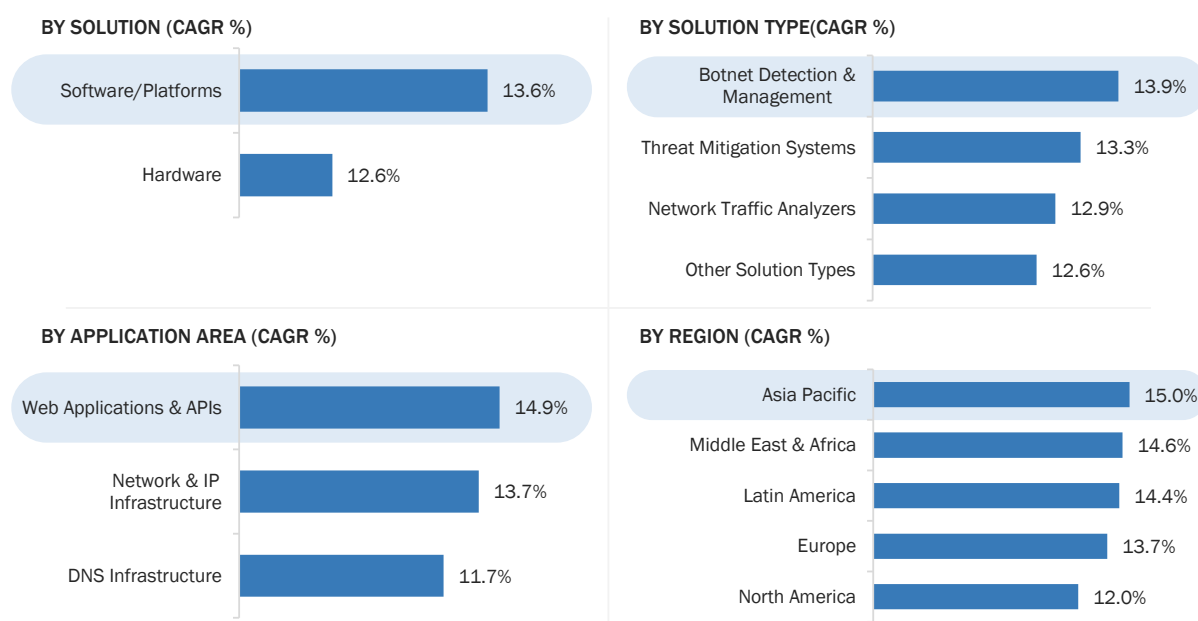


Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

Various industries such as BFSI, retail and ecommerce, IT & telecommunications, government, and healthcare are increasingly relying on advanced DDoS protection as disruptive trends reshape the threat landscape. AI-powered predictive mitigation helps these sectors detect anomalies earlier and automate real-time response to complex, multi-vector attacks. Edge-based DDoS defense is becoming critical for industries dependent on low-latency operations, especially gaming, telecom, and IoT-driven manufacturing, by enabling faster mitigation closer to users and devices. Cloud-native and multi-cloud protection is expanding rapidly across BFSI, ecommerce, and IT services as organizations seek unified, scalable security across hybrid infrastructures. The rise of botnet-as-a-service platforms is intensifying attack frequency and volume, posing significant risks to online retailers, financial institutions, and public-sector systems. Meanwhile, the surge in API and application-layer attacks is creating new vulnerabilities for ecommerce, healthcare, and digital service providers, driving the adoption of behavioral analytics and API-aware mitigation capabilities.

2.4 HIGH-GROWTH SEGMENTS

FIGURE 7 HIGH-GROWTH SEGMENTS IN DDOS PROTECTION AND MITIGATION MARKET, 2025

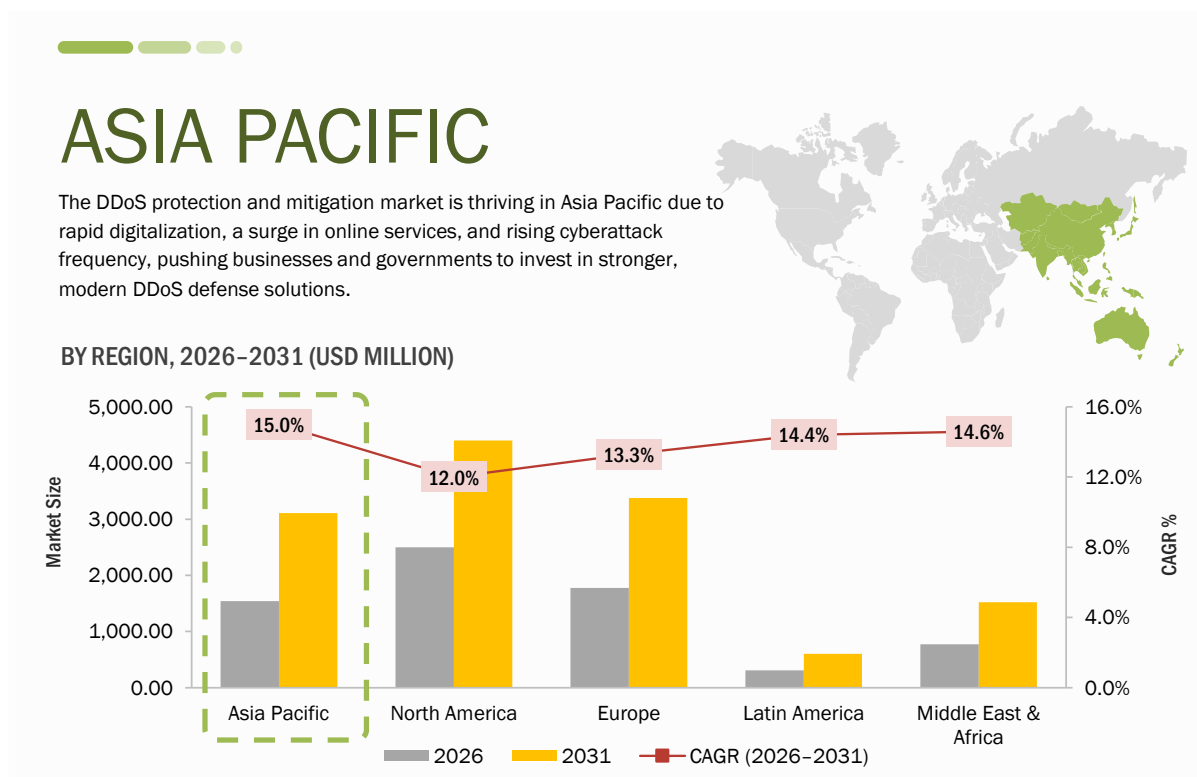


Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

The infographic highlights the fastest-growing segments within the DDoS protection and mitigation market across solution, solution type, and application area. Software solutions emerge as the largest and most rapidly expanding segment, driven by rising demand for cloud-native, AI-enabled, and automated mitigation tools, followed by hardware solutions, which remain essential for high-performance scrubbing and on-premises deployments. Services also show strong growth as enterprises increasingly rely on managed security services and 24/7 monitoring to counter evolving multi-vector attacks. From a deployment perspective, cloud-based DDoS protection leads the market with the highest adoption, fueled by the shift toward hybrid and multi-cloud environments requiring scalable and globally distributed defense capabilities, whereas on-premises solutions continue to grow steadily in organizations with strict compliance, data privacy, and low-latency network requirements.

2.5 SNAPSHOT: GLOBAL MARKET SIZE, GROWTH RATE, AND FORECAST

FIGURE 8 ASIA PACIFIC TO REGISTER HIGHEST GROWTH DURING FORECAST PERIOD



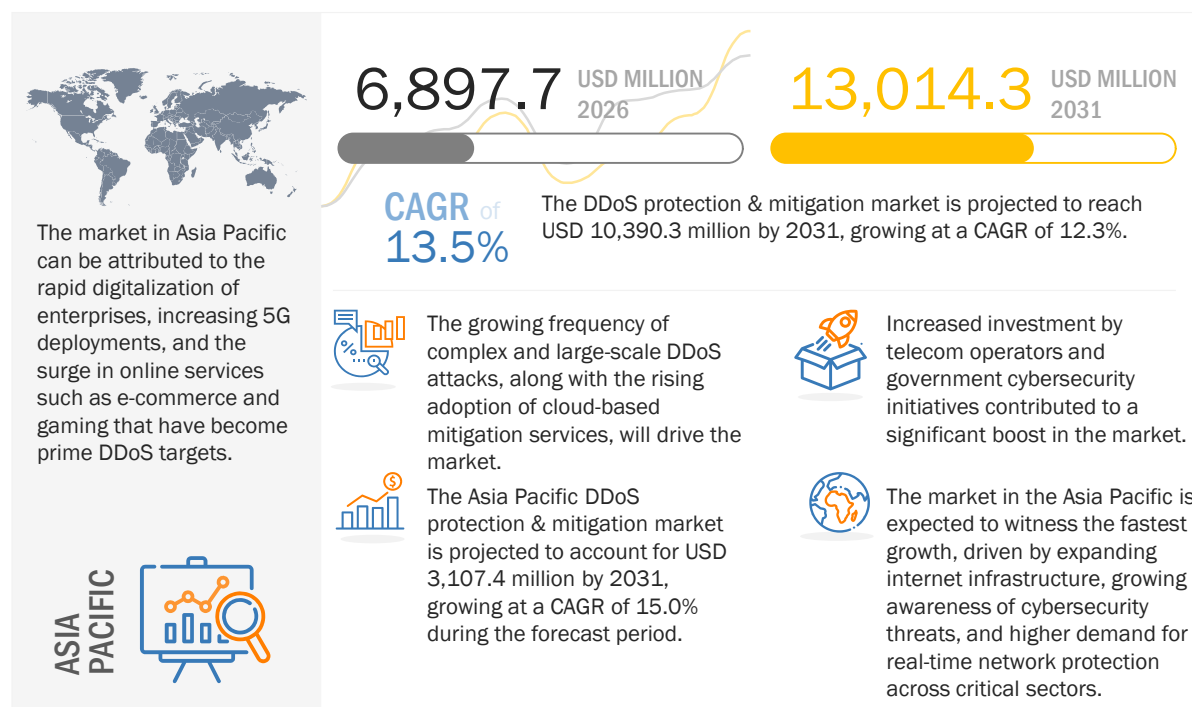
Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

The DDoS protection and mitigation market in Asia Pacific is expanding rapidly, driven by accelerated digital transformation, mass adoption of ecommerce, fintech, cloud platforms, and online services, and a sharp rise in high-volume cyberattacks targeting enterprises and government systems. Growing internet penetration, 5G rollout, and the surge in connected devices are increasing network vulnerabilities, pushing organizations to upgrade to modern, automated DDoS defense solutions. Countries like India, China, and Japan are investing heavily in cybersecurity due to strict regulations, rising attack sophistication, and the need to ensure service reliability in sectors such as BFSI, telecommunications, IT & ITeS, healthcare, and ecommerce. As a result, Asia Pacific has become one of the most dynamic markets, with strong demand for scalable, cloud-based protection and next-generation mitigation technologies.

3 PREMIUM INSIGHTS

3.1 ATTRACTIVE OPPORTUNITIES FOR PLAYERS IN DDOS PROTECTION & MITIGATION MARKET

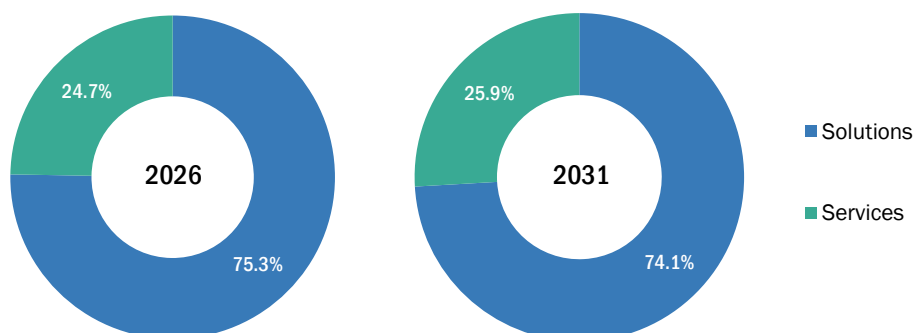
FIGURE 9 GROWTH IN FREQUENCY OF LARGE-SCALE DDOS ATTACKS AND RISING ADOPTION OF CLOUD-BASED MITIGATION SERVICES DRIVE MARKET



Source: Interviews with Experts, Company Presentations, Associations, Secondary Analysis, and MarketsandMarkets Analysis

3.2 DDOS PROTECTION & MITIGATION MARKET, BY OFFERING

FIGURE 10 SERVICES SEGMENT TO ACCOUNT FOR LARGER MARKET SHARE DURING FORECAST PERIOD

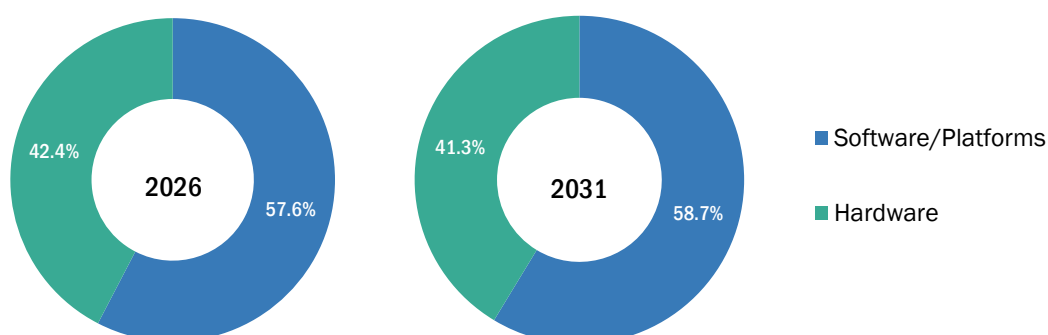


Note: Percentage values indicate the market share of segments in 2026 and 2031.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.3 DDOS PROTECTION & MITIGATION MARKET, BY SOLUTION

FIGURE 11 SOFTWARE/PLATFORMS SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD

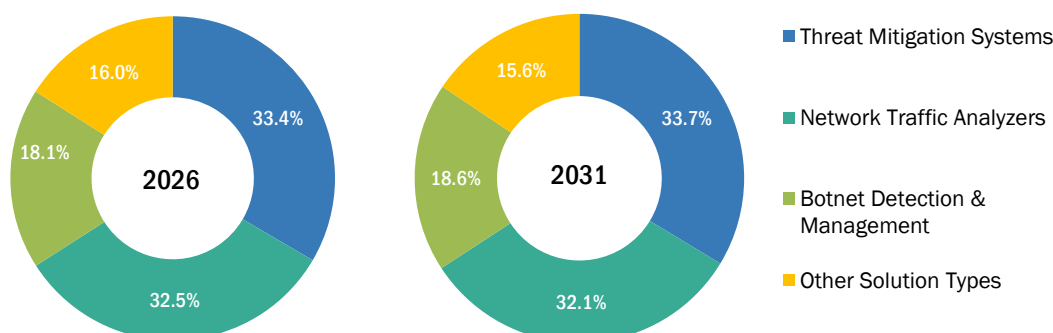


Note: Percentage values indicate the market share of segments in 2026 and 2031.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.4 DDOS PROTECTION & MITIGATION MARKET, BY SOLUTION TYPE

FIGURE 12 NETWORK TRAFFIC ANALYZERS SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD

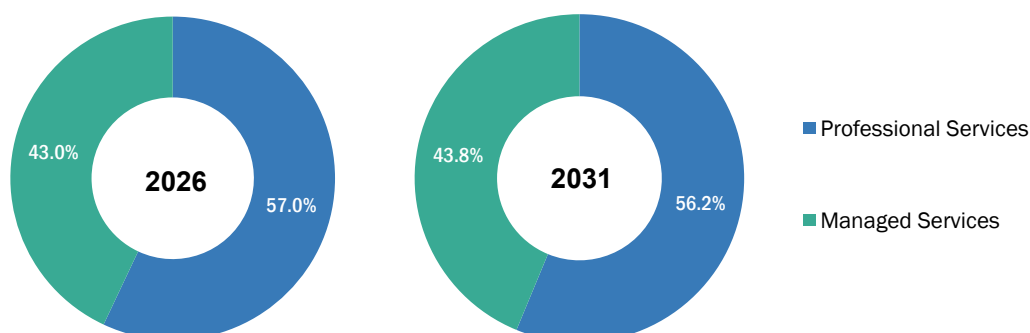


Note: Percentage values indicate the market share of segments in 2026 and 2031.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.5 DDOS PROTECTION & MITIGATION MARKET, BY SERVICE

FIGURE 13 PROFESSIONAL SERVICES SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD

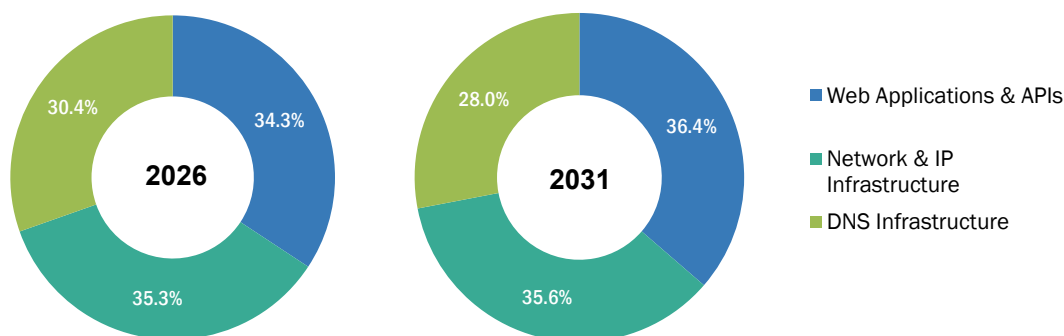


Note: Percentage values indicate the market share of segments in 2026 and 2031.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.6 DDOS PROTECTION & MITIGATION MARKET, BY APPLICATION AREA

FIGURE 14 NETWORK & IP INFRASTRUCTURE SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD

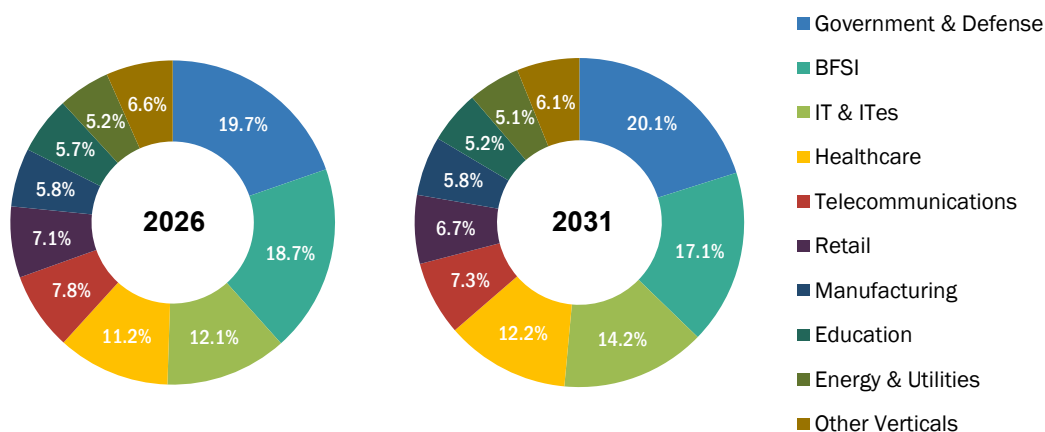


Note: Percentage values indicate the market share of segments in 2026 and 2031.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.7 DDOS PROTECTION & MITIGATION MARKET, BY VERTICAL

FIGURE 15 BFSI SEGMENT TO ACCOUNT FOR LARGEST MARKET SHARE DURING FORECAST PERIOD

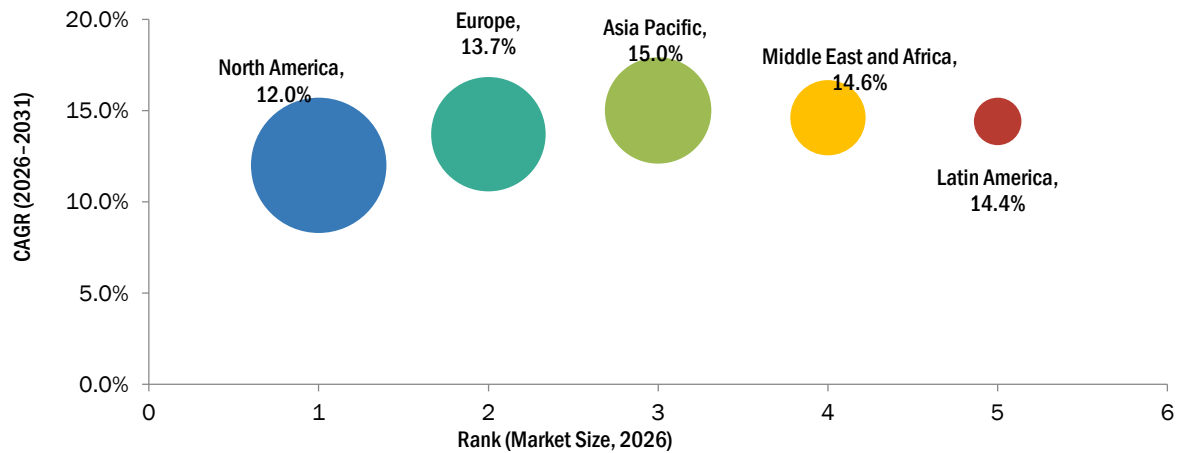


Note: Percentage values indicate the market share of segments in 2026 and 2031.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

3.8 DDOS PROTECTION & MITIGATION MARKET, BY REGION

FIGURE 16 ASIA PACIFIC TO EMERGE AS BEST MARKET FOR INVESTMENT IN NEXT FIVE YEARS



Note: The bubble size represents the market share of the regions in 2026.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

4 MARKET OVERVIEW

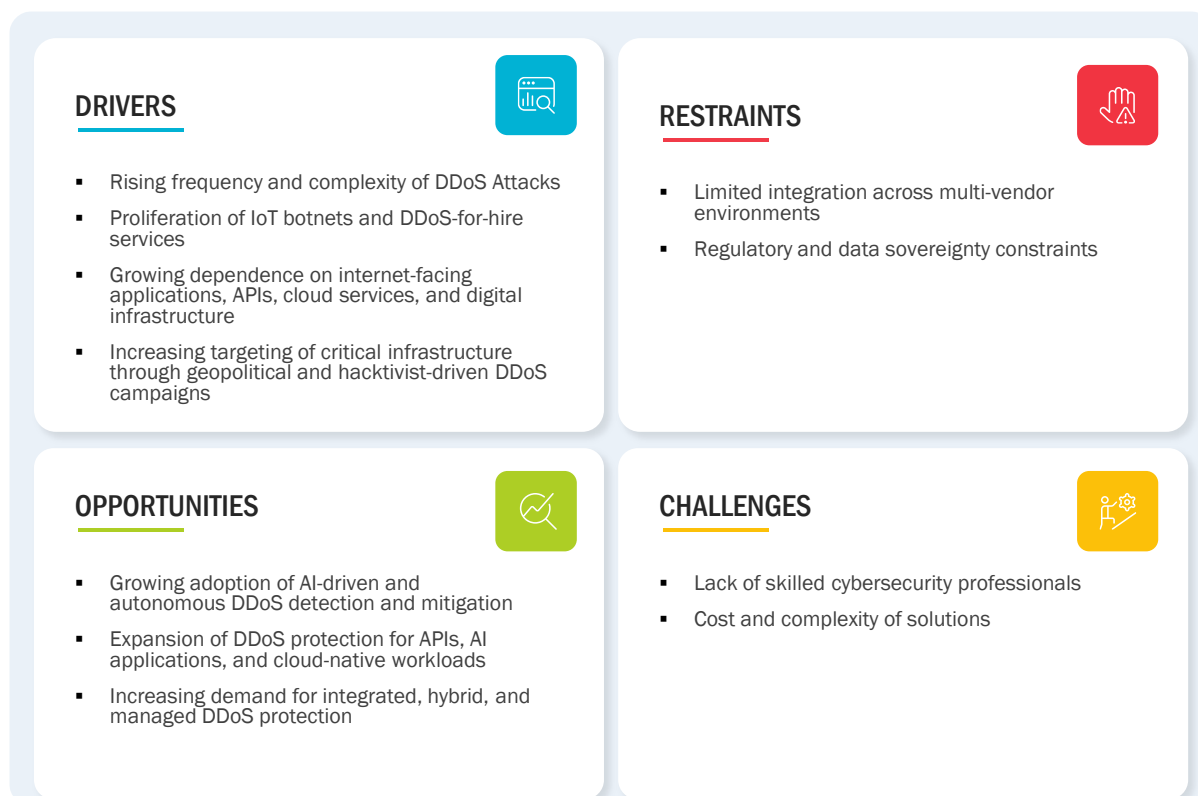
4.1 INTRODUCTION

The market overview chapter provides detailed information on the factors driving the growth of the DDoS protection & mitigation market. It comprises market dynamics, such as drivers, restraints, opportunities, and challenges. It further explains the impact of use cases and various industry standards on the market. Globally, companies are rapidly adopting DDoS protection and mitigation solutions and services to gain a competitive edge in the market. The vendors are rapidly adopting various business strategies, including collaborations, partnerships, and mergers and acquisitions, to provide customers with integrated and innovative DDoS protection and mitigation hardware solutions, software solutions, and services. The high growth potential of emerging regional markets, such as the Asia Pacific, the Middle East, and Africa, is expected to increase competition in the DDoS protection & mitigation market.

4.2 MARKET DYNAMICS

This research study indicates that the DDoS protection & mitigation market is of utmost importance for every firm and technology vendor. The market is expected to experience significant growth during the forecast period, due to various business drivers. Some of the factors driving the market are the growing need to safeguard enterprises and government organizations from volumetric attacks, attacks focused on consuming computational power and exploiting software vulnerabilities, and attacks causing time-outs. DDoS protection and mitigation solutions can be deployed on-premises as well as in cloud and hybrid environments. The drivers, restraints, opportunities, and challenges impacting the growth of the DDoS protection & mitigation market are listed below.

FIGURE 17 DDOS PROTECTION AND MITIGATION MARKET: DRIVERS, RESTRAINTS, OPPORTUNITIES, AND CHALLENGES



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

4.2.1 DRIVERS

4.2.1.1 Rising frequency and complexity of DDoS attacks

Multi-vector, high-volume attacks now combine volumetric floods with application-layer and protocol abuses, forcing mitigation stacks to operate at both massive scale and fine granularity. The practical effect is accelerated procurement of elastic, cloud-native scrubbing and automated detection: when Google disclosed the HTTP/2 Rapid Reset incidents that produced peaks of about 398 million requests per second and Cloudflare reported consecutive record attacks (including an 11.5 Tbps event in 2025), many enterprises re-architected to route traffic through global mitigation fabrics rather than rely on in-house appliances. Microsoft's July 2024 Azure/Azure Front Door incident, where a DDoS-triggered outage and subsequent implementation issues caused prolonged service disruption, showed that even hyperscalers must refine controls and that customers demand third-party mitigation SLAs. The rise of organized groups (e.g., NoName057(16)) and expanded IoT botnet families (Mozi/Mantis variants) has shortened the window for manual response, increasing appetite for always-on services and vendor-managed SOC. For vendors, this translates into larger enterprise deals, investment in terabit-scale capacity, and premium pricing for rapid, automated mitigation and telemetry services.

4.2.1.2 Proliferation of IoT botnets and DDoS-for-hire services

The proliferation of compromised IoT devices, routers, servers, and customer-premises equipment is increasing the availability of distributed resources that can be weaponized to launch large-scale DDoS attacks. Vulnerable connected devices provide attackers with geographically dispersed attack infrastructure, enabling sustained volumetric and multi-vector campaigns while making attribution and remediation more challenging. NETSCOUT observed more than 27,000 botnet-driven DDoS attacks in March 2025 alone, with attacks increasingly exploiting vulnerabilities in web servers, routers, and IoT devices. Its 2H 2025 research also identified IoT botnets capable of generating attacks exceeding 30 Tbps

and 4 Gbps, highlighting the growing capacity of compromised devices to overwhelm conventional network defenses. In parallel, the expansion of DDoS-for-hire or booter/stresser services is lowering the technical and financial barriers to launching attacks. The integration of automation, APIs, and AI into these services enables less-skilled threat actors to conduct sophisticated, multi-vector campaigns with limited technical expertise. This evolution is driving organizations and service providers to invest in automated DDoS detection, botnet identification, traffic filtering, rate limiting, and mitigation systems capable of responding to rapidly changing attack patterns without extensive manual intervention.

4.2.1.3 Growing dependence on internet-facing applications, APIs, cloud services, and digital infrastructure

The increasing dependence of enterprises on internet-facing applications, APIs, cloud platforms, and digitally connected infrastructure is expanding the attack surface that must remain continuously available. Organizations across industries are shifting critical business processes, customer interactions, transactions, and services to web applications and API-driven architectures, making availability a core operational requirement. This creates greater exposure to both network-layer and application-layer DDoS attacks. The growing use of APIs as the connective layer between applications, cloud services, and digital platforms is particularly relevant because API endpoints can become targets for high-volume requests designed to exhaust application and infrastructure resources. Akamai's latest research reported a 104% increase in Layer 7 DDoS attacks over two years, reinforcing the increasing exposure of application environments. As organizations expand hybrid and cloud-native environments, DDoS protection requirements are also moving beyond traditional network infrastructure toward web applications, APIs, DNS infrastructure, and other Internet-facing services. This is driving demand for scalable, cloud-based, automated, and application-aware DDoS protection and mitigation solutions capable of maintaining service availability across distributed digital environments.

4.2.1.4 Increasing targeting of critical infrastructure through geopolitical and hacktivist-driven DDoS campaigns

The increasing use of DDoS attacks as a tool for geopolitical disruption, hacktivism, and politically motivated campaigns is driving demand for resilient protection across critical infrastructure and essential digital services. Unlike financially motivated attacks that may focus on specific organizations, politically motivated campaigns can rapidly shift targets and generate coordinated attack waves against government agencies, financial institutions, telecommunications providers, transportation networks, energy organizations, and other critical services. NETSCOUT recorded more than 8 million DDoS attacks globally during the first half of 2025 and reported significant attack spikes associated with geopolitical events. During the India-Pakistan conflict, hacktivist groups targeted Indian government and financial-sector organizations, while the Iran-Israel conflict was associated with more than 15,000 attacks against Iran. The threat is extending beyond conventional corporate networks, with DNS, NTP, telecommunications, transportation, energy, and other critical Internet infrastructure becoming targets. NETSCOUT's 2H 2025 findings also highlighted sustained attacks against DNS and NTP infrastructure and continued targeting of government, financial services, telecommunications, transportation, and hospitality sectors. Consequently, organizations operating critical infrastructure are increasingly prioritizing always-on protection, high-capacity mitigation, automated response, traffic scrubbing, and geographically distributed DDoS defense architectures to maintain availability and operational continuity during coordinated attack campaigns.

4.2.2 RESTRAINTS

4.2.2.1 Limited integration across multi-vendor environments

Hybrid estates blending on-prem appliances, cloud front ends, CDNs, ISP scrubbing, and WAFs create operational friction when telemetry, policy orchestration, and routing controls do not align, slowing coordinated mitigation. During high-impact incidents, teams frequently encounter handoffs, such as on-premises to cloud scrubbing or ISP filter activation, that introduce latency or partial filtering. Microsoft's Azure outage in July 2024 exposed how configuration and integration issues can amplify an event. Large

vendors provide GRE routing, BGP steering, and managed route-on options (Akamai Prolexic's always-on/route-on choices illustrate operational complexity), yet integrating these with existing MPLS backbones, SD-WAN overlays, and SIEM/SOAR toolchains remains non-trivial for mid-market and regional enterprises. Vendors are introducing standardized APIs and telemetry feeds, and joint solutions (e.g., LevelBlue + Akamai managed WAAP) are showing progress; however, adoption is uneven across geographies, where local telcos and legacy systems still dominate. The integration burden increases TCO, complicates procurement, and can delay time-to-protect, particularly for financial institutions and service providers that require coordinated, low-latency failover across multiple vendors and jurisdictions.

4.2.2.2 Regulatory and data sovereignty constraints

Data localization laws and national security rules restrict cross-border traffic inspection and the use of foreign scrubbing centers, forcing vendors and customers to design mitigation architectures that respect in-country processing mandates. The European GDPR, China's Cybersecurity Law, and India's growing localization guidance have compelled security vendors to deploy in-region scrubbing capacity, separate logging enclaves, or hybrid models where only metadata is shared offshore, raising capex and time-to-market. For example, global providers must now negotiate local hosting arrangements or partner with regional telcos to offer compliant DDoS services; these arrangements increase unit cost and complicate SLAs for global customers. Critical sectors (BFSI, government, telecom) often demand in-country inspection, reducing the utility of global reroute strategies during peak attacks and pushing organizations toward appliance-first or carrier-based filtering. Nexusguard highlights regional variance for APAC, EMEA, Latin America, and Americas of mitigations in 2025, underlining how cross-border routing and local rules limit global scrubbing choices. The commercial consequence is slower expansion into regulated markets and higher pricing tiers for localized, compliant mitigation, which in turn shapes vendor go-to-market strategies, favoring partnerships, localized PoPs, and managed offerings that can meet sovereign controls.

4.2.3 OPPORTUNITIES

4.2.3.1 Growing adoption of AI-driven and autonomous DDoS detection and mitigation

The increasing scale and sophistication of DDoS attacks are creating an opportunity for vendors to differentiate through AI/ML-driven detection, behavioral analytics, and autonomous mitigation. Traditional threshold-based approaches can struggle with rapidly changing, multi-vector attacks, creating demand for systems that continuously learn legitimate traffic patterns and dynamically identify deviations. Cloudflare's current DDoS architecture, for example, uses traffic profiling, machine learning models, threat intelligence, and dynamic mitigation rules to automatically detect and mitigate attacks across Layers 3/4 and 7. Its Adaptive DDoS Protection builds customer-specific traffic profiles and uses ML to identify potentially automated traffic. The emergence of hyper-volumetric attacks further strengthens this opportunity, as Cloudflare reported 47.1 million DDoS attacks in 2025 and attacks reaching 31.4 Tbps. Vendors can capitalize by developing self-learning DDoS protection, autonomous traffic filtering, predictive attack detection, and AI-assisted mitigation orchestration that reduce dependence on manual intervention and improve response speed.

4.2.3.2 Expansion of DDoS protection for APIs, AI applications, and cloud-native workloads

The rapid adoption of APIs, cloud-native applications, and AI-enabled applications is creating new opportunities for application-layer and API-specific DDoS protection. APIs are becoming increasingly important components of enterprise digital architectures and AI ecosystems, while their high availability requirements make them attractive targets for attackers. Akamai reported that Layer 7 DDoS attacks increased 104% over two years, while the average number of daily API attacks increased 113% year over year. This creates opportunities for vendors to develop solutions that combine DDoS protection with API discovery, behavioral analysis, application-layer traffic profiling, bot detection, and automated mitigation. The opportunity is particularly relevant for cloud-native and distributed environments where applications

can span multiple cloud providers and data centers. Vendors can also expand into specialized protection for AI workloads, APIs supporting generative AI services, and high-volume digital platforms. Cloudflare reported that generative AI services were among the industries heavily targeted by hyper-volumetric DDoS attacks during 2025.

4.2.3.3 Increasing demand for integrated, hybrid, and managed DDoS protection

The growing complexity of enterprise infrastructure is creating an opportunity for integrated and managed DDoS protection combining on-premises appliances, cloud-based mitigation, traffic scrubbing, and centralized orchestration. Organizations operating hybrid and multi-cloud environments increasingly require protection that can extend across network infrastructure, DNS, applications, and APIs rather than relying on isolated protection mechanisms. Cloudflare, for instance, combines network-layer and application-layer protection with advanced TCP and DNS protection, while Akamai offers DDoS protection across cloud, on-premises, and hybrid environments. This creates opportunities for vendors to offer hybrid DDoS architectures, always-on cloud scrubbing, on-demand mitigation, centralized orchestration, and managed DDoS services. The opportunity is particularly relevant for SMEs and organizations without dedicated security teams, which can outsource continuous monitoring and mitigation instead of deploying and managing specialized infrastructure internally.

4.2.4 CHALLENGES

4.2.4.1 Lack of skilled cybersecurity professionals

The lack of skilled cybersecurity professionals represents a widening gap between the demand for advanced DDoS defense expertise and the availability of engineers trained in traffic engineering, protocol analysis, BGP routing, and multi-vector mitigation. This gap creates operational challenges because modern DDoS events require teams capable of interpreting real-time telemetry, coordinating with ISPs, adjusting scrubbing thresholds, and handling L7 API-targeted surges without disrupting legitimate traffic. Recent incidents highlight this pressure: during the 2024 Azure platform disruptions, Microsoft acknowledged that mitigation complexity required the involvement of specialized internal teams, increasing response time. Similarly, several APAC ISPs, such as Optus (Australia) and PLDT (Philippines), reported delays in stabilizing services after targeted DDoS bursts due to limited on-ground expertise. Vendors like Cloudflare, Radware, Nexusguard, and Akamai have expanded their managed SOC offerings to compensate for customer skill shortages; however, enterprises still face difficulty in building in-house response units because experienced DDoS analysts command premium salaries and are concentrated in North America and Western Europe. As attacks increasingly exploit encrypted channels, API endpoints, and multi-vector switching, the skill deficit becomes more pronounced, forcing organizations to rely heavily on outsourced 24×7 monitoring and automation-driven mitigation, which may not always match the speed required during peak attack windows.

4.2.4.2 Cost and complexity of solutions

The cost and complexity of solutions capture the high financial and operational burden associated with deploying hybrid DDoS architectures that combine cloud scrubbing, on-premises appliances, global routing adjustments, and continuous SOC oversight. This presents a significant challenge, as enterprises must manage complex integrations, such as GRE tunneling, BGP diversion, CDN interconnects, and L7 behavioral analytics, all of which require technical expertise and recurring expenditures. Nexusguard reports that the largest observed carpet-bombing event in 2025 simultaneously targeted 177 /24 prefixes. Implementing the distributed filtering and control plane capacity needed to detect these stealthy, low-rate floods, which bypass standard volumetric sensors, presents a significant financial and technical hurdle for most enterprises and mid-tier service providers. In 2024, several mid-market organizations in sectors such as fintech and ecommerce reported scaling back the adoption of Akamai Prolexic and NETSCOUT Arbor Edge services because always-on configurations and multi-site scrubbing could push annual costs into the high six-figure range. The complexity surfaced again when Cloudflare, AWS Shield, and Google Cloud Armor

issued emergency advisories during the HTTP/2 Rapid Reset attacks, requiring sudden customer-side configuration changes to mitigate protocol exploitation. Smaller enterprises and regional ISPs struggle with these adjustments, as they often lack the necessary staff and budget to maintain synchronized routing tables, traffic signatures, and scrubbing policies across their distributed networks. As DDoS vectors increasingly target APIs, microservices, and encrypted channels, solution stacks continue to grow more layered, making full-scale implementation and optimization increasingly difficult without significant investment in both infrastructure and operational expertise.

4.3 UNMET NEEDS AND WHITE SPACES

The DDoS protection & mitigation market presents several unmet needs and white-space opportunities as organizations face increasingly sophisticated attacks across network infrastructure, applications, APIs, DNS, and cloud environments. Existing solutions often operate across fragmented security layers, creating opportunities for unified platforms that provide centralized visibility, cross-layer attack correlation, and automated mitigation. Growing adoption of AI, multi-cloud architectures, APIs, IoT, and digital services is further creating demand for specialized protection capabilities. In addition, SMEs and organizations with limited cybersecurity expertise require affordable, simplified, and managed solutions, while continuous DDoS resilience testing can strengthen preparedness against evolving attack techniques.

TABLE 3 UNMET NEEDS AND WHITE SPACES IN DDOS PROTECTION AND MITIGATION MARKET

UNMET NEED/ WHITE SPACE	DESCRIPTION
Unified Multi-Layer DDoS Protection Platforms	- Organizations often deploy separate controls for network, application, API, and DNS protection, resulting in fragmented visibility and mitigation workflows. - There is increasing demand for unified platforms that correlate attack signals across infrastructure layers and enable centralized detection, policy management, and automated mitigation.
Cross-Layer DDoS Intelligence and Attack Correlation	- DDoS events targeting network infrastructure, DNS, web applications, and APIs are frequently analyzed through separate security controls. - Platforms capable of correlating traffic behavior, attack indicators, and threat intelligence across layers can improve detection accuracy and provide a consolidated view of multi-vector attacks.
AI-Driven Autonomous DDoS Detection and Mitigation	- Conventional threshold-based approaches can generate false positives and may require manual tuning as legitimate traffic patterns change. - AI/ML-driven solutions that establish dynamic traffic baselines, identify behavioral anomalies, and automatically adapt mitigation policies represent a significant opportunity for faster and more autonomous response.
API-Specific DDoS Protection	- Increasing API adoption across digital banking, ecommerce, cloud applications, and AI services is creating attack surfaces that require protection beyond conventional network-level mitigation. - There is an opportunity for solutions combining API discovery, behavioral analysis, rate limiting, bot detection, and DDoS mitigation specifically for API environments.
DDoS Protection for AI and High-Compute Workloads	- AI applications and high-compute digital services can be particularly resource-intensive, making them attractive targets for resource-exhaustion and application-layer attacks. - Specialized DDoS protection capable of understanding AI/API traffic patterns and dynamically controlling abusive requests represents an emerging opportunity.
Cloud-Native and Multi-Cloud DDoS	- Enterprises increasingly operate applications across multiple public clouds, private clouds, and on-premises environments, creating fragmented protection architectures. - Cloud-native solutions providing consistent DDoS policies, centralized visibility, and

Protection	automated mitigation across multi-cloud environments can address this interoperability gap.
Affordable DDoS Protection for SMEs	- SMEs often lack dedicated security teams and the infrastructure required to operate sophisticated DDoS mitigation environments. - There is whitespace for cost-effective, easy-to-deploy DDoS protection combining automated detection, managed mitigation, and simplified security management without requiring specialized expertise.
Integrated DDoS Protection and Network Security	- Organizations commonly operate DDoS protection alongside firewalls, IPS, WAF, SIEM, and other security controls, creating operational silos. - Solutions that integrate DDoS detection and mitigation with broader network security and security operations workflows can improve incident visibility, response coordination, and operational efficiency.
Continuous DDoS Resilience Testing and Validation	- Many organizations validate DDoS readiness periodically rather than continuously assessing whether their infrastructure can withstand evolving attack techniques and traffic volumes. - Automated testing and validation solutions that simulate DDoS scenarios, identify mitigation gaps, and continuously assess resilience can strengthen preparedness and reduce response uncertainty.
DDoS Protection for IoT and Botnet-Driven Infrastructure	- The proliferation of connected devices, routers, and IoT endpoints is expanding the infrastructure available for botnet-driven DDoS campaigns. - There is increasing scope for solutions that combine botnet intelligence, device behavior analysis, source identification, and automated traffic controls to mitigate attacks originating from distributed compromised devices.

Source: Company Website and MarketsandMarkets Analysis

4.4 INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES

The DDoS protection & mitigation market is closely interconnected with adjacent cybersecurity, network infrastructure, cloud security, and resilience markets, as organizations increasingly seek integrated protection across their digital environments. DDoS capabilities are being combined with network security, web application and API security, DNS protection, cloud and edge security, security operations, bot management, and cybersecurity testing to improve threat visibility and response. These interconnections enable organizations to correlate attack intelligence, automate mitigation, strengthen infrastructure resilience, and maintain continuous availability across increasingly distributed and Internet-facing environments.

4.4.1 INTERCONNECTED MARKETS

INTERCONNECTED MARKET	APPLICATION
Network Security and Network Infrastructure Protection	Integrates DDoS protection with firewalls, intrusion prevention, traffic analysis, and network security controls to detect malicious traffic, protect network infrastructure, and maintain service availability.
Web Application & API Security	Combines DDoS mitigation with WAF, API security, bot management, behavioral analysis, and rate limiting to protect Internet-facing applications and APIs against application-layer attacks and resource exhaustion.
DNS Security and Infrastructure Protection	Integrates DDoS protection with DNS security, traffic monitoring, DNS filtering, and resilient DNS infrastructure to prevent DNS-based attacks and maintain continuous availability of domain resolution services.

Cloud and Edge Security	Combines cloud-based DDoS mitigation with edge security, traffic scrubbing, application protection, and distributed infrastructure to provide scalable protection across public cloud, hybrid, multi-cloud, and edge environments.
Security Operations & Threat Intelligence Platforms	Integrates DDoS alerts and attack telemetry with SIEM, SOAR, threat intelligence, and security analytics platforms to improve attack correlation, automated response, incident investigation, and enterprise-wide security visibility.
Bot Management & Fraud Prevention	Correlates DDoS and bot detection with behavioral analytics, device intelligence, and automated traffic controls to distinguish malicious automated traffic from legitimate users and mitigate bot-driven attacks.
Network Performance & Traffic Management	Integrates DDoS traffic analysis with load balancing, traffic routing, rate limiting, and network performance management to maintain application availability and optimize legitimate traffic during attack conditions.
Cybersecurity Testing & Resilience	Connects DDoS protection with security testing, attack simulation, vulnerability assessment, and resilience validation to identify mitigation gaps and continuously assess an organization's ability to withstand DDoS attacks.

Source: Secondary Research and MarketsandMarkets Analysis

4.4.2 CROSS-SECTOR OPPORTUNITIES

- **AI-Driven DDoS Detection and Autonomous Mitigation:** The increasing scale and sophistication of DDoS attacks are creating opportunities for AI/ML-driven traffic analysis, behavioral anomaly detection, predictive attack identification, and automated mitigation. Vendors capable of dynamically adapting traffic-filtering policies and reducing manual intervention can improve response speed and protection accuracy across enterprise and service-provider environments.
- **Application, API, and DNS Protection:** The rapid adoption of web applications, APIs, cloud services, and digital platforms is expanding demand for application-aware DDoS protection. Integrating DDoS mitigation with WAF, API security, bot management, rate limiting, and DNS protection can enable vendors to address attacks across multiple digital infrastructure layers through unified security platforms.
- **Cloud, Edge, and Multi-Cloud Protection:** Increasing migration toward public cloud, hybrid infrastructure, and edge computing is creating opportunities for scalable DDoS protection delivered across distributed environments. Vendors can strengthen their offerings through cloud scrubbing, distributed mitigation capacity, centralized policy management, and consistent protection across multi-cloud and hybrid infrastructures.
- **IoT and Botnet-Driven DDoS Protection:** The proliferation of connected devices, routers, and IoT endpoints is expanding the infrastructure available for botnet-driven attacks. Solutions combining botnet intelligence, device behavior analysis, traffic profiling, and automated source blocking can address the growing requirement to detect and mitigate attacks generated by distributed compromised devices.
- **Integration with Security Operations and Threat Intelligence:** Integration of DDoS protection with SIEM, SOAR, threat intelligence, and security analytics platforms presents opportunities to improve attack correlation and automated incident response. Coordinating DDoS telemetry with broader cybersecurity workflows can provide centralized visibility, accelerate investigations, and enable organizations to orchestrate mitigation across network and application environments.

- **DDoS Resilience Testing and Continuous Validation:** Organizations increasingly require assurance that their infrastructure can withstand evolving attack techniques and traffic volumes. Integration of DDoS protection with attack simulation, resilience testing, and continuous validation can help identify mitigation gaps, assess response readiness, and improve business continuity across critical digital services.
- **Managed DDoS Protection for SMEs and Resource-Constrained Organizations:** SMEs and organizations with limited cybersecurity expertise represent an opportunity for simplified managed DDoS services combining continuous monitoring, automated detection, cloud-based mitigation, and expert response. Such offerings can reduce the infrastructure and specialist skills required to implement enterprise-grade DDoS protection and broaden adoption across underserved customer segments.

4.5 STRATEGIC MOVES BY TIER-1/2/3 PLAYERS

The DDoS protection & mitigation market is evolving rapidly as organizations strengthen defenses against increasingly sophisticated volumetric, protocol, application-layer, and multi-vector attacks. The growing dependence on cloud services, web applications, APIs, DNS infrastructure, and digitally connected networks is driving demand for scalable, automated, and multi-layer DDoS protection. Organizations are increasingly seeking integrated solutions that combine network traffic analysis, threat detection, mitigation, botnet detection, application and API protection, and cloud-based scrubbing to improve attack response while reducing operational complexity. Strategic initiatives such as AI-driven traffic analytics, autonomous mitigation, behavioral anomaly detection, automated traffic filtering, botnet intelligence, and hybrid cloud protection are enabling vendors to strengthen DDoS resilience and accelerate response to evolving attack patterns. Vendors are also expanding cloud-native and managed DDoS protection services and integrating DDoS intelligence with network security, application security, DNS protection, SIEM, SOAR, and broader cybersecurity platforms to provide end-to-end protection across digital infrastructure.

The competitive landscape of the DDoS protection & mitigation market can be categorized into Tier 1 global market leaders, Tier 2 established and specialized players, and Tier 3 niche and emerging providers. Tier 1 vendors such as Akamai, Cloudflare, NETSCOUT, Radware, and Fortinet leverage extensive global infrastructure, high-capacity mitigation networks, advanced traffic analytics, cloud-based protection, and broad cybersecurity portfolios to deliver enterprise-scale DDoS protection. Tier 2 vendors including A10 Networks, F5, Huawei, Thales (Imperva), Fastly, Link11, NSFOCUS, Corero, and Nexusguard focus on specialized capabilities such as DDoS detection and mitigation, network traffic analysis, application and API protection, bot management, DNS security, and managed DDoS services. Tier 3 vendors such as Haltdos, DDoS-GUARD, Indusface, Gcore, Qrator Labs, StormWall, Cloudbric, MazeBolt, and Andrisoft are driving innovation through cloud-native mitigation, automated traffic filtering, application-layer protection, botnet detection, DDoS resilience testing, and specialized managed services designed for SMEs, digital businesses, cloud environments, and regional service providers.

TABLE 4 STRATEGIC MOVES BY PLAYERS IN DDoS PROTECTION & MITIGATION MARKET

TIER	FOCUS AREAS	EXAMPLES	STRATEGIC INITIATIVES/DESCRIPTION
Tier 1 – Market Leaders	DDoS detection and mitigation, network traffic analysis, cloud-based protection, application and API security, automated mitigation, hybrid protection, managed DDoS services.	Akamai, Cloudflare, NETSCOUT, Radware, Fortinet	Expanding integrated DDoS protection through AI-driven traffic analytics, automated detection and mitigation, cloud-based scrubbing, application and API protection, and hybrid deployment capabilities. Vendors are strengthening global mitigation capacity and integrating DDoS protection with broader network and cybersecurity platforms across enterprise, cloud, BFSI, telecom, and critical infrastructure environments.
Tier 2 – Established & Specialized Players	DDoS mitigation platforms, network traffic analysis, application-layer protection, bot management, DNS protection, managed DDoS services, network security.	A10 Networks, F5, Huawei, Thales (Imperva), Fastly, Link11, NSFOCUS, Corero, Nexusguard	Strengthening specialized DDoS capabilities through high-capacity mitigation, traffic detection, application and API protection, cloud-based scrubbing, and integration with network security portfolios. Players are expanding managed and cloud-delivered services while enhancing protection across network infrastructure, web applications, APIs, and DNS environments.
Tier 3 – Niche & Emerging Players	Cloud-based DDoS protection, managed mitigation, botnet detection, application security, traffic filtering, DDoS resilience and testing.	Haltdos, DDoS-GUARD, Indusface, Gcore, Qrator Labs, StormWall, Cloudbric, MazeBolt, Andrisoft	Driving innovation through specialized DDoS protection, automated traffic filtering, cloud-based mitigation, application-layer security, botnet protection, and DDoS resilience testing. These vendors are targeting SMEs, digital businesses, cloud environments, and regional service providers with scalable, specialized, and managed protection offerings.

Source: Company Website and MarketsandMarkets Analysis

4.5.1 CROSS-TIER STRATEGIC PATTERNS

The cross-tier strategic patterns in the DDoS protection and mitigation market reflect the industry's transition from traditional, reactive mitigation toward automated, intelligent, and distributed DDoS defense architectures. The growing frequency of volumetric, multi-vector, and application-layer attacks, along with the emergence of hyper-volumetric attacks, is increasing demand for solutions capable of detecting and mitigating threats in real time. Organizations are increasingly adopting cloud-based and hybrid DDoS protection solutions that provide scalable mitigation across network, application, API, and DNS infrastructure. Vendors across Tier 1, Tier 2, and Tier 3 categories are strengthening their offerings through AI/ML-driven anomaly detection, automated mitigation, behavioral analysis, real-time traffic inspection, and integration with CDN, WAF, DNS, cloud security, and network infrastructure.

Strategic differentiation across tiers is increasingly defined by mitigation scale, detection intelligence, automation, deployment flexibility, and breadth of attack-vector coverage. Tier 1 vendors are focusing on globally distributed DDoS protection platforms that combine network-layer and application-layer mitigation with CDN, WAF, DNS, and edge security capabilities. Tier 2 players are strengthening specialized capabilities such as automated traffic analysis, botnet detection, behavioral analytics, and application/API protection while expanding cloud-based deployments and managed DDoS services. Tier 3 vendors are driving innovation through AI-powered detection, advanced traffic analytics, attack-specific mitigation, and cloud-native architectures tailored to emerging digital businesses, service providers, and enterprises. Across all tiers, vendors are prioritizing real-time detection, automated mitigation, adaptive traffic filtering,

multi-vector protection, and high-capacity mitigation infrastructure to minimize service disruption and maintain application and network availability.

TABLE 5 CROSS-TIER STRATEGIC PATTERNS OF VENDORS

STRATEGIC THEME	KEY INSIGHTS
Platform Consolidation and Unified Financial Crime Management	Vendors across all tiers are expanding capabilities across fraud analytics, authentication, identity verification, transaction monitoring, AML, KYC, and case management to deliver unified financial crime platforms. Organizations increasingly prefer integrated solutions that reduce operational complexity, improve fraud visibility, and enable centralized risk management across digital channels.
AI-driven Fraud Analytics and Automated Decisioning	Vendors are embedding artificial intelligence, machine learning, graph analytics, and behavioral intelligence into fraud detection, transaction risk scoring, and investigation workflows. AI-driven capabilities improve fraud detection accuracy, reduce false positives, automate investigations, and enable adaptive decision-making against emerging fraud threats.
Identity-centric Fraud Prevention and Adaptive Authentication	Organizations are increasingly adopting identity intelligence, behavioral biometrics, device intelligence, continuous authentication, and risk-based authentication to prevent account takeover, synthetic identity fraud, and digital onboarding fraud while maintaining seamless customer experiences.
Real-time Transaction Monitoring and Payment Fraud Prevention	Vendors continue strengthening real-time fraud detection capabilities for instant payments, digital wallets, open banking, embedded finance, and cross-border payment ecosystems. Real-time analytics and behavioral monitoring enable rapid identification of fraudulent transactions before financial losses occur.
Cloud-native Fraud Prevention and Fraud Prevention as a Service (FPaaS)	Across all tiers, vendors are expanding cloud-delivered fraud prevention platforms that offer scalable deployment, centralized fraud monitoring, managed services, AI model updates, and simplified integration across hybrid and multi-cloud environments.
Developer-friendly APIs and Ecosystem Integration	Vendors are increasing interoperability with payment gateways, digital identity providers, core banking systems, CRM platforms, SIEM, SOAR, and threat intelligence platforms through APIs and ecosystem partnerships. These integrations improve enterprise-wide fraud visibility, automate workflows, and strengthen coordinated fraud response.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

4.5.2 STRATEGIC TRENDS

The DDoS protection & mitigation market is undergoing significant strategic transformation as organizations strengthen resilience across increasingly distributed digital infrastructures. The rapid growth of cloud services, web applications, APIs, DNS infrastructure, and connected devices is driving adoption of scalable and intelligent DDoS protection capable of detecting and mitigating attacks across multiple layers. Organizations are increasingly moving toward unified, multi-layer DDoS protection platforms that integrate traffic analysis, threat detection, automated mitigation, botnet management, application and API protection, and cloud-based scrubbing. Artificial intelligence, machine learning, behavioral analytics, and automation are becoming fundamental technologies for improving detection accuracy and accelerating mitigation. Vendors are also expanding cloud-native and managed DDoS services, hybrid protection architectures, and integration with SIEM, SOAR, WAF, and broader cybersecurity platforms. These strategic trends are enabling organizations to improve attack visibility, automate response, maintain service availability, and strengthen resilience against increasingly sophisticated and high-volume DDoS attacks.

4.5.2.1 AI-Driven and Autonomous DDoS Detection and Mitigation

Artificial intelligence and machine learning are increasingly being incorporated into DDoS protection to improve detection accuracy and accelerate mitigation. Vendors are using behavioral analytics and traffic profiling to establish dynamic baselines and identify deviations associated with malicious activity. Automated mitigation can subsequently trigger traffic filtering, rate limiting, or diversion to scrubbing infrastructure without extensive manual intervention. This is particularly important as attacks become more volumetric, multi-vector, and application-aware. Cloudflare reported mitigating 47.1 million DDoS attacks in 2025, including attacks reaching 31.4 Tbps, demonstrating the scale at which automated defenses must operate. AI-driven capabilities are therefore becoming an important differentiator for vendors seeking to provide adaptive and autonomous DDoS protection.

4.5.2.2 Increasing Focus on Application, API, and DNS Protection

DDoS protection is increasingly extending beyond traditional network infrastructure toward web applications, APIs, and DNS services. Organizations are increasingly dependent on Internet-facing applications and API-driven architectures, creating additional attack surfaces that can be targeted through application-layer request floods and resource-exhaustion attacks. Akamai reported a 104% increase in Layer 7 DDoS attacks over two years, highlighting the growing importance of application-aware protection. Vendors are consequently integrating DDoS mitigation with WAF, API security, bot management, rate limiting, and DNS protection. This convergence enables organizations to identify malicious traffic more accurately while maintaining legitimate application traffic and protecting critical digital services across multiple infrastructure layers.

4.5.2.3 Shift Toward Cloud-Native and Hybrid DDoS Protection

The increasing adoption of public cloud, hybrid infrastructure, and distributed digital environments is driving a shift toward cloud-native and hybrid DDoS protection architectures. Cloud-based mitigation enables organizations to absorb large-scale attacks through geographically distributed scrubbing infrastructure before malicious traffic reaches critical systems. Hybrid approaches combine cloud-based mitigation with on-premises appliances or network controls, allowing organizations to address both high-volume attacks and attacks requiring localized traffic inspection. Vendors are expanding globally distributed mitigation capacity and integrating cloud protection with network, application, and DNS security. This trend is particularly relevant for enterprises operating multi-cloud environments, where centralized visibility and consistent protection policies are increasingly required across distributed workloads and Internet-facing services.

5 INDUSTRY TRENDS

5.1 PORTER'S FIVE FORCES ANALYSIS

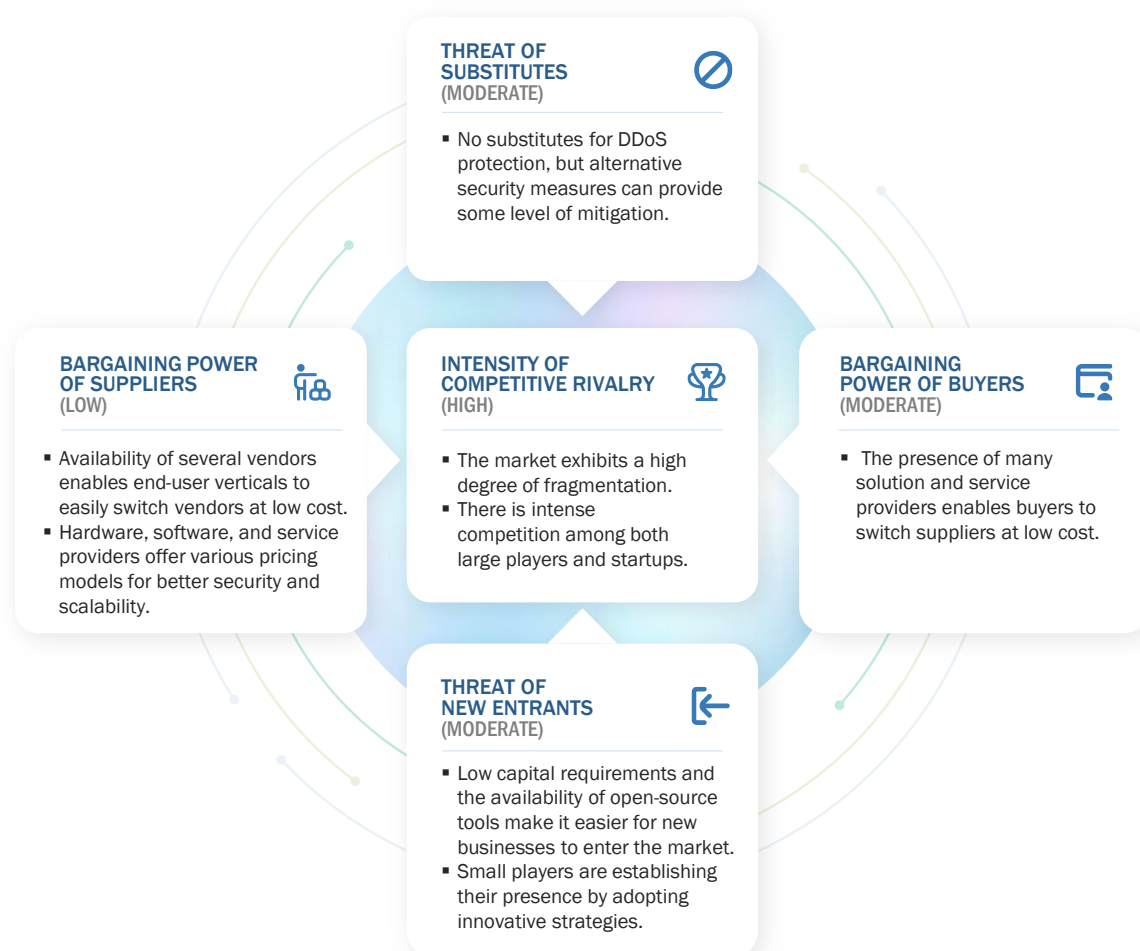
Porter's Five Forces analysis is a framework that determines the competitive intensity of a market. This section analyzes the DDoS protection & mitigation market from five different perspectives: the intensity of competitive rivalry, the threat of new entrants, the bargaining power of suppliers, the bargaining power of buyers, and the threat of substitutes. It draws insights from organizations' economics to find five forces that determine the competitive intensity and, therefore, the attractiveness of the DDoS protection & mitigation market in terms of profitability.

TABLE 6 IMPACT OF PORTER'S FIVE FORCES ON DDoS PROTECTION AND MITIGATION MARKET

PORTER'S FIVE FORCES	IMPACT
Intensity of Competitive Rivalry	High
Bargaining Power of Suppliers	Low
Bargaining Power of Buyers	Moderate
Threat of Substitutes	Moderate
Threat of New Entrants	Moderate

Source: Interviews with Experts and MarketsandMarkets Analysis

FIGURE 18 DDOS PROTECTION AND MITIGATION MARKET: PORTER'S FIVE FORCES ANALYSIS



Source: MarketsandMarkets Analysis

5.1.1 THREAT OF NEW ENTRANTS

Moderate: While the market is relatively accessible due to low capital requirements and the availability of open-source tools, the barriers to entry are moderate. Established players with significant market share, brand recognition, and existing customer relationships can create challenges for newcomers. The growing number of cyber-attack instances is responsible for increasing the global demand for cybersecurity. Thus, cybersecurity solutions are widely adopted by companies across the globe to implement business and operational security strategies. These market traits have led to high growth in the overall market size. The attractiveness of the market has also lured many new market entrants who have eaten into customer mindshare and diluted profitability.

5.1.2 THREAT OF SUBSTITUTES

Moderate: While there are no direct substitutes for DDoS protection, alternative security measures, such as firewalls, intrusion detection systems, and web application firewalls, can provide some level of mitigation. However, these solutions may not offer the same level of specialized protection against DDoS attacks. Small enterprises have largely adopted the product imitator competitive strategy by offering identical cybersecurity solutions at lower prices. The buyer's propensity toward low-cost solutions and services has increased the threat of product substitution in the DDoS protection & mitigation market.

5.1.3 BARGAINING POWER OF SUPPLIERS

Low: Suppliers have low bargaining power due to intense competition in the market. The cost of switching suppliers is also low in the DDoS protection & mitigation market; hence, suppliers face constant pressure to lose customers to their competitors. The suppliers for organizations in the DDoS protection & mitigation market have low strength in the distribution channel for supplying IT and hardware products. The firms in the market could achieve a better supplier status through backward vertical integration to accommodate supplier operations.

5.1.4 BARGAINING POWER OF BUYERS

Moderate: The buyer base comprises organizations of varying sizes and industries. Larger enterprises with substantial IT budgets may have greater bargaining power, demanding competitive pricing and customized solutions. However, smaller organizations may be more reliant on a limited number of vendors. Buyers in the DDoS protection & mitigation market have major price sensitivity issues due to the availability of cost-competitive DDoS protection and mitigation solutions from small-scale solution providers. The DDoS protection & mitigation market exhibits a growing demand for inelasticity, where price sensitivity changes do not reflect a change in demand but rather a shift in demand toward low-priced solutions.

5.1.5 INTENSITY OF COMPETITIVE RIVALRY

High: The DDoS protection & mitigation market is highly competitive, characterized by numerous players, product differentiation, and price competition. This intensity is driven by factors such as the rapid evolution of attack techniques, the criticality of DDoS protection, and the low switching costs for buyers. The intense competition in the DDoS protection & mitigation market has prompted companies to adopt robust strategies to overcome the competition and ensure sustainability. Large enterprises have adopted product innovations to retain and expand their clientele. SMEs have adopted cost leadership strategies to counter the product portfolios of larger enterprises. The emergence of vulnerability management software providers catering to niche segments involves various competitive strategies for business expansion and tackling fierce competition.

5.2 MACROECONOMICS INDICATORS

5.2.1 INTRODUCTION

Macroeconomic conditions play a significant role in shaping investment priorities for DDoS protection and mitigation, as enterprises adjust cybersecurity spending in response to global economic cycles, digitalization momentum, and sector-specific growth patterns. As organizations across BFSI, ecommerce, telecom, cloud services, and public-sector digital programs expand their online operations, the need for uninterrupted service availability becomes tightly linked to economic productivity. High-value digital infrastructures, such as digital payments, online trading platforms, OTT content delivery, and distributed cloud workloads, are increasingly sensitive to service outages, making DDoS resilience an operational necessity rather than a discretionary expenditure. Economic recovery in key regions, combined with accelerated enterprise cloud migration and infrastructure modernization, strengthens demand for scalable and automated DDoS protection solutions capable of supporting global traffic surges. At the same time, periods of economic strain prompt organizations to shift from large capital-heavy deployments toward managed services and consumption-based models, influencing how solution providers position and price their offerings. Overall, macroeconomic dynamics direct both the pace and structure of cybersecurity investments, reshaping market behavior across regions.

5.2.2 GDP TRENDS AND FORECAST

Gross Domestic Product (GDP) reflects a country's economic strength and its capacity to invest in digital infrastructure, cloud computing, telecommunications, and cybersecurity capabilities, including DDoS protection and mitigation solutions. Countries experiencing sustained economic growth typically demonstrate higher investments in digital transformation, cloud adoption, ecommerce, data centers, and Internet infrastructure, increasing demand for solutions that ensure service availability and resilience. As digital banking, online commerce, APIs, cloud applications, and connected services continue to expand, organizations face greater exposure to disruptive DDoS attacks. Regions such as North America, Europe, and Asia Pacific demonstrate strong demand due to extensive digital infrastructure, increasing cybersecurity investments, and growing cloud ecosystems. Economic development also accelerates investments in AI, edge computing, 5G, and distributed networks, creating additional requirements for scalable and automated DDoS protection. As economies become increasingly digital and interconnected, organizations are prioritizing cloud-based, AI-driven, and multi-layer DDoS protection to maintain business continuity, protect critical infrastructure, and ensure uninterrupted access to digital services.

TABLE 7 GDP PERCENTAGE CHANGE, BY KEY COUNTRY, 2021-2030

Country	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Argentina	10.7%	5%	-1.6%	-2.8%	5.0%	4.5%	3.9%	3.1%	2.3%	3.2%
Australia	5.6%	3.8%	2.1%	1.5%	2.0%	2.1%	2.2%	2.2%	2.3%	2.3%
Austria	4.2%	4.8%	-0.7%	0.4%	1.6%	1.4%	1.0%	0.9%	0.9%	0.7%
Belgium	6.9%	3%	1.5%	1.2%	1.2%	1.2%	1.2%	1.3%	1.3%	1.3%
Brazil	4.8%	3%	2.9%	2.2%	2.1%	2.1%	2.0%	2.0%	2.0%	2.5%
Chile	11.3%	2.1%	0.2%	2.0%	2.5%	2.4%	2.3%	2.3%	2.3%	2.2%
China	8.4%	3%	5.2%	4.6%	4.1%	3.8%	3.6%	3.4%	3.3%	3.4%
Colombia	10.8%	7.3%	0.6%	1.1%	2.5%	3.0%	3.0%	3.0%	3.0%	2.8%
Denmark	6.8%	2.7%	1.8%	2.1%	1.5%	1.5%	1.4%	1.4%	1.4%	1.5%
Egypt	3.3%	6.7%	3.8%	3.0%	4.4%	4.7%	5.1%	5.5%	5.6%	5.3%
Finland	2.8%	1.3%	-1.0%	0.4%	1.9%	1.9%	1.7%	1.6%	1.5%	1.2%
France	6.3%	2.5%	0.9%	0.7%	1.4%	1.6%	1.5%	1.4%	1.3%	1.2%
Germany	3.2%	1.8%	-0.3%	0.2%	1.3%	1.5%	1.1%	0.8%	0.7%	0.7%
India	9.7%	7%	7.8%	6.8%	6.5%	6.5%	6.5%	6.5%	6.5%	6.5%
Indonesia	3.7%	5.3%	5.0%	5.0%	5.1%	5.1%	5.1%	5.1%	5.1%	5.1%
Iran	4.7%	3.8%	4.7%	3.3%	3.1%	2.7%	2.3%	2.0%	2.0%	2%
Iraq	1.6%	7.0%	-2.2%	1.4%	5.3%	3.8%	3.6%	3.6%	3.6%	4.1%
Italy	8.3%	4.0%	0.9%	0.7%	0.7%	0.2%	0.3%	0.8%	0.8%	0.7%
Japan	2.6%	1.0%	1.9%	0.9%	1.0%	0.8%	0.6%	0.6%	0.4%	0.5%
South Korea	4.3%	2.6%	1.4%	2.3%	2.3%	2.2%	2.1%	2.1%	2.0%	1.9%
Kuwait	1.7%	6.1%	-2.2%	-1.4%	3.8%	2.5%	2.6%	2.6%	2.6%	2.3%
Malaysia	3.3%	8.7%	3.7%	4.4%	4.4%	4.4%	4.0%	4.0%	4.0%	4%
Mexico	5.7%	3.9%	3.2%	2.4%	1.4%	1.9%	2.1%	2.1%	2.1%	2.1%
Netherlands	6.2%	4.3%	0.1%	0.6%	1.3%	1.9%	1.9%	1.8%	1.6%	1.2%
New Zealand	5.6%	2.4%	0.6%	1.0%	2.0%	2.4%	2.4%	2.4%	2.4%	2.2%
Philippines	5.7%	7.6%	5.6%	6.2%	6.2%	6.2%	6.3%	6.3%	6.4%	6%

Poland	6.9%	5.3%	0.2%	3.1%	3.5%	3.3%	3.0%	3.0%	3.0%	2.6%
Qatar	1.6%	4.2%	1.6%	2.0%	2.0%	5.9%	7.6%	3.4%	1.6%	3.4%
Saudi Arabia	5.1%	7.5%	-0.8%	2.6%	6.0%	4.0%	3.5%	3.0%	3.5%	3.3%
Singapore	9.7%	3.8%	1.1%	2.1%	2.3%	2.5%	2.5%	2.5%	2.5%	2.5%
South Africa	4.7%	1.9%	0.6%	0.9%	1.2%	1.4%	1.4%	1.4%	1.4%	1.8%
Spain	6.4%	5.8%	2.5%	1.9%	2.1%	1.8%	1.6%	1.6%	1.6%	1.6%
Sweden	6.1%	2.7%	-0.2%	0.2%	2.2%	2.2%	2.2%	2.1%	2.1%	1.7%
Switzerland	5.4%	2.7%	0.8%	1.3%	1.4%	1.8%	1.2%	1.8%	1.2%	1.8%
Thailand	1.5%	2.5%	1.9%	2.7%	2.9%	3.0%	3.0%	3.0%	3.0%	2.5%
Türkiye	11.4%	5.5%	4.5%	3.1%	3.2%	3.3%	3.4%	3.5%	3.5%	3.8%
UAE	4.4%	7.9%	3.4%	3.5%	4.2%	4.3%	4.4%	4.5%	4.5%	3.9%
UK	8.7%	4.3%	0.1%	0.5%	1.5%	1.7%	1.7%	1.6%	1.4%	1.4%
US	5.8%	1.9%	2.5%	2.7%	1.9%	2.0%	2.1%	2.1%	2.1%	1.8%
Vietnam	2.6%	8.1%	5.0%	5.8%	6.5%	6.5%	6.5%	6.5%	6.5%	5.3%

Source: International Monetary Fund (IMF)

According to the International Monetary Fund (IMF) World Economic Outlook Update, published in July 2026, global GDP growth is projected at 3.0% in 2026 and 3.4% in 2027, reflecting continued economic resilience despite geopolitical and macroeconomic uncertainties. The improving macroeconomic environment supports investments in digital transformation, cloud infrastructure, data centers, telecommunications, and connected digital services, increasing the need for DDoS protection and mitigation capabilities. Regions such as North America, Europe, and Asia Pacific are witnessing expanding adoption of cloud computing, 5G, ecommerce, APIs, and Internet-facing applications, creating larger attack surfaces. Although inflationary pressures, geopolitical tensions, and tighter financial conditions may influence cybersecurity spending, DDoS protection remains a strategic investment as organizations seek to maintain service availability, protect critical infrastructure, and ensure business continuity. Growing investments in AI, edge computing, multi-cloud environments, and digital infrastructure continue to create favorable conditions for adoption of scalable, automated, and multi-layer DDoS protection solutions.

5.2.3 TRENDS IN GLOBAL DDOS PROTECTION & MITIGATION INDUSTRY

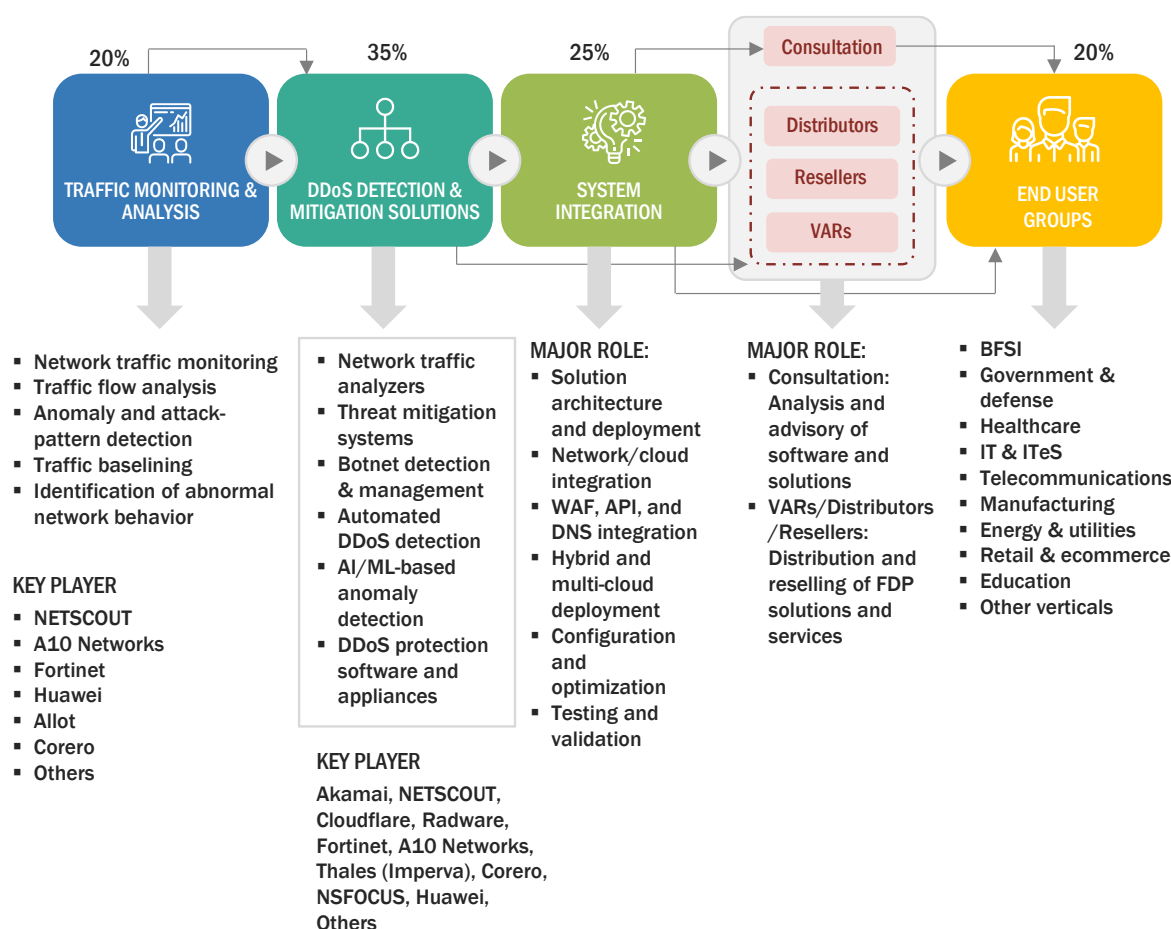
- Hybrid mitigation architectures combining on-prem appliances with cloud scrubbing are becoming standard to counter multi-vector attacks.
- Providers are rapidly expanding cloud scrubbing capacity with multi-terabit bandwidth to handle record-breaking attack volumes.
- Attackers now frequently blend volumetric, protocol, and application-layer vectors, requiring automated and adaptive mitigation.
- AI- and ML-based detection is becoming critical for real-time anomaly identification and reducing false positives.
- Demand is rising sharply from the telecom, BFSI, gaming, ecommerce, and government sectors, which require high service uptime.
- Enterprises are shifting toward always-on cloud mitigation for continuous monitoring and instant attack handling.
- Application-layer and API-focused security capabilities are gaining importance as attackers increasingly target L7 traffic.

- Regulatory mandates in regions like the EU, US, and APAC are accelerating the adoption of DDoS protection solutions.
- MSSPs and telecom operators are bundling DDoS mitigation into connectivity and security offerings to attract SMB and mid-market clients.
- Vendors are pushing sub-second mitigation performance through intelligent traffic profiling and automated routing.

5.3 VALUE CHAIN ANALYSIS

The DDoS protection & mitigation market comprises a range of solution and service providers. The following figure highlights market players' roles in the market.

FIGURE 19 DDoS PROTECTION AND MITIGATION MARKET: VALUE CHAIN ANALYSIS



Source: Secondary Literature and MarketsandMarkets Analysis

5.3.1 TRAFFIC MONITORING & ANALYSIS

This stage involves continuous monitoring and analysis of network traffic to identify abnormal patterns, traffic spikes, protocol anomalies, and potential DDoS activity. Network traffic analyzers establish traffic baselines and examine packet flows, source behavior, and destination patterns to distinguish legitimate traffic from malicious activity. This stage provides the visibility required for timely DDoS detection and enables organizations to initiate appropriate mitigation measures before attacks significantly affect network availability.

5.3.2 DDOS PROTECTION SOLUTIONS

This stage encompasses technologies used to detect, filter, and mitigate DDoS attacks across network, application, API, and DNS environments. Solutions include network traffic analyzers, threat mitigation systems, botnet detection and management, software platforms, hardware appliances, and cloud-based protection. Vendors increasingly incorporate AI/ML, behavioral analytics, automated traffic filtering, rate limiting, and multi-vector mitigation to improve detection accuracy, accelerate response, and maintain service availability during sophisticated attacks.

5.3.3 SYSTEM INTEGRATION & DEPLOYMENT

System integration and deployment involve implementing DDoS protection within customers' existing network, cloud, application, API, and DNS environments. Providers configure protection policies, integrate DDoS platforms with WAF, load balancers, security operations, and network infrastructure, and support hybrid or multi-cloud architectures. Deployment activities also include solution testing, configuration, optimization, and validation to ensure mitigation capabilities operate effectively without disrupting legitimate traffic or critical business applications.

5.3.4 MANAGED SERVICES & DISTRIBUTION

This stage covers the delivery and commercialization of DDoS protection through managed security services, cloud-based scrubbing, DDoS-as-a-Service, consulting, distribution, reselling, and value-added services. Telecommunications operators, managed security providers, distributors, resellers, and VARs extend DDoS capabilities to organizations that may lack specialized internal expertise. Managed services provide continuous monitoring, automated mitigation, incident support, and scalable protection while enabling customers to adopt DDoS security through recurring service-based models.

5.3.5 END USERS

End users represent organizations deploying DDoS protection to maintain availability, business continuity, and resilience across digital infrastructure. Key users include BFSI, government and defense, healthcare, IT & ITeS, telecommunications, manufacturing, energy and utilities, retail and ecommerce, education, and other sectors. Adoption is driven by increasing digital dependency, exposure of Internet-facing infrastructure, cloud and API expansion, growing attack sophistication, and the financial and operational consequences of service disruption.

5.4 ECOSYSTEM ANALYSIS

A DDoS protection and mitigation ecosystem is a complex network of tools, technologies, and services designed to mitigate and prevent DDoS attacks. This ecosystem typically involves multiple layers of defense, each addressing different aspects of the attack. The following figure illustrates the ecosystem of the DDoS protection & mitigation market.

FIGURE 20 DDoS PROTECTION AND MITIGATION MARKET: ECOSYSTEM ANALYSIS



Source: MarketsandMarkets Analysis

TABLE 8 ROLE OF COMPANIES IN ECOSYSTEM

ROLE IN ECOSYSTEM	COMPANY
Solution Provider	Fortinet
	A10 Networks
	Corero
	NSFOCUS
	Seceon
	Xcitium
	FastNetMon
	MazeBolt
	Andrisoft
Service Provider	AT&T
	BT
	Lumen Technologies
	StrataCore
	ActiveReach
Solution & Service Provider	PhoenixNAP
	Akamai
	NETSCOUT
	Radware
	Huawei
	AWS

- Microsoft
- Thales (Imperva)
- Cloudflare
- Link11
- Fastly
- Sucuri (GoDaddy)
- RioRey
- Nexusguard
- Haltdos
- DDoS-Guard
- Indusface
- Gcore
- Qrator Labs
- StormWall
- Cloudbric
- Mlytics
- Allot

Source: MarketsandMarkets Analysis

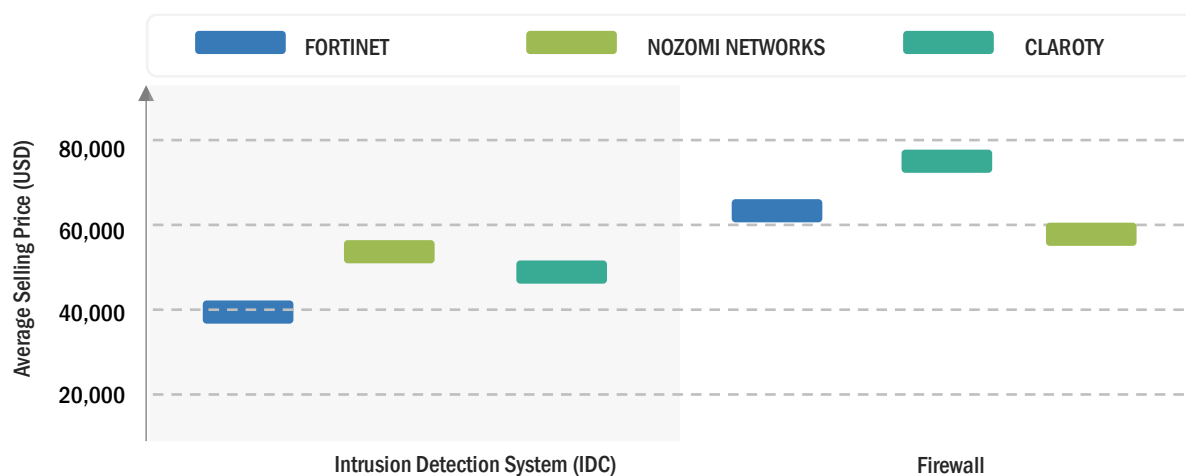
5.5 PRICING ANALYSIS

The pricing of DDoS protection and mitigation can vary depending on the hardware and software being offered. The solutions offered by different vendors in different regions vary according to demand and market trends. The average selling price of DDoS protection and mitigation solutions has been on an upward trend in recent years as organizations recognize the need and impact of these solutions.

5.5.1 AVERAGE SELLING PRICE TREND OF KEY PLAYERS, BY OFFERING, 2025

As shown in the figure below, the pricing for intrusion detection systems and firewalls varies among all vendors. The pricing varies due to changes in features and required specifications from customers or end users.

FIGURE 21 AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2025 (USD)



Source: Company Websites and MarketsandMarkets Analysis

TABLE 9 AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2025

Offering/ Company	Fortinet	Nozomi Networks	Claroity
Intrusion Detection Systems (IDS)	USD 37,500	USD 50,000	USD 45,000
Firewalls	USD 60,000	USD 75,000	USD 55,000

Note: The above pricing is an estimate, and actual pricing can vary depending on specific requirements and negotiations

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

5.5.2 INDICATIVE PRICING ANALYSIS OF DDOS PROTECTION AND MITIGATION, BY OFFERING, 2025

DDoS protection and mitigation solutions are provided to customers on an annual subscription basis. Further, the customizations and add-on integrations can significantly increase the overall cost of the entire system.

TABLE 10 INDICATIVE PRICING ANALYSIS OF DDOS PROTECTION AND MITIGATION, BY OFFERING, 2025

COMPANY	OFFERING	DEPLOYMENT MODE	PRICING MODEL
Akamai	Akamai DDoS Protection	Cloud	For each public IP above 100, there is a USD 29.5/resource/month charge. Total monthly bill for DDoS Standard will be USD 2,944/month + USD 295/resource/month (10 public IPs above 100) = USD 3,238/month.
Radware	Application layer against volumetric attacks & protocol-based DoS attacks	Cloud	▪ <u>Basic</u>- USD 199.99/year ▪ <u>Pro</u>- USD 299.99/year ▪ <u>Business</u>- USD 499.99/year
Cloudflare	Application Services	▪ Cloud ▪ On-premises ▪ Hybrid	▪ <u>Free</u>- for personal or hobby projects that are not business-critical ▪ <u>Pro</u>- for business websites that are not business-critical - USD 20/month ▪ <u>Business</u>- for small businesses operating online - USD 200/month ▪ Enterprise- for mission-critical applications that are core to businesses
Microsoft	Azure DDoS Protection	▪ Cloud	▪ Monthly charge (includes protection for 100 public IP resources) – USD 2,944/month ▪ Overage charges (more than 100 public IP resources) – USD 29.5 per resource per month

Note: The pricing has been given for reference. It is not the final price of the product.

Source: Company Website

5.6 KEY CONFERENCES AND EVENTS

TABLE 11 DDOS PROTECTION AND MITIGATION MARKET: LIST OF KEY CONFERENCES AND EVENTS, 2026–2027

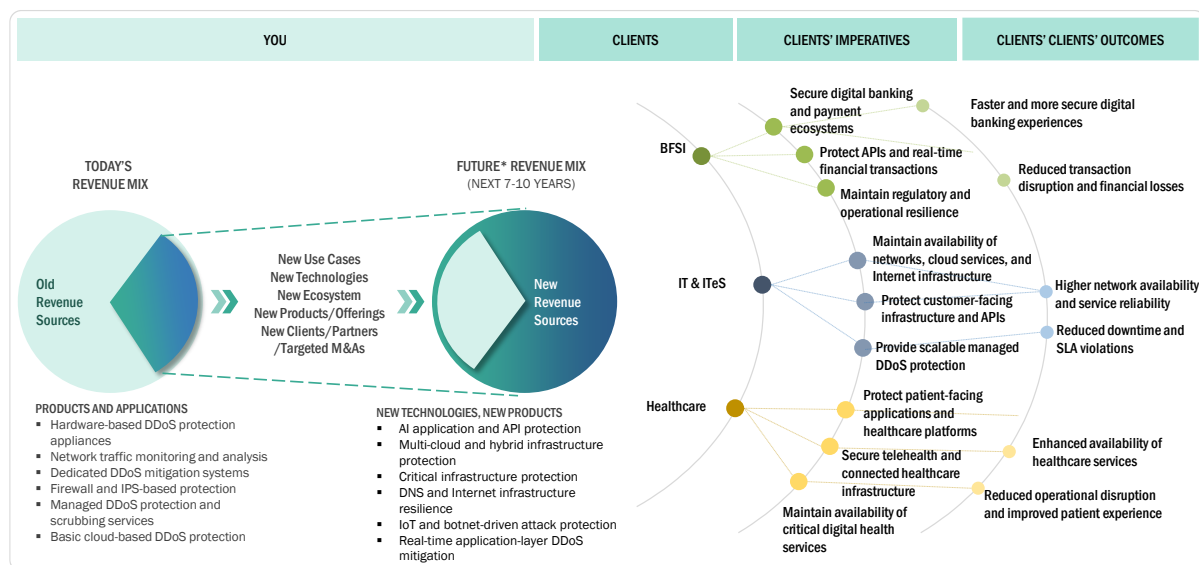
YEAR/QUARTER	NORTH AMERICA	EUROPE	ASIA PACIFIC	REST OF THE WORLD
Q4 '26	-	[December] Black Hat Europe 2026	[October] GovWare 2026	GITEX GLOBAL 2026 [December]
Q1 '27	-	-	Black Hat Asia 2027 [February]	Intersec Global 2027 [January]
Q2 '27	RSA Conference 2027 [April]	Infosecurity Europe 2027 [June]	-	-

Note: Secondary Research and MarketsandMarkets Analysis

5.7 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS

The market is steadily transitioning from legacy, hardware-heavy DDoS protection models toward cloud-delivered, automated, and AI-enhanced security architectures that offer greater scalability, faster response, and broader threat visibility. Enterprises increasingly expect proactive threat intelligence, continuous monitoring, and multi-layered defenses that integrate seamlessly across hybrid environments, prompting leading vendors such as NETSCOUT, Akamai, Nexustguard, Radware, Fortinet, Cloudflare, Huawei, and Microsoft to shift their portfolios toward fully managed, cloud-based, and AI-driven mitigation services. This shift supports customer goals of reducing downtime, improving network resilience, meeting regulatory requirements, and enhancing digital trust, ultimately enabling stronger performance outcomes and higher retention across their own client base.

FIGURE 22 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS

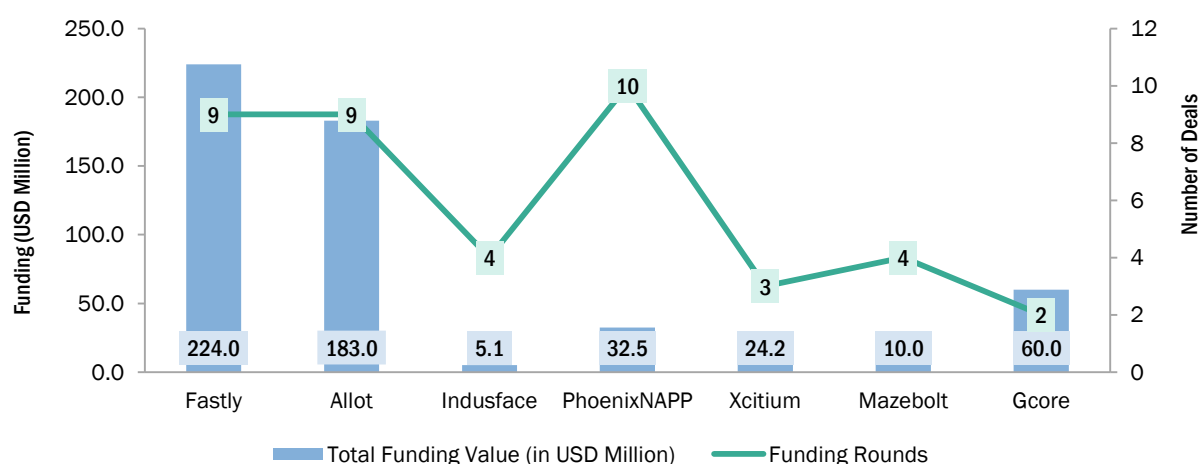


Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

5.8 INVESTMENT AND FUNDING SCENARIO

The investment and funding scenario for the DDoS protection & mitigation market has been driven by the increasing frequency and sophistication of DDoS attacks, the expansion of digital services, and the growing adoption of cloud services. Venture capital and private equity investments have flowed into cybersecurity firms, enabling them to enhance their DDoS mitigation capabilities, with notable players like Cloudflare and Akamai attracting significant funding. Mergers and acquisitions are also common as larger companies seek to integrate DDoS protection into their cybersecurity offerings, evidenced by deals like Akamai's acquisition of Prolexic. Government investments in cybersecurity, especially for critical infrastructure sectors, further bolster the market, while cloud-based DDoS solutions are gaining attention for their scalability and efficiency.

FIGURE 23 INVESTMENT AND FUNDING SCENARIO, 2025



Source: Secondary Research and MarketsandMarkets Analysis

5.9 CASE STUDY ANALYSIS

This section comprises deployment scenarios and case studies from various vendors who deliver comprehensive DDoS protection solutions. DDoS protection and mitigation companies are increasingly gearing up to address the challenges of their clients with innovative solutions.

5.9.1 NEXUSGUARD EMPOWERED IRIX AND SAINS TO OVERCOME DDOS THREATS

CLIENT	SAINS (SARAWAK INFORMATION SYSTEMS)
Vendor	Nexusguard
Overview	SAINS is a leading ICT Systems Integrator and Solutions Provider wholly owned by the Sarawak Government. Faced with increasing DDoS sophistication and the need to migrate critical workloads into a highly reliable environment, the organization sought a managed, scalable DDoS-protection solution that would deliver visibility, operational simplicity, and a service for downstream customers.
Description	SAINS faced an increasingly sophisticated cyber threat landscape that required a more proactive and robust approach to cybersecurity. To ensure uninterrupted service for its customers and bolster its defenses, the organization needed a strategic shift in how it managed cybersecurity and identified long-term resilience solutions.
Solution Offered	Nexusguard deployed its Bastions Hybrid Platform as a fully managed solution for IRIX (SAINS' partner), which combined on-premises and cloud-based mitigation. This platform provided a "Clean Pipe" DDoS protection service featuring multi-tenancy capabilities, individual dashboards, granular

profiling, and detailed monthly reporting. The solution was managed by Nexusguard's experts, handling threat detection and 24/7 monitoring while IRIX's team focused on core operations.

Benefits Gained

The implementation provided SAINS with unparalleled visibility and control over its network while enhancing overall security. Nexusguard's flat-rate pricing eliminated financial risks during attacks, allowing for predictable costs. Additionally, the partner, IRIX, was able to bundle DDoS protection with its internet services without additional technology investments, unlocking new revenue streams and enabling the seamless scaling of cybersecurity services.

Source: Company Website

5.9.2 XTEL COMMUNICATIONS CHOSE NETSCOUT TO IMPROVE VISIBILITY INTO NETWORK TRAFFIC

CLIENT	XTEL COMMUNICATIONS
Vendor	NETSCOUT
Overview	Xtel Communications is widely recognized for its commitment to the telecommunications and carrier needs of government entities, school districts, other carriers, MSPs, and businesses of every size. It provides IT, office applications, and telecommunication services.
Description	The lack of visibility into network traffic and the inability to protect against distributed denial of service (DDoS) attacks were becoming a significant challenge for Xtel's network team.
Solution Offered	NETSCOUT's Arbor Sightline provided comprehensive network visibility and reporting capabilities to help Xtel detect and understand threats, improve traffic engineering, and enhance service performance. It also serves as a platform for managed DDoS protection services, which Xtel offers to its customers. NETSCOUT's Arbor Threat Mitigation System provided a comprehensive suite of countermeasures that effectively removed up to 400 Gbps of DDoS attack traffic while allowing the flow of legitimate traffic – all without interrupting network services.
Benefits Gained	With NETSCOUT's Arbor Sightline and Threat Mitigation System in Xtel's environment, the network operation center can respond to events in less time with greater precision. Targeted attacks are effectively mitigated, relieving Xtel of expensive engineering resources and reducing time to mitigation.

Source: Company Website

5.9.3 PENTELEDATA SELECTED RADWARE'S AMS FOR TECHNICAL INTEGRATION WITH KENTIK TECHNOLOGIES

CLIENT	PENTELEDATA
Vendor	Radware
Overview	PenTeleData required a new solution to protect its infrastructure consistently. It would be able to integrate with DDoS detection from Kentik Technologies, a cloud-based NetFlow analytics solution. PenTeleData also sought to use this new security offering as the foundation for launching a new DDoS mitigation service it could sell to its customers, allowing them to stay operational during a cyber-attack.
Description	PenTeleData is a strategic partnership of cable and telephone companies that serve customers in all facets of life, from their homes to businesses. PenTeleData's legacy solution sometimes resulted in application disruptions, connectivity disruptions, and security threats. It needed a new solution that could protect its internal infrastructure and provide the ability to sell DDoS mitigation as a service to its customers.

Solution Offered	PenTeleData selected Radware's AMS for its pricing, technical integration with Kentik Technologies, and the ability to resell it as a managed service to PenTeleData's customers. AMS is a behavior-based, real-time cybersecurity solution that detects and mitigates emerging network attacks in real-time, including zero-day attacks, DoS/DDoS attacks, and application misuse attacks. AMS does this without human intervention and without blocking legitimate user traffic. Radware's AMS is deployed in two locations: one is internally at PenTeleData's scrubbing center, and a second implementation is with a customer that is leveraging Radware's cloud scrubbing center for volumetric attack mitigation.
Benefits Gained	Deploying Radware's AMS enabled PenTeleData to eliminate half of the maintenance efforts associated with the prior solution. The integration between Radware and Kentik's NetFlow monitoring allowed PenTeleData to trigger mitigation in its scrubbing center for its customers. The new DDoS solution also presented the opportunity for PenTeleData to improve its customers' cybersecurity infrastructure. Customers who required scrubbing capabilities beyond what PenTeleData provides were able to purchase Radware's DDoS cloud protection from PenTeleData, thereby gaining access to Radware's cloud-based scrubbing centers.

Source: Company Website

5.9.4 CNI CHOSE CORERO TO PROTECT ITS CUSTOMERS FROM DDOS ATTACKS

CLIENT	CNI
Vendor	Corero
Overview	CNI needed a proactive, automated approach to protect its customers from DDoS attacks.
Description	CNI's network is targeted by more than 1,000 DDoS attacks per month. The network experiences an attack that lasts approximately 1 to 15 minutes, with some lasting up to 45 minutes or even an hour. The attack volumes range from 200 Mbps to 15 Gbps. Prior to deploying the Corero DDoS mitigation solution, CNI attempted to block DDoS attacks manually; however, this approach proved to be time-consuming, labor-intensive, and ineffective.
Solution Offered	Due to its advantages, such as the way it reviews and scrubs data, as well as the optical bypass option in the event of maintenance or failure, CNI selected Corero's SmartWall solution.
Benefits Gained	Deploying Corero's DDoS protection solution resulted in the following benefits for CNI: - Improved network security by letting CNI provide Dedicated Internet Access (DIA) without worrying about DDoS attacks on its customers - No need to blackhole or null route all traffic to a DDoS target - Negligible false positives impacting legitimate traffic - Maximum levels of service availability are maintained for users, even in the face of a DDoS event - DDoS attacks are automatically mitigated locally at each of their PoPs, avoiding the need to backhaul traffic across the network for mitigation - Increased staff efficiency resulting from the automatic and accurate protection - Increased user satisfaction resulting from the speed and accuracy of protection

Source: Company Website

5.10 DDOS PREVENTION TECHNIQUES

TECHNIQUE	USAGE
Traffic Scrubbing / Clean Pipes	Filters traffic through high-capacity scrubbing centers, removing malicious packets before they reach the network; effective for large volumetric attacks and used by major global mitigation vendors.
Anycast Network Diffusion	Distributes incoming traffic across multiple geographically dispersed servers, preventing overload and improving latency, widely used by global CDN and cloud networks.
Blackholing / Null Routing	Redirects traffic to a null route during extreme attacks to safeguard network infrastructure, though it discards both legitimate and malicious traffic.
Sinkholing	Redirects malicious traffic to controlled servers for monitoring and forensic analysis, enabling insights into botnet behavior and attack vectors.
Rate Limiting / Throttling	Restricts the number of requests an IP or user can send within a set time window, helping mitigate HTTP floods and bot-driven spikes at the application layer.
Web Application Firewall (WAF)	Inspects HTTP/HTTPS requests and blocks malicious patterns using rule sets, bot challenges, and deep packet inspection to stop Layer-7 attacks.
Behavioral & Anomaly-Based Detection	Identifies deviations from normal traffic baselines using analytics or ML to detect evolving or zero-day DDoS vectors and trigger automated mitigation.
Infrastructure Scaling & Load Balancing	Provides additional compute/bandwidth capacity and distributes traffic across multiple servers or regions to absorb high-volume attacks.
IP Masking / Hidden Origin	Hides actual server IPs behind CDNs, proxies, or load balancers to prevent attackers from directly targeting the origin infrastructure.
Proactive Edge Filtering	Blocks malicious traffic at the nearest edge location (PoP) before it enters the core network, reducing congestion and improving overall performance.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

5.11 IMPACT OF 2025 US TARIFF – DDOS PROTECTION AND MITIGATION MARKET

5.11.1 INTRODUCTION

The US tariff environment has evolved considerably since the broad reciprocal tariff measures introduced in April 2025. For the DDoS protection & mitigation market, the direct impact is concentrated on imported hardware solutions, including firewalls, intrusion detection and prevention systems, load balancers, scrubbing appliances, rate-limiting devices, and anti-DDoS gateways. Software/platforms and cloud- or managed-DDoS services are generally less directly exposed because they are delivered digitally or as services rather than physical imports.

In July 2026, the US announced new Section 301 actions covering goods from 60 economies, with a 10% tariff for several economies including India, Canada, Mexico, and the UK; 10% or 12.5% net of MFN for certain products from the EU, Taiwan, Japan, South Korea, and Switzerland; and 12.5% for other investigated economies, subject to specified exemptions. These measures can increase procurement and manufacturing costs for DDoS hardware sourced through affected countries. China remains subject to a 10% additional reciprocal tariff, with the suspension of higher reciprocal rates extended until November 10, 2026.

- Higher hardware procurement costs: Tariffs can increase the landed cost of imported network security appliances and components used in DDoS mitigation infrastructure.
- Supply-chain diversification: Vendors may increasingly diversify manufacturing and sourcing toward the US and lower-tariff jurisdictions to reduce exposure to trade-policy changes.
- Shift toward software and cloud-based protection: Higher costs for physical appliances can strengthen the relative attractiveness of cloud-based DDoS mitigation, SaaS platforms, and managed DDoS services, which require less customer-side hardware.
- Greater regional manufacturing and localization: DDoS vendors and network-security providers may increase local assembly or sourcing to reduce tariff exposure and improve supply-chain resilience.
- Potential impact on service-provider infrastructure: Telecommunications and cloud providers deploying large-scale scrubbing infrastructure may face higher costs for imported networking equipment, although the actual impact depends on the specific HTS classification and country of origin.

5.11.2 KEY TARIFF RATES

TABLE 12 KEY TARIFF RATES

SR. NO.	COUNTRY	KEY DDOS PROTECTION & MITIGATION – RELATED COMPONENTS AFFECTED	ESTIMATED TARIFF (%)	EFFECTIVE DATE	DDOS PROTECTION & MITIGATION IMPACT LEVEL	REMARKS/ CONFIDENCE LEVEL
1	China	Network security appliances, DDoS mitigation hardware, networking equipment, servers, switches, and other physical infrastructure supporting DDoS protection	10% reciprocal + 10% synthetic-opioid duty; additional product-specific Section 301 duties may apply	2025 onward; current framework through Nov. 10, 2026	High	China remains the most exposed sourcing market because multiple additional duties can apply depending on HTS classification. The US currently maintains a 10% reciprocal tariff and a separate 10% synthetic-opioid-related duty; legacy Section 301 duties can also apply to specific products. High confidence
2	European Union	Network security appliances, servers, networking equipment, cloud/data-center infrastructure, and hardware components	10% net of MFN where MFN <10%; otherwise 0% additional Section 301	July 2026 onward	Medium	The July 2026 Section 301 action caps the combined MFN + new Section 301 component at 10% for qualifying EU goods, subject to exemptions. Actual duty depends on the specific HTS

						classification. High confidence
3	Japan & Taiwan	Network appliances, semiconductor components, processors, networking equipment, servers, and cloud infrastructure hardware	Up to 12.5% net of MFN	July 2026 onward	Medium	For Japan and Taiwan, the July 2026 measure provides for a combined MFN + Section 301 rate of 12.5% where the MFN rate is below 12.5%; no additional Section 301 duty applies where MFN is already $\geq 12.5\%$, subject to exemptions. High confidence
4	South Korea	Networking equipment, security appliances, semiconductor components, servers, and data-center infrastructure	Up to 12.5% net of MFN	July 2026 onward	Medium	South Korean products are subject to the same 12.5% net-of-MFN framework as Japan and Switzerland under the July 2026 Section 301 action. The actual duty applicable to a DDoS appliance depends on its HTS classification and existing MFN rate. High confidence
5	India	Servers, networking equipment, security appliances, cloud/data-center hardware, and electronic components	10% additional Section 301	July 2026 onward	Medium	India is explicitly included in the economies subject to a 10% Section 301 tariff under the July 2026 action. This is an additional tariff and does not necessarily represent the total customs duty applicable to a particular DDoS hardware product. High confidence
6	United Kingdom	Networking equipment, security appliances, servers, and cloud infrastructure equipment	10% additional Section 301	July 2026 onward	Low-Medium	The UK is subject to a 10% Section 301 rate under the July 2026 action, with product-specific exemptions. The

						impact on DDoS hardware is therefore dependent on the applicable HTS classification and existing MFN rate. High confidence
7	Israel	Network security hardware, DDoS mitigation appliances, servers, and networking equipment	12.5% additional Section 301	July 2026 onward	Medium	Israel is among the investigated economies receiving the 12.5% Section 301 rate under the July 2026 framework. This is particularly relevant to the DDoS market given the presence of Israeli cybersecurity vendors and technology manufacturing. High confidence
8	Global Average	DDoS hardware, networking equipment, servers, data-center infrastructure, and electronic components	~10–12.5% additional tariff exposure	2026 onward	Medium	The current US framework creates differentiated country-level exposure, with 10% applying to several major sourcing economies and 12.5% applying to many other investigated economies. Actual DDoS hardware duties vary according to HTS classification, MFN rates, exemptions, and other applicable tariff measures. Medium confidence

Note: Tariff rates are based on the latest US tariff measures available as of August 25, 2026. Rates shown represent additional country-specific tariff exposure and should not be interpreted as the total landed duty, which varies by HTSUS classification, MFN duty, applicable Section 301/232 measures, exemptions, and country of origin. The analysis focuses on physical DDoS protection and mitigation hardware; software, cloud-based platforms, and managed services are less directly exposed to import tariffs.

Source: WITS, World Bank, White House Press Release, and Desk Research

5.11.3 PRICE IMPACT ANALYSIS

Recent US tariff adjustments on foreign-made networking hardware, semiconductor components, and telecom-grade infrastructure have indirectly increased the cost of delivering DDoS protection services. Many providers rely on routing hardware, edge appliances, NIC cards, FPGA-based packet processors, and data-center equipment sourced from tariff-affected regions. As suppliers revise hardware prices upward,

DDoS vendors face higher infrastructure, deployment, and maintenance expenses, which can translate into increased subscription rates, especially for hardware-assisted scrubbing, on-prem appliances, and high-throughput mitigation clusters. Cloud-native offerings experience a softer impact but still incur elevated operational costs tied to data-center expansions and network equipment upgrades.

TABLE 13 EXPECTED CHANGE IN PRICES AND LIKELY IMPACT ON END-USE MARKET DUE TO TARIFF IMPACT

END-USE CATEGORY	TARGET SERVICE (PRICE CHANGE)	SERVICE (PRICE INCREASES)	END-USE PRODUCT (PRICE CHANGE)	KEY SERVICE IMPACTED	KEY PLAYER IMPACTED
BFSI	High-capacity scrubbing services (↑5–8%)	Enterprise DDoS mitigation SLAs (↑4–6%)	On-prem mitigation appliances (↑6–10%)	Traffic scrubbing & rate-limiting	Akamai, NETSCOUT
Government	Critical infrastructure protection plans (↑4–7%)	Managed SOC & monitoring (↑3–5%)	Edge security routers/firewalls (↑7–12%)	Real-time threat monitoring	Fortinet, Radware
Healthcare	Cloud-based DDoS filtering (↑3–5%)	API protection bundles (↑2–4%)	Healthcare-grade gateways & network devices (↑5–9%)	API-layer mitigation	Cloudflare, Akamai
Retail & Ecommerce	High-throughput CDN+DDoS plans (↑4–6%)	Bot management add-ons (↑3–5%)	Multi-site edge appliances (↑6–9%)	Multi-vector mitigation	Cloudflare, Radware
Telecom	Backbone DDoS filtering (↑6–9%)	ISP-grade volumetric mitigation (↑5–8%)	Core network hardware (↑8–14%)	Volumetric attack handling	NETSCOUT, Fortinet

Source: Desk Research

Vendors can counter tariff-driven cost pressures by shifting toward software-based mitigation, increasing reliance on cloud-native scrubbing nodes, and optimizing routing to reduce dependency on tariff-affected hardware. Multi-vendor sourcing, long-term component contracts, and regional manufacturing diversification reduce exposure to tariff volatility. Clients can mitigate price increases by adopting usage-based models, leveraging hybrid deployments, and consolidating protection layers (WAF + CDN + DDoS) under unified platforms to lower overall TCO.

5.11.4 IMPACT ON COUNTRY/REGION

The US tariffs on networking hardware, semiconductor components, and telecom infrastructure have raised equipment procurement costs worldwide, pushing up expenses for scrubbing centers, edge appliances, and high-throughput mitigation clusters. While cloud-native DDoS services face a smaller cost shock, regions dependent on imported US or China-origin hardware are experiencing cascading supply-chain price inflation, affecting service pricing, deployment timelines, and data-center modernization efforts.

5.11.4.1 North America

The region experiences moderate price inflation as US tariffs increase hardware acquisition costs for scrubbing centers and on-prem appliances. Cloud-focused providers cushion the impact, but hybrid and ISP-grade deployments face notable cost increases due to reliance on tariff-affected components.

US

The US sees the most direct impact: tariffs increase local manufacturing costs, affecting DDoS appliance procurement, backbone upgrades, and ISP security infrastructure. Providers may pass incremental costs into enterprise mitigation plans.

Canada

Canada faces indirect price rises as it imports tariff-affected US hardware. The telecom and government sectors, which rely on US-made network infrastructure, observe higher deployment and maintenance costs.

Market Challenges:

- Higher hardware procurement costs for scrubbing clusters
- Increased ISP backbone upgrade expenses
- Slower deployment of on-prem mitigation appliances
- Pressures on managed SOC pricing models
- Dependency on US-origin equipment limits flexibility

Mitigation Measures:

- Shift to cloud-native mitigation models
- Adopt multi-vendor sourcing beyond US suppliers
- Extend hardware refresh cycles strategically
- Negotiate long-term fixed-price contracts
- Expand regional scrubbing capacity to reduce hardware load

5.11.4.2 Europe

Europe experiences mixed effects: while local manufacturing softens dependency on US hardware, many telcos and enterprises still rely on US-made networking infrastructure. Tariffs increase import costs indirectly, affecting capital expenditure for DDoS infrastructure upgrades.

Germany

Germany faces increased costs for high-grade routers and firewalls used in industrial and telecom networks, especially in critical infrastructure. Local cloud providers absorb part of the impact, but hardware-centric deployments become more expensive.

France

France sees moderate cost inflation in public-sector and financial networks due to reliance on US-origin security appliances. Cloud-based protection remains less affected.

UK

The UK faces tariff-driven inflation in ISP-level security deployments and hybrid mitigation systems as many hardware vendors route supply chains through US channels.

Market Challenges:

- Rising costs for enterprise-grade routers and scrubbing hardware
- Delays in modernization of national cyber infrastructure
- Increased TCO for hybrid DDoS mitigation deployments

- Budget constraints in public-sector cyber programs
- Pressure on telcos to absorb higher upgrade costs

Mitigation Measures:

- Shift to European-made network infrastructure
- Prioritize software-defined mitigation layers
- Increase reliance on localized cloud scrubbing centers
- Restructure procurement cycles to avoid tariff peaks
- Promote multi-cloud strategies to lower hardware dependency

5.11.4.3 Asia Pacific

The Asia Pacific region experiences both cost escalation and supply chain uncertainty. Economies relying on US networking hardware see price increases, while China faces additional export complexities. Cloud adoption mitigates some of the impact, but telcos and fintech players still feel direct procurement pressure.

China

China faces dual pressure: tariffs limit the export of its hardware to the US and raise the cost of US-made components used by its domestic security vendors. This complicates equipment availability for large-scale DDoS scrubbing.

India

India sees increased hardware import costs for telcos, BFSI, and hyperscalers building new data centers. Mid-size enterprises face higher upfront costs for on-prem security appliances.

Australia

Australia experiences equipment price inflation due to heavy reliance on imported US-grade routers, switches, and mitigation appliances, impacting telecom and government cyber projects.

Market Challenges:

- Higher import costs for US-origin network hardware
- Extended delivery timelines due to supply-chain bottlenecks
- Increased CAPEX for telecom and BFSI security upgrades
- Rising subscription prices for hardware-assisted services
- Limited local manufacturing alternatives

Mitigation Measures:

- Accelerate cloud-first DDoS protection adoption
- Source hardware from non-US suppliers (Japan, South Korea, Taiwan)
- Increase automation to reduce reliance on hardware scaling
- Strengthen hybrid-cloud mitigation to reduce appliance load
- Engage in regional procurement alliances for bulk pricing

5.11.5 IMPACT ON END-USE INDUSTRIES

BFSI:

- Higher procurement costs for high-throughput appliances used in core banking and payment networks
- Increased subscription pricing for enterprise-grade DDoS mitigation SLAs due to more expensive scrubbing hardware
- Rising costs for upgrading ATM network security routers and CDN-based protection layers
- Delays in deploying hybrid mitigation setups across data centers and DR sites
- Elevated operational costs for maintaining 24/7 SOC infrastructure supported by US-imported components
- Larger budget allocations required for bandwidth expansion during mitigation events
- Higher TCO for fraud-prevention and API-security bundles integrated with DDoS tools
- Slower modernization of legacy banking networks due to increased hardware refresh expense

Government:

- Increased cost of upgrading critical public-sector networks reliant on US-made routing and scrubbing appliances
- Budget strain on national CERT and SOC operations due to rising equipment and data-center expenses
- More expensive infrastructure for protecting citizen portals, tax systems, and public-service websites
- Slowdown in deploying new edge security routers in emergency and public-safety communication networks
- Rising integration cost for hardware-based DDoS mitigation used in defense and telecom projects
- Challenges in scaling security infrastructure ahead of elections or large public events
- Greater reliance on cloud-based protection due to costlier on-prem hardware
- Procurement delays in government cybersecurity tenders tied to tariff-affected imports

Healthcare:

- Increased cost of securing EMR, telehealth, and IoMT networks due to higher prices for medical-grade gateways and firewalls
- Higher expenses for deploying on-prem mitigation appliances across hospital networks
- Rising cost for API protection and cloud DDoS plans supporting digital health platforms
- Delays in expanding data-center capacity for healthcare systems due to expensive US-origin hardware
- Elevated operational burden on IT teams as infrastructure refresh becomes costlier
- Increased TCO for securing remote patient-monitoring systems that need resilient edge protection
- Slower adoption of integrated WAF + DDoS bundles due to rising subscription costs

6 TECHNOLOGICAL ADVANCEMENTS, AI-DRIVEN IMPACT, PATENTS, INNOVATIONS, AND FUTURE APPLICATIONS

6.1 TECHNOLOGY ANALYSIS

The technology landscape of the DDoS protection & mitigation market is evolving as organizations adopt advanced capabilities to detect, analyze, and mitigate increasingly sophisticated attacks across network, application, API, and DNS environments. Technologies such as AI and machine learning, behavioral analytics, automated traffic filtering, cloud-based scrubbing, botnet detection, and real-time traffic analysis are becoming increasingly important for improving detection accuracy and reducing response time. Vendors are also integrating DDoS protection with WAF, API security, threat intelligence, SIEM, and SOAR platforms. The shift toward cloud-native, hybrid, and automated architectures is further enabling scalable protection across distributed digital infrastructures.

6.1.1 KEY EMERGING TECHNOLOGIES

6.1.1.1 Traffic filtering

Traffic filtering technology is a crucial component of DDoS protection and mitigation. It works by continuously monitoring incoming traffic, distinguishing between legitimate user requests and malicious traffic generated by attackers. The technology analyzes various factors, such as source IP addresses, protocols, and packet sizes, to identify irregular traffic patterns. Once suspicious traffic is detected, filtering mechanisms block or drop the harmful packets, often employing methods such as IP blocklisting, rate limiting, and deep packet inspection (DPI). Traffic filtering tools can also implement geofencing to block traffic from specific regions. By reducing the volume of malicious traffic and working alongside other security solutions, such as firewalls and web application firewalls (WAFs), traffic filtering ensures system availability and performance during DDoS attacks while constantly adapting to new attack methods to provide ongoing protection.

6.1.1.2 Rate limiting

Rate limiting is a crucial technology used in DDoS protection and mitigation to manage the flow of traffic to a network or service by restricting the number of requests from a single IP address or region within a given time frame. This method helps prevent attackers from overwhelming the system with a flood of requests, a hallmark of a DDoS attack. By controlling traffic rates, rate limiting ensures that legitimate users can still access the service while suspicious or malicious traffic is curtailed. It also aids in detecting abnormal traffic patterns, triggering mitigation measures before the system becomes unresponsive. Additionally, rate limiting conserves critical resources like bandwidth, CPU, and memory, preventing system overload and ensuring continued operation during an attack. This technique often works alongside other security measures, such as traffic filtering and load balancing, to provide a comprehensive defense against DDoS threats.

6.1.1.3 Web application firewall (WAF)

A web application firewall (WAF) plays a critical role in DDoS protection and mitigation by monitoring, filtering, and blocking malicious HTTP traffic directed at web applications. It is particularly effective against application-layer DDoS attacks, which target vulnerabilities in web applications rather than overwhelming the network. WAF analyzes incoming traffic to distinguish between legitimate and harmful requests, helping to prevent attackers from overloading servers. It also offers automated responses, detecting and mitigating DDoS threats in real-time by identifying abnormal traffic patterns. With customizable rules, WAF can block specific attack vectors, enhancing security for individual applications. By integrating WAF with other security tools, such as Intrusion Prevention Systems (IPS) and Content Delivery Networks (CDNs),

organizations can significantly bolster their defenses, ensuring the availability and performance of their web applications during a DDoS attack.

6.1.2 COMPLEMENTARY TECHNOLOGIES

6.1.2.1 Artificial intelligence (AI)

AI technology is increasingly being integrated into DDoS protection and mitigation, enhancing the effectiveness and efficiency of defense mechanisms. By utilizing AI algorithms, organizations can analyze vast amounts of network traffic in real-time to distinguish between normal and malicious patterns. Machine learning models can identify anomalies indicative of DDoS attacks, enabling automated responses that quickly mitigate threats, such as adjusting firewall rules or blocking malicious IP addresses. Additionally, predictive analytics allows systems to leverage historical data to anticipate potential attacks, bolstering defenses proactively. AI also employs behavioral analysis to establish baselines of normal activity, making it easier to detect irregularities. Its scalability enables AI-driven systems to adapt to evolving threats without extensive manual intervention, ultimately reducing operational costs through automation. Furthermore, AI can be integrated with other cybersecurity measures, such as intrusion detection systems (IDS) and security information and event management (SIEM) tools, providing a comprehensive security posture. Overall, the integration of AI in DDoS protection significantly enhances the speed, accuracy, and scalability of defense mechanisms, helping organizations effectively manage and mitigate the risks associated with DDoS attacks.

6.1.2.2 Machine learning (ML)

Machine learning (ML) plays a critical role in DDoS protection and mitigation by enhancing the detection, analysis, and response to attacks in real-time. ML algorithms can analyze normal traffic patterns to identify anomalies indicative of potential DDoS attacks, distinguishing between legitimate spikes in traffic and malicious activities. By classifying incoming traffic, these systems can differentiate between legitimate users and potential attackers, allowing for prioritized responses and efficient resource allocation. Furthermore, ML-based systems can automate responses, dynamically adjusting firewall rules or rate limits to mitigate the impact of ongoing attacks. Through predictive analytics, ML can analyze trends in network traffic and historical attack patterns, helping organizations proactively implement countermeasures. Additionally, ML continuously improves over time by learning from new data, enhancing its ability to detect and respond to evolving attack strategies. By refining detection algorithms, ML significantly reduces false positive rates, ensuring that legitimate traffic is not mistakenly blocked during an attack. Overall, by leveraging machine learning, organizations can enhance their DDoS protection strategies, making them more efficient and effective against increasingly sophisticated threats.

6.1.3 ADJACENT TECHNOLOGIES

6.1.3.1 Load balancers

Load balancers play a crucial role in DDoS protection and mitigation by effectively distributing network traffic across multiple servers, thereby preventing any single server from becoming overwhelmed during an attack. They can identify and filter out malicious traffic patterns commonly associated with DDoS attacks, redirecting or blocking these harmful requests before they reach the targeted servers. Additionally, load balancers enhance scalability by automatically adding more servers to accommodate increased traffic during an attack, thereby minimizing its impact. If a server goes down due to an attack, load balancers ensure availability by redirecting traffic to healthy servers. Some advanced load balancers even offer application-layer DDoS protection by analyzing traffic at the application level and blocking requests that target specific vulnerabilities. Overall, load balancers enhance an organization's resilience against DDoS attacks by distributing and filtering traffic, ensuring resource scalability, and maintaining service availability.

6.1.3.2 Content delivery networks (CDNs)

Content delivery networks (CDNs) are essential in providing DDoS protection and mitigation through their distributed architecture and caching capabilities. By distributing incoming traffic across multiple geographically diverse servers, CDNs help absorb and mitigate the effects of DDoS attacks that typically overwhelm a single point of entry. They employ load-balancing techniques to ensure that no single server is overloaded while also caching static content at edge servers to reduce the load on the origin server. In the event of an attack, CDNs can serve cached content, minimizing impact on the original server. Additionally, features such as rate limiting, IP allowlisting, and blocklisting help control traffic and filter out malicious requests. With real-time monitoring and analytics tools, CDNs enable organizations to detect unusual traffic patterns and respond swiftly to DDoS threats. Many CDN providers offer automatic DDoS mitigation services that detect and respond to attacks without manual intervention, thereby enhancing resilience and ensuring better uptime and availability of services.

6.2 TECHNOLOGY ROADMAP

The DDoS protection and mitigation technology landscape is progressing from conventional, rule-based traffic filtering toward intelligent, automated, and adaptive protection architectures. Increasing attack scale, short attack durations, multi-vector campaigns, and application-layer targeting are accelerating the adoption of real-time analytics, cloud scrubbing, behavioral detection, and automated mitigation. Cloudflare reported mitigating 23.2 million network-layer DDoS attacks in H1 2026, while hyper-volumetric attacks exceeding 1 Tbps increased sharply, reinforcing the need for automated, always-on protection. The roadmap is expected to progress through three stages: foundational cloud and hybrid protection, scaled automation and platform convergence, followed by autonomous and adaptive DDoS defense.

6.2.1 SHORT-TERM (2026–2027) | FOUNDATION & CLOUD-BASED PROTECTION

In the short term, DDoS protection technology will focus on strengthening cloud-based, hybrid, and always-on mitigation architectures while improving real-time traffic visibility. Vendors will expand network traffic analyzers, cloud scrubbing, Anycast routing, rate limiting, DNS protection, and application-layer mitigation to address increasingly diverse attack vectors. Integration of DDoS protection with WAF, API security, bot management, and network security will also increase. The emphasis will remain on reducing detection and mitigation time while providing scalable protection across distributed infrastructure. The need for rapid automated response is particularly important as most attacks are short-lived, leaving limited opportunity for manual intervention.

6.2.2 MID-TERM (2027–2030) | INTELLIGENT AUTOMATION & UNIFIED DDOS PROTECTION

During the mid-term period, DDoS protection is expected to shift toward greater automation, AI-assisted detection, and unified security platforms. Machine learning and behavioral analytics will increasingly identify abnormal traffic patterns, correlate signals across network, application, API, and DNS layers, and automatically initiate mitigation policies. Vendors are likely to integrate DDoS capabilities more deeply with SIEM, SOAR, threat intelligence, WAF, API security, and bot management platforms. Cloud, edge, and hybrid architectures will support distributed mitigation closer to attack sources and protected assets. The growing use of AI by attackers will further accelerate investment in adaptive defenses capable of continuously adjusting detection and mitigation strategies.

6.2.3 LONG-TERM (2030-2035+) | AUTONOMOUS, ADAPTIVE & AI-DRIVEN DDOS DEFENSE

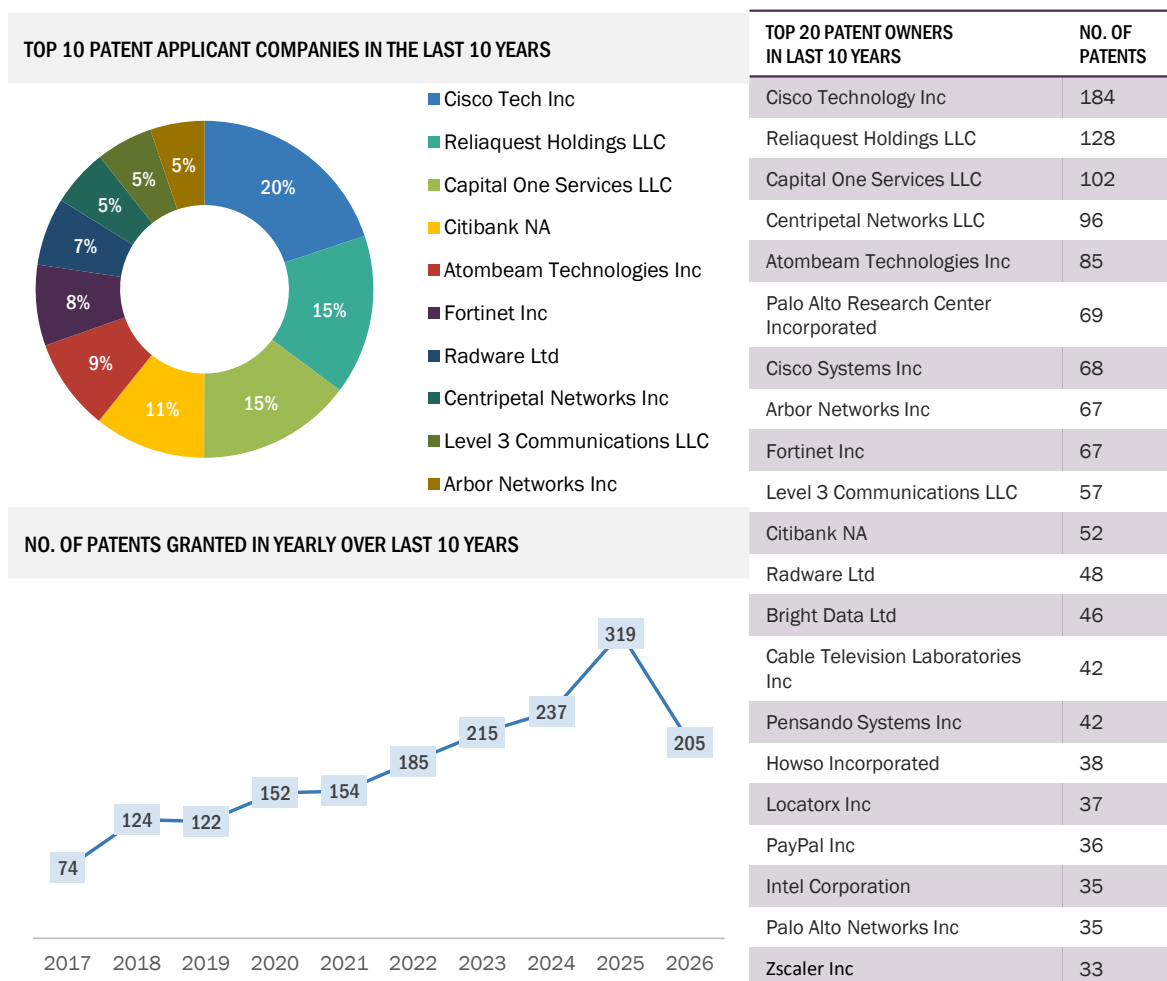
Over the long term, the technology landscape is expected to evolve toward autonomous and adaptive DDoS defense, where AI-driven systems continuously analyze traffic, predict attack behavior, and dynamically modify mitigation strategies with minimal human intervention. Protection will increasingly span network infrastructure, cloud workloads, APIs, applications, DNS, edge environments, and connected devices through unified policy and intelligence layers. Autonomous systems will be capable of correlating multiple attack indicators, identifying emerging attack patterns, and orchestrating mitigation across distributed infrastructure in real time. This evolution will be driven by increasingly adaptive attacks, including AI-assisted and multi-vector campaigns, requiring defensive technologies capable of responding at the same speed as attackers.

6.3 PATENT ANALYSIS

The patent analysis offers crucial insights into patent filings, business interests, and patenting activities, year- and country-wise. It is a technique used to extract information from patents. The patent analysis helps identify and forecast industry trends, including the development of new products and services.

This section discusses the prevailing industry affiliations among stakeholders, including R&D organizations, regulatory bodies, government agencies, dealers, distributors, and cybersecurity manufacturers. It considers new product innovations and applications through an overview of the patents. Over the last decade, the DDoS protection & mitigation market has seen numerous patent filings. Some of the granted and applied patents are listed below.

FIGURE 24 NUMBER OF PATENTS GRANTED FOR DDOS PROTECTION & MITIGATION MARKET, 2017–2026



Note: The data given for 2017–2026 is dated as of August 25, 2026.

Source: Lens.org

TABLE 14 LIST OF TOP PATENTS IN DDOS PROTECTION & MITIGATION MARKET, 2024–2026

APPLICANT	PUBLICATION NUMBER	PUBLISHED YEAR	DESCRIPTION
Tracey Bernath / Inception Security Solutions LLC	US2026 0089189A1	March 2026	The patent describes a stateless proxy-gateway architecture for DDoS mitigation that uses cryptographic hashing and selective packet validation to authenticate traffic and selectively redirect legitimate packets to protected resources.
Salesforce, Inc.	US2026 0006071A1	January 2026	The patent describes an autonomous AI-agent-based system for detecting and mitigating application-layer DDoS attacks, using AI agents to evaluate, review, correct, and execute mitigation plans across shared cloud infrastructure.
Verizon Patent and Licensing Inc.	US2025 0373654A1	December 2025	The patent describes a DDoS detection and remediation method based on energy-consumption patterns, using network, QoS-flow, and network-slice energy thresholds to identify abnormal behavior associated with DDoS attacks in telecommunications environments.

F5, Inc.	US2025 0350632A1	November 2025	The patent describes a hardware-assisted DDoS mitigation technique that generates and validates connection-identification cookies and drops network packets when the validation cookie does not match, enabling efficient stateless packet filtering.
Radware Ltd.	US2025 0220040A1	July 2025	The patent describes a method for detecting encrypted TLS-based DDoS attacks without decrypting traffic, using rate-based and rate-invariant parameters to establish traffic baselines, identify anomalies, and initiate mitigation.
AT&T Intellectual Property I, L.P.	US2025 0097262A1	March 2025	The patent describes a system that correlates DDoS attack profiles with anomalous behavior of compromised IoT devices to identify devices participating in botnets and establish bot-match records for subsequent DDoS attacks.
Level 3 Communications, LLC	US2024 0259403A1	August 2024	The patent describes a DDoS and fraud protection system for SIP-based communications, using traffic analysis and abnormality detection to identify malicious communications traffic and initiate mitigation for VoIP and other SIP-based services.
Individual Applicant	US2024 0259421A1	August 2024	The patent describes a distributed DDoS mitigation system using network nodes, anomaly detection, attack-pattern matching, and AI-based learning to identify traffic anomalies, distinguish legitimate traffic, and continuously update attack patterns.
University of Manitoba / Innotesel Hi-Tech Inc.	US2024 0244072A1	July 2024	The patent describes a network traffic analysis system for detecting DDoS attacks, using traffic preprocessing, feature extraction, and machine-learning-based analysis to identify attack characteristics and support mitigation.
Indian Institute of Technology Delhi	US2024 0223600A1	July 2024	The patent describes a real-time, lightweight DDoS detection and mitigation system for IoT network slices in 5G, combining intrusion detection, honeypots, machine learning, and security-policy enforcement across 5G core network functions.
Tracey Bernath / Inception Security Solutions LLC	US2026 0089189A1	March 2026	The patent describes a stateless proxy-gateway architecture for DDoS mitigation that uses cryptographic hashing and selective packet validation to authenticate traffic and selectively redirect legitimate packets to protected resources.

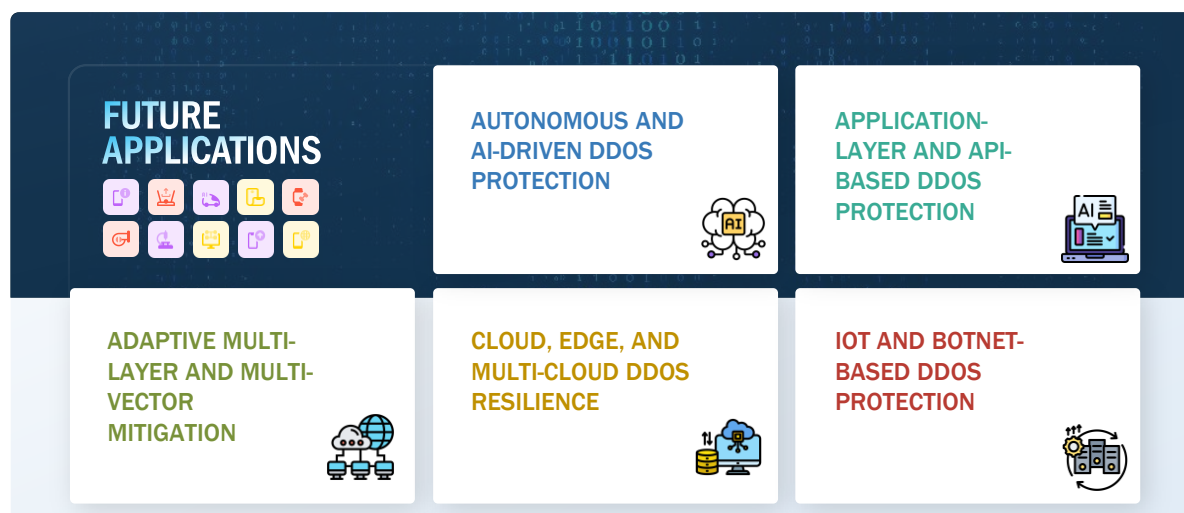
Note: The data given for 2024–2026 is dated as of August 25, 2026.

Source: Lens.org

6.4 FUTURE APPLICATIONS

This comprehensive analysis examines five critical future applications through a standardized framework examining technical breakthroughs, implementation scalability, market impact, and commercial development.

FIGURE 25 FUTURE APPLICATIONS OF DDOS PROTECTION & MITIGATION



Source: Secondary Research and MarketsandMarkets Analysis

6.4.1 AUTONOMOUS AND AI-DRIVEN DDOS PROTECTION

Technical Breakthroughs	AI/ML-based traffic profiling, behavioral anomaly detection, adaptive thresholds, automated mitigation, and real-time traffic analysis are enabling DDoS protection systems to identify abnormal traffic patterns and dynamically respond to attacks. Cloudflare's adaptive DDoS protection, for example, learns customer-specific traffic profiles and uses ML to identify potentially malicious deviations.
Implementation Scalability	Modern DDoS protection is increasingly deployed across cloud, edge, on-premises, hybrid, and multicloud environments, enabling organizations to protect distributed applications and infrastructure through centralized controls. Cloudflare and F5 provide DDoS protection across network and application layers, while supporting distributed deployment architectures.
Market Impact	Autonomous mitigation reduces dependence on manual intervention, shortens detection and response times, and helps maintain application and network availability during high-volume attacks. Cloudflare states that its systems automatically mitigate volumetric and application-layer DDoS attacks, while its network-layer and HTTP protection can detect and mitigate attacks at the edge within seconds.
Commercial Development	Vendors including Akamai, Cloudflare, F5, and Google Cloud are expanding AI/ML-driven DDoS capabilities through adaptive traffic analysis, behavioral detection, automated mitigation, and integrated application security. Akamai combines behavioral DDoS protection with WAF, API security, and bot controls, while Google Cloud Armor uses ML-based Adaptive Protection for Layer 7 DDoS attacks.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.4.2 APPLICATION-LAYER AND API-BASED DDOS PROTECTION

Technical Breakthroughs	Application-aware traffic analysis, behavioral analytics, rate limiting, API discovery, and machine learning are improving the ability to distinguish legitimate application requests from Layer 7 DDoS traffic. Akamai's App & API Protector combines WAF, API protection, bot controls, and advanced DDoS protection, while its Behavioral DDoS Engine adapts to sophisticated volumetric attacks.
Implementation Scalability	Application and API DDoS protection can be deployed in distributed cloud and edge environments, allowing organizations to protect Internet-facing applications, APIs, microservices, and hybrid infrastructures without relying solely on origin-side capacity. Akamai supports protection across on-premises, hybrid cloud, and multi-CDN environments.
Market Impact	Increasing reliance on APIs and Internet-facing applications is expanding the attack surface and increasing demand for application-aware DDoS mitigation. Integrated protection enables organizations to control excessive request rates, protect critical URLs, and mitigate application-layer attacks while preserving legitimate traffic and application availability.
Commercial Development	Vendors including Akamai, Cloudflare, and Fastly are integrating DDoS protection with WAF, API security, bot management, and edge security. Cloudflare provides automated protection against both network- and application-layer DDoS attacks, while its API and bot security capabilities extend protection across application traffic.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.4.3 ADAPTIVE MULTI-LAYER AND MULTI-VECTOR DDOS MITIGATION

Technical Breakthroughs	DDoS protection is evolving toward adaptive systems capable of analyzing multiple attack characteristics across network and application layers. Dynamic mitigation rules, traffic profiling, protocol analysis, rate controls, and behavioral detection enable systems to identify changing attack patterns and apply appropriate countermeasures rather than relying on static signatures.
Implementation Scalability	Multi-layer protection can be deployed across network infrastructure, cloud environments, applications, DNS, and edge locations, providing consistent defense against volumetric, protocol, and application-layer attacks. Cloudflare, for example, protects Layers 3/4 and Layer 7 through its autonomous DDoS systems.
Market Impact	The increasing use of multi-vector attacks is driving organizations away from single-layer protection toward coordinated defense architectures. Integrated mitigation helps organizations address simultaneous network floods, DNS attacks, TCP attacks, and application-layer traffic anomalies while reducing the risk of overblocking legitimate users.
Commercial Development	Cloudflare, NETSCOUT, Akamai, and Radware are strengthening multi-layer DDoS capabilities through adaptive traffic analysis, network intelligence, application protection, and automated mitigation. NETSCOUT combines global threat intelligence with packet-level visibility and transparent automated mitigation across enterprise and service-provider environments.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.4.4 CLOUD, EDGE AND MULTI-CLOUD DDOS RESILIENCE

Technical Breakthroughs	Cloud and edge architectures enable DDoS traffic to be identified and mitigated closer to attack sources before it reaches protected infrastructure. Distributed scrubbing, Anycast routing, edge-based filtering, traffic profiling, and automated mitigation provide scalable protection without requiring organizations to maintain equivalent on-premises capacity.
Implementation Scalability	Cloud-based DDoS protection can scale dynamically across distributed workloads and support on-premises, public cloud, hybrid, and multi-cloud environments. NETSCOUT provides hybrid protection spanning on-premises, colocation, and public cloud applications, while Akamai supports cloud, on-premises, and hybrid DDoS protection.

Market Impact	Increasing cloud adoption and distributed application architectures are creating demand for protection that follows workloads across multiple environments. Cloud and edge mitigation reduces dependence on local infrastructure capacity and enables organizations to maintain availability during attacks that exceed the capacity of individual networks or data centers.
Commercial Development	Akamai, Cloudflare, NETSCOUT, AWS, and Radware are expanding cloud-based and distributed DDoS protection capabilities. Cloudflare provides automated mitigation at the network edge, while Akamai offers dedicated DDoS protection across cloud, on-premises, and hybrid environments.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.4.5 IOT AND BOTNET-BASED DDOS PROTECTION

Technical Breakthroughs	DDoS protection is increasingly incorporating device behavior analysis, botnet intelligence, traffic profiling, and automated source identification to detect compromised IoT devices participating in distributed attacks. These capabilities enable providers to identify malicious outbound traffic and compromised devices before they contribute to larger DDoS campaigns.
Implementation Scalability	IoT-focused protection can be implemented across telecommunications and broadband networks, allowing service providers to monitor large populations of connected devices and identify compromised endpoints at network scale. NETSCOUT recently expanded its Adaptive DDoS Protection to automatically detect and mitigate outbound DDoS traffic generated by compromised subscriber devices.
Market Impact	The proliferation of connected cameras, routers, broadband devices, and other IoT endpoints is expanding the infrastructure available for botnet-based attacks. This is creating demand for DDoS solutions capable of protecting both attack targets and networks from compromised devices generating malicious outbound traffic.
Commercial Development	NETSCOUT is expanding this area through Adaptive DDoS Protection for service providers, enabling automated detection and mitigation of outbound DDoS traffic from compromised broadband and IoT devices. Its approach combines network-wide intelligence, local traffic evidence, and automated mitigation to reduce disruption and Internet-wide attack risk.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.5 IMPACT OF AI/GEN AI ON DDOS PROTECTION AND MITIGATION MARKET

Generative AI (GenAI) is fundamentally reshaping the defense layer of the DDoS market by enabling more accurate, real-time traffic intelligence and automated mitigation workflows. Modern mitigation engines now use GenAI-driven behavior modeling to distinguish between legitimate surges (such as retail flash sales or streaming events) and sophisticated bot-driven anomalies. Vendors like Cloudflare, Akamai, Nexusguard, Radware, and Fortinet are integrating GenAI into their inspection pipelines to auto-generate mitigation rules, predict attack escalation patterns, and reduce analyst intervention time from minutes to seconds. GenAI also enhances deep-packet behavioral context by learning subtle L7 interaction patterns, helping detect advanced threats such as HTTP/2 Rapid Reset or adaptive bot frameworks that mimic human browsing behavior. This significantly lowers false positives and improves the quality of automated responses, making always-on, AI-orchestrated protection a core buying criterion for enterprises.

At the same time, GenAI is dramatically evolving the threat landscape, prompting enterprises to adopt higher-capacity and intelligence-driven mitigation solutions. Attackers are now using AI to optimize botnet behavior, generate traffic that mimics real user fingerprints, rotate identities faster, and automatically identify weak CDN endpoints or misconfigured APIs. AI-generated botnets can execute coordinated multi-vector attacks that adapt in real-time to mitigation rules, forcing vendors to develop more resilient, learning-based systems. This rise in AI-enhanced attacks is accelerating market demand for cloud-based, high-bandwidth scrubbing, AI-first anomaly engines, and predictive mitigation. As a result, GenAI is not only

improving vendor capabilities but also expanding overall market necessity, pushing DDoS mitigation from a preventive tool to a mission-critical, intelligence-driven security layer for all digital enterprises.

TABLE 15 TOP USE CASES AND MARKET POTENTIAL

TOP USE CASES	MARKET POTENTIAL
Generative AI-Assisted DDoS Detection & Threat Analysis	Growing use of GenAI can help security teams analyze large volumes of traffic and security telemetry, summarize attack patterns, identify anomalies, and accelerate DDoS investigation. This can improve analyst productivity as attack campaigns become increasingly complex and multi-vector.
AI-Generated Attack Simulation & DDoS Testing	GenAI can support automated generation of diverse attack scenarios, traffic patterns, and attack simulations for testing DDoS defenses. This creates opportunities for continuous validation of mitigation policies and helps organizations identify weaknesses before real attacks occur.
GenAI-Powered Adaptive Mitigation & Response	GenAI can assist in translating detected attack characteristics into mitigation recommendations, including traffic filtering, rate limiting, routing changes, and policy adjustments. Combined with existing autonomous mitigation engines, this can reduce manual intervention and accelerate response to rapidly changing attacks. Cloudflare already uses autonomous systems to automatically detect and mitigate DDoS attacks across Layers 3/4 and 7.
Generative AI Application & API Protection	The expansion of generative AI applications creates a new category of high-value, resource-intensive Internet-facing workloads. Attackers can generate high-volume requests designed to exhaust AI inference resources, making DDoS protection increasingly important for AI services. AWS recommends DDoS protection, rate limiting, and traffic filtering for generative AI applications to maintain availability and control resource consumption.
GenAI-Enhanced Multi-Vector Attack Correlation	GenAI can correlate network, application, API, DNS, and behavioral signals to provide a unified view of multi-vector attacks and help security teams understand how attack patterns evolve. This can complement existing AI/ML-based detection and automated mitigation capabilities, particularly as attackers increasingly combine volumetric and application-layer techniques. Radware, for example, uses AI-powered behavioral algorithms and dynamic signatures to detect and mitigate sophisticated L7 DDoS attacks.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

6.5.1 BEST PRACTICES IN DDOS PROTECTION & MITIGATION MARKET

TABLE 16 BEST PRACTICES: COMPANIES IMPLEMENTING USE CASES

OEM	USE CASE	VALUE CHAIN
Cloudflare	Automated, always-on DDoS protection across network and application layers, with dynamic rules, adaptive protection, WAF, rate limiting, and edge-based mitigation to maintain application and infrastructure availability	Network Traffic Analysis, Threat Mitigation, Application & API Protection
Akamai	Multi-layer DDoS protection combining behavioral detection, cloud-based mitigation, application and API protection, and DNS security across on-premises, cloud, and hybrid environments	Threat Mitigation, Application & API Protection, DNS Protection
NETSCOUT	Intelligent DDoS detection and automated mitigation using network-wide visibility, packet-level evidence, and adaptive protection across enterprise and service-provider environments. Its solutions support network-edge protection and automated mitigation while enabling providers to offer DDoS services to customers	Network Traffic Analysis, Threat Mitigation, Managed DDoS Services

Radware	Hybrid DDoS protection combining cloud and on-premises mitigation to help data-center and cloud providers protect customer environments, with integrated DDoS and WAF capabilities	Threat Mitigation, Application Security, Managed DDoS Services
Corero	Automated DDoS detection and mitigation designed for real-time protection of network infrastructure, enabling service providers and enterprises to mitigate attacks while minimizing operational intervention	Network Traffic Analysis, Threat Mitigation, Managed DDoS Services

Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

6.5.2 CASE STUDIES OF AI IMPLEMENTATION IN DDOS PROTECTION & MITIGATION MARKET

TABLE 17 DDOS PROTECTION & MITIGATION MARKET: CASE STUDIES RELATED TO GEN AI IMPLEMENTATION

CASE STUDY	DETAILS
Cloudflare strengthens autonomous DDoS mitigation using AI and adaptive protection	Cloudflare uses autonomous DDoS systems to automatically detect and mitigate attacks across Layers 3/4 and 7. Its Adaptive DDoS Protection learns customer-specific traffic patterns and uses ML models to identify anomalous traffic, enabling dynamic mitigation without requiring manual intervention.
NETSCOUT applies AI-driven intelligence for adaptive DDoS protection	NETSCOUT combines AI-driven ATLAS Intelligence Feed with Adaptive DDoS Protection to detect evolving attack patterns and dynamically adjust mitigation. Its hybrid architecture combines on-premises Arbor Edge Defense with cloud-scale Arbor Cloud mitigation for multi-vector attacks.
NETSCOUT extends AI-driven DDoS protection to IoT and broadband networks	NETSCOUT is applying adaptive DDoS protection to outbound traffic from compromised broadband and IoT devices. The approach uses network-wide visibility, AI-driven intelligence, and automated mitigation to identify weaponized devices and reduce their contribution to DDoS campaigns.
Akamai applies behavioral analytics to sophisticated DDoS attacks	Akamai combines behavioral DDoS defense with dedicated cloud infrastructure to protect applications, DNS, and Internet-facing systems. Its approach uses traffic behavior and adaptive detection to mitigate sophisticated attacks while maintaining legitimate traffic and service availability.
Radware uses AI-enabled behavioral analysis for DDoS detection	Radware uses behavioral-based detection algorithms to identify deviations in traffic patterns and automatically generate defense signatures for mitigation. The technology is designed to address sophisticated attack vectors, including encrypted attacks, burst attacks, dynamic IP attacks, and IoT botnets.

Source: Press Releases, Company Websites, and MarketsandMarkets Analysis

6.5.3 INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS

TABLE 18 INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS

ECOSYSTEM	INTEGRATION	IMPACT
Network Security & Infrastructure Platforms	Integrates DDoS detection and mitigation with firewalls, IPS, routers, load balancers, traffic analysis, and network-edge controls to identify and block malicious traffic before it reaches critical infrastructure.	Strengthens network resilience, reduces attack traffic reaching core infrastructure, and enables coordinated protection across network and DDoS security layers. Cisco, for example, integrates DDoS detection and mitigation directly into supported network-edge routers.
Web Application & API Security Platforms	Combines DDoS protection with WAF, API security, bot management, rate limiting, and application-layer traffic analysis to protect websites, applications, and APIs from sophisticated Layer 7 attacks.	Expands protection beyond volumetric attacks, improves application availability, and enables vendors to offer integrated application and DDoS security. Akamai and Cloudflare integrate DDoS protection with WAF, API, and bot-security capabilities.
DNS Security & Domain Infrastructure	Integrates DDoS mitigation with DNS security, DNS traffic analysis, filtering, and resilient DNS infrastructure to identify and mitigate DNS floods and attacks targeting domain-resolution services.	Improves availability of critical Internet services and reduces exposure to DNS-based DDoS attacks. Cloudflare and other edge-security providers integrate DNS capabilities with broader DDoS protection architectures.
Cloud, Edge & Multi-Cloud Platforms	Combines DDoS protection with cloud infrastructure, edge networks, load balancing, distributed scrubbing, and multi-cloud security to protect workloads across distributed environments.	Enables scalable protection against high-volume attacks while reducing dependence on on-premises mitigation capacity. Cloudflare, Google Cloud, and Oracle provide DDoS protection through globally distributed cloud and edge infrastructure.
Security Operations Platforms (SIEM, SOAR & Threat Intelligence)	Integrates DDoS alerts, attack telemetry, threat intelligence, and mitigation events with SIEM and SOAR platforms to correlate attacks with broader security incidents and automate response workflows.	Improves attack investigation and response coordination, strengthens enterprise-wide security visibility, and enables automated orchestration of DDoS mitigation alongside other cybersecurity controls.

Source: Press Releases, Investor Presentations, Journals, Interviews with Experts, and MarketsandMarkets Analysis

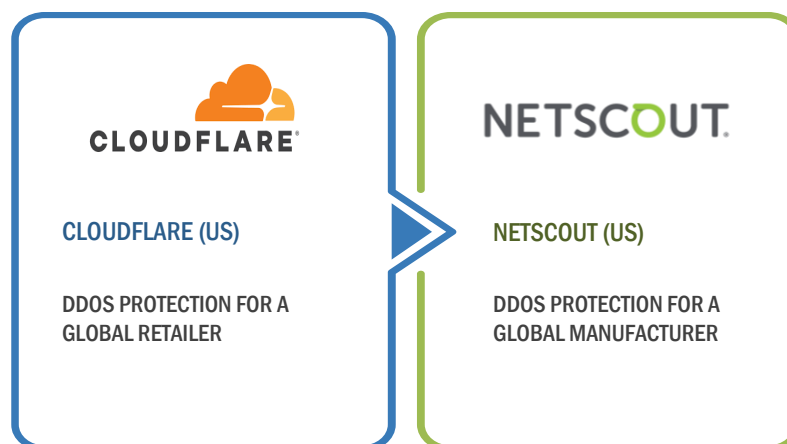
6.5.4 CLIENTS' READINESS TO ADOPT GENERATIVE AI IN DDOS PROTECTION & MITIGATION MARKET

Organizations across BFSI, telecommunications, IT & ITeS, healthcare, government, retail, manufacturing, energy, and cloud services are increasingly evaluating Artificial Intelligence (AI) and Generative AI (GenAI) for DDoS protection and mitigation. Early adoption is focused on AI-assisted traffic analysis, attack investigation, anomaly detection, mitigation recommendations, threat intelligence, and automated security operations. DDoS protection vendors are increasingly incorporating AI and machine learning to analyze large-scale traffic patterns, identify evolving attack signatures, and accelerate mitigation decisions. These capabilities can help organizations reduce detection and response times, improve mitigation accuracy, minimize false positives, and maintain service availability during sophisticated attacks.

Client readiness is being driven by the growing frequency, scale, and complexity of DDoS attacks, particularly against cloud applications, APIs, DNS infrastructure, and distributed digital services. Organizations are prioritizing intelligent DDoS solutions that integrate with WAF, API security, SIEM, SOAR, threat intelligence, cloud platforms, and network infrastructure. GenAI is also creating opportunities for security analysts to summarize incidents, investigate attack campaigns, generate mitigation

recommendations, and support security operations. As cloud-native architectures, automated mitigation, and AI-enabled security platforms mature, enterprises and service providers are expected to increasingly adopt GenAI-assisted DDoS protection as a complement to established ML-based detection and automated mitigation technologies.

6.6 SUCCESS STORIES AND REAL-WORLD APPLICATIONS



6.6.1 CLOUDFLARE: DDOS PROTECTION FOR A GLOBAL RETAILER

A global retail company, AllSaints, adopted Cloudflare to strengthen website availability and security against traffic surges and DDoS attacks across its localized ecommerce platforms. Cloudflare's DDoS Protection, DNS, WAF, and CDN enabled AllSaints to prevent attackers from overwhelming its systems while protecting public-facing applications. The company reported zero website outages since partnering with Cloudflare, including during DDoS attacks, along with reduced downtime and improved performance. The implementation also supported PCI DSS and GDPR requirements while improving customer confidence in the security and availability of its digital commerce platform.

6.6.2 NETSCOUT: DDOS PROTECTION FOR A GLOBAL MANUFACTURER

A global equipment manufacturer deployed NETSCOUT's Arbor Edge Defense 2800, together with its nGeniusONE Service Assurance platform and InfiniStreamNG appliances, to strengthen DDoS protection following data-center ISP upgrades and the rapid transition of thousands of employees to remote work. The solution provided visibility into network performance and DDoS threats while protecting the manufacturer's data-center environment. NETSCOUT reports that the implementation helped the organization maintain network availability and deliver a consistent end-user experience for employees across its global operations.

7 REGULATORY LANDSCAPE

7.1 REGULATORY LANDSCAPE

Regulatory bodies play a key role in the DDoS protection & mitigation market by setting security standards, enforcing compliance, and driving cybersecurity efforts. While these regulations can pose challenges for vendors, such as compliance costs and adapting to diverse regional rules, they also create significant opportunities. Vendors offering regulation-compliant solutions are in high demand, and aligning products with these standards can provide a competitive edge. Additionally, regulations encourage innovation, helping vendors develop advanced solutions and form strategic partnerships in the growing, regulated market.

7.1.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

This section includes a region-wise list of key regulatory bodies, government agencies, industry associations, and non-profit organizations relevant to the market.

TABLE 19 NORTH AMERICA: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
US	National Institute of Standards and Technology (NIST)	Government Body	NIST develops cybersecurity standards and resources for the US industry and federal agencies, guided by statutes and stakeholder input. It addresses emerging challenges, including privacy risks, focusing on cryptography, workforce, emerging tech, risk, identity, privacy, and trustworthy systems.
US	Cybersecurity and Infrastructure Security Agency (CISA)	Government Body	CISA, under the US Department of Homeland Security (DHS), strengthens critical-infrastructure cybersecurity and resilience by providing guidance to mitigate DDoS attacks and protect internet-facing services.
Canada	Canadian Centre for Cyber Security	Government Body	The Canadian Centre for Cyber Security (CCCS) is Canada's authority on cybersecurity. It is part of the Communications Security Establishment (CSE) and is responsible for leading the government's response to cybersecurity events. The CCCS offers expert guidance, services, and support to the Canadian public, industry, and governments on cybersecurity.
Canada	Communications Security Establishment (CSE)	Government Agency	The Communications Security Establishment (CSE) is a Canadian government agency that provides guidance, services, and support on cybersecurity. The CSE's Cyber Centre is a unified source of expert advice and support on cybersecurity for Canadians. The Cyber Centre also defends the Government of Canada's networks and protects the country's federal elections infrastructure from cyber activity.
US	Federal Communications Commission (FCC)	Government Agency	It is an independent US government agency, overseen by Congress, that regulates interstate and international communications. The Federal Communications Commission focuses on promoting broadband innovation, ensuring competitive frameworks, optimizing spectrum use, adapting

			media regulations for technological evolution, and enhancing national communication infrastructure defense.
US	Cloud Security Alliance (CSA)	Cloud Security Association	The Cloud Security Alliance (CSA) stands as the global authority on establishing and promoting best practices for secure cloud computing environments. Leveraging industry expertise, CSA offers research, education, certification, and events, fostering collaboration across stakeholders to ensure a trusted cloud ecosystem.
US	SANS Institute	Cybersecurity Training Association	Established in 1989, the SANS Institute is dedicated to advancing information security thought leadership. Through comprehensive training, certifications, academies, and resources, SANS empowers cybersecurity professionals worldwide, fostering a safer digital environment.

Source: Secondary Research and MarketsandMarkets Analysis

TABLE 20 EUROPE: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
EU	European Union Agency for Cybersecurity (ENISA)	Government Body	ENISA is an agency that aims to achieve a high level of cybersecurity across Europe. It was established by Regulation (EC) No 460/2004, 53 and has offices in Athens, Greece; Brussels, Belgium; and Heraklion, Greece.
UK	National Cyber Security Centre (NCSC)	Government Body	The National Cyber Security Centre (NCSC) is a governmental body in the UK dedicated to safeguarding critical services from cyber threats. It actively enhances the nation's internet security and effectively manages significant cyber incidents.
Germany	Federal Ministry of the Interior and Community (BMI)	Government Body	The German Federal Ministry of the Interior and Community (BMI) oversees IT security in collaboration with the Federal Office for Information Security (BSI). With a primary focus on safeguarding internal security and citizens, BMI manages diverse responsibilities, including civil service, emergency aid, state visits, security protocols, integration efforts, and sports funding.
Germany	Federal Office for Information Security (BSI)	Government Agency	The Federal Office for Information Security (BSI) is a government agency that manages the country's computer and communication security. The BSI's objective is to promote information and cybersecurity to help society securely use communication technology and information.
France	National Agency for the Security of Information Systems (ANSSI)	Government Agency	Established in 2009 by the French government, the National Agency for the Security of Information Systems (ANSSI) serves as France's primary cybersecurity agency. ANSSI's mandate includes safeguarding the nation from cyber threats, enhancing the security of French networks, and protecting citizens' and businesses' data.
Italy	National Cybersecurity Agency (ACN)	Government Agency	The National Cybersecurity Agency (ACN) is an Italian governmental entity formed in 2021 with the mandate to safeguard the nation's cyberspace. ACN is committed to protecting Italy's cybersecurity interests and ensuring the security of national digital assets.

Germany	TeleTrust	IT Security Association	TeleTrust, also known as the IT Security Association Germany, is a non-profit organization established in 1989 and headquartered in Berlin. It serves as a hub for IT security expertise, fostering collaboration among various stakeholders. TeleTrust's network encompasses members and partner organizations from industry, administration, consultancy, and research, as well as national and international entities.
Italy	Assintel	ICT & Cybersecurity Industry Association	Assintel (Associazione Nazionale Imprese ICT) serves as a cybersecurity think tank in Italy, acting as a collaborative hub where companies and professionals unite to tackle the challenges in the realm of cybersecurity.
Italy	CLUSIT	Information Security Association	CLUSIT, the Italian Association for Information Security, is a non-profit organization committed to advancing all facets of information security. Its mission encompasses raising awareness among IT specialists and the public, advising the government, and advocating for issues pertinent to information security. CLUSIT's membership includes security customer companies, security providers, security professionals, and individuals with an interest in the field.

Source: Secondary Research and MarketsandMarkets Analysis

TABLE 21 ASIA PACIFIC: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
China	Ministry of Industry and Information Technology (MIIT)	Government Body	The Ministry of Industry and Information Technology (MIIT) of China is responsible for regulating and managing the country's IT, telecommunications, and software sectors. The MIIT is also responsible for developing policies, standards, and industrial plans to promote innovation and communications technology.
Japan	National Center of Incident Response & Security Coordination (NISC)	Government Body	Established in 2015 as part of the Cybersecurity Strategy Headquarters, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) is a Japanese governmental organization. It plays a pivotal role in setting cybersecurity standards for government agencies and collaborates with the public and private sectors on initiatives to ensure a "free, fair, and secure cyberspace" in Japan.
India	Ministry of Electronics and Information Technology (MeitY)	Government Agency	Established in 2008, the Ministry of Electronics and Information Technology (MeitY) is a key Indian government body fostering the development of the electronics and IT industry. MeitY actively promotes cybersecurity through various initiatives, enhancing the nation's defense capabilities.
India	CERT-In	Government Agency	CERT-In, operational since January 2004, serves India's cyber community as the national agency for responding to cybersecurity incidents. Designated by the Information Technology Amendment Act 2008, it collects, analyzes, and disseminates cyber incident information, issues alerts, coordinates response activities, and provides guidance.
Australia	Australian Signals	Government Agency	The Australian Signals Directorate (ASD) is an intelligence agency that provides cybersecurity, intelligence, and offensive

	Directorate (ASD)		operations to the Australian Government and the Australian Defence Forces. The ASD's purpose is to protect Australia from global threats and advance the country's national interests.
China	Cyberspace Administration (CAC)	Government Agency	The CAC, also known as the State Internet Information Office (SIIO), oversees cyberspace security and internet content regulation. Its key roles include directing, coordinating, and supervising online content management, as well as administering licenses for internet news reporting and financial information services. It also functions as the enforcement agency for the internet content provision sector, taking over certain responsibilities from SCIO in April 2014.
Australia	Cyber Security Cooperative Research Centre (CSCRC)	Cybersecurity Association	The Cyber Security Cooperative Research Centre (CSCRC) aims to strengthen Australia's cybersecurity capabilities. The CSCRC is a collaborative center that works with industry, government, and research partners to create new products, services, and systems. The CSCRC also aims to train the next generation of cybersecurity professionals.
Australia	Australian Information Security Association (AISA)	Cybersecurity Association	The Australian Information Security Association (AISA) is a non-profit professional membership organization and a leading industry body in Australia. Dedicated to advancing cybersecurity, AISA's mission is to enhance the safety and security of the Australian public.

Source: Secondary Research and MarketsandMarkets Analysis

TABLE 22 REST OF THE WORLD: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS

COUNTRY	ORGANIZATION NAME	ORGANIZATION TYPE	SHORT DESCRIPTION
UAE	Signals Intelligence Agency	Government Body	The Signals Intelligence Agency (SIA), formerly known as the National Electronic Security Authority (NESA), is a government body in the United Arab Emirates (UAE) that protects the country's critical information infrastructure and improves cybersecurity.
Qatar	Communications Regulatory Authority (CRA)	Government Body	Established by Emiri Decree 42 of 2014, the Communications Regulatory Authority (CRA) serves as Qatar's communications regulator. It oversees telecommunications, information technology, postal services, and digital media access, fostering an open and competitive ICT sector for advanced, innovative, and reliable communication services.
Brazil	National Telecommunications Agency (Anatel)	Government Body	The National Telecommunications Agency (Anatel) is a regulatory and supervisory body in Brazil that regulates telecommunications equipment. Established in 1997, Anatel is responsible for approving telecommunications products that meet quality and safety standards.
Mexico	Federal Telecommunications Institute	Government Agency	The Federal Telecommunications Institute, an autonomous entity, regulates and promotes telecommunications and broadcasting in Mexico. Its responsibilities include overseeing the radio spectrum, orbital resources, satellite services, networks, broadcasting, and ensuring access to infrastructure.

KSA	National Cybersecurity Authority (NCA)	Government Agency	The NCA holds dual roles in cybersecurity, encompassing both regulatory and operational functions. Collaborating with public and private entities, it endeavors to enhance the nation's cybersecurity framework to protect vital interests, national security, critical infrastructure, key sectors, and governmental operations, aligning with Vision 2030.
Colombia	Communications Regulatory Commission (CRC)	Government Agency	The CRC, an autonomous regulatory agency, oversees various sectors, including telecommunications, broadcasting, postal services, and the Internet. Its mandate is to uphold competition, supervise network provisions, and safeguard public interests.
Oman	ITU Arab Regional Cyber Security Center (ITU-ARCC)	Cybersecurity Coordination Association	Established in December 2012, the ITU Arab Regional Cyber Security Center (ITU-ARCC), founded by the ITU and Oman's Ministry of Transport, aims to foster a secure cybersecurity environment in the Arab Region. Since its launch in March 2013, it has served as the ITU's regional cybersecurity hub, hosted and operated by Oman National CERT.

Source: Secondary Research and MarketsandMarkets Analysis

7.1.2 INDUSTRY STANDARDS

Global standardization in the DDoS protection & mitigation market is essential to ensure consistent security practices, interoperability, resilience, and effective mitigation across increasingly distributed digital infrastructures. Organizations rely on frameworks and standards from bodies such as ISO, NIST, IETF, ETSI, and ENISA, including ISO/IEC 27001, NIST Cybersecurity Framework, NIST DDoS guidance, and relevant network-security and telecommunications standards. These frameworks support organizations in implementing traffic monitoring, anomaly detection, incident response, network resilience, access controls, and business continuity measures. Standardized practices help enterprises, cloud providers, telecommunications operators, and governments strengthen DDoS preparedness, improve interoperability across security platforms, reduce service disruptions, and enhance compliance and operational resilience as attacks increasingly target cloud, network, application, API, and DNS infrastructure.

TABLE 23 GLOBAL INDUSTRY STANDARDS IN DDOS PROTECTION & MITIGATION MARKET

STANDARD/GUIDELINE	ISSUING BODY	DESCRIPTION
ISO/IEC 27001:2022	ISO/IEC	Establishes requirements for an Information Security Management System (ISMS), supporting risk management, protection of information assets, and organizational cyber resilience. Its availability and risk-management principles provide a foundation for DDoS preparedness and protection.
NIST Cybersecurity Framework (CSF) 2.0	NIST (US)	Provides a cybersecurity risk-management framework covering Govern, Identify, Protect, Detect, Respond, and Recover functions. Organizations can apply these functions to DDoS risk assessment, detection, response, mitigation, and service recovery.
NIST SP 800-61 Rev. 3	NIST (US)	Provides guidance for incident response, including preparation, detection, response, and recovery. The framework supports organizations in establishing procedures for identifying and responding to DDoS and other cybersecurity incidents. Rev. 3 superseded Rev. 2 in April 2025.
ITU-T X.1051:2023	ITU-T	Defines information-security controls specifically for telecommunications organizations and includes TEL 5.41 – Response to DoS/DDoS attacks, covering policies, traffic filtering, port restrictions, service continuity, and coordination with interconnected operators.

ITU-T X.1814:2022	ITU-T	Defines security guidelines for IMT-2020/5G systems, including DDoS mitigation capabilities for cloud web services, network function virtualization, and 5G network environments.
ITU-T X.1818:2024	ITU-T	Establishes security controls for operation and maintenance of 5G network systems. Its DDoS protection control requires network functions exposed to targeted DDoS attacks or traffic spikes to be protected through measures such as redundancy, failover, and load balancing.
RFC 8612 – DDoS Open Threat Signaling (DOTS) Requirements	IETF	Defines requirements for DDoS Open Threat Signaling, supporting communication of DDoS attack telemetry and mitigation requests between systems. It provides a framework for coordinating countermeasures and mitigation across network environments.
ENISA Threat Landscape for DoS Attacks	ENISA (European Union)	Provides recommendations for preventing and remediating DoS/DDoS attacks, including threat modeling, risk assessment, DDoS protection services, CDN deployment, provider coordination, proactive defense, and regular testing of mitigation capabilities.
ETSI TS 102 165-1	ETSI	Provides threat, risk, and vulnerability analysis guidance covering DDoS attack characteristics and defense considerations, including protection of network bandwidth and processing resources against distributed attacks.

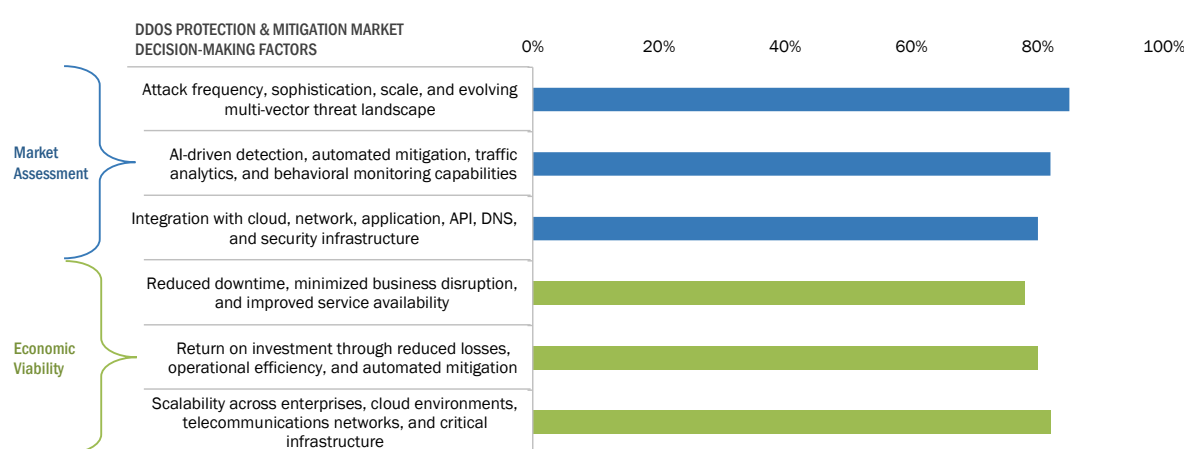
Source: Secondary Research, Company Websites, Regional Government Bodies, and MarketsandMarkets Analysis

8 CUSTOMER LANDSCAPE AND BUYER BEHAVIOR

8.1 DECISION-MAKING PROCESS

Enterprises typically follow a structured buying approach to DDoS protection. The process begins with assessing current network vulnerability, traffic loads, and historical attack patterns. IT and security teams then shortlist solutions based on scalability, latency tolerance, integration needs, and SLAs. Procurement evaluates pricing models, deployment options (on-prem, cloud, or hybrid), and vendor reliability. Final approval generally comes from CISOs, CTOs, or risk committees, ensuring alignment with compliance mandates and long-term security modernization plans.

FIGURE 26 DDOS PROTECTION & MITIGATION MARKET: DECISION-MAKING FACTORS



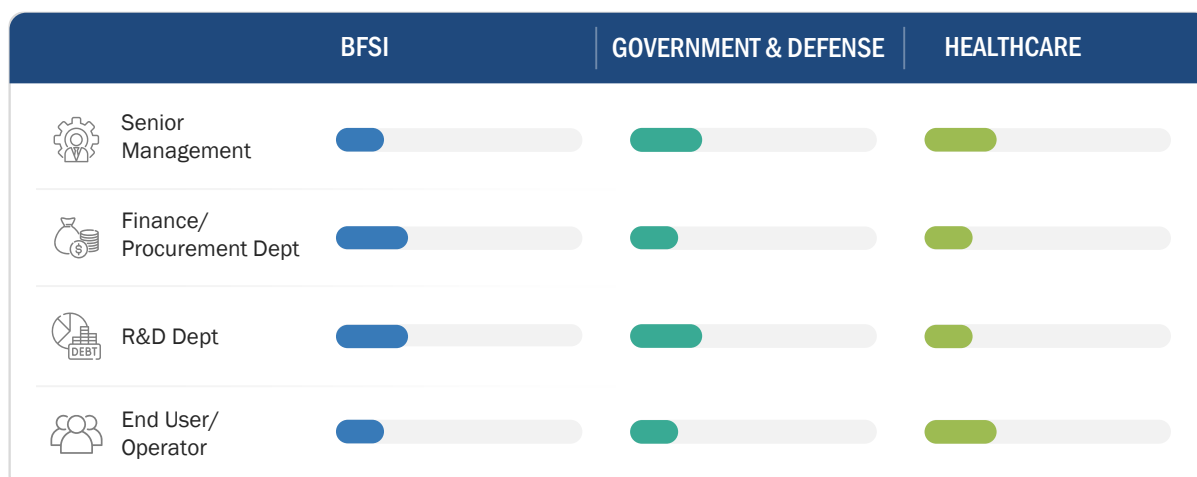
Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

The DDoS protection & mitigation market is influenced by a combination of market assessment and economic viability factors when organizations evaluate solutions. Within market assessment, attack frequency, sophistication, scale, and the growing prevalence of multi-vector attacks represent key considerations, as organizations seek protection capable of addressing evolving threats. AI-driven detection, behavioral analytics, automated mitigation, and real-time traffic monitoring are also increasingly important for improving detection accuracy and response speed. Integration with cloud, network, application, API, DNS, and broader security infrastructure further influences purchasing decisions by enabling unified and scalable protection. From an economic viability perspective, organizations prioritize solutions that reduce downtime, minimize business disruption, and maintain service availability during attacks. Return on investment is assessed through reduced financial losses, operational efficiency, and automation of mitigation activities. Scalability across enterprises, cloud environments, telecommunications networks, and critical infrastructure also remains essential as organizations expand their digital infrastructure and require flexible protection against increasingly large and sophisticated DDoS attacks.

8.2 BUYER STAKEHOLDERS AND BUYING EVALUATION CRITERIA

8.2.1 KEY STAKEHOLDERS IN BUYING PROCESS

FIGURE 27 INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

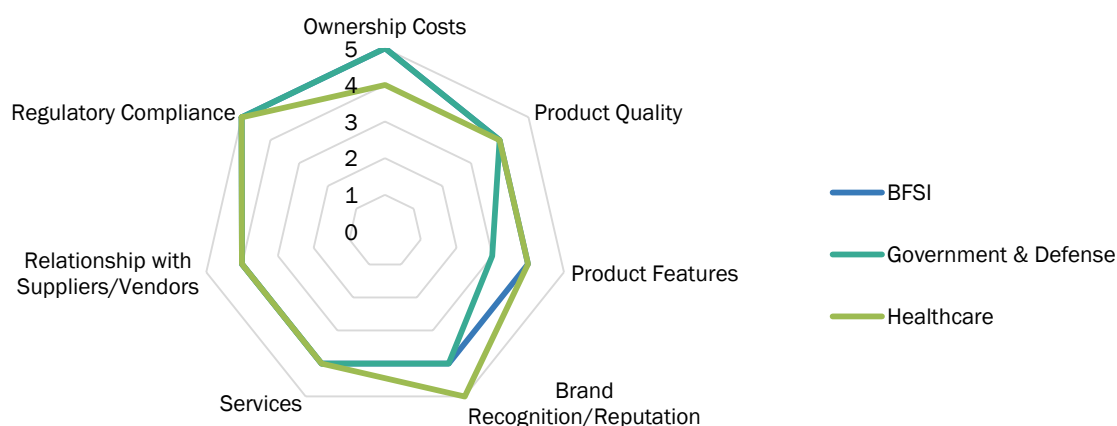
TABLE 24 INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS (%)

Key Stakeholder	BFSI	Government & Defense	Healthcare
Senior Management	20	30	30
Finance/Procurement Dept.	10	20	20
R&D Dept.	30	30	20
End User/Operator	40	20	30
Total	100	100	100

8.2.2 BUYING CRITERIA

This sub-section identifies the key criteria for selecting a supplier or vendor and their weights for each of the top three verticals.

FIGURE 28 KEY BUYING CRITERIA FOR TOP THREE VERTICALS



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 25 KEY BUYING CRITERIA FOR TOP THREE VERTICALS

Buying Criteria	BFSI	Government & Defense	Healthcare
Ownership Cost	5	5	4
Product Quality	4	4	4
Product Features	4	3	4
Brand Recognition/Reputation	4	4	5
Services	4	4	4
Relationship with Supplier/Vendors	4	4	4
Regulatory Compliance	5	5	5

Note: Respondents rated each criterion on a scale of 1–5, where 1 indicates Least Important, and 5 indicates Most Important or Critical.

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

8.2.3 ADOPTION BARRIERS AND INTERNAL CHALLENGES

Organizations face several hurdles that slow or complicate DDoS mitigation adoption. Budget constraints limit investment in high-capacity scrubbing infrastructure and premium SLAs. Legacy network architectures make integration difficult, while skills gaps hinder the effective operation of advanced mitigation platforms. Internal alignment issues arise between IT, security, and procurement teams, delaying deployment decisions. Blind spots in traffic visibility, concerns about false positives, and uncertainty about cloud vs. hybrid models also contribute to slower adoption.

FIGURE 29 ADOPTION BARRIERS AND INTERNAL CHALLENGES

Source: Secondary Research

8.3 UNMET NEEDS IN VARIOUS END-USE INDUSTRIES

The DDoS protection & mitigation market continues to face industry-specific unmet needs as organizations increasingly depend on digital infrastructure, cloud applications, APIs, connected devices, and mission-critical online services. While BFSI, telecommunications, IT & ITeS, government, healthcare, retail, and other sectors have adopted DDoS protection, requirements vary based on infrastructure complexity, attack exposure, availability requirements, and regulatory considerations. Organizations increasingly seek real-time, automated, scalable, and integrated protection capable of addressing volumetric, protocol, application-layer, DNS, and multi-vector attacks. Key gaps include seamless integration across hybrid environments, protection of critical applications and networks, rapid mitigation, IoT and botnet visibility, and access to cost-effective managed services for organizations with limited internal expertise.

TABLE 26 UNMET NEEDS IN DDOS PROTECTION & MITIGATION MARKET, BY END-USE INDUSTRY

END-USE INDUSTRY	UNMET NEEDS
IT & ITeS	- Real-time DDoS protection for cloud applications, APIs, and distributed enterprise infrastructure - Unified visibility across hybrid and multicloud environments with automated mitigation and minimal service disruption - Scalable protection against high-volume and application-layer attacks without excessive infrastructure costs
BFSI	- Always-on protection for digital banking, payment platforms, APIs, and customer-facing applications - Advanced mitigation capable of maintaining transaction availability during volumetric and application-layer attacks - Integration with existing cybersecurity, fraud prevention, and business continuity infrastructure
Healthcare	- DDoS protection for patient portals, telehealth platforms, connected healthcare systems, and critical digital services - Protection that maintains availability without disrupting time-sensitive healthcare applications and connected devices - Scalable cloud and hybrid protection aligned with healthcare security and privacy requirements
Government & Defense	- High-assurance DDoS protection for citizen-facing portals, defense networks, and mission-critical digital services - Rapid mitigation of coordinated and multi-vector attacks targeting critical government infrastructure - Sovereign, resilient, and continuously available protection with strong network visibility and incident-response capabilities
Energy & Utilities	- High-availability DDoS protection for energy-management systems, utility platforms, and connected infrastructure - Rapid detection and mitigation without disrupting critical operational and customer-facing services - Resilient protection across distributed networks, remote assets, and increasingly connected infrastructure
Manufacturing	- Protection for connected manufacturing networks, industrial applications, and Internet-facing operational systems - DDoS mitigation that minimizes disruption to production, supply-chain, and connected-device operations - Integration of network monitoring and DDoS protection across increasingly distributed IT/OT environments

Source: Secondary Research

8.3.1 REVENUE POTENTIAL

Revenue opportunities in the DDoS protection & mitigation market are increasingly concentrated in high-value solution areas such as cloud-based DDoS protection, automated threat mitigation, network traffic analytics, application and API protection, DNS security, botnet detection, and managed DDoS services. Organizations are prioritizing integrated protection platforms that provide end-to-end visibility across network infrastructure, cloud workloads, applications, APIs, DNS, and edge environments. High-demand industries such as telecommunications, IT & ITeS, BFSI, government, healthcare, retail & ecommerce, and

energy & utilities remain important revenue contributors due to increasing digital dependency, rising attack frequency, and stringent availability requirements.

Vendors offering AI-driven detection, adaptive mitigation, behavioral analytics, automated traffic filtering, multi-vector protection, and hybrid cloud architectures are positioned to capture premium revenue opportunities. Recurring revenue models, including cloud-based subscriptions, managed DDoS services, usage-based pricing, and security-as-a-service, are becoming increasingly important for long-term growth. In addition, platform consolidation, integration with WAF, API security, SIEM/SOAR, CDN, and network infrastructure, and partnerships with telecommunications operators, cloud providers, and managed security service providers are enabling ecosystem-driven expansion, improving customer retention, and increasing lifetime customer value.

8.3.2 COST DYNAMICS

The cost structure of the DDoS protection & mitigation market is influenced by the complexity of protecting distributed digital infrastructure, processing large volumes of network traffic, and continuously adapting mitigation capabilities to evolving attack techniques. DDoS vendors incur ongoing investments in cloud scrubbing capacity, global network infrastructure, traffic analytics, AI and machine learning, threat intelligence, automated mitigation engines, and high-capacity network connectivity. Enterprises also incur costs related to deployment, integration with network infrastructure, applications, APIs, DNS, cloud environments, and security operations platforms. Additional expenses arise from bandwidth requirements, mitigation capacity, security monitoring, testing and validation, and skilled cybersecurity personnel.

The rapid adoption of cloud computing, hybrid infrastructure, APIs, connected devices, and distributed applications is increasing traffic volumes and protection requirements. However, cloud-native architectures, automated mitigation, AI-driven traffic analysis, and managed DDoS services can help organizations optimize infrastructure utilization and reduce operational overhead. Enterprises are increasingly moving toward integrated protection platforms that combine network traffic analysis, threat mitigation, application and API security, DNS protection, and security operations integration within a unified architecture. This enables more predictable spending, faster response, improved security-team productivity, and lower total cost of ownership while maintaining scalable protection against increasingly sophisticated DDoS attacks.

8.3.3 MARGIN OPPORTUNITIES IN KEY APPLICATIONS

- **IT & ITes:** Strong margin opportunities are driven by increasing cloud adoption, distributed applications, APIs, and enterprise Internet exposure. Demand for cloud-based DDoS protection, application-layer mitigation, automated threat detection, and managed services supports recurring SaaS subscriptions, usage-based pricing, and premium protection tiers.
- **BFSI:** DDoS protection for digital banking, payment platforms, APIs, and customer-facing applications creates attractive margin opportunities because service availability and transaction continuity are critical. Vendors can command premium pricing through always-on protection, advanced multi-layer mitigation, dedicated scrubbing capacity, and integration with broader cybersecurity infrastructure.
- **Government & Defense:** Stable margins are supported by mission-critical digital services, public-sector networks, citizen-facing applications, and stringent resilience requirements. Demand for high-assurance DDoS protection, sovereign infrastructure, continuous monitoring, and managed mitigation creates opportunities for long-term contracts and premium security services.
- **Healthcare:** Increasing dependence on telehealth, patient portals, connected healthcare platforms, and digital health services creates opportunities for specialized DDoS protection. Vendors can generate premium revenues through high-availability protection, cloud-based mitigation, application-layer security, and managed services supporting critical healthcare infrastructure.

- **Retail & ecommerce:** Strong margin opportunities are supported by continuous dependence on ecommerce websites, APIs, digital payment interfaces, and customer-facing applications. Demand for application-aware DDoS mitigation, bot protection, WAF integration, and scalable cloud protection supports recurring subscriptions, transaction-oriented pricing, and premium managed services.
- **Energy & Utilities:** Increasing digitalization of utility infrastructure, connected systems, and customer-facing platforms is creating demand for resilient DDoS protection. Vendors can benefit from premium pricing through high-availability architectures, hybrid protection, continuous monitoring, and long-term security partnerships covering critical infrastructure.

9 DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING

KEY FINDINGS

- By offering, the services segment is projected to register the highest CAGR of 14.6% during the forecast period, reaching USD 3,372.3 million by 2031.
- The solutions segment is expected to dominate the DDoS protection and mitigation market, with USD 5,192.2 million in 2026, and is projected to register a CAGR of 13.2% during the forecast period.
- In the overall offering segment, Asia Pacific is anticipated to experience the highest growth rate. This increase is largely due to the rising adoption of IoT devices. Organizations in this region are actively focused on safeguarding their network infrastructure.
- The growth of the DDoS protection and mitigation market is expected to be driven by increasingly sophisticated cyber threats and the use of web and mobile applications for business-critical operations.

9.1 INTRODUCTION

The DDoS protection and mitigation market, by offering, has been segmented into solutions and services. DDoS protection and mitigation solutions and services play a crucial role in safeguarding data, servers, endpoints, cloud infrastructure, applications, and organizational networks against increasingly sophisticated DDoS attacks.

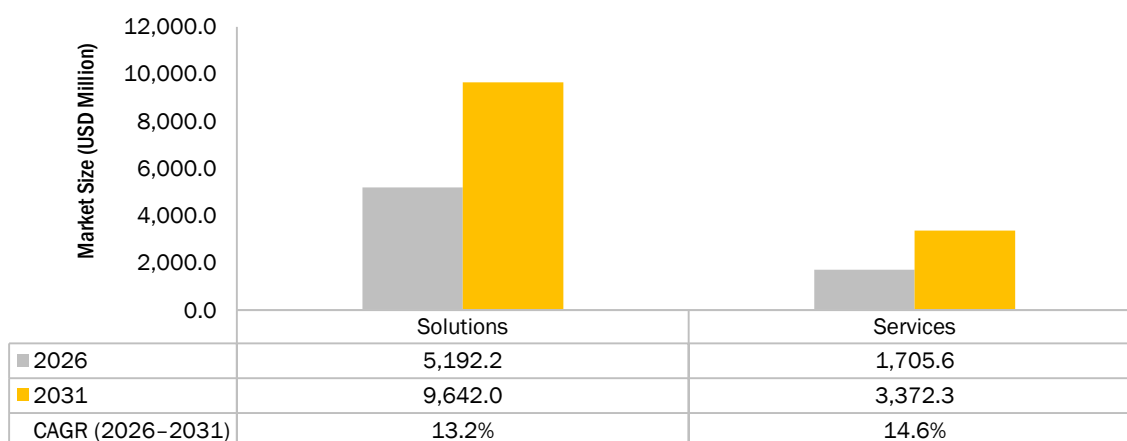
A DDoS (distributed denial of service) attack is a malicious attempt to disrupt the availability or normal functioning of a targeted system, application, network, or service by overwhelming it with a large volume of illegitimate traffic or requests. Unlike DoS (denial of service) attacks, which typically originate from a single source, DDoS attacks leverage multiple compromised devices, often organized into botnets, to generate distributed attack traffic. Attackers may compromise devices using malware or other unauthorized access methods and subsequently use these devices to flood target resources with malicious traffic.

DDoS attacks can target network bandwidth, protocol layers, and application layers, resulting in degraded performance, service disruption, or complete unavailability for legitimate users. Organizations therefore deploy DDoS protection and mitigation solutions and associated services to detect, absorb, filter, and mitigate malicious traffic while maintaining the availability of critical resources. The increasing frequency and sophistication of DDoS attacks, growing awareness of cybersecurity threats, rising dependence on digital and cloud-based infrastructure, and the need for business continuity and disaster recovery are driving the adoption of DDoS protection and mitigation solutions and services across industries such as retail, BFSI, government and defense, healthcare, energy and utilities, and manufacturing.

9.1.1 OFFERING: DDOS PROTECTION AND MITIGATION MARKET DRIVERS

- The increasing demand for ensuring operational efficiency is fueling the demand for hardware solutions.
- Seamless, flexible, and easy-to-deploy options are fueling the demand for DDoS protection and mitigation software and platforms.
- The services segment is expected to grow due to the increasing demand for DDoS protection and mitigation services to manage effective deployment.
- The rising prevalence of ransom distributed denial of service (RDDoS) attacks, new threats to DNS traffic, and the vulnerabilities surrounding web applications drive the DDoS protection and mitigation market.

FIGURE 30 SERVICES SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 27 DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solutions	2,174.4	2,544.4	2,959.4	3,415.9	3,920.3	4,555.3	15.9%
Services	660.7	783.4	923.2	1,079.7	1,255.2	1,477.4	17.5%
Total	2,835.0	3,327.8	3,882.6	4,495.6	5,175.5	6,032.8	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

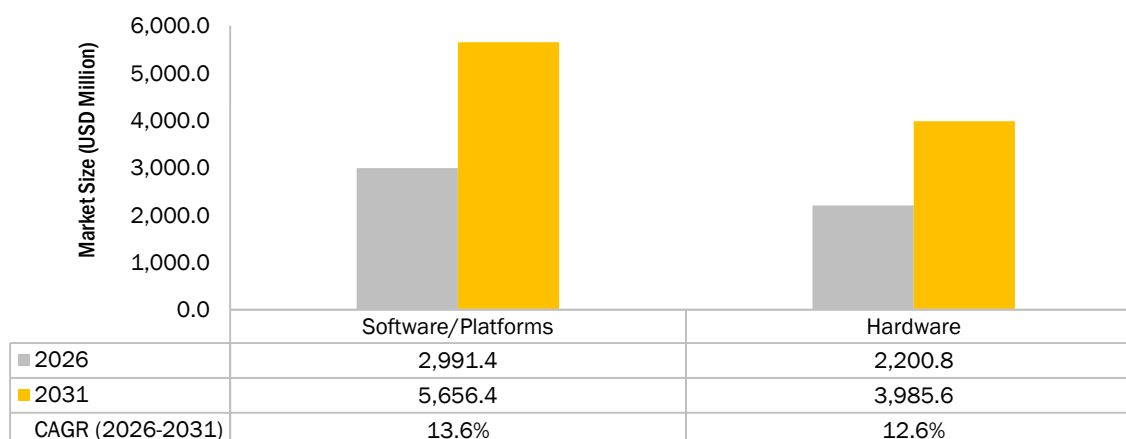
TABLE 28 DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solutions	5,192.2	5,903.8	6,697.1	7,579.4	8,558.2	9,642.0	13.2%
Services	1,705.6	1,964.1	2,256.3	2,585.7	2,956.4	3,372.3	14.6%
Total	6,897.7	7,867.9	8,953.4	10,165.1	11,514.7	13,014.3	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.2 SOLUTIONS

The solutions segment of the DDoS protection and mitigation market comprises hardware and software/platforms designed to detect, analyze, filter, and mitigate malicious traffic associated with DDoS attacks. These solutions help organizations protect critical network infrastructure, applications, servers, endpoints, and cloud environments by identifying anomalous traffic patterns and preventing illegitimate requests from disrupting legitimate services. Hardware-based solutions provide dedicated, on-premises capabilities for traffic inspection and mitigation, while software and platform-based solutions offer scalable and flexible protection through cloud-based, virtual, or software-defined architectures. The adoption of these solutions is increasing as organizations seek to strengthen their cybersecurity posture, maintain service availability, and minimize operational and financial disruptions caused by increasingly sophisticated DDoS attacks.

FIGURE 31 SOFTWARE/PLATFORMS SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD


Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 29 DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	949.0	1,105.2	1,279.3	1,469.5	1,678.2	1,940.5	15.4%
Software/Platforms	1,225.4	1,439.2	1,680.1	1,946.4	2,242.1	2,614.9	16.4%
Total	2,174.4	2,544.4	2,959.4	3,415.9	3,920.3	4,555.3	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 30 DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	2,200.8	2,489.9	2,810.4	3,164.5	3,555.2	3,985.6	12.6%
Software/Platforms	2,991.4	3,413.9	3,886.8	4,414.9	5,003.1	5,656.4	13.6%
Total	5,192.2	5,903.8	6,697.1	7,579.4	8,558.2	9,642.0	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 31 DDOS PROTECTION AND MITIGATION SOLUTIONS MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	896.2	1,025.4	1,164.9	1,312.6	1,469.6	1,673.3	13.3%
Europe	550.5	647.0	755.7	875.4	1,007.2	1,172.4	16.3%
Asia Pacific	410.6	495.2	594.0	707.3	838.3	1,005.7	19.6%
Middle East & Africa	223.1	264.8	312.3	365.7	425.6	501.6	17.6%
Latin America	94.0	112.0	132.4	154.9	179.6	202.3	16.6%
Total	2,174.4	2,544.4	2,959.4	3,415.9	3,920.3	4,555.3	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 32 DDOS PROTECTION AND MITIGATION SOLUTIONS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,881.2	2,110.0	2,361.0	2,635.7	2,935.6	3,262.3	11.6%
Europe	1,338.1	1,523.2	1,729.2	1,958.0	2,209.2	2,503.4	13.3%
Asia Pacific	1,161.4	1,337.9	1,537.6	1,763.1	2,016.9	2,302.2	14.7%
Middle East & Africa	579.8	668.7	764.7	872.5	993.1	1,128.0	14.2%
Latin America	231.5	264.0	304.6	350.2	403.4	446.1	14.0%
Total	5,192.2	5,903.8	6,697.1	7,579.4	8,558.2	9,642.0	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.2.1 HARDWARE

DDoS attacks pose a real threat to organizations that operate their businesses online. Such critical websites have become the main targets of cyber terrorists or hackers. DDoS attacks can be addressed using DDoS hardware protection solutions. Hardware appliances are configured in local networks or data centers to protect an organization's network from evolving, sophisticated threats. These hardware solutions are easy to install and suitable for high-volume amplified traffic, which requires high throughput. The hardware solutions are set up on a remote network and can be managed in the data center hosting environment itself.

DDoS protection appliances can mitigate large network-based DDoS attacks, floods, reflective amplified spoof attacks, and application-layer attacks. Additionally, hardware solutions ensure network connectivity and eliminate downtime in the event of power or equipment failures, as well as during maintenance. These solutions can be easily moved and reconfigured with minimal interference in the network infrastructure. DDoS protection appliances provide effective protection against cyberattacks, such as advanced DNS DDoS and layer 4 and layer 7 volumetric attacks.

TABLE 33 DDoS PROTECTION AND MITIGATION HARDWARE MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	395.1	449.9	508.7	570.5	635.7	720.2	12.8%
Europe	236.9	277.2	322.3	371.5	425.4	492.9	15.8%
Asia Pacific	180.2	216.3	258.1	305.9	360.7	430.6	19.0%
Middle East & Africa	96.2	113.7	133.5	155.6	180.2	211.4	17.0%
Latin America	40.6	48.2	56.7	66.0	76.1	85.3	16.0%
Total	949.0	1,105.2	1,279.3	1,469.5	1,678.2	1,940.5	15.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 34 DDoS PROTECTION AND MITIGATION HARDWARE MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	805.8	899.3	1,001.2	1,112.1	1,232.5	1,363.0	11.1%
Europe	559.9	634.2	716.5	807.3	906.4	1,022.2	12.8%
Asia Pacific	494.7	567.0	648.3	739.5	841.5	955.7	14.1%
Middle East & Africa	243.2	279.2	317.8	360.8	408.7	462.0	13.7%
Latin America	97.2	110.3	126.6	144.8	166.0	182.7	13.5%
Total	2,200.8	2,489.9	2,810.4	3,164.5	3,555.2	3,985.6	12.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.2.1.1 Firewalls

9.2.1.1.1 Hardware firewalls filter and block malicious traffic to enable efficient server access for legitimate requests

A hardware firewall is a physical appliance designed to protect a network by filtering incoming and outgoing traffic. Positioned between the external network and internal servers, it serves as a gatekeeper, analyzing data packets to enforce security policies and prevent unauthorized access. In DDoS protection and mitigation, hardware firewalls play a crucial role as they can absorb and filter large volumes of malicious traffic, ensuring that legitimate requests reach their destination without disruption. By employing advanced techniques such as traffic shaping and rate limiting, these appliances help maintain service availability during an attack. Additionally, for mitigation, these firewalls implement rules to block specific types of traffic, thereby minimizing potential vulnerabilities and maintaining network integrity. Overall, hardware firewalls provide a robust solution for organizations seeking to enhance their cybersecurity posture against evolving threats while ensuring reliable network performance.

9.2.1.2 Intrusion Detection and Prevention Systems (IDPS)

9.2.1.2.1 IDPS prevents DDoS attacks by continuously monitoring network traffic and actively blocking malicious requests

Intrusion detection and prevention systems (IDPS) detect and respond to malicious traffic in real-time. These systems monitor network traffic to identify suspicious patterns, such as high volumes of requests or unusual behavior, which may signal potential DDoS attacks. Intrusion Detection Systems (IDS) alert security teams when anomalies are detected, allowing for a rapid response, while Intrusion Prevention Systems (IPS) proactively block or throttle harmful traffic, drop packets, and enforce rate limiting. IDPS is particularly effective against application-layer (Layer 7) DDoS attacks through deep packet inspection and can be integrated with firewalls, Web Application Firewalls (WAF), and other security tools for comprehensive defense. With features like automated responses, blocklisting, and geo-blocking, IDPS enhances a multi-layered security strategy. Modern systems also leverage AI and machine learning to improve detection accuracy by analyzing evolving attack patterns, making IDPS a critical component in minimizing the impact of DDoS attacks.

9.2.1.3 Load Balancers

9.2.1.3.1 Load balancers protect against DDoS attacks by distributing traffic across multiple servers

Hardware load balancers are dedicated devices that distribute network traffic across multiple servers to enhance performance and reliability. By managing incoming requests, they prevent any single server from becoming overwhelmed, which is crucial for maintaining service availability. For protection against DDoS attacks, hardware load balancers can effectively mitigate attacks by rerouting malicious traffic and ensuring that legitimate requests are processed without delay. They employ various algorithms to dynamically allocate resources, enabling efficient handling of spikes in traffic that often accompany DDoS attacks. Additionally, these devices can integrate with DDoS mitigation services, further strengthening security. Overall, hardware load balancers play a vital role in optimizing application delivery while providing robust defenses against DDoS attacks, ensuring both performance and security in network environments.

9.2.1.4 Other hardware

Scrubbing devices, rate limiters, and anti-DDoS gateways are vital offerings in the DDoS protection and mitigation market, enabling enterprises to defend against sophisticated cyber threats. Scrubbing devices filter incoming traffic, redirecting it for deep packet inspection to remove malicious packets while allowing legitimate traffic to pass through, particularly effective against large-scale volumetric attacks. Rate limiters

control the volume of requests sent to a server, preventing overload during DDoS attacks and ensuring service availability. Anti-DDoS gateways act as the first line of defense, monitoring traffic in real-time and applying various mitigation strategies, including redirecting suspicious traffic for further analysis. The market is rapidly growing due to the increasing frequency of DDoS attacks, with organizations investing in integrated solutions to enhance resilience and protect their digital assets. By employing these technologies, businesses can maintain operational continuity and safeguard their reputations in an evolving threat landscape.

9.2.2 SOFTWARE/PLATFORMS

9.2.2.1 Global rise in IoT devices to drive market

DDoS protection and mitigation software/platforms are designed to safeguard organizations against increasingly sophisticated and large-scale DDoS attacks targeting applications, networks, DNS infrastructure, and other critical digital resources. These platforms detect and mitigate malicious traffic associated with various attack vectors, including volumetric, protocol, and application-layer attacks such as NTP amplification, DNS attacks, SYN floods, R.U.D.Y., and HTTP POST attacks. Software/platform-based solutions can be deployed across cloud, on-premises, and hybrid environments, providing organizations with scalable and flexible protection based on their infrastructure requirements.

Organizations are increasingly seeking DDoS protection platforms that offer rapid deployment, automated mitigation, scalability, and minimal impact on legitimate traffic and network performance. Advanced platforms leverage technologies such as machine learning (ML), artificial intelligence (AI), behavioral analytics, and big data analytics to identify anomalous traffic patterns and detect both known and emerging attack techniques. These capabilities enable automated and adaptive threat detection and mitigation while reducing false positives. The proliferation of IoT devices, expansion of cloud-based infrastructure, and increasing reliance on internet-facing applications are further driving the adoption of software/platform-based DDoS protection and mitigation solutions.

TABLE 35 DDOS PROTECTION AND MITIGATION SOFTWARE/PLATFORMS MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	501.1	575.5	656.2	742.1	833.9	953.0	13.7%
Europe	313.6	369.8	433.5	503.9	581.7	679.5	16.7%
Asia Pacific	230.4	278.9	335.8	401.4	477.6	575.1	20.1%
Middle East & Africa	126.9	151.1	178.8	210.1	245.4	290.2	18.0%
Latin America	53.4	63.8	75.8	88.9	103.5	117.0	17.0%
Total	1,225.4	1,439.2	1,680.1	1,946.4	2,242.1	2,614.9	16.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 36 DDOS PROTECTION AND MITIGATION SOFTWARE/PLATFORMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,075.5	1,210.7	1,359.8	1,523.5	1,703.1	1,899.4	12.0%
Europe	778.3	889.0	1,012.7	1,150.7	1,302.8	1,481.2	13.7%
Asia Pacific	666.7	770.9	889.4	1,023.6	1,175.4	1,346.5	15.1%
Middle East & Africa	336.6	389.5	446.9	511.7	584.4	665.9	14.6%
Latin America	134.4	153.8	178.0	205.4	237.4	263.4	14.4%
Total	2,991.4	3,413.9	3,886.8	4,414.9	5,003.1	5,656.4	13.6%

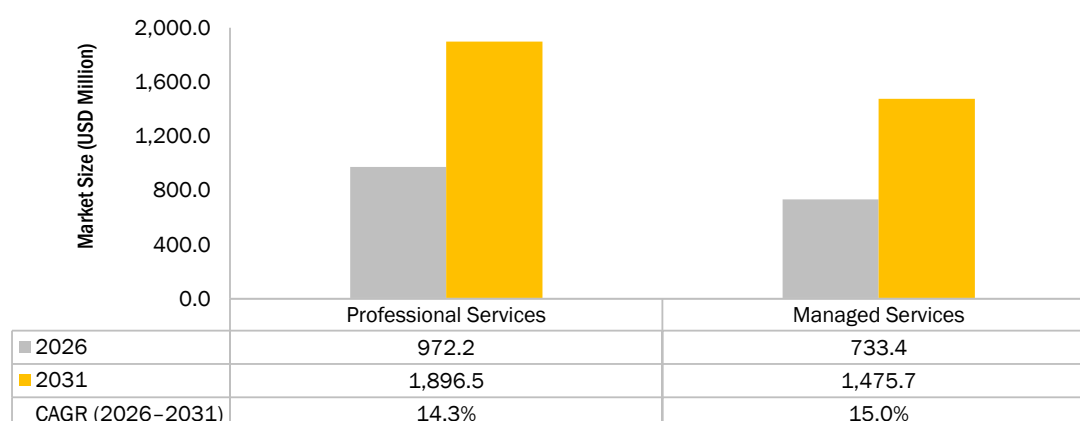
Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3 SERVICES

Cyberattacks on websites are on the rise, prompting organizations to implement robust security measures to manage risks in an increasingly complex threat landscape. As more organizations and service providers adopt DDoS solutions, the demand for support services is expected to grow. The DDoS protection and mitigation market has been segmented based on services into professional and managed services. The professional services segment encompasses design and implementation, consulting and advisory services, training and education, and support and maintenance. As most businesses lack the technical expertise to manage their network infrastructure and application-layer attacks, professional service providers offer ways to overcome this problem. The services offered by DDoS protection and mitigation vendors help safeguard websites, networks, and layer three and layer seven threats. DDoS services protect websites, networks, and critical infrastructure devices, while also reducing downtime and business risks. These services protect organizations from NTP amplification, DNS amplification, HTTP flood, SYN flood, Slowloris, spoofing, and volumetric attacks. DDoS service providers are continuously integrating advanced technologies to stop such DoS/DDoS attacks. Additionally, they provide support services and access to a 24/7 DDoS response team.

DDoS attacks cause 3 million or more packets per second to be transferred illegitimately, thereby blocking the resources for legitimate users. Services offered by DDoS protection and mitigation vendors have been classified into professional and managed services. Some vendors also offer DDoS testing services to assess resources against high-intensity DDoS attacks.

FIGURE 32 MANAGED SERVICES SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 37 DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	382.7	452.6	531.9	620.4	719.3	844.4	17.2%
Managed Services	278.0	330.8	391.3	459.3	535.9	633.0	17.9%
Total	660.7	783.4	923.2	1,079.7	1,255.2	1,477.4	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 38 DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	972.2	1,116.6	1,279.2	1,462.1	1,667.2	1,896.5	14.3%
Managed Services	733.4	847.5	977.0	1,123.6	1,289.3	1,475.7	15.0%
Total	1,705.6	1,964.1	2,256.3	2,585.7	2,956.4	3,372.3	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 39 DDOS PROTECTION AND MITIGATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	272.3	315.7	363.4	414.9	470.6	542.7	14.8%
Europe	167.3	199.2	235.8	276.7	322.5	380.3	17.9%
Asia Pacific	124.8	152.5	185.3	223.6	268.4	326.2	21.2%
Middle East & Africa	67.8	81.5	97.4	115.6	136.3	162.7	19.1%
Latin America	28.6	34.5	41.3	49.0	57.5	65.6	18.1%
Total	660.7	783.4	923.2	1,079.7	1,255.2	1,477.4	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 40 DDOS PROTECTION AND MITIGATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

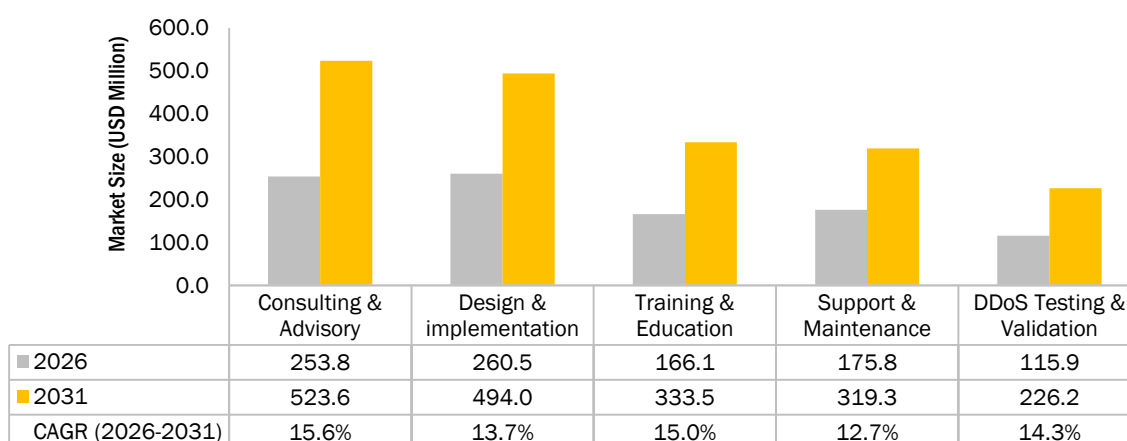
Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	618.0	702.0	795.4	899.2	1,014.1	1,141.0	13.0%
Europe	439.6	506.7	582.6	668.0	763.2	875.6	14.8%
Asia Pacific	381.5	445.1	518.0	601.5	696.7	805.2	16.1%
Middle East & Africa	190.5	222.5	257.6	297.6	343.1	394.5	15.7%
Latin America	76.1	87.8	102.6	119.5	139.4	156.0	15.5%
Total	1,705.6	1,964.1	2,256.3	2,585.7	2,956.4	3,372.3	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3.1 PROFESSIONAL SERVICES

Professional services are services offered through professionals, specialists, or experts to support businesses. Professional services support businesses of all sizes and are applicable to all verticals. These include design and implementation, consulting and advisory, training and education, and support and maintenance. The latest techniques, strategies, and skills adopted by professionals enable organizations to implement DDoS protection and mitigation features. They also offer customized implementation and risk assessment and assist in the deployment of DDoS protection and mitigation solutions via industry-defined best practices. The professionals provide solutions and fully support business goals through enhanced communication services. Professional services help organizations stay protected from advanced threats.

FIGURE 33 CONSULTING & ADVISORY SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 41 DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	158.4	183.2	210.4	239.6	271.0	311.8	14.5%
Europe	96.8	114.9	135.7	158.8	184.6	217.1	17.5%
Asia Pacific	72.2	88.0	106.6	128.3	153.7	186.3	20.9%
Middle East & Africa	38.8	46.5	55.5	65.6	77.1	91.8	18.8%
Latin America	16.5	19.9	23.8	28.1	32.9	37.5	17.8%
Total	382.7	452.6	531.9	620.4	719.3	844.4	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 42 DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	354.2	401.3	453.6	511.5	575.4	645.8	12.8%
Europe	250.3	287.8	330.0	377.4	430.1	492.1	14.5%
Asia Pacific	217.3	252.8	293.5	339.8	392.6	452.5	15.8%
Middle East & Africa	107.1	124.7	144.0	165.9	190.6	218.5	15.3%
Latin America	43.3	49.9	58.1	67.5	78.5	87.7	15.1%
Total	972.2	1,116.6	1,279.2	1,462.1	1,667.2	1,896.5	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 43 DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY TYPE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	106.0	124.7	145.7	169.0	194.9	227.6	16.5%
Consulting & Advisory	93.0	111.4	132.5	156.4	183.5	217.9	18.6%
Training & Education	63.1	75.0	88.7	104.1	121.4	143.4	17.9%
Support & Maintenance	74.9	87.5	101.5	116.9	133.7	154.8	15.6%
DDoS Testing & Validation	45.6	54.0	63.4	74.0	85.8	100.7	17.1%
Total	382.7	452.6	531.9	620.4	719.3	844.4	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 44 DDOS PROTECTION AND MITIGATION PROFESSIONAL SERVICES MARKET, BY TYPE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	260.5	297.5	339.0	385.2	436.8	494.0	13.7%
Consulting & Advisory	253.8	294.9	341.7	394.9	455.3	523.6	15.6%
Training & Education	166.1	191.9	221.1	254.1	291.5	333.5	15.0%
Support & Maintenance	175.8	199.1	224.9	253.4	284.8	319.3	12.7%
DDoS Testing & Validation	115.9	133.2	152.5	174.4	198.8	226.2	14.3%
Total	972.2	1,116.6	1,279.2	1,462.1	1,667.2	1,896.5	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3.1.1 Design and implementation

9.3.1.1.1 Increase in need to improve network performance and reliability

Design and implementation services help organizations configure, validate, and implement DDoS protection and mitigation solutions. These services ensure that organizations achieve better network performance and reliability, which in turn helps them enhance business efficiency. These services may also include design planning workshops, operational planning, and staff guidance, as well as easy product deployment and integration. Designing helps organizations develop a suitable network architecture according to their needs and operational capabilities. The implementation guarantees design review, product orientation, and application fine-tuning. Integrating DDoS products with other third-party products helps provide more reliable and advanced protection to critical assets.

TABLE 45 DDOS PROTECTION AND MITIGATION DESIGN AND IMPLEMENTATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	43.8	50.4	57.6	65.2	73.3	83.9	13.9%
Europe	26.8	31.7	37.2	43.3	50.1	58.6	16.9%
Asia Pacific	20.0	24.3	29.2	35.0	41.7	50.2	20.2%
Middle East & Africa	10.8	12.8	15.2	17.9	20.9	24.7	18.1%
Latin America	4.6	5.5	6.5	7.7	8.9	10.1	17.2%
Total	106.0	124.7	145.7	169.0	194.9	227.6	16.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 46 DDOS PROTECTION AND MITIGATION DESIGN AND IMPLEMENTATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	94.8	106.8	120.0	134.6	150.5	167.9	12.1%
Europe	67.1	76.8	87.5	99.5	112.8	128.3	13.8%
Asia Pacific	58.3	67.4	77.8	89.6	102.9	118.0	15.2%
Middle East & Africa	28.7	33.3	38.2	43.7	50.0	57.0	14.7%
Latin America	11.6	13.3	15.4	17.8	20.6	22.9	14.5%
Total	260.5	297.5	339.0	385.2	436.8	494.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3.1.2 Consulting and advisory

9.3.1.2.1 Growing concerns for cybersecurity and adoption of advanced technologies

Consulting and advisory services are essential during the early phase of implementing DDoS protection and mitigation solutions. Depending on market trends, these services provide organizations with tailored recommendations to enhance their business efficiency. Consultation services offer guidance and advice to organizations, helping them protect themselves from advanced threats. The rise in the adoption of consulting and advisory services among verticals can be attributed to a lack of awareness about the latest technologies for addressing cybersecurity concerns.

The world-class expertise of consulting and advisory teams helps identify network threats and loopholes in infrastructure, which may be potential targets for attackers. Controlled and monitored DDoS attack simulations can also be delivered to organizations to identify vulnerabilities in their systems and networks. Advisors help organizations achieve their business goals with the utmost security and without operational delays. These services also help lower risks, reduce complexities, and increase revenue, as they can be easily customized and applied, delivering maximum product assurance.

TABLE 47 DDOS PROTECTION AND MITIGATION CONSULTING AND ADVISORY SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	38.6	45.2	52.5	60.5	69.3	80.7	15.9%
Europe	23.5	28.2	33.7	40.0	47.0	56.0	19.0%
Asia Pacific	17.5	21.6	26.5	32.3	39.1	48.0	22.3%
Middle East & Africa	9.4	11.4	13.8	16.5	19.6	23.6	20.2%
Latin America	4.0	4.9	5.9	7.1	8.4	9.7	19.2%
Total	93.0	111.4	132.5	156.4	183.5	217.9	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 48 DDOS PROTECTION AND MITIGATION CONSULTING AND ADVISORY SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	92.7	106.3	121.5	138.5	157.6	178.8	14.0%
Europe	65.3	75.9	88.0	101.8	117.3	135.7	15.8%
Asia Pacific	56.6	66.7	78.3	91.7	107.1	124.8	17.1%
Middle East & Africa	27.9	32.9	38.4	44.7	52.0	60.2	16.6%
Latin America	11.3	13.2	15.5	18.2	21.4	24.2	16.4%
Total	253.8	294.9	341.7	394.9	455.3	523.6	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3.1.3 Training and education

9.3.1.3.1 Rising need for training and creating awareness of DDoS attacks

The training and education segment comprises a team of well-trained and dedicated professionals. Training and education services help staff maintain and configure DDoS solutions, as well as raise awareness of threats among the staff. The best-in-class engineers and DDoS mitigation experts provide live training, which helps organizations understand the nature of the attack and prepares them to mitigate it. Courses available from vendors help organizations choose the right DDoS product, defend against volumetric and application-layer-oriented DDoS attacks, mitigate SYN floods, detect connections from proxies, inspect HTTP traffic on non-standard ports, and deploy products to protect network appliances and servers.

TABLE 49 DDOS PROTECTION AND MITIGATION TRAINING AND EDUCATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	26.1	30.4	35.1	40.2	45.8	53.0	15.2%
Europe	15.9	19.0	22.6	26.6	31.1	36.8	18.3%
Asia Pacific	11.9	14.6	17.8	21.5	25.9	31.6	21.6%
Middle East & Africa	6.4	7.7	9.2	11.0	13.0	15.6	19.5%
Latin America	2.7	3.3	4.0	4.7	5.6	6.4	18.5%
Total	63.1	75.0	88.7	104.1	121.4	143.4	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 50 DDOS PROTECTION AND MITIGATION TRAINING AND EDUCATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	60.6	69.0	78.5	89.0	100.7	113.7	13.4%
Europe	42.7	49.4	57.0	65.6	75.1	86.5	15.1%
Asia Pacific	37.1	43.4	50.7	59.0	68.6	79.5	16.5%
Middle East & Africa	18.3	21.4	24.9	28.8	33.3	38.4	16.0%
Latin America	7.4	8.6	10.0	11.7	13.7	15.4	15.8%
Total	166.1	191.9	221.1	254.1	291.5	333.5	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3.1.4 Support and maintenance

9.3.1.4.1 Rising need for support for technical issues and guidance

Support and maintenance services include functional support, technical support, remote support, and database support, which companies offer to their end customers during the installation and maintenance of the software. Support and maintenance services help in the proper functioning of DDoS protection solutions and services. The support team provides 24/7 support and resolves technical issues faced by organizations. The customer support portal with dashboards creates a direct link between organizations and DDoS support and maintenance teams. Online support resources offer documentation, technical Frequently Asked Questions (FAQs), software updates, and user guides to facilitate the smooth operation of deployed DDoS protection and mitigation products.

TABLE 51 DDOS PROTECTION AND MITIGATION SUPPORT AND MAINTENANCE SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	30.9	35.3	40.0	45.0	50.2	57.0	13.0%
Europe	19.0	22.3	25.9	30.0	34.4	39.9	16.0%
Asia Pacific	14.2	17.0	20.4	24.2	28.6	34.2	19.3%
Middle East & Africa	7.6	9.0	10.6	12.4	14.4	16.9	17.2%
Latin America	3.2	3.9	4.5	5.3	6.1	6.9	16.3%
Total	74.9	87.5	101.5	116.9	133.7	154.8	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 52 DDOS PROTECTION AND MITIGATION SUPPORT AND MAINTENANCE SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	63.8	71.3	79.5	88.3	97.9	108.3	11.1%
Europe	45.4	51.4	58.2	65.6	73.6	83.0	12.8%
Asia Pacific	39.4	45.2	51.7	59.0	67.2	76.3	14.2%
Middle East & Africa	19.4	22.3	25.4	28.8	32.6	36.9	13.7%
Latin America	7.8	8.9	10.2	11.7	13.4	14.8	13.5%
Total	175.8	199.1	224.9	253.4	284.8	319.3	12.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3.1.5 DDoS testing and validation

9.3.1.5.1 Identify vulnerabilities and evaluate the effectiveness, capacity, and responsiveness of existing DDoS mitigation mechanisms

DDoS testing and validation services involve the controlled simulation of DDoS attacks to assess an organization's ability to detect, withstand, and mitigate malicious traffic without disrupting legitimate operations. These services help organizations identify vulnerabilities and evaluate the effectiveness, capacity, and responsiveness of their existing DDoS protection and mitigation mechanisms. They typically include attack simulation and stress testing across different vectors, such as volumetric, protocol, and application-layer attacks; assessment of network, application, and infrastructure resilience; evaluation of detection and mitigation capabilities; and measurement of response times, traffic-handling capacity, and service availability during simulated attacks. These services also include validation of mitigation policies, identification of performance bottlenecks, analysis of gaps in existing defenses, and recommendations for improving DDoS response strategies. By conducting controlled and authorized testing, organizations can validate their DDoS preparedness, strengthen business continuity and incident response capabilities, and ensure that protection mechanisms remain effective against evolving attack techniques.

TABLE 53 DDOS PROTECTION AND MITIGATION DDOS TESTING AND VALIDATION SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	18.9	21.9	25.1	28.6	32.3	37.2	14.5%
Europe	11.5	13.7	16.2	18.9	22.0	25.9	17.5%
Asia Pacific	8.6	10.5	12.7	15.3	18.3	22.2	20.9%
Middle East & Africa	4.6	5.5	6.6	7.8	9.2	10.9	18.8%
Latin America	2.0	2.4	2.8	3.4	3.9	4.5	17.8%
Total	45.6	54.0	63.4	74.0	85.8	100.7	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 54 DDOS PROTECTION AND MITIGATION DDOS TESTING AND VALIDATION SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	42.3	47.9	54.1	61.0	68.7	77.1	12.8%
Europe	29.8	34.3	39.3	45.0	51.3	58.7	14.5%
Asia Pacific	25.9	30.1	35.0	40.5	46.8	53.9	15.8%
Middle East & Africa	12.8	14.9	17.2	19.8	22.7	26.0	15.3%
Latin America	5.2	5.9	6.9	8.0	9.4	10.5	15.1%
Total	115.9	133.2	152.5	174.4	198.8	226.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

9.3.2 MANAGED SERVICES

9.3.2.1 Need to increase business efficiency and operations

Security systems must be regularly upgraded to counter newly emerging threats, including DDoS attacks, ransomware, and sophisticated cybercriminals. As a result, companies are rapidly outsourcing their network security concerns to specialized service providers, known as Managed Security Service Providers (MSSPs). Managed Security Services (MSS) help provide network assessment, targeted scanning and reporting, unlimited report generation, security controls and remediation, vulnerability analysis, and live monitoring. Managed service is an approach that enables organizations to outsource their IT operations according to their specific business requirements. The rising cyberattacks and ever-changing threat landscape are leading to illegitimate traffic, which forces organizations to upgrade their current IT infrastructures. Managed services help customers safeguard against DDoS attacks, allowing them to concentrate on their core business activities. These services offer DDoS protection through cloud-based, on-premises, and hybrid deployments. Managed service providers handle DDoS detection and mitigation for clients who may lack the necessary expertise or resources to manage these threats themselves. By using managed services, online businesses and corporate data are better protected, as these services proactively monitor network traffic and detect and mitigate DDoS attacks and other abnormalities in internet traffic.

Organizations help customers control and access sensitive data and achieve regulatory compliance by providing strong encryption-managed services. Under managed services, customers' pre- and post-deployment queries and needs are addressed. Overall, managed services provide access to industry best practices and deep-rooted transformation expertise without impairing organizations' internal operations.

TABLE 55 DDOS PROTECTION AND MITIGATION MANAGED SERVICES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	113.9	132.5	153.1	175.3	199.5	230.9	15.2%
Europe	70.5	84.3	100.1	117.9	137.9	163.1	18.3%
Asia Pacific	52.6	64.5	78.7	95.2	114.8	139.9	21.6%
Middle East & Africa	29.0	35.0	42.0	50.0	59.2	70.9	19.6%
Latin America	12.0	14.6	17.5	20.9	24.6	28.1	18.5%
Total	278.0	330.8	391.3	459.3	535.9	633.0	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 56 DDOS PROTECTION AND MITIGATION MANAGED SERVICES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	263.8	300.6	341.8	387.7	438.7	495.2	13.4%
Europe	189.2	218.9	252.5	290.6	333.1	383.5	15.2%
Asia Pacific	164.2	192.3	224.6	261.6	304.1	352.7	16.5%
Middle East & Africa	83.4	97.7	113.6	131.8	152.5	176.0	16.1%
Latin America	32.7	37.9	44.5	52.0	60.8	68.3	15.9%
Total	733.4	847.5	977.0	1,123.6	1,289.3	1,475.7	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

10 DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE

KEY FINDINGS

- By solution type, the network traffic analyzers segment is estimated to account for the second-largest market size of USD 1,687.0 million in 2026. It is projected to reach USD 3,097.6 million by 2031, at a CAGR of 12.9% during the forecast period.
- The botnet detection & management segment is projected to register the highest CAGR of 13.9% during the forecast period, reaching USD 1,794.4 million by 2031.
- The demand for DDoS protection and mitigation solutions is expected to grow rapidly over the next five years, as the sophistication level of DDoS attacks increases and the need to protect organizations' network infrastructure becomes more pressing.
- Increased awareness among businesses about the potential financial and reputational damage from DDoS attacks is driving investment in comprehensive protection solutions.

10.1 INTRODUCTION

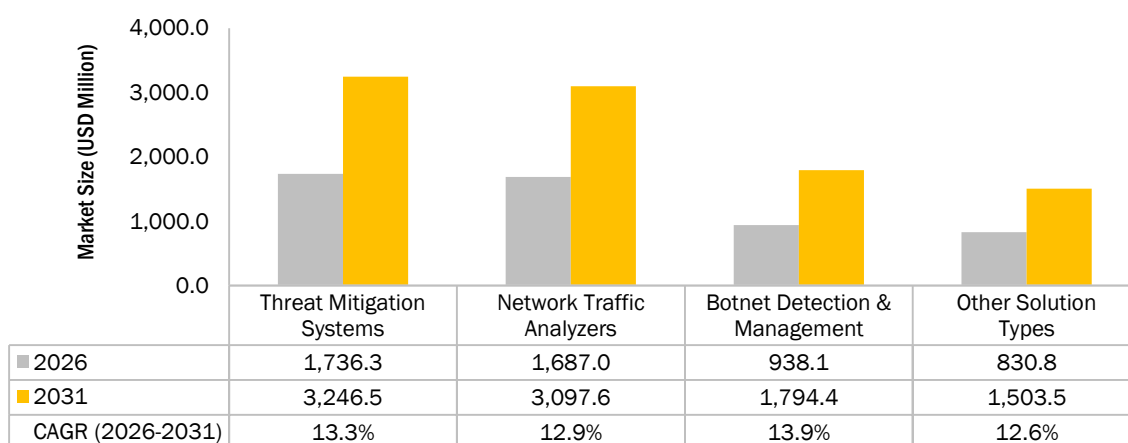
The cybersecurity landscape faces significant threats from increasingly sophisticated DDoS attacks. Cybercriminals utilize advanced hacking tools to infiltrate organizations' network infrastructures, obstructing legitimate traffic and disrupting vital services, often resulting in financial losses that can reach millions of dollars. The motivations for these attacks vary widely, including extortion, vandalism, and competitive rivalry.

Considering this escalating threat, organizations across various sectors, including retail, banking, government, healthcare, and manufacturing, are increasingly investing in advanced DDoS protection and mitigation solutions. This shift is also fueled by a growing recognition of the need to defend against severe volumetric attacks that can render operations incapacitated. The DDoS protection & mitigation market has emerged as a focal point, with solutions spanning network security, application security, database security, and endpoint security. As the need for strong cybersecurity measures increases, software solutions play a vital role in the DDoS protection landscape. These tools not only identify and respond to threats but also offer comprehensive prevention and recovery strategies. By harnessing technologies such as machine learning and artificial intelligence, organizations can enhance their defenses against complex DDoS attack vectors, thereby ensuring the protection of their digital assets in an evolving threat environment.

10.1.1 SOLUTION TYPE: DDOS PROTECTION AND MITIGATION MARKET DRIVERS

- The growing shift toward cloud-based services drives demand for DDoS protection solutions that can secure cloud environments against potential vulnerabilities and attacks.
- Organizations are increasingly required to comply with stringent cybersecurity regulations, prompting investments in DDoS mitigation systems to ensure compliance and protect sensitive data.
- There is a heightened need for threat mitigation systems that provide immediate responses to attacks, minimizing downtime and preserving business continuity.

FIGURE 34 BOTNET DETECTION & MANAGEMENT SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 57 DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	717.7	837.4	971.3	1,118.1	1,280.0	1,483.7	15.6%
Threat Mitigation Systems	723.1	847.0	986.1	1,139.0	1,307.9	1,521.0	16.0%
Botnet Detection & Management	376.5	443.7	519.8	604.5	699.2	818.2	16.8%
Other Solution Types	357.1	416.2	482.2	554.2	633.3	732.4	15.5%
Total	2,174.4	2,544.4	2,959.4	3,415.9	3,920.3	4,555.3	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 58 DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	1,687.0	1,913.6	2,165.7	2,445.5	2,755.1	3,097.6	12.9%
Threat Mitigation Systems	1,736.3	1,977.3	2,246.1	2,545.5	2,878.3	3,246.5	13.3%
Botnet Detection & Management	938.1	1,072.9	1,224.3	1,393.9	1,582.9	1,794.4	13.9%
Other Solution Types	830.8	940.0	1,061.0	1,194.6	1,341.8	1,503.5	12.6%
Total	5,192.2	5,903.8	6,697.1	7,579.4	8,558.2	9,642.0	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

10.2 NETWORK TRAFFIC ANALYZERS

10.2.1 NETWORK LAYER ATTACKS TO INCREASE ADOPTION OF DDOS PROTECTION SOLUTIONS

Network analyzers play a crucial role in the DDoS protection and mitigation market by providing organizations with the tools needed to monitor, analyze, and respond to potential DDoS attacks effectively. These solutions continuously assess network traffic, enabling early detection of anomalies that may indicate an ongoing attack.

By establishing a baseline of normal traffic behavior, network analyzers can identify deviations that signal malicious activity. Techniques such as flow analysis and anomaly detection enhance the ability to spot unusual patterns associated with DDoS attacks. This proactive monitoring allows IT teams to implement rapid responses, mitigating the potential impact on critical infrastructure. Advanced network analyzers also facilitate real-time traffic filtering and rate limiting, ensuring that legitimate requests are prioritized while blocking malicious traffic. This dual approach not only protects against volumetric attacks but also preserves the overall performance of network services.

Furthermore, integration with machine learning algorithms enhances detection capabilities, allowing organizations to adapt to evolving attack vectors. As cyber threats become increasingly sophisticated, the importance of robust network analyzers in safeguarding against DDoS attacks continues to grow, making them a crucial component of comprehensive cybersecurity strategies.

TABLE 59 DDOS PROTECTION AND MITIGATION NETWORK TRAFFIC ANALYZERS MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	295.9	336.2	379.4	424.6	472.2	534.0	12.5%
Europe	181.9	213.8	249.6	289.1	332.4	386.8	16.3%
Asia Pacific	136.0	164.4	197.5	235.6	279.7	336.1	19.8%
Middle East & Africa	73.6	86.8	101.8	118.5	137.2	160.8	16.9%
Latin America	30.3	36.2	42.9	50.3	58.5	66.0	16.8%
Total	717.7	837.4	971.3	1,118.1	1,280.0	1,483.7	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 60 DDOS PROTECTION AND MITIGATION NETWORK TRAFFIC ANALYZERS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	596.4	664.5	738.7	819.1	906.2	1,000.7	10.9%
Europe	441.2	501.9	569.3	644.1	726.1	821.9	13.2%
Asia Pacific	388.8	448.7	516.7	593.5	680.2	777.9	14.9%
Middle East & Africa	184.8	211.9	241.0	273.4	309.5	349.6	13.6%
Latin America	75.7	86.6	100.1	115.3	133.1	147.5	14.3%
Total	1,687.0	1,913.6	2,165.7	2,445.5	2,755.1	3,097.6	12.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

10.3 THREAT MITIGATION SYSTEMS

10.3.1 RISE IN LAYER 7 ATTACKS TO INCREASE DEMAND FOR DDOS PROTECTION AND MITIGATION SOLUTIONS

Threat mitigation systems are essential software solutions in the DDoS protection and mitigation market, designed to effectively counteract and neutralize DDoS attacks. These systems automatically detect and respond to malicious traffic, ensuring that legitimate users continue to have access to network services. By employing advanced traffic filtering techniques, threat mitigation systems can distinguish between harmful and legitimate traffic, allowing only the latter to pass through. This capability is crucial for maintaining service availability during an attack. Key features include real-time monitoring, which enables organizations to identify unusual traffic patterns indicative of an ongoing DDoS attack.

These systems integrate seamlessly with existing network infrastructure, providing scalable solutions that can handle varying levels of attack intensity. They employ machine learning algorithms to enhance detection accuracy, adapting to new attack vectors as they emerge.

Threat mitigation systems often include automated response mechanisms that implement predefined countermeasures upon detecting an attack. This rapid response is vital for minimizing downtime and preserving business continuity. As DDoS threats continue to evolve, the role of threat mitigation systems becomes increasingly critical in safeguarding organizational assets and ensuring uninterrupted service delivery.

TABLE 61 DDOS PROTECTION AND MITIGATION THREAT MITIGATION SYSTEMS MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	330.7	380.5	434.7	492.4	554.2	634.0	13.9%
Europe	167.6	197.3	230.8	267.8	308.7	360.1	16.5%
Asia Pacific	118.2	142.1	170.0	202.0	238.8	285.7	19.3%
Middle East & Africa	80.4	95.9	113.7	133.8	156.5	185.3	18.2%
Latin America	26.3	31.2	36.8	43.0	49.7	55.9	16.3%
Total	723.1	847.0	986.1	1,139.0	1,307.9	1,521.0	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 62 DDOS PROTECTION AND MITIGATION THREAT MITIGATION SYSTEMS MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	716.2	807.2	907.6	1,018.4	1,140.2	1,272.2	12.2%
Europe	411.9	469.9	534.7	606.8	686.4	779.8	13.6%
Asia Pacific	329.2	378.3	433.7	496.1	566.1	644.6	14.4%
Middle East & Africa	215.2	249.4	286.6	328.5	375.6	428.6	14.8%
Latin America	63.8	72.5	83.5	95.7	110.0	121.3	13.7%
Total	1,736.3	1,977.3	2,246.1	2,545.5	2,878.3	3,246.5	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

10.4 BOTNET DETECTION & MANAGEMENT

10.4.1 EVOLVING DISRUPTIVE TECHNOLOGIES AND EASY AVAILABILITY OF CLOUD-BASED APPLICATIONS TO DRIVE MARKET

Botnet detection and management are critical software solutions within the DDoS protection and mitigation market, specifically designed to identify and neutralize botnets that orchestrate DDoS attacks. These systems continuously monitor network traffic to detect unusual patterns that may indicate the presence of compromised devices.

By employing advanced analytics and machine learning algorithms, botnet detection tools can effectively distinguish between legitimate and malicious traffic. This capability is essential for recognizing botnet activity before it escalates into a full-blown DDoS attack. The systems analyze data packets from various protocols, such as TCP and UDP, to identify irregularities that suggest botnet behavior. Once a botnet is detected, management solutions implement countermeasures to mitigate its impact. This includes blocking communication with infected devices, thereby preventing them from executing coordinated attacks. Additionally, these tools often provide real-time alerts and detailed reporting, enabling organizations to respond swiftly to emerging threats.

As the sophistication of botnets increases, effective detection and management solutions become vital for maintaining network integrity and ensuring uninterrupted service availability. By leveraging these technologies, organizations can significantly enhance their defenses against the growing threat of DDoS attacks orchestrated by botnets.

TABLE 63 DDOS PROTECTION AND MITIGATION BOTNET DETECTION & MANAGEMENT MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	125.6	143.7	163.3	184.1	206.3	235.3	13.4%
Europe	108.5	128.1	150.3	174.8	201.9	236.0	16.8%
Asia Pacific	88.7	107.8	130.4	156.5	186.9	226.0	20.6%
Middle East & Africa	33.6	39.9	47.2	55.3	64.4	76.0	17.7%
Latin America	20.1	24.1	28.8	33.9	39.6	45.0	17.5%
Total	376.5	443.7	519.8	604.5	699.2	818.2	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 64 DDOS PROTECTION AND MITIGATION BOTNET DETECTION & MANAGEMENT MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	265.0	297.6	333.4	372.4	414.9	462.4	11.8%
Europe	270.3	308.8	351.8	399.8	452.6	514.4	13.7%
Asia Pacific	263.0	305.3	353.6	408.5	470.8	541.5	15.5%
Middle East & Africa	88.0	101.6	116.3	132.9	151.6	172.4	14.4%
Latin America	51.9	59.6	69.3	80.2	93.1	103.7	14.9%
Total	938.1	1,072.9	1,224.3	1,393.9	1,582.9	1,794.4	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

10.5 OTHER SOLUTION TYPES

In the DDoS protection and mitigation market, orchestration and management and threat intelligence are important solution types that enhance the effectiveness and responsiveness of DDoS defense strategies. Orchestration and management solutions provide centralized visibility and control over DDoS protection environments, enabling organizations to configure security policies, coordinate mitigation workflows, automate response actions, and manage protection across distributed network, application, and cloud environments. These capabilities help security teams reduce manual intervention and accelerate response times during attacks. Threat intelligence solutions complement DDoS protection by providing contextual and actionable information on emerging attack vectors, malicious IP addresses, botnets, attack patterns, and other indicators associated with DDoS activity. By integrating threat intelligence with DDoS protection platforms, organizations can improve the identification of malicious traffic and proactively strengthen mitigation policies. The growing complexity and frequency of multi-vector DDoS attacks are increasing the need for centralized management, automated mitigation, and timely threat intelligence to improve organizational resilience and maintain the availability of critical digital services.

Anomaly detection technology focuses on recognizing unusual patterns in network traffic that could indicate a DDoS attack. By establishing a baseline of normal operations, these systems can quickly alert security teams to deviations requiring immediate action, which is crucial for minimizing potential damage.

Orchestration and automation streamline the response to DDoS threats by coordinating various security tools and processes. Automation enables the rapid deployment of countermeasures without manual intervention, thereby significantly reducing response times during an attack. Orchestration ensures that all

offerings of the security infrastructure function together seamlessly, enhancing overall effectiveness in mitigating DDoS attacks.

Together, these solution types create a robust defense strategy against DDoS threats, empowering organizations to proactively protect their networks and maintain operational integrity in an increasingly hostile cyber environment.

TABLE 65 OTHER DDOS PROTECTION AND MITIGATION SOLUTION TYPES MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	144.1	165.0	187.5	211.5	236.9	269.9	13.4%
Europe	92.5	107.9	125.0	143.7	164.1	189.6	15.4%
Asia Pacific	67.7	80.9	96.1	113.3	133.0	157.9	18.5%
Middle East & Africa	35.6	42.2	49.7	58.1	67.5	79.5	17.5%
Latin America	17.3	20.4	23.9	27.7	31.8	35.4	15.5%
Total	357.1	416.2	482.2	554.2	633.3	732.4	15.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 66 OTHER DDOS PROTECTION AND MITIGATION SOLUTION TYPES MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	303.6	340.7	381.3	425.7	474.2	527.0	11.7%
Europe	214.7	242.6	273.4	307.3	344.2	387.2	12.5%
Asia Pacific	180.4	205.6	233.7	265.0	299.7	338.3	13.4%
Middle East & Africa	91.8	105.7	120.8	137.6	156.4	177.4	14.1%
Latin America	40.2	45.4	51.8	59.0	67.2	73.6	12.9%
Total	830.8	940.0	1,061.0	1,194.6	1,341.8	1,503.5	12.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

11 DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA

KEY FINDINGS

- By application area, the network and IP infrastructure segment is estimated to account for the largest market size of USD 2,435.8 million in 2026, and it is projected to reach USD 4,635.5 million by 2031, at a CAGR of 13.7% during the forecast period.
- The web applications and APIs segment is projected to register the highest CAGR of 14.9% during the forecast period and reach USD 4,732.2 million by 2031.
- The migration of workloads and applications to cloud and hybrid environments, combined with increasingly distributed IT infrastructure, is increasing the complexity of protecting network and IP resources against DDoS attacks.
- DDoS attacks can result in application downtime, loss of customer access, revenue losses, and reputational damage. The growing focus on business continuity, service availability, and resilience is encouraging organizations to deploy DDoS protection across critical network, application, API, and DNS infrastructure.

11.1 INTRODUCTION

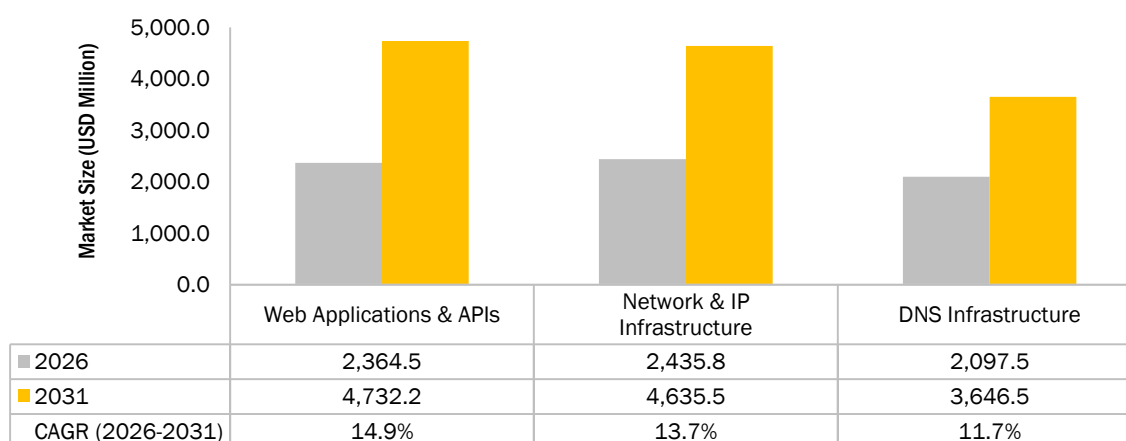
Cybercriminals use increasingly sophisticated tools and techniques to target organizations' digital infrastructure and disrupt the availability of legitimate services. DDoS attacks can overwhelm network resources, applications, APIs, and DNS infrastructure with malicious traffic, resulting in degraded performance, service unavailability, operational disruptions, and significant financial losses. Attackers may launch DDoS attacks for various motives, including extortion, vandalism, political disputes, competitive rivalry, financial gain, and disruption of critical services.

The growing adoption of DDoS protection and mitigation solutions and services across industries such as retail, BFSI, government and defense, healthcare, manufacturing, and other sectors is driving the need to protect multiple internet-facing infrastructure components. Accordingly, the DDoS protection and mitigation market has been segmented by application area into network & IP infrastructure, web applications & APIs, and DNS infrastructure. network & IP infrastructure protection focuses on safeguarding network connectivity, IP addresses, routers, and other network resources against traffic-based and protocol-level attacks. Web Applications & APIs protection addresses attacks targeting websites, web applications, APIs, and application-layer resources, while DNS infrastructure protection helps maintain the availability and integrity of DNS services that enable users and applications to access internet-facing resources. Increasing dependence on digital services, cloud infrastructure, APIs, and internet-based applications is further driving organizations to implement DDoS protection across these critical application areas.

11.1.1 APPLICATION AREA: DDOS PROTECTION AND MITIGATION MARKET DRIVERS

- The growing scale, complexity, and multi-vector nature of DDoS attacks are driving organizations to strengthen protection across network infrastructure, applications, APIs, and DNS environments.
- The expansion of web applications, APIs, digital platforms, and online services is increasing the attack surface, particularly at the application layer, creating greater demand for dedicated protection of web applications & APIs.
- DNS serves as a critical component for accessing websites, applications, APIs, and other internet-based services. Disruption of DNS infrastructure can affect multiple downstream services, increasing the need for dedicated DNS protection and mitigation capabilities.

FIGURE 35 WEB APPLICATIONS AND APIS SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 67 DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	990.8	1,165.1	1,361.6	1,579.3	1,821.3	2,126.7	16.5%
Web Applications & APIs	900.9	1,071.4	1,266.2	1,484.8	1,731.0	2,042.8	17.8%
DNS Infrastructure	943.3	1,091.4	1,254.8	1,431.4	1,623.2	1,863.3	14.6%
Total	2,835.0	3,327.8	3,882.6	4,495.6	5,175.5	6,032.8	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 68 DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	2,435.8	2,783.2	3,172.6	3,608.2	4,094.3	4,635.5	13.7%
Web Applications & APIs	2,364.5	2,729.8	3,143.7	3,611.5	4,139.0	4,732.2	14.9%
DNS Infrastructure	2,097.5	2,354.9	2,637.1	2,945.4	3,281.4	3,646.5	11.7%
Total	6,897.7	7,867.9	8,953.4	10,165.1	11,514.7	13,014.3	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

11.2 NETWORK & IP INFRASTRUCTURE

11.2.1 INCREASING NEED FOR HIGH-CAPACITY, ALWAYS-ON PROTECTION CAPABLE OF ABSORBING AND FILTERING MALICIOUS TRAFFIC

Network & IP infrastructure encompasses the network-layer and transport-layer resources that enable connectivity between users, devices, applications, and digital services. DDoS attacks targeting these resources primarily operate at Layers 3 and 4 of the OSI model and can overwhelm bandwidth, exhaust connection states, or consume network resources, resulting in congestion and service unavailability. Common attack vectors include UDP floods, SYN floods, ICMP floods, DNS amplification, and other reflection and amplification attacks. The growing scale of these attacks is increasing the need for high-capacity, always-on protection capable of absorbing and filtering malicious traffic before it reaches critical infrastructure. According to Cloudflare, 34.4 million network-layer DDoS attacks were mitigated in 2025, more than three times the 11.4 million recorded in 2024. In addition, Cloudflare reported that network-layer attacks accounted for 78% of all DDoS attacks in Q4 2025. Radware also reported that network-layer DDoS attacks increased 84% in H1 2025 compared with H2 2024, highlighting the growing requirement for resilient network and IP infrastructure.

TABLE 69 DDOS PROTECTION AND MITIGATION MARKET IN NETWORK & IP INFRASTRUCTURE, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	408.4	469.5	536.0	606.9	682.8	781.2	13.9%
Europe	250.8	296.3	347.7	404.7	467.9	547.4	16.9%
Asia Pacific	187.1	226.7	273.3	327.0	389.5	469.5	20.2%
Middle East & Africa	101.7	121.2	143.7	169.1	197.7	234.2	18.2%
Latin America	42.8	51.3	60.9	71.6	83.4	94.5	17.1%
Total	990.8	1,165.1	1,361.6	1,579.3	1,821.3	2,126.7	16.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 70 DDOS PROTECTION AND MITIGATION MARKET IN NETWORK & IP INFRASTRUCTURE, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	882.5	994.7	1,118.5	1,254.7	1,404.4	1,568.4	12.2%
Europe	627.8	718.0	819.2	932.1	1,056.9	1,203.6	13.9%
Asia Pacific	544.8	630.7	728.4	839.3	964.9	1,106.8	15.2%
Middle East & Africa	272.0	315.2	362.3	415.3	475.1	542.3	14.8%
Latin America	108.6	124.5	144.3	166.7	193.0	214.5	14.6%
Total	2,435.8	2,783.2	3,172.6	3,608.2	4,094.3	4,635.5	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

11.3 WEB APPLICATIONS & APIS

11.3.1 RISING NEED TO MITIGATE DDOS ATTACKS AND MAINTAIN PROTECTION

Web applications & APIs are increasingly targeted by application-layer DDoS attacks designed to exhaust application resources rather than saturate network bandwidth. These attacks can generate large volumes of seemingly legitimate HTTP requests, target resource-intensive functions, or exploit application and API logic, making them more difficult to distinguish from genuine user traffic. The rapid expansion of digital services, API-driven architectures, e-commerce platforms, and cloud-hosted applications is consequently increasing the attack surface and demand for specialized application-layer DDoS protection. According to Akamai, the volume of Layer 7 DDoS attacks targeting web applications and APIs increased 94% between Q1 2023 and Q4 2024, rising from slightly more than 500 billion monthly attacks to over 1.1 trillion. Radware's 2025 Global Threat Analysis further reported that Web DDoS attacks increased almost 550% year over year compared with 2023, with individual attacks reaching peaks of 14.7 million and 16 million requests per second. These trends are driving demand for behavioral analytics, automated mitigation, rate limiting, and application-aware traffic inspection.

TABLE 71 DDOS PROTECTION AND MITIGATION MARKET IN WEB APPLICATIONS & APIS, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	371.3	431.8	498.4	570.6	648.9	750.4	15.1%
Europe	228.1	272.5	323.3	380.5	444.7	525.8	18.2%
Asia Pacific	170.1	208.5	254.1	307.5	370.2	451.0	21.5%
Middle East & Africa	92.4	111.5	133.6	158.9	187.9	224.9	19.5%
Latin America	38.9	47.2	56.7	67.3	79.3	90.7	18.4%
Total	900.9	1,071.4	1,266.2	1,484.8	1,731.0	2,042.8	17.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 72 DDOS PROTECTION AND MITIGATION MARKET IN WEB APPLICATIONS & APIS, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	856.7	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	38.7%
Europe	609.4	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	40.9%
Asia Pacific	528.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	42.5%
Middle East & Africa	264.1	891.1	1,022.3	1,170.1	1,336.2	1,522.5	42.0%
Latin America	105.4	351.9	407.2	469.7	542.7	602.1	41.7%
Total	2,364.5	7,867.9	8,953.4	10,165.1	11,514.7	13,014.3	40.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

11.4 DNS INFRASTRUCTURE

11.4.1 INCREASING DEPENDENCE ON ONLINE APPLICATIONS AND DISTRIBUTED DIGITAL INFRASTRUCTURE IS DRIVING MARKET

DNS (Domain Name System) infrastructure is a critical application area for DDoS protection because DNS enables users, applications, and connected devices to locate and access internet-facing resources. DDoS attacks against DNS infrastructure can overwhelm authoritative or recursive DNS servers, generate excessive query volumes, or exploit DNS reflection and amplification techniques, potentially preventing legitimate users from resolving domain names and accessing associated services. The increasing dependence on online applications and distributed digital infrastructure is therefore driving organizations to strengthen DNS resilience through dedicated traffic analysis, filtering, rate limiting, and automated mitigation capabilities. Cloudflare's H1 2026 DDoS Threat Report found that DNS-based attacks accounted for 34.3% of all network-layer DDoS activity during the first half of 2026, while DNS floods alone increased from 25.7% to 40.0% of network-layer attacks between Q1 and Q2. Similarly, Akamai reported that DNS attacks remain a leading volumetric DDoS vector in financial services, with DNS flood activity increasing 29% year over year in 2025. The increasing frequency of DNS floods and amplification attacks is consequently strengthening demand for resilient and continuously available DNS protection.

TABLE 73 DDOS PROTECTION AND MITIGATION MARKET IN DNS INFRASTRUCTURE, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	388.8	439.8	493.9	550.1	608.5	684.4	12.0%
Europe	238.8	277.5	320.4	366.8	417.0	479.6	15.0%
Asia Pacific	178.1	212.4	251.8	296.4	347.1	411.4	18.2%
Middle East & Africa	96.8	113.6	132.4	153.2	176.2	205.2	16.2%
Latin America	40.8	48.0	56.1	64.9	74.4	82.8	15.2%
Total	943.3	1,091.4	1,254.8	1,431.4	1,623.2	1,863.3	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 74 DDOS PROTECTION AND MITIGATION MARKET IN DNS INFRASTRUCTURE, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	760.0	841.6	929.7	1,024.2	1,125.6	1,233.8	10.2%
Europe	540.6	607.6	680.9	760.9	847.1	946.8	11.9%
Asia Pacific	469.2	533.7	605.5	685.1	773.3	870.7	13.2%
Middle East & Africa	234.2	266.7	301.1	339.0	380.8	426.6	12.7%
Latin America	93.5	105.3	119.9	136.1	154.7	168.7	12.5%
Total	2,097.5	2,354.9	2,637.1	2,945.4	3,281.4	3,646.5	11.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

12 DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE

KEY FINDINGS

- By deployment mode, the cloud segment is projected to register the highest CAGR of 14.1% during the forecast period. This segment is projected to reach USD 5,996.3 million by 2031.
- Cloud DDoS protection and mitigation services are expected to gain traction among SMEs, as they are cost-efficient and do not require the purchase of hardware or software, nor the costs associated with installation or maintenance.
- North America is expected to dominate the cloud segment as organizations in the region rapidly adopt SaaS-based applications.
- The on-premises segment is projected to grow from USD 2,202.4 million in 2026 to USD 4,010.2 million by 2031, at a CAGR of 12.7% during the forecast period.
- The on-premises deployment mode is popular mostly among large organizations, particularly in verticals such as BFSI and government, where critical data is stored on-premises.

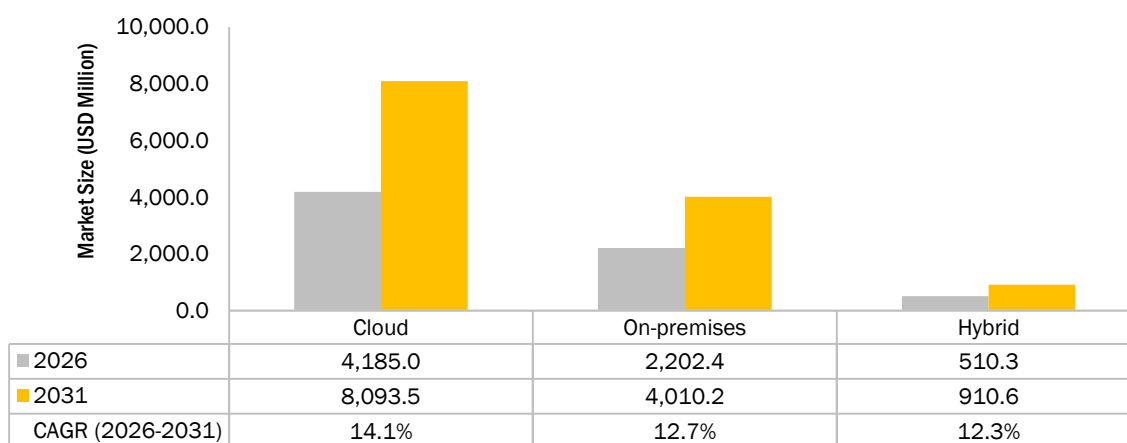
12.1 INTRODUCTION

DDoS protection and mitigation solutions and services can be deployed on-premises or in the cloud, as needed to meet business requirements. The on-premises deployment mode enables organizations to control all systems and data; however, organizations must bear the costs for hardware, software, and other resources. Additionally, this deployment mode restricts the storage capacity necessary for maintaining new functionalities and technologies. The cloud deployment mode offers increased scalability, speed, 24/7 support services, and improved IT security. The demand for SaaS-based DDoS protection solutions is expected to increase, as its central delivery model meets IT security needs. The hybrid deployment mode enables organizations to keep critical data on their premises and transfer non-critical data to a cloud environment.

12.1.1 DEPLOYMENT MODE: DDoS PROTECTION AND MITIGATION MARKET DRIVERS

- Cost-effectiveness and scalability will pave the way for organizations to adopt cloud-based DDoS protection and mitigation solutions.
- The market for cloud-based products related to DDoS protection and mitigation is expected to grow as SMEs increasingly adopt these solutions.
- Cloud deployment involves less capital investment and IT resources, thus benefiting SMEs by helping them overcome budgetary constraints.
- The government, defense, and BFSI verticals are likely to prefer on-premises deployment of DDoS protection solutions and services because they cannot afford to put national security at risk by losing sensitive data, financial records, accounting information, and information related to monetary transactions.
- Increasing multi-vector DDoS attacks will fuel the adoption of hybrid DDoS protection and mitigation solutions.

FIGURE 36 CLOUD SEGMENT TO RECORD FASTER GROWTH DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 75 DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	947.7	1,103.8	1,277.9	1,468.2	1,677.1	1,940.2	15.4%
Cloud	1,678.1	1,978.1	2,317.6	2,694.8	3,115.4	3,646.1	16.8%
Hybrid	209.2	245.9	287.1	332.6	383.0	446.4	16.4%
Total	2,835.0	3,327.8	3,882.6	4,495.6	5,175.5	6,032.8	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 76 DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	2,202.4	2,494.2	2,818.2	3,177.0	3,573.7	4,010.2	12.7%
Cloud	4,185.0	4,791.8	5,473.6	6,237.7	7,092.1	8,093.5	14.1%
Hybrid	510.3	581.8	661.6	750.4	848.9	910.6	12.3%
Total	6,897.7	7,867.9	8,953.4	10,165.1	11,514.7	13,014.3	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

12.2 ON-PREMISES

12.2.1 ON-PREMISE SERVICES PROVIDE FULL CONTROL OF DEPLOYED SOLUTIONS TO IT STAFF

On-premise deployment is the traditional approach to implementing DDoS protection solutions and services across organizations. On-premise services provide organizations with full control over all the platforms, applications, systems, networks, and data. The organization's IT staff can handle and manage the deployed solutions. The on-premise deployment mode also provides local detection and mitigation of DDoS attacks, such as spoofed/non-spoofed DoS attacks, TCP (such as SYN flood and FIN flood), ICMP, UDP floods, botnets, Slowloris, application attacks, HTTP URLGET/POST floods, malformed HTTP header attacks, slow-HTTP request attacks, SYN floods against SSL protocols, malformed SSL attacks, SSL renegotiation attacks, SSL exhaustion, DNS attacks, and Session Initiation Protocol (SIP) request floods.

TABLE 77 ON-PREMISE DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	420.6	479.4	542.5	608.9	678.9	769.8	12.8%
Europe	227.0	266.0	309.7	357.7	410.2	476.1	16.0%
Asia Pacific	169.3	203.6	243.4	289.0	341.5	408.4	19.3%
Middle East & Africa	92.0	108.8	128.0	149.4	173.4	203.7	17.2%
Latin America	38.8	46.0	54.3	63.3	73.1	82.2	16.2%
Total	947.7	1,103.8	1,277.9	1,468.2	1,677.1	1,940.2	15.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 78 ON-PREMISE DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	862.0	962.9	1,073.2	1,193.5	1,324.5	1,465.8	11.2%
Europe	541.8	614.8	695.9	785.6	883.7	998.4	13.0%
Asia Pacific	470.2	540.0	618.8	707.4	806.8	918.2	14.3%
Middle East & Africa	234.7	269.9	307.7	350.0	397.3	449.9	13.9%
Latin America	93.7	106.6	122.6	140.5	161.4	177.9	13.7%
Total	2,202.4	2,494.2	2,818.2	3,177.0	3,573.7	4,010.2	12.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

12.3 CLOUD

12.3.1 CLOUD DEPLOYMENT HELPS MANAGE DNS, REROUTE TRAFFIC, AND SAFEGUARD WEBSITE TRAFFIC

Cloud is a fast-growing deployment mode in the DDoS protection and mitigation market, especially among SMEs, as it is cost-effective. Cloud deployment helps SMEs avoid costs related to hardware, software, storage, and technical staff.

SMEs have implemented cloud services to focus on their core competencies rather than investing in security infrastructure. Cloud-based solutions utilize detection and scrubbing technologies to mitigate DDoS attacks. By deploying DDoS protection and mitigation solutions and services on the cloud, organizations can avoid spending on hardware, software, storage, and technical staff.

The cloud deployment mode also helps protect and mitigate DDoS attacks. It helps in managing DNS, rerouting traffic, and safeguarding website traffic. Security Operations Centers (SOCs) support and facilitate threat management. Additionally, organizations can scale up or down, depending on their use of services.

The findings from the Cloud Security Alliance (CSA) survey, titled "Cloud Adoption, Practices, and Priorities Survey Report," state that although data security remains one of the top barriers to cloud adoption, organizations are still adopting cloud services. According to the survey, 74% of respondents indicated that they are either moving the full team forward or exercising caution when adopting cloud services.

TABLE 79 CLOUD-BASED DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	660.9	761.8	871.8	989.7	1,116.4	1,280.6	14.1%
Europe	438.1	518.1	608.9	709.7	821.5	962.3	17.0%
Asia Pacific	326.8	396.5	478.6	573.4	683.8	825.5	20.4%
Middle East & Africa	177.5	212.0	251.7	296.4	347.2	411.7	18.3%
Latin America	74.8	89.7	106.7	125.6	146.5	166.1	17.3%
Total	1,678.1	1,978.1	2,317.6	2,694.8	3,115.4	3,646.1	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 80 CLOUD-BASED DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,450.7	1,639.2	1,847.9	2,078.1	2,331.6	2,615.2	12.5%
Europe	1,105.1	1,265.7	1,445.9	1,647.4	1,870.5	2,149.7	14.2%
Asia Pacific	959.1	1,111.8	1,285.7	1,483.4	1,707.6	1,976.9	15.6%
Middle East & Africa	478.9	555.7	639.4	734.1	840.8	968.6	15.1%
Latin America	191.2	219.4	254.7	294.7	341.5	383.0	14.9%
Total	4,185.0	4,791.8	5,473.6	6,237.7	7,092.1	8,093.5	14.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

12.4 HYBRID

12.4.1 ENABLE ORGANIZATIONS TO DISTRIBUTE PROTECTION ACCORDING TO THE CHARACTERISTICS AND SCALE OF THEIR INFRASTRUCTURE

Hybrid deployment mode combines cloud-based DDoS protection with on-premises or network-edge mitigation capabilities, enabling organizations to distribute protection according to the characteristics and scale of their infrastructure. In this model, on-premises appliances can provide rapid detection and mitigation of attacks that require low-latency, local enforcement, while cloud-based scrubbing capabilities can absorb large-scale volumetric attacks that could overwhelm Internet links or on-premises appliances. This approach is particularly relevant for organizations operating hybrid IT environments across data centers, private infrastructure, public clouds, and distributed networks. Cloudflare notes that on-premises hardware can be overwhelmed by volumetric attacks and bandwidth-constrained links, while cloud-based protection provides greater scalability for large attacks. The increasing scale and frequency of DDoS attacks is strengthening demand for such architectures. Cloudflare reported that it mitigated 47.1 million DDoS attacks in 2025, including 34.4 million network-layer attacks, more than triple the 2024 level. Radware also reported a 168.2% increase in DDoS attacks in 2025, while its average customer faced more than 25,351 attacks in H2 2025. These trends are encouraging organizations to adopt hybrid deployment models for scalable, resilient, and low-latency DDoS protection.

TABLE 81 HYBRID DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	86.9	99.9	114.0	128.9	144.9	165.5	13.7%
Europe	52.7	62.2	72.9	84.8	97.9	114.3	16.8%
Asia Pacific	39.3	47.6	57.3	68.5	81.5	98.0	20.1%
Middle East & Africa	21.3	25.4	30.1	35.4	41.4	48.9	18.0%
Latin America	9.0	10.8	12.8	15.0	17.4	19.7	17.0%
Total	209.2	245.9	287.1	332.6	383.0	446.4	16.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 82 **HYBRID DDOS PROTECTION AND MITIGATION MARKET, BY REGION,
2026–2031 (USD MILLION)**

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	186.6	209.8	235.3	263.2	293.6	322.3	11.6%
Europe	130.9	149.4	170.0	193.0	218.2	230.8	12.0%
Asia Pacific	113.6	131.2	151.2	173.8	199.2	212.3	13.3%
Middle East & Africa	56.7	65.6	75.2	86.0	98.1	104.0	12.9%
Latin America	22.6	25.9	29.9	34.5	39.8	41.1	12.7%
Total	510.3	581.8	661.6	750.4	848.9	910.6	12.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

13 DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE

KEY FINDINGS

- By organization size, the SMEs segment is projected to register a higher CAGR of 13.4% during the forecast period. It is projected to grow from USD 2,220.0 million in 2026 to USD 4,161.7 million by 2031.
- With the increasing adoption of BYOD and cloud-based applications for business operations, SMEs are adopting DDoS protection and mitigation solutions to protect their critical data from theft.
- The large enterprises segment is projected to grow from USD 3,586.3 million in 2026 to USD 6,228.6 million by 2031, at a CAGR of 11.7% during the forecast period.
- The Asia Pacific market is expected to witness the highest CAGR during the forecast period as SMEs, as well as large organizations in the region, are increasingly adopting DDoS protection and mitigation solutions for data security.

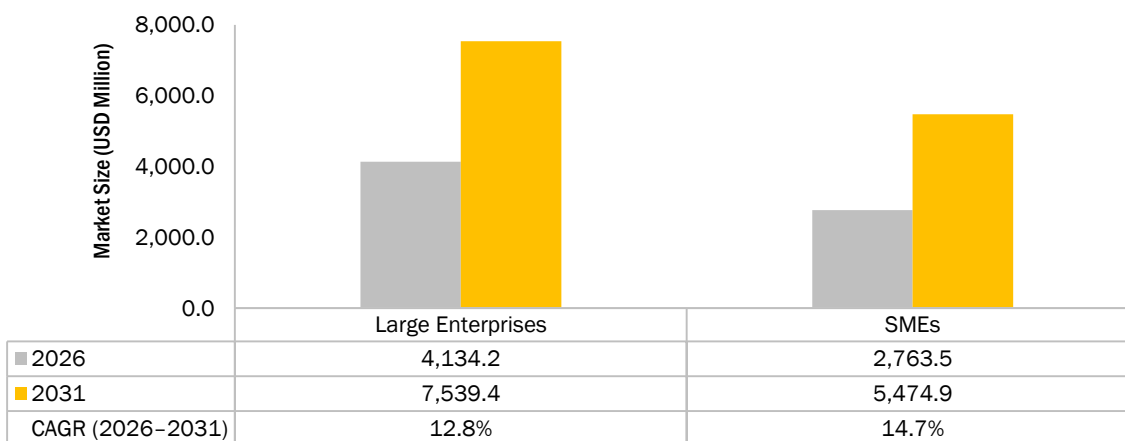
13.1 INTRODUCTION

Small & medium enterprises (SMEs) and large enterprises are focusing on leveraging DDoS protection and mitigation solutions to counter active and passive DDoS attacks. The success of all enterprises depends on the revenue model and loss prevention strategies. When one of these factors is hit hard, both enterprises suffer. To stay protected, organizations are incorporating DDoS security solutions. The adoption rate of advanced DDoS protection and mitigation solutions is expected to be higher among large enterprises, while it is growing among SMEs. Enterprises are well-protected from volumetric attacks and Layer 3, Layer 4, and Layer 7 DDoS attacks. A few critical DDoS attacks include HTTP flood, SYN flood, NTP amplification, and DNS amplification. The increasing adoption of DDoS protection and mitigation solutions among SMEs and large enterprises is expected to drive the growth of the DDoS protection and mitigation market.

13.1.1 ORGANIZATION SIZE: DDOS PROTECTION AND MITIGATION MARKET DRIVERS

- The growing need to secure data from vulnerabilities will fuel the adoption of DDoS protection and mitigation solutions in large enterprises.
- Large enterprises are more receptive to implementing DDoS protection and mitigation solutions to secure their data against vulnerabilities.
- Rising security issues compel SMEs to focus on the adoption of DDoS protection and mitigation solutions.
- SMEs use mobile devices to access organizational data. The growing usage of mobile devices fuels the growth of the DDoS protection and mitigation market.

FIGURE 37 SMES SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 83 DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020-2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020-2025)
SMEs	1,767.2	2,061.1	2,389.3	2,748.6	3,143.6	3,640.1	15.5%
Large Enterprises	1,067.8	1,266.7	1,493.3	1,747.0	2,031.9	2,392.7	17.5%
Total	2,835.0	3,327.8	3,882.6	4,495.6	5,175.5	6,032.8	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 84 DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
SMEs	4,134.2	4,684.1	5,294.5	5,970.3	6,717.1	7,539.4	12.8%
Large Enterprises	2,763.5	3,183.8	3,658.9	4,194.8	4,797.6	5,474.9	14.7%
Total	6,897.7	7,867.9	8,953.4	10,165.1	11,514.7	13,014.3	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

13.2 LARGE ENTERPRISES

13.2.1 INCREASING SEVERITY OF DDOS DAMAGE CAUSED BY SINGLE ATTACK TO DRIVE MARKET

Organizations with more than 1,000 employees are categorized as large enterprises. Large enterprises are the early adopters of DDoS protection and mitigation solutions and services, as they store a huge amount of confidential customer data. Moreover, their large business networks are susceptible to cyberattacks. As these enterprises have different types of IT infrastructures, they face significant difficulties in effectively reviewing and upgrading their current security systems due to the growing number of cyberattacks. A DDoS attack targeting large enterprises can range from 250 Mbps to 15 Gbps. The attack duration can be as short as 30 minutes, which is enough to bring the entire enterprise down. The rise in the adoption of DDoS protection solutions across large enterprises can be attributed to the increasing severity of DDoS damage caused by a single attack or accelerated traffic rates resulting from new network technologies, such as high-speed 5G mobile networks.

Recently, massive DDoS attacks were observed on the developer platform GitHub. GitHub experienced up to 1.35 Tbps of traffic, handling 126.9 million packets per second. The attack employed a Memcached-based approach, resulting in the disruption of GitHub.com's website services.

TABLE 85 DDOS PROTECTION AND MITIGATION MARKET FOR LARGE ENTERPRISES, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	723.9	825.4	934.3	1,049.0	1,170.0	1,327.1	12.9%
Europe	449.3	526.4	612.7	707.4	811.1	940.9	15.9%
Asia Pacific	335.1	402.9	481.6	571.6	675.1	807.1	19.2%
Middle East & Africa	182.1	215.4	253.2	295.5	342.8	402.5	17.2%
Latin America	76.7	91.1	107.4	125.2	144.6	162.4	16.2%
Total	1,767.2	2,061.1	2,389.3	2,748.6	3,143.6	3,640.1	15.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 86 DDOS PROTECTION AND MITIGATION MARKET FOR LARGE ENTERPRISES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,486.3	1,660.6	1,851.0	2,058.5	2,284.0	2,527.8	11.2%
Europe	1,070.2	1,213.9	1,373.2	1,549.3	1,741.8	1,966.6	12.9%
Asia Pacific	928.8	1,066.2	1,221.1	1,395.1	1,590.2	1,808.5	14.3%
Middle East & Africa	463.7	532.9	607.3	690.4	783.0	886.1	13.8%
Latin America	185.2	210.4	241.9	277.1	318.0	350.4	13.6%
Total	4,134.2	4,684.1	5,294.5	5,970.3	6,717.1	7,539.4	12.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

13.3 SMALL & MEDIUM-SIZED ENTERPRISES

13.3.1 GROWING NEED TO MITIGATE SECURITY ATTACKS TO ENHANCE MARKET GROWTH

Organizations with fewer than 1,000 employees are categorized as SMEs. These enterprises face a greater resource crunch than larger enterprises and require more effective methods to address the complexities of network infrastructure, thereby optimizing their business processes at a lower cost. With the increasing number of SMEs worldwide, the requirement for DDoS protection and mitigation solutions is increasing rapidly. SMEs have become the key target for cyber terrorists or hackers. SMEs need to assess their security systems and effectively close the gaps that slow down their server performance. Cybercriminals exploit the weak security in SMEs.

SMEs are focusing more on network management solutions to streamline their network infrastructure and enhance business functions. They also face challenges related to network management due to the increasingly complex network infrastructure, which is targeted by the growing network security attacks. Additionally, SMEs often have unknown gaps in their network security processes, combined with a lack of funds to employ a full-time network security expert, which makes them vulnerable to network breaches. SMEs have a lower security budget compared to large enterprises. They are easy targets because they are less protected and lack the resources and capabilities to detect theft and attacks.

It has become essential for SMEs to adopt DDoS protection techniques, including scrubbing services, BGP routing, sinkholing, null routing, and DNS routing, to mitigate the risks associated with DDoS attacks. SMEs are increasingly implementing DDoS protection and mitigation solutions to defend against threats such as HTTP floods, SYN floods, and NTP and DNS amplification attacks. In response to these challenges, the UK government has initiated measures to protect such businesses from cyberattacks by introducing data protection laws that require SMEs to implement appropriate security measures. Additionally, SMEs contribute approximately 50% to the country's GDP, underscoring the importance of protecting these businesses. These factors are expected to drive growth in the DDoS protection and mitigation market among SMEs.

TABLE 87 DDOS PROTECTION AND MITIGATION MARKET FOR SMALL & MEDIUM-SIZED ENTERPRISES, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	444.6	515.7	594.0	678.6	770.1	888.9	14.9%
Europe	268.4	319.9	378.8	444.7	518.6	611.8	17.9%
Asia Pacific	200.2	244.8	297.7	359.3	431.6	524.8	21.3%
Middle East & Africa	108.8	130.9	156.5	185.8	219.1	261.7	19.2%
Latin America	45.8	55.4	66.4	78.7	92.5	105.6	18.2%
Total	1,067.8	1,266.7	1,493.3	1,747.0	2,031.9	2,392.7	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 88 DDOS PROTECTION AND MITIGATION MARKET FOR SMALL & MEDIUM-SIZED ENTERPRISES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	1,012.9	1,151.3	1,305.4	1,476.4	1,665.7	1,875.5	13.1%
Europe	707.5	816.0	938.6	1,076.6	1,230.6	1,412.4	14.8%
Asia Pacific	614.1	716.8	834.6	969.5	1,123.5	1,298.9	16.2%
Middle East & Africa	306.6	358.2	415.1	479.7	553.2	636.4	15.7%
Latin America	122.4	141.5	165.3	192.6	224.7	251.7	15.5%
Total	2,763.5	3,183.8	3,658.9	4,194.8	4,797.6	5,474.9	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14 DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL

KEY FINDINGS

- By vertical, the BFSI segment is projected to register the highest CAGR of 15.5% during the forecast period, reaching a market size of USD 3,154.0 million by 2031.
- The IT & ITeS segment is projected to register the second-highest CAGR of 15.0% during the forecast period. This segment is projected to grow from USD 542.6 million in 2026 to USD 1,090.4 million by 2031.
- In the healthcare vertical, the use of DDoS protection and mitigation helps improve the efficiency of clinical and IT staff, providing real-time access in case of emergencies.
- The increased adoption of IoT-connected devices and the BYOD trend have expanded the attack surface, making networks more vulnerable. Regulatory compliance now necessitates DDoS protection and mitigation across various sectors.

14.1 INTRODUCTION

Based on vertical, the DDoS protection and mitigation market has been segmented into government and defense, BFSI, IT and ITeS, telecom, manufacturing, healthcare, energy and utilities, retail, education, and other verticals (ISP hosting, media and entertainment [including gaming], and transport and logistics). With the threat landscape continuously evolving across verticals, enterprises' awareness of sophisticated threats and the need to deploy advanced security solutions and services has increased over the years. Enterprise networks are frequently targeted by the most disruptive DDoS attacks, which threaten network performance, availability, and integrity.

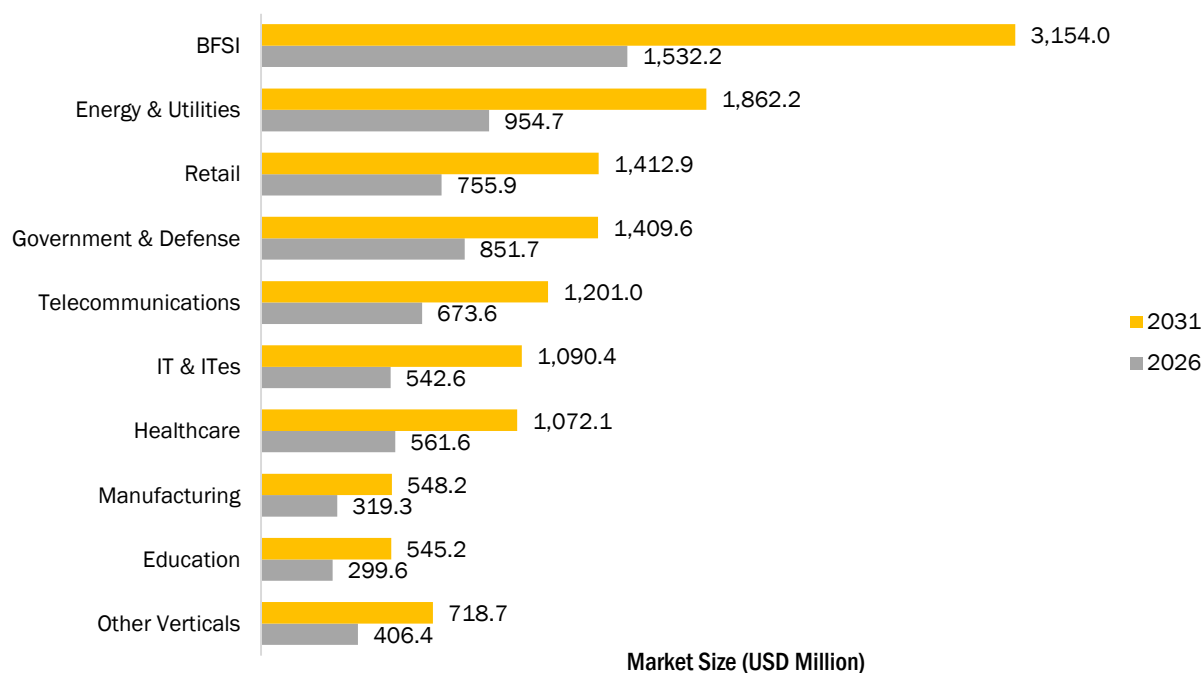
The increasing adoption of IoT-connected devices and the BYOD trend have expanded the attack surface, making networks more susceptible to infiltration and infection. Additionally, the need to comply with regulations has heightened the demand for DDoS protection and mitigation across various sectors. Businesses are not only focused on meeting government and industry regulations but are also implementing their own security guidelines and techniques to safeguard their environments.

Moreover, the shift toward cloud technology and the widespread use of mobile devices in enterprises have made organizational data more vulnerable to cyberattacks. As cyberattacks continue to rise, enterprises are increasingly adopting next-generation DDoS protection and mitigation solutions. These services utilize signature-based attack detection, signature-less attack detection, and behavioral analytics to enhance their security measures.

14.1.1 VERTICAL: DDOS PROTECTION AND MITIGATION MARKET DRIVERS

- Government and defense agencies must adhere to all regulations and serve as role models in adopting effective network security practices. Hence, government agencies are adopting the latest DDoS protection solutions available on the market.
- The increasing adoption of BYOD, MPOS, and IoT trends will drive demand for DDoS protection and mitigation solutions and services in the retail sector.
- Educational institutions are expected to deploy DDoS protection and mitigation to safeguard customers' sensitive information from increasing DDoS attacks.
- Healthcare organizations are increasingly relying on cloud services to store patient information. A DDoS attack can significantly impact the efficiency of these organizations.
- The increasing number of web and mobile applications will drive the adoption of DDoS protection and mitigation solutions in the IT and ITeS sectors.
- Protecting critical infrastructures, such as energy and utilities, from DDoS attacks is necessary to ensure 24/7 uptime in services. It is also one of the top priorities for governments.
- The increasing demand for upgrading security systems will drive the adoption of DDoS protection and mitigation solutions in the manufacturing vertical.
- The increasing need to protect information from DDoS-based attacks drives the adoption of DDoS protection and mitigation solutions in the BFSI vertical.

FIGURE 38 BFSI SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 89 DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	560.9	671.8	799.6	944.0	1,107.7	1,315.6	18.6%
Government & Defense	401.6	461.4	526.5	596.0	670.5	763.2	13.7%
Healthcare	227.6	267.8	313.2	363.5	419.4	490.0	16.6%
IT & ITes	205.6	244.8	289.6	339.9	396.6	468.4	17.9%
Telecommunications	295.4	343.1	396.0	453.7	516.7	595.7	15.1%
Manufacturing	145.5	168.0	192.7	219.4	248.2	284.3	14.3%
Energy & Utilities	376.4	445.0	522.8	609.6	706.6	829.3	17.1%
Retail	314.3	368.2	428.7	495.5	569.3	662.4	16.1%
Education	128.3	149.6	173.3	199.4	227.9	263.9	15.5%
Other Verticals	179.4	208.2	240.1	274.8	312.6	359.9	14.9%
Total	2,835.0	3,327.8	3,882.6	4,495.6	5,175.5	6,032.8	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 90 DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	1,532.2	1,779.5	2,061.2	2,381.2	2,743.8	3,154.0	15.5%
Government & Defense	851.7	947.7	1,051.2	1,162.7	1,282.0	1,409.6	10.6%
Healthcare	561.6	642.1	732.4	833.5	946.3	1,072.1	13.8%
IT & ITeS	542.6	627.0	722.7	830.9	953.0	1,090.4	15.0%
Telecommunications	673.6	759.9	855.1	960.0	1,075.0	1,201.0	12.3%
Manufacturing	319.3	357.7	399.6	445.2	494.8	548.2	11.4%
Energy & Utilities	954.7	1,096.3	1,256.0	1,435.5	1,636.8	1,862.2	14.3%
Retail	755.9	860.6	977.6	1,107.9	1,252.6	1,412.9	13.3%
Education	299.6	339.3	383.3	432.0	485.8	545.2	12.7%
Other Verticals	406.4	457.7	514.3	576.4	644.5	718.7	12.1%
Total	6,897.7	7,867.9	8,953.4	10,165.1	11,514.7	13,014.3	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.2 BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI)

14.2.1 FRAGILE DATA CENTER SECURITY AND RISK OF CLOUD STORAGE DATA LEAKS TO DRIVE MARKET

The BFSI vertical comprises a variety of institutions, including banking, insurance, securities, and finance, as well as non-banking financial organizations, which provide financial products and services. These institutions face distinctive challenges related to economic risks, such as loss of financial data and customer information. The networks are vulnerable to threats due to network tampering or cyberattacks, which can lead to network failure or financial instability. To overcome such challenges, 24/7 network connectivity and flawless network availability are crucial, which can be achieved by continually monitoring and analyzing the network to ensure its optimal performance. The growing adoption of BYOD policies and work-from-home arrangements, combined with the increasing prevalence of botnet attacks, particularly those originating from the Mirai botnet, has significantly put the BFSI infrastructure at risk. Factors such as data leaks from cloud storage and vulnerabilities in data center security further exacerbate this threat. As a result, DDoS protection and mitigation solutions are essential for safeguarding the BFSI sector.

TABLE 91 DDOS PROTECTION AND MITIGATION MARKET IN BFSI, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	231.2	270.7	314.7	362.8	415.3	483.3	15.9%
Europe	142.0	170.8	204.2	241.9	284.6	338.6	19.0%
Asia Pacific	105.9	130.8	160.5	195.5	236.9	290.5	22.4%
Middle East & Africa	57.5	69.9	84.4	101.1	120.3	144.9	20.3%
Latin America	24.2	29.6	35.8	42.8	50.7	58.4	19.2%
Total	560.9	671.8	799.6	944.0	1,107.7	1,315.6	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 92 DDOS PROTECTION AND MITIGATION MARKET IN BFSI, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	555.2	636.0	726.7	828.0	941.1	1,067.1	14.0%
Europe	394.9	459.1	532.2	615.1	708.3	818.9	15.7%
Asia Pacific	342.7	403.3	473.2	553.9	646.6	753.1	17.1%
Middle East & Africa	171.1	201.6	235.4	274.1	318.4	369.0	16.6%
Latin America	68.3	79.6	93.8	110.0	129.3	145.9	16.4%
Total	1,532.2	1,779.5	2,061.2	2,381.2	2,743.8	3,154.0	15.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.3 GOVERNMENT & DEFENSE

14.3.1 INCREASING NEED FOR DDOS PROTECTION AND MITIGATION SOLUTIONS AND SERVICES TO HELP MARKET GROWTH

The government and defense vertical is focusing on strengthening its entire network infrastructure, as it is under constant threat. Government databases and websites contain highly confidential data that is not entirely secure. Attackers can bring government and defense operations to a standstill by launching DDoS attacks into the network or application layer. Government agencies face the unique challenge of protecting operational information as a matter of national security. Such mission-critical environments cannot afford downtime and outages in their network infrastructure. Moreover, the government and defense vertical is shifting toward real-time communication. Therefore, threats from web browsing, email correspondence, and file exchange have considerably increased. This vertical requires highly upgraded security solutions to meet the emerging sophisticated DDoS attacks.

TABLE 93 DDOS PROTECTION AND MITIGATION MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	165.5	185.9	207.3	229.0	251.3	280.3	11.1%
Europe	101.7	117.3	134.5	152.7	172.2	196.4	14.1%
Asia Pacific	75.8	89.8	105.7	123.4	143.4	168.5	17.3%
Middle East & Africa	41.2	48.0	55.6	63.8	72.8	84.0	15.3%
Latin America	17.4	20.3	23.6	27.0	30.7	33.9	14.3%
Total	401.6	461.4	526.5	596.0	670.5	763.2	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 94 DDOS PROTECTION AND MITIGATION MARKET IN GOVERNMENT AND DEFENSE, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	308.6	338.7	370.6	404.3	439.8	476.9	9.1%
Europe	219.5	244.5	271.4	300.3	330.9	366.0	10.8%
Asia Pacific	190.5	214.8	241.4	270.4	302.1	336.6	12.1%
Middle East & Africa	95.1	107.3	120.0	133.8	148.8	164.9	11.6%
Latin America	38.0	42.4	47.8	53.7	60.4	65.2	11.4%
Total	851.7	947.7	1,051.2	1,162.7	1,282.0	1,409.6	10.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.4 MANUFACTURING

14.4.1 EVOLVING VOLUMETRIC DDOS ATTACKS ON MANUFACTURING PROCESSES TO CONTRIBUTE TO MARKET GROWTH

In the manufacturing sector, organizations are leveraging a new generation of machine-to-machine systems, mobile applications, and hosted services. Manufacturers must maintain strong relationships with their suppliers, as these connections are crucial for making and selling products. This involves financial transactions conducted through web applications. Additionally, manufacturing companies heavily rely on software to automate processes, manage supply chains, facilitate research and development, and digitalize both processes and products. DDoS attacks threaten data confidentiality by causing data loss and system breakdowns, which can ultimately slow down manufacturing speed. Therefore, it is essential for the manufacturing sector to safeguard its entire production process and network infrastructure against the growing threat of volumetric DDoS attacks.

Manufacturing companies strive to develop operational effectiveness and secure IT resources whenever they find the resources to be feasible, thereby delivering a cost-effective infrastructure. With the growing demand from customers for customized and individualized products and solutions, manufacturing units must ensure their production lines are managed properly to meet current demand in a rapid and flexible manner, with prompt responses. With the increase in the number of manufacturing units, remote locations are expected to rise as well, creating a potential market for DDoS mitigation and protection solutions and services. This results in the need for packaged solution providers for networks. This is expected to create more opportunities for DDoS protection and mitigation solution providers during the forecast period.

TABLE 95 DDOS PROTECTION AND MITIGATION MARKET IN MANUFACTURING, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	60.0	67.7	75.9	84.3	93.1	104.4	11.7%
Europe	36.8	42.7	49.2	56.2	63.8	73.2	14.7%
Asia Pacific	27.5	32.7	38.7	45.4	53.1	62.8	18.0%
Middle East & Africa	14.9	17.5	20.3	23.5	27.0	31.3	16.0%
Latin America	6.3	7.4	8.6	9.9	11.4	12.6	15.0%
Total	145.5	168.0	192.7	219.4	248.2	284.3	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 96 DDOS PROTECTION AND MITIGATION MARKET IN MANUFACTURING, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	115.7	127.8	140.9	154.8	169.7	185.5	9.9%
Europe	82.3	92.3	103.2	115.0	127.7	142.3	11.6%
Asia Pacific	71.4	81.1	91.7	103.6	116.6	130.9	12.9%
Middle East & Africa	35.7	40.5	45.6	51.2	57.4	64.1	12.5%
Latin America	14.2	16.0	18.2	20.6	23.3	25.4	12.2%
Total	319.3	357.7	399.6	445.2	494.8	548.2	11.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.5 ENERGY & UTILITIES

14.5.1 INCREASING ADOPTION OF SMART SYSTEMS AND APPLICATIONS TO DRIVE MARKET

The energy and utilities sector has begun to implement online services and utilize IoT technology to automate its business processes. As the adoption of cloud and virtualization increases, this sector has also become an appealing target for hackers. Consequently, companies in energy and utilities are adopting advanced technologies to efficiently manage power distribution and consumption. The evolving volumetric DDoS attacks affect the delivery of essential services due to latency or downtime in the network infrastructure. The increasing adoption of smart systems and applications connected over the internet has resulted in an expansion of the attack surface for volumetric DDoS attacks, leading to significant business disruptions and economic losses.

The current trend in the energy and utilities vertical is the smart grid initiative, which includes smart electricity grids, solar panel equipment, smart meters, smart appliances, and flexible gas power plants, making network devices vulnerable to security threats. Hence, this vertical is expected to increase its investments in DDoS protection and mitigation solutions in the future to strengthen network security and reduce network complexity.

TABLE 97 DDOS PROTECTION AND MITIGATION MARKET IN ENERGY AND UTILITIES, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	155.2	179.3	205.8	234.2	264.9	304.6	14.4%
Europe	95.3	113.2	133.5	156.2	181.5	213.4	17.5%
Asia Pacific	71.1	86.6	104.9	126.2	151.1	183.1	20.8%
Middle East & Africa	38.6	46.3	55.2	65.3	76.7	91.3	18.8%
Latin America	16.3	19.6	23.4	27.6	32.4	36.8	17.8%
Total	376.4	445.0	522.8	609.6	706.6	829.3	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 98 DDOS PROTECTION AND MITIGATION MARKET IN ENERGY AND UTILITIES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	345.9	391.8	442.8	499.2	561.4	630.1	12.7%
Europe	246.0	282.8	324.3	370.8	422.5	483.5	14.5%
Asia Pacific	213.5	248.5	288.4	333.9	385.7	444.6	15.8%
Middle East & Africa	106.6	124.2	143.4	165.2	189.9	217.8	15.4%
Latin America	42.6	49.0	57.1	66.3	77.1	86.2	15.1%
Total	954.7	1,096.3	1,256.0	1,435.5	1,636.8	1,862.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.6 IT AND ITES

14.6.1 RISE OF ADVANCED TECHNOLOGIES TO FUEL MARKET

The DDoS protection and mitigation market in the IT and ITeS vertical is increasingly critical due to the vast amounts of personal and sensitive data being managed. As organizations in this sector utilize advanced technologies, such as cloud computing, mobile applications, and social media, they become prime targets for cybercriminals. The rise of remote work during the pandemic has further intensified reliance on telecom services, making businesses more vulnerable to DDoS attacks.

Cybercriminals exploit this vulnerability through various tactics, including ransomware attacks, data theft, and business email compromise. As a result, communication service providers are implementing advanced DDoS technologies to ensure uninterrupted service delivery for their customers. The increasing use of mobile devices enables users to access sensitive information from anywhere, heightening the risk of cyber threats.

To combat these challenges, companies in the IT and ITeS vertical are implementing robust DDoS protection and mitigation solutions. These tools enable organizations to safeguard critical data stored on mobile devices and accessed via the cloud, ensuring a secure user experience. With the growth of web and mobile applications, there is an urgent need for effective security countermeasures against DDoS attacks. Additionally, the surge in online financial transactions makes this vertical particularly attractive to cybercriminals, underscoring the importance of comprehensive DDoS protection strategies to maintain operational integrity and customer trust.

TABLE 99 DDOS PROTECTION AND MITIGATION MARKET IN IT AND ITES, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	84.8	98.6	114.0	130.6	148.7	172.1	15.2%
Europe	52.1	62.2	73.9	87.1	101.9	120.6	18.3%
Asia Pacific	38.8	47.6	58.1	70.4	84.8	103.4	21.6%
Middle East & Africa	21.1	25.5	30.6	36.4	43.1	51.6	19.6%
Latin America	8.9	10.8	13.0	15.4	18.2	20.8	18.5%
Total	205.6	244.8	289.6	339.9	396.6	468.4	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 100 DDOS PROTECTION AND MITIGATION MARKET IN IT AND ITES, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	196.6	224.1	254.8	288.9	326.9	368.9	13.4%
Europe	139.8	161.8	186.6	214.6	246.0	283.1	15.1%
Asia Pacific	121.4	142.1	165.9	193.3	224.6	260.3	16.5%
Middle East & Africa	60.6	71.0	82.5	95.6	110.6	127.6	16.1%
Latin America	24.2	28.0	32.9	38.4	44.9	50.4	15.8%
Total	542.6	627.0	722.7	830.9	953.0	1,090.4	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.7 TELECOMMUNICATIONS

14.7.1 RISE IN NUMBER OF WEB AND MOBILE APPLICATIONS TO FUEL MARKET

The DDoS protection and mitigation market within the telecommunications (telecom) vertical is increasingly crucial as telecommunications companies confront a rapidly evolving threat landscape. With the advent of advanced technologies like 5G and the Internet of Things (IoT), telecom operators manage vast amounts of sensitive data, making them prime targets for cybercriminals. DDoS attacks can severely disrupt internet services, potentially affecting millions of consumers and halting critical operations for businesses and government entities.

Recent reports indicate a staggering 210% increase in DDoS incidents targeting telecom companies, as cybercriminals exploit vulnerabilities in their networks through tactics such as ransomware and data theft. In response, telecom operators are adopting sophisticated DDoS protection technologies to ensure uninterrupted service delivery and safeguard customer data. Advanced solutions, such as network function virtualization (NFV) and automated threat detection systems, enhance resilience against DDoS attacks by filtering out malicious traffic while maintaining high service availability. The growing reliance on cloud-based services further necessitates robust mitigation strategies to defend against large-scale volumetric attacks. As online transactions within the telecom sector continue to rise, so does the risk of cyber threats. By investing in comprehensive DDoS protection and mitigation solutions, telecom companies can maintain operational integrity, protect sensitive information, and create a secure environment for their customers in an increasingly digital world.

TABLE 101 DDOS PROTECTION AND MITIGATION MARKET IN TELECOMMUNICATIONS, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	121.7	138.4	156.2	174.8	194.4	219.9	12.6%
Europe	74.8	87.2	101.0	116.1	132.4	152.9	15.4%
Asia Pacific	55.8	66.7	79.4	93.8	110.2	131.1	18.6%
Middle East & Africa	30.3	35.7	41.8	48.5	56.0	65.4	16.6%
Latin America	12.8	15.1	17.7	20.5	23.6	26.4	15.6%
Total	295.4	343.1	396.0	453.7	516.7	595.7	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 102 DDOS PROTECTION AND MITIGATION MARKET IN TELECOMMUNICATIONS, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	245.6	273.7	304.2	337.4	373.3	412.2	10.9%
Europe	173.0	195.2	219.7	246.6	275.7	309.5	12.3%
Asia Pacific	150.1	171.5	195.4	222.0	251.7	284.7	13.6%
Middle East & Africa	75.0	85.7	97.2	109.9	123.9	139.5	13.2%
Latin America	29.9	33.8	38.7	44.1	50.3	55.2	13.0%
Total	673.6	759.9	855.1	960.0	1,075.0	1,201.0	12.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.8 HEALTHCARE

14.8.1 REGULATORY NORMS TO INCREASE DEPLOYMENT OF DDOS PROTECTION AND MITIGATION SOLUTIONS

The healthcare vertical comprises companies that generate and commercialize healthcare goods and services. The vertical is continuously incorporating newer technologies to improve the diagnostic process for patients. Organizations in the healthcare vertical majorly rely on secure network environments to transfer the Protected Health Information (PHI). These networks must be stable to provide clinicians access to mission-critical applications and regulate the usage of the network for personal content. In the current scenario, the healthcare vertical is delivering the best services by using advanced equipment and mobile devices specially designed for doctors and nurses. These devices keep doctors connected to patients and enable them to reach colleagues and access a vast wealth of medical data. As mobility has become an essential part of efficient and accurate care delivery, internet connectivity has also become a necessity. Moreover, certain regulatory norms, such as HIPAA, which require healthcare providers to protect confidential patient information, also contribute to the increasing deployment of DDoS protection and mitigation solutions in the healthcare vertical.

Healthcare professionals maintain patients' records online for faster access. Data related to doctors, patients, staff, and administrators is also highly confidential. The data stored online is exploited by DDoS attacks, which compromise the integrity of systems and the privacy of patients, cause losses amounting to millions, and disrupt facilities' ability to provide patient care. The increasing instances of volumetric attacks on the healthcare sector are expected to drive the adoption of DDoS protection and mitigation solutions and services.

TABLE 103 DDOS PROTECTION AND MITIGATION MARKET IN HEALTHCARE, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	93.8	107.9	123.3	139.7	157.2	180.0	13.9%
Europe	57.6	68.1	80.0	93.1	107.8	126.1	17.0%
Asia Pacific	43.0	52.1	62.9	75.3	89.7	108.2	20.3%
Middle East & Africa	23.4	27.9	33.1	38.9	45.5	54.0	18.2%
Latin America	9.8	11.8	14.0	16.5	19.2	21.8	17.2%
Total	227.6	267.8	313.2	363.5	419.4	490.0	16.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 104 DDOS PROTECTION AND MITIGATION MARKET IN HEALTHCARE, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	203.5	229.5	258.2	289.8	324.6	362.7	12.3%
Europe	144.7	165.7	189.1	215.3	244.3	278.3	14.0%
Asia Pacific	125.6	145.5	168.2	193.9	223.0	256.0	15.3%
Middle East & Africa	62.7	72.7	83.6	95.9	109.8	125.4	14.9%
Latin America	25.0	28.7	33.3	38.5	44.6	49.6	14.6%
Total	561.6	642.1	732.4	833.5	946.3	1,072.1	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.9 EDUCATION

14.9.1 NEED FOR CONFIDENTIALITY, INTEGRITY, AND EASY AVAILABILITY OF DATA AND RESOURCES TO AUGMENT MARKET GROWTH

Organizations in the education vertical need a reliable network environment. These networks must be stable to provide users with access to mission-critical applications and regulate the use of the network for personal content. The education vertical aims to secure the confidentiality, integrity, and availability of data and resources, and reduce lagging periods that may affect the vertical's performance. Moreover, education professionals nowadays use newer technologies and internet-enabled devices in classrooms. The deployment of advanced technologies, web and mobile applications, has also increased in this vertical. Data, including student records, parent records, staff records, research papers, and patent information, is stored online to make it easily accessible when needed. DDoS attacks target the network and application layers of resources in the education vertical, thereby causing leakage of important research and patient information. The attacks can impact the smooth functioning of colleges and schools by affecting their servers and networks. Hence, to stay secure, the education vertical needs advanced DDoS protection and mitigation solutions and services.

TABLE 105 DDOS PROTECTION AND MITIGATION MARKET IN EDUCATION, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	52.9	60.3	68.2	76.6	85.5	96.9	12.9%
Europe	32.5	38.0	44.3	51.1	58.6	67.9	15.9%
Asia Pacific	24.2	29.1	34.8	41.3	48.7	58.3	19.2%
Middle East & Africa	13.2	15.6	18.3	21.3	24.7	29.1	17.2%
Latin America	5.5	6.6	7.8	9.0	10.4	11.7	16.1%
Total	128.3	149.6	173.3	199.4	227.9	263.9	15.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 106 DDOS PROTECTION AND MITIGATION MARKET IN EDUCATION, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	108.5	121.3	135.1	150.2	166.6	184.5	11.2%
Europe	77.2	87.5	99.0	111.6	125.4	141.6	12.9%
Asia Pacific	67.0	76.9	88.0	100.5	114.5	130.2	14.2%
Middle East & Africa	33.5	38.4	43.8	49.7	56.4	63.8	13.8%
Latin America	13.4	15.2	17.4	20.0	22.9	25.2	13.6%
Total	299.6	339.3	383.3	432.0	485.8	545.2	12.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.10 RETAIL

14.10.1 GROWING CYBERATTACKS AND DATA THEFT TO INCREASE ADOPTION OF DDOS PROTECTION AND MITIGATION SOLUTIONS

Retail organizations are distributed across various locations. Managing the distributed network is important for network administrators to achieve higher operational efficiency. Retail distribution centers must monitor their networks to stay informed about trends and deliver a superior customer experience. This is necessary, as the customer base is expected to increase for online facilities. These capabilities can be facilitated using real-time insights.

The advancement of mobile technologies has encouraged the vertical to adopt mobile devices, providing real-time access to better-quality services for its customers. However, the use of mobile devices has led to an increase in data theft and data losses among retailers with direct access to customers' private information. Furthermore, the growing number of cyber-attacks and data theft activities has increased pressure on retailers, forcing them to adopt DDoS protection and mitigation solutions to protect the confidential and private information of their customers. Additionally, regulations such as GDPR and PCI DSS have prompted organizations to ensure the privacy of their customers' data.

TABLE 107 DDOS PROTECTION AND MITIGATION MARKET IN RETAIL, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	129.6	148.4	168.8	190.4	213.4	243.3	13.4%
Europe	79.6	93.6	109.5	127.0	146.3	170.5	16.5%
Asia Pacific	59.4	71.7	86.1	102.6	121.7	146.2	19.8%
Middle East & Africa	32.3	38.3	45.3	53.0	61.8	72.9	17.7%
Latin America	13.6	16.2	19.2	22.5	26.1	29.4	16.7%
Total	314.3	368.2	428.7	495.5	569.3	662.4	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 108 DDOS PROTECTION AND MITIGATION MARKET IN RETAIL, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	273.9	307.6	344.6	385.3	429.7	478.0	11.8%
Europe	194.8	222.0	252.4	286.2	323.4	366.8	13.5%
Asia Pacific	169.1	195.0	224.5	257.7	295.2	337.3	14.8%
Middle East & Africa	84.4	97.5	111.6	127.5	145.4	165.3	14.4%
Latin America	33.7	38.5	44.5	51.2	59.0	65.4	14.2%
Total	755.9	860.6	977.6	1,107.9	1,252.6	1,412.9	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

14.11 OTHER VERTICALS

The DDoS protection and mitigation market is increasingly critical across various sectors, including oil and gas, media and entertainment, transportation and logistics, and travel and hospitality. Each of these industries faces unique cyber threats, particularly from DDoS attacks, which can significantly disrupt operations. In the oil and gas sector, the digitalization of infrastructure and the integration of IoT devices have heightened vulnerability to cyberattacks. Recent data indicate an increase in DDoS incidents, with notable attacks, such as the Colonial Pipeline incident, underscoring the potential for widespread operational disruption. As a result, companies are investing in advanced DDoS protection technologies to secure their networks. The media and entertainment industry is also a prime target, especially during major events when traffic peaks. Cybercriminals often exploit these times to launch disruptive attacks, prompting organizations to enhance their DDoS mitigation strategies to ensure uninterrupted service. In transportation and logistics, reliance on digital platforms makes this sector particularly susceptible to threats that can lead to significant financial losses. Companies are implementing multi-layered security measures, including real-time monitoring and automated responses. Additionally, the travel and hospitality industry faces increasing risks as online transactions surge. DDoS protection solutions are vital for maintaining operational integrity during peak booking periods. Overall, organizations across these verticals recognize the necessity of comprehensive DDoS protection strategies to safeguard sensitive information and ensure service continuity in an increasingly digital environment.

TABLE 109 DDOS PROTECTION AND MITIGATION MARKET IN OTHER VERTICALS, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	74.0	83.8	94.3	105.1	116.4	131.1	12.1%
Europe	45.4	53.0	61.4	70.6	80.6	93.1	15.4%
Asia Pacific	33.9	40.6	48.3	57.1	67.1	79.8	18.7%
Middle East & Africa	18.4	21.7	25.4	29.5	34.1	39.8	16.7%
Latin America	7.8	9.2	10.8	12.5	14.4	16.1	15.7%
Total	179.4	208.2	240.1	274.8	312.6	359.9	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 110 DDOS PROTECTION AND MITIGATION MARKET IN OTHER VERTICALS, BY REGION, 2026–2031 (USD MILLION)

Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	145.7	161.5	178.5	196.8	216.5	237.3	10.2%
Europe	105.4	118.9	133.9	150.3	168.2	188.9	12.4%
Asia Pacific	91.4	104.5	119.1	135.3	153.5	173.7	13.7%
Middle East & Africa	45.7	52.2	59.2	67.0	75.6	85.1	13.3%
Latin America	18.2	20.6	23.6	26.9	30.7	33.7	13.0%
Total	406.4	457.7	514.3	576.4	644.5	718.7	12.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15 DDOS PROTECTION AND MITIGATION MARKET, BY REGION

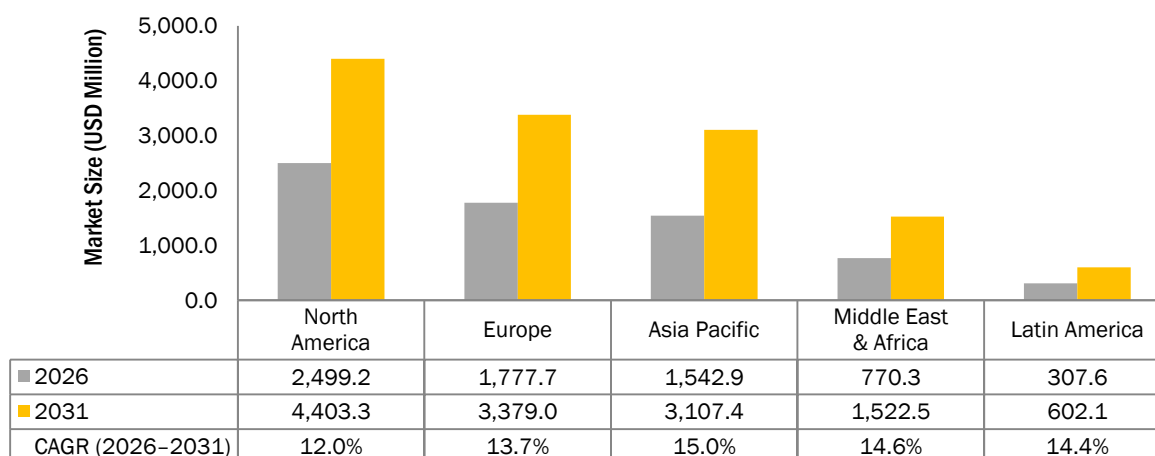
KEY FINDINGS

- North America is estimated to account for the largest share of the DDoS protection and mitigation market in 2026, and it is projected to grow at a CAGR of 12.0% from 2026 to 2031.
- Asia Pacific is expected to be a favorable market for investments during the forecast period, with the market in this region projected to record the highest CAGR of 15.0%.
- The widespread adoption of IoT devices expands the attack surface for cybercriminals. Many IoT devices have weak security features, making them easy targets for botnets, which are often used in DDoS attacks.
- Governments and regulatory bodies are implementing stringent data protection regulations that mandate organizations to secure their networks and customer data. This drives the adoption of DDoS protection solutions to comply with these laws and avoid penalties.
- Organizations are increasingly recognizing the financial and reputational damage that DDoS attacks can cause. Ensuring business continuity through robust DDoS protection is becoming a top priority for businesses across industries.

15.1 INTRODUCTION

The DDoS protection and mitigation market is broadly classified into five major regions: North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America. This chapter offers insights into regional markets, including their market size, growth rates, and future trends. The widespread adoption of PCs and internet services for business purposes, as well as the storage of critical data globally, has increased risks, including data breaches and thefts. Additionally, the rapid penetration of mobile devices, such as smartphones, has further increased the risk of data theft and loss, as well as the need for Universal Serial Bus (USB) and Digital Video Discs (DVDs) for accessing and transferring organizational content. Active and passive attacks on data during transmission over networks by attackers and masqueraders have heightened the importance of DDoS protection and mitigation among diverse users across various regions. The key growth factors driving the adoption of DDoS protection and mitigation solutions include the presence of dynamic business environments, rising commercial espionage and cyberattacks, and the growing need to adhere to regulatory standards for implementing DDoS protection and mitigation solutions. North America and Europe are the largest revenue contributors to the DDoS protection and mitigation market. These regions are driven by the early adoption of advanced technologies, such as the cloud and IoT, high IT capabilities, and higher IT investments.

FIGURE 39 NORTH AMERICA TO LEAD MARKET FROM 2026 TO 2031



Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 111 DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2020–2025 (USD MILLION)

Region	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
North America	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	2,216.0	13.7%
Europe	717.7	846.3	991.5	1,152.1	1,329.6	1,552.7	16.7%
Asia Pacific	535.4	647.7	779.3	930.9	1,106.8	1,331.9	20.0%
Middle East & Africa	290.9	346.3	409.8	481.2	561.9	664.3	18.0%
Latin America	122.5	146.5	173.7	203.9	237.1	267.9	16.9%
Total	2,835.0	3,327.8	3,882.6	4,495.6	5,175.5	6,032.8	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 112 DDOS PROTECTION AND MITIGATION MARKET, BY REGION, 2026–2031 (USD MILLION)

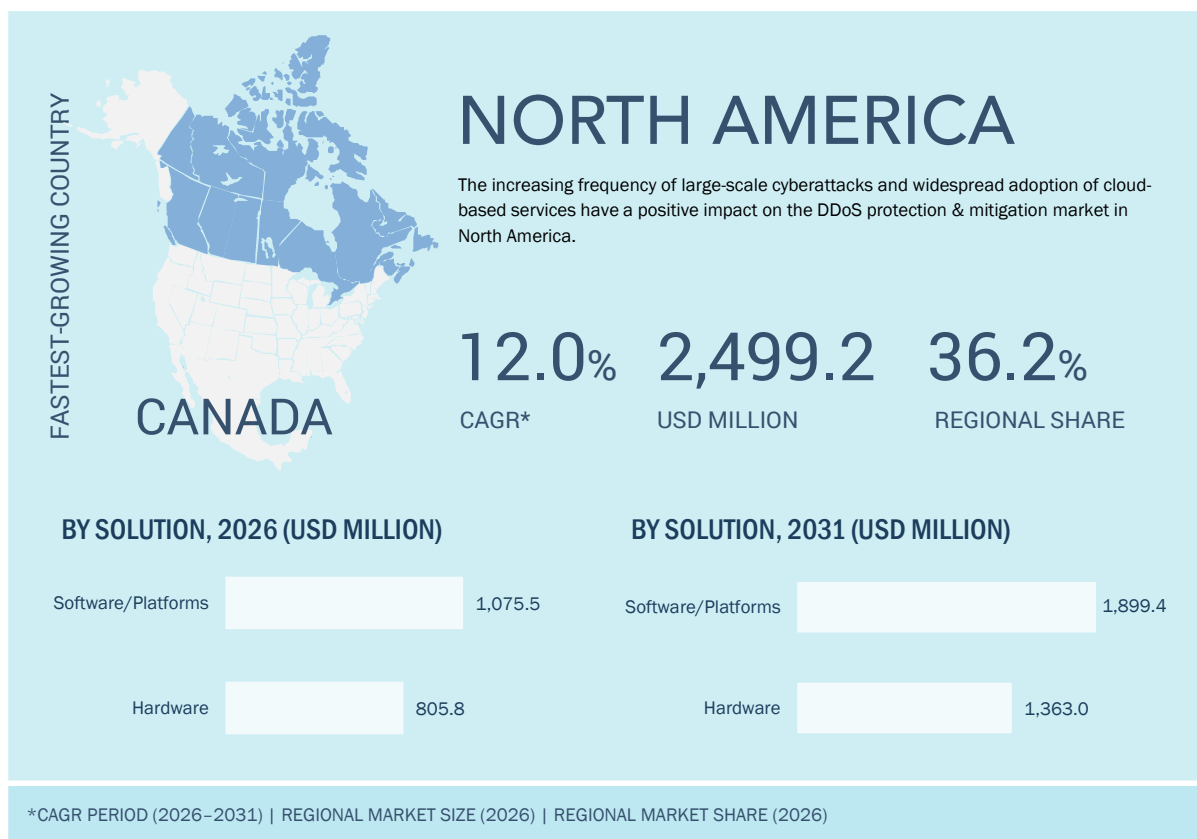
Region	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
North America	2,499.2	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	12.0%
Europe	1,777.7	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	13.7%
Asia Pacific	1,542.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	15.0%
Middle East & Africa	770.3	891.1	1,022.3	1,170.1	1,336.2	1,522.5	14.6%
Latin America	307.6	351.9	407.2	469.7	542.7	602.1	14.4%
Total	6,897.7	7,867.9	8,953.4	10,165.1	11,514.7	13,014.3	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.2 NORTH AMERICA

North America is estimated to lead the DDoS protection and mitigation market during the forecast period. Organizations in this region, especially in the US, have leveraged the benefits of AI, ML, and deep learning technologies to stay ahead in the market. North American countries have well-established economies, which enable DDoS protection and mitigation vendors to invest in new technologies. Additionally, the region is considered the hub of innovation as major North American IT companies introduce new products and engage in proactive collaborations. The rapid penetration of mobile devices, such as smartphones, laptops, and USB drives, as well as the increasing need to secure data residing within companies and being transferred over business networks, are driving the adoption of DDoS protection and mitigation solutions in North America.

The broad adoption of data compliance regulations by all businesses and the increasing use of cloud computing are the two main growth drivers of the North American DDoS protection and mitigation market. Furthermore, attacks are rapidly growing and getting more sophisticated due to the widespread use of cloud-based applications in North America. The countries in this region are expected to extensively implement DDoS protection and mitigation solutions to ensure data security, prevent cyberattacks and commercial espionage, and maintain the security and privacy of data, thereby facilitating business continuity.

FIGURE 40 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET SNAPSHOT

Source: Interviews with Experts and MarketsandMarkets Analysis

TABLE 113 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solutions	896.2	1,025.4	1,164.9	1,312.6	1,469.6	1,673.3	13.3%
Services	272.3	315.7	363.4	414.9	470.6	542.7	14.8%
Total	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	2,216.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 114 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solutions	1,881.2	2,110.0	2,361.0	2,635.7	2,935.6	3,262.3	11.6%
Services	618.0	702.0	795.4	899.2	1,014.1	1,141.0	13.0%
Total	2,499.2	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	12.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 115 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	395.1	449.9	508.7	570.5	635.7	720.2	12.8%
Software/Platforms	501.1	575.5	656.2	742.1	833.9	953.0	13.7%
Total	896.2	1,025.4	1,164.9	1,312.6	1,469.6	1,673.3	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 116 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	805.8	899.3	1,001.2	1,112.1	1,232.5	1,363.0	11.1%
Software/Platforms	1,075.5	1,210.7	1,359.8	1,523.5	1,703.1	1,899.4	12.0%
Total	1,881.2	2,110.0	2,361.0	2,635.7	2,935.6	3,262.3	11.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 117 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	158.4	183.2	210.4	239.6	271.0	311.8	14.5%
Managed Services	113.9	132.5	153.1	175.3	199.5	230.9	15.2%
Total	272.3	315.7	363.4	414.9	470.6	542.7	14.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 118 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	354.2	401.3	453.6	511.5	575.4	645.8	12.8%
Managed Services	263.8	300.6	341.8	387.7	438.7	495.2	13.4%
Total	618.0	702.0	795.4	899.2	1,014.1	1,141.0	13.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 119 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	43.8	50.4	57.6	65.2	73.3	83.9	13.9%
Consulting & Advisory	38.6	45.2	52.5	60.5	69.3	80.7	15.9%
Training & Education	26.1	30.4	35.1	40.2	45.8	53.0	15.2%
Support & Maintenance	30.9	35.3	40.0	45.0	50.2	57.0	13.0%
DDoS Testing & Validation	18.9	21.9	25.1	28.6	32.3	37.2	14.5%
Total	158.4	183.2	210.4	239.6	271.0	311.8	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 120 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	94.8	106.8	120.0	134.6	150.5	167.9	12.1%
Consulting & Advisory	92.7	106.3	121.5	138.5	157.6	178.8	14.0%
Training & Education	60.6	69.0	78.5	89.0	100.7	113.7	13.4%
Support & Maintenance	63.8	71.3	79.5	88.3	97.9	108.3	11.1%
DDoS Testing & Validation	42.3	47.9	54.1	61.0	68.7	77.1	12.8%
Total	354.2	401.3	453.6	511.5	575.4	645.8	12.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 121 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	295.9	336.2	379.4	424.6	472.2	534.0	12.5%
Threat Mitigation Systems	330.7	380.5	434.7	492.4	554.2	634.0	13.9%
Botnet Detection & Management	125.6	143.7	163.3	184.1	206.3	235.3	13.4%
Other Solution Types	144.1	165.0	187.5	211.5	236.9	269.9	13.4%
Total	896.2	1,025.4	1,164.9	1,312.6	1,469.6	1,673.3	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 122 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	596.4	664.5	738.7	819.1	906.2	1,000.7	10.9%
Threat Mitigation Systems	716.2	807.2	907.6	1,018.4	1,140.2	1,272.2	12.2%
Botnet Detection & Management	265.0	297.6	333.4	372.4	414.9	462.4	11.8%
Other Solution Types	303.6	340.7	381.3	425.7	474.2	527.0	11.7%
Total	1,881.2	2,110.0	2,361.0	2,635.7	2,935.6	3,262.3	11.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 123 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	408.4	469.5	536.0	606.9	682.8	781.2	13.9%
Web Applications & APIs	371.3	431.8	498.4	570.6	648.9	750.4	15.1%
DNS Infrastructure	388.8	439.8	493.9	550.1	608.5	684.4	12.0%
Total	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	2,216.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 124 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	882.5	994.7	1,118.5	1,254.7	1,404.4	1,568.4	12.2%
Web Applications & APIs	856.7	975.6	1,108.3	1,255.9	1,419.7	1,601.1	13.3%
DNS Infrastructure	760.0	841.6	929.7	1,024.2	1,125.6	1,233.8	10.2%
Total	2,499.2	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	12.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 125 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	420.6	479.4	542.5	608.9	678.9	769.8	12.8%
Cloud	660.9	761.8	871.8	989.7	1,116.4	1,280.6	14.1%
Hybrid	86.9	99.9	114.0	128.9	144.9	165.5	13.7%
Total	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	2,216.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 126 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	862.0	962.9	1,073.2	1,193.5	1,324.5	1,465.8	11.2%
Cloud	1,450.7	1,639.2	1,847.9	2,078.1	2,331.6	2,615.2	12.5%
Hybrid	186.6	209.8	235.3	263.2	293.6	322.3	11.6%
Total	2,499.2	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	12.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 127 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	723.9	825.4	934.3	1,049.0	1,170.0	1,327.1	12.9%
SMEs	444.6	515.7	594.0	678.6	770.1	888.9	14.9%
Total	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	2,216.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 128 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	1,486.3	1,660.6	1,851.0	2,058.5	2,284.0	2,527.8	11.2%
SMEs	1,012.9	1,151.3	1,305.4	1,476.4	1,665.7	1,875.5	13.1%
Total	2,499.2	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	12.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 129 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	231.2	270.7	314.7	362.8	415.3	483.3	15.9%
Government & Defense	165.5	185.9	207.3	229.0	251.3	280.3	11.1%
Healthcare	93.8	107.9	123.3	139.7	157.2	180.0	13.9%
IT & ITeS	84.8	98.6	114.0	130.6	148.7	172.1	15.2%
Telecommunications	121.7	138.4	156.2	174.8	194.4	219.9	12.6%
Manufacturing	60.0	67.7	75.9	84.3	93.1	104.4	11.7%
Energy & Utilities	155.2	179.3	205.8	234.2	264.9	304.6	14.4%
Retail	129.6	148.4	168.8	190.4	213.4	243.3	13.4%
Education	52.9	60.3	68.2	76.6	85.5	96.9	12.9%
Other Verticals	74.0	83.8	94.3	105.1	116.4	131.1	12.1%
Total	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	2,216.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 130 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	555.2	636.0	726.7	828.0	941.1	1,067.1	14.0%
Government & Defense	308.6	338.7	370.6	404.3	439.8	476.9	9.1%
Healthcare	203.5	229.5	258.2	289.8	324.6	362.7	12.3%
IT & ITeS	196.6	224.1	254.8	288.9	326.9	368.9	13.4%
Telecommunications	245.6	273.7	304.2	337.4	373.3	412.2	10.9%
Manufacturing	115.7	127.8	140.9	154.8	169.7	185.5	9.9%
Energy & Utilities	345.9	391.8	442.8	499.2	561.4	630.1	12.7%
Retail	273.9	307.6	344.6	385.3	429.7	478.0	11.8%
Education	108.5	121.3	135.1	150.2	166.6	184.5	11.2%
Other Verticals	145.7	161.5	178.5	196.8	216.5	237.3	10.2%
Total	2,499.2	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	12.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 131 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)

Country	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
US	980.0	1,121.2	1,273.6	1,434.1	1,603.3	1,821.9	13.2%
Canada	188.5	219.9	254.7	293.4	336.8	394.1	15.9%
Total	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	2,216.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 132 NORTH AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
US	2,044.2	2,289.4	2,559.8	2,857.7	3,186.2	3,530.0	11.5%
Canada	455.0	522.5	596.6	677.1	763.5	873.3	13.9%
Total	2,499.2	2,812.0	3,156.4	3,534.8	3,949.7	4,403.3	12.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.2.1 US

15.2.1.1 Presence of major vendors in US driving market growth

The US is inclined toward innovation and state-of-the-art infrastructure. It is the major contributor to the overall DDoS protection and mitigation market in North America. It is home to many DDoS protection and mitigation vendors and is recognized as a global center for technology and innovation. Organizations in the US focus on delivering frictionless experiences to their customers and protecting their confidential data. Additionally, the US has a well-documented history of applicable policies and laws, which provide a roadmap for the country's cybersecurity. The National Cybersecurity and Communications Integration

Center (NCCIC) is responsible for coordinating and sharing cyber information, as well as proactively managing the country's cyber risks.

There has been a significant increase in DDoS attacks in the US. According to data presented by Atlas VPN, attackers tend to target computers and the internet sector in the US. In June 2021 alone, more than a third of DDoS attacks worldwide targeted servers in the US. The US government has started taking serious action against DDoS attacks. Under the Computer Fraud and Abuse Act, DDoS attacks can be classified as a federal criminal offense. One can be charged with imprisonment of up to 10 years if found guilty of a DDoS attack. The country has a strategic focus on technological innovation, primarily focusing on preventing data breaches and cyber threats, as well as delivering personalized customer experiences.

TABLE 133 US: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	751.6	857.2	970.8	1,089.7	1,214.5	1,375.7	12.8%
Services	228.4	263.9	302.9	344.4	388.9	446.2	14.3%
Total	980.0	1,121.2	1,273.6	1,434.1	1,603.3	1,821.9	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 134 US: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	1,538.8	1,717.9	1,914.7	2,130.8	2,368.1	2,615.3	11.2%
Services	505.5	571.5	645.1	726.9	818.1	914.7	12.6%
Total	2,044.2	2,289.4	2,559.8	2,857.7	3,186.2	3,530.0	11.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 135 US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	333.8	379.0	427.3	477.4	529.6	597.1	12.3%
Software/Platforms	417.8	478.2	543.5	612.3	684.9	778.6	13.3%
Total	751.6	857.2	970.8	1,089.7	1,214.5	1,375.7	12.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 136 US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	664.7	738.5	819.2	907.1	1,003.2	1,102.8	10.7%
Software/Platforms	874.1	979.4	1,095.6	1,223.6	1,364.9	1,512.5	11.6%
Total	1,538.8	1,717.9	1,914.7	2,130.8	2,368.1	2,615.3	11.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 137 US: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	132.1	152.3	174.3	197.7	222.6	254.8	14.0%
Managed Services	96.3	111.6	128.6	146.7	166.2	191.4	14.7%
Total	228.4	263.9	302.9	344.4	388.9	446.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 138 US: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	287.9	324.6	365.4	410.7	461.0	514.1	12.3%
Managed Services	217.6	246.9	279.6	316.2	357.1	400.6	13.0%
Total	505.5	571.5	645.1	726.9	818.1	914.7	12.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 139 US: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	36.6	42.0	47.8	53.9	60.4	68.7	13.4%
Consulting & Advisory	32.1	37.4	43.3	49.8	56.7	65.6	15.4%
Training & Education	21.8	25.2	29.0	33.1	37.5	43.2	14.7%
Support & Maintenance	25.9	29.5	33.3	37.3	41.4	46.8	12.5%
DDoS Testing & Validation	15.8	18.2	20.8	23.6	26.6	30.4	14.0%
Total	132.1	152.3	174.3	197.7	222.6	254.8	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 140 US: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	77.2	86.6	96.9	108.3	120.8	134.0	11.7%
Consulting & Advisory	75.0	85.6	97.4	110.8	125.7	141.7	13.6%
Training & Education	49.1	55.7	63.1	71.3	80.5	90.3	12.9%
Support & Maintenance	52.1	58.0	64.4	71.3	78.9	86.7	10.7%
DDoS Testing & Validation	34.4	38.8	43.6	49.0	55.0	61.4	12.3%
Total	287.9	324.6	365.4	410.7	461.0	514.1	12.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 141 US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	248.9	281.5	316.1	351.8	388.6	436.4	11.9%
Threat Mitigation Systems	290.1	333.5	380.5	430.4	483.4	551.6	13.7%
Botnet Detection & Management	95.0	107.8	121.5	135.8	150.6	169.8	12.3%
Other Solution Types	117.6	134.4	152.6	171.7	191.9	217.9	13.1%
Total	751.6	857.2	970.8	1,089.7	1,214.5	1,375.7	12.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 142 US: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	483.8	535.3	591.3	652.0	718.0	785.6	10.2%
Threat Mitigation Systems	621.7	699.2	785.0	880.0	985.1	1,095.8	12.0%
Botnet Detection & Management	189.0	209.9	232.8	257.8	285.1	313.3	10.6%
Other Solution Types	244.4	273.5	305.6	340.9	379.8	420.5	11.5%
Total	1,538.8	1,717.9	1,914.7	2,130.8	2,368.1	2,615.3	11.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 143 US: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	342.5	392.5	446.7	503.8	564.2	642.2	13.4%
Web Applications & APIs	311.4	361.0	415.4	473.7	536.2	616.9	14.6%
DNS Infrastructure	326.1	367.7	411.6	456.6	502.9	562.7	11.5%
Total	980.0	1,121.2	1,273.6	1,434.1	1,603.3	1,821.9	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 144 US: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	721.9	809.9	907.1	1,014.4	1,132.9	1,257.3	11.7%
Web Applications & APIs	700.7	794.3	898.8	1,015.3	1,145.3	1,283.6	12.9%
DNS Infrastructure	621.6	685.2	753.9	828.0	908.0	989.1	9.7%
Total	2,044.2	2,289.4	2,559.8	2,857.7	3,186.2	3,530.0	11.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 145 US: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	361.0	410.3	462.9	517.8	575.0	649.0	12.4%
Cloud	545.9	627.1	715.4	809.0	908.2	1,036.4	13.7%
Hybrid	73.1	83.8	95.3	107.4	120.1	136.5	13.3%
Total	980.0	1,121.2	1,273.6	1,434.1	1,603.3	1,821.9	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 146 US: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	723.3	804.7	893.7	991.0	1,097.5	1,207.8	10.8%
Cloud	1,167.8	1,313.4	1,474.8	1,653.3	1,851.2	2,059.6	12.0%
Hybrid	153.1	171.3	191.4	213.4	237.5	262.6	11.4%
Total	2,044.2	2,289.4	2,559.8	2,857.7	3,186.2	3,530.0	11.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 147 US: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	613.5	697.4	787.1	880.5	978.0	1,104.0	12.5%
SMEs	366.5	423.8	486.5	553.6	625.3	717.8	14.4%
Total	980.0	1,121.2	1,273.6	1,434.1	1,603.3	1,821.9	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 148 US: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	1,230.6	1,369.1	1,520.5	1,686.0	1,867.1	2,054.5	10.8%
SMEs	813.6	920.3	1,039.3	1,171.7	1,319.1	1,475.5	12.6%
Total	2,044.2	2,289.4	2,559.8	2,857.7	3,186.2	3,530.0	11.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 149 US: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	193.9	226.3	262.3	301.1	343.2	397.3	15.4%
Government & Defense	138.8	155.4	172.7	190.1	207.7	230.5	10.7%
Healthcare	78.7	90.2	102.7	115.9	129.9	148.0	13.5%
IT & ITeS	71.1	82.5	95.0	108.4	122.9	141.5	14.8%
Telecommunications	102.1	115.7	130.1	145.1	160.7	180.8	12.1%
Manufacturing	50.3	56.6	63.2	70.0	76.9	85.9	11.3%
Energy & Utilities	130.1	149.9	171.5	194.5	218.9	250.4	14.0%
Retail	108.7	124.1	140.6	158.1	176.4	200.0	13.0%
Education	44.3	50.4	56.9	63.6	70.6	79.7	12.4%
Other Verticals	62.0	70.1	78.5	87.3	96.2	107.8	11.7%
Total	980.0	1,121.2	1,273.6	1,434.1	1,603.3	1,821.9	13.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 150 US: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	454.1	517.8	589.3	669.4	759.2	855.5	13.5%
Government & Defense	252.4	275.8	300.6	326.9	354.8	382.3	8.7%
Healthcare	166.4	186.8	209.4	234.3	261.9	290.8	11.8%
IT & ITeS	160.8	182.4	206.6	233.6	263.7	295.8	13.0%
Telecommunications	200.9	222.8	246.7	272.8	301.2	330.4	10.5%
Manufacturing	94.6	104.1	114.2	125.2	136.9	148.7	9.5%
Energy & Utilities	282.9	319.0	359.1	403.5	452.9	505.1	12.3%
Retail	224.0	250.4	279.5	311.5	346.6	383.2	11.3%
Education	88.8	98.7	109.6	121.5	134.4	147.9	10.7%
Other Verticals	119.2	131.5	144.8	159.1	174.6	190.3	9.8%
Total	2,044.2	2,289.4	2,559.8	2,857.7	3,186.2	3,530.0	11.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.2.2 CANADA

15.2.2.1 Rapid technological advancements and increasing DDoS attacks on network infrastructure to drive market

Canada is a major economy in North America that has witnessed a significant increase in the adoption of DDoS protection and mitigation solutions in recent years. The rapid increase in technological advancements and security attacks on network infrastructure is expected to put significant pressure on enterprises across Canada. Canadian businesses are increasingly adopting modern technologies and becoming more reliant on the internet. Hence, there is an increase in online fraud, DDoS attacks, and cyber and bad bot attacks. Government institutions and organizations have begun adopting cybersecurity

solutions to protect against current and future cyberattacks within their networks. DDoS prevention and mitigation solutions help Canadian organizations address the issue of cyber risks and compliance management.

There are several globally recognized certification guidelines and standards useful for protecting business assets. The ISO 27001 certification standard and ISO 27032 cybersecurity guideline are implemented together to offer a robust cyber standard approach. The Canadian government is also taking initiatives to secure the country's cyber systems. The government has established a Cyber Incident Response Center to give advice on cyber threats. The entire world is experiencing a rise in DDoS attacks, and Canada is no exception. However, Canada is aware of its cybersecurity needs, which fosters innovation and economic activity. As a leader in cybersecurity research and development, Canada has the potential to effectively tackle innovative DDoS threats.

TABLE 151 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	144.6	168.2	194.1	222.9	255.1	297.6	15.5%
Services	43.9	51.8	60.6	70.5	81.7	96.5	17.1%
Total	188.5	219.9	254.7	293.4	336.8	394.1	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 152 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	342.5	392.1	446.2	504.9	567.4	647.0	13.6%
Services	112.5	130.4	150.3	172.2	196.0	226.3	15.0%
Total	455.0	522.5	596.6	677.1	763.5	873.3	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 153 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	61.2	70.9	81.5	93.1	106.1	123.2	15.0%
Software/Platforms	83.3	97.3	112.7	129.8	149.1	174.4	15.9%
Total	144.6	168.2	194.1	222.9	255.1	297.6	15.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 154 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	141.1	160.7	182.0	205.0	229.3	260.2	13.0%
Software/Platforms	201.4	231.4	264.2	299.9	338.2	386.9	13.9%
Total	342.5	392.1	446.2	504.9	567.4	647.0	13.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 155 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	26.3	30.9	36.1	41.9	48.4	57.0	16.8%
Managed Services	17.6	20.9	24.5	28.6	33.3	39.5	17.5%
Total	43.9	51.8	60.6	70.5	81.7	96.5	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 156 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	66.3	76.7	88.2	100.8	114.4	131.7	14.7%
Managed Services	46.2	53.7	62.2	71.5	81.6	94.6	15.4%
Total	112.5	130.4	150.3	172.2	196.0	226.3	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 157 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	7.2	8.4	9.8	11.3	13.0	15.2	16.1%
Consulting & Advisory	6.5	7.8	9.2	10.8	12.6	15.0	18.1%
Training & Education	4.4	5.2	6.1	7.1	8.3	9.8	17.5%
Support & Maintenance	5.0	5.8	6.7	7.7	8.8	10.2	15.2%
DDoS Testing & Validation	3.1	3.7	4.3	5.0	5.8	6.8	16.8%
Total	26.3	30.9	36.1	41.9	48.4	57.0	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 158 CANADA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	17.6	20.2	23.1	26.3	29.6	33.9	14.1%
Consulting & Advisory	17.7	20.7	24.0	27.8	31.9	37.1	16.0%
Training & Education	11.5	13.3	15.4	17.7	20.2	23.4	15.4%
Support & Maintenance	11.7	13.3	15.1	17.0	19.0	21.6	13.0%
DDoS Testing & Validation	7.9	9.1	10.5	12.0	13.6	15.7	14.7%
Total	66.3	76.7	88.2	100.8	114.4	131.7	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 159 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	46.9	54.7	63.3	72.9	83.6	97.7	15.8%
Threat Mitigation Systems	40.5	47.0	54.1	62.0	70.8	82.4	15.2%
Botnet Detection & Management	30.6	35.9	41.8	48.3	55.7	65.5	16.4%
Other Solution Types	26.5	30.5	34.9	39.7	45.0	52.0	14.4%
Total	144.6	168.2	194.1	222.9	255.1	297.6	15.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 160 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	112.6	129.2	147.4	167.1	188.2	215.1	13.8%
Threat Mitigation Systems	94.6	108.0	122.6	138.3	155.1	176.4	13.3%
Botnet Detection & Management	76.0	87.7	100.5	114.6	129.8	149.1	14.4%
Other Solution Types	59.3	67.2	75.7	84.8	94.4	106.5	12.4%
Total	342.5	392.1	446.2	504.9	567.4	647.0	13.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 161 CANADA: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	65.9	77.0	89.3	103.1	118.5	138.9	16.1%
Web Applications & APIs	59.9	70.8	83.1	96.9	112.7	133.5	17.4%
DNS Infrastructure	62.7	72.1	82.3	93.4	105.6	121.7	14.2%
Total	188.5	219.9	254.7	293.4	336.8	394.1	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 162 CANADA: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	160.7	184.8	211.4	240.3	271.5	311.1	14.1%
Web Applications & APIs	156.0	181.3	209.5	240.6	274.4	317.5	15.3%
DNS Infrastructure	138.4	156.4	175.7	196.2	217.6	244.7	12.1%
Total	455.0	522.5	596.6	677.1	763.5	873.3	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 163 CANADA: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	59.6	69.1	79.6	91.1	103.9	120.8	15.2%
Cloud	115.0	134.7	156.4	180.7	208.1	244.2	16.3%
Hybrid	13.8	16.2	18.7	21.6	24.8	29.0	16.0%
Total	188.5	219.9	254.7	293.4	336.8	394.1	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 164 CANADA: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	138.7	158.3	179.6	202.6	227.0	258.0	13.2%
Cloud	282.8	325.8	373.1	424.8	480.4	555.6	14.5%
Hybrid	33.5	38.4	43.9	49.8	56.0	59.7	12.2%
Total	455.0	522.5	596.6	677.1	763.5	873.3	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 165 CANADA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	110.4	128.0	147.2	168.4	192.0	223.1	15.1%
SMEs	78.0	91.9	107.5	125.0	144.8	171.0	17.0%
Total	188.5	219.9	254.7	293.4	336.8	394.1	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 166 CANADA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	255.7	291.6	330.5	372.4	416.8	473.3	13.1%
SMEs	199.3	231.0	266.1	304.7	346.6	400.0	15.0%
Total	455.0	522.5	596.6	677.1	763.5	873.3	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 167 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	37.3	44.4	52.5	61.6	72.1	85.9	18.2%
Government & Defense	26.7	30.5	34.5	38.9	43.6	49.9	13.3%
Healthcare	15.1	17.7	20.5	23.7	27.3	32.0	16.2%
IT & ITeS	13.7	16.2	19.0	22.2	25.8	30.6	17.5%
Telecommunications	19.6	22.7	26.0	29.7	33.8	39.1	14.8%
Manufacturing	9.7	11.1	12.6	14.3	16.2	18.6	13.9%
Energy & Utilities	25.0	29.4	34.3	39.8	46.0	54.2	16.7%
Retail	20.9	24.3	28.1	32.3	37.1	43.3	15.7%
Education	8.5	9.9	11.4	13.0	14.8	17.2	15.1%
Other Verticals	11.9	13.7	15.7	17.9	20.2	23.3	14.3%
Total	188.5	219.9	254.7	293.4	336.8	394.1	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 168 CANADA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	101.1	118.2	137.3	158.6	181.9	211.6	15.9%
Government & Defense	56.2	62.9	70.0	77.4	85.0	94.6	11.0%
Healthcare	37.0	42.6	48.8	55.5	62.7	71.9	14.2%
IT & ITeS	35.8	41.6	48.2	55.3	63.2	73.2	15.4%
Telecommunications	44.7	50.9	57.5	64.6	72.2	81.7	12.8%
Manufacturing	21.1	23.8	26.6	29.7	32.8	36.8	11.8%
Energy & Utilities	63.0	72.8	83.7	95.6	108.5	125.0	14.7%
Retail	49.9	57.2	65.1	73.8	83.1	94.8	13.7%
Education	19.8	22.5	25.5	28.8	32.2	36.6	13.1%
Other Verticals	26.5	30.0	33.7	37.7	41.8	47.1	12.2%
Total	455.0	522.5	596.6	677.1	763.5	873.3	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.3 EUROPE

Europe comprises major growing economies, including the UK, Germany, France, Italy, and Russia. The region has shown consistent growth in the adoption of DDoS protection and mitigation solutions. It is expected to hold the second-largest share of the DDoS protection and mitigation market, following North America. The increasing number of mobile users accessing significant amounts of business data has raised concerns about data security and privacy breaches in the region. Additionally, the widespread adoption of cloud technology has made data more accessible across enterprise networks. However, this growing reliance on cloud services has also led to an increase in sophisticated cyberattacks targeting cloud data. These concerns have led to the substantial adoption of solutions among European businesses.

Organizations in Europe are increasingly integrating advanced technologies, and there is massive growth in internet usage. According to a study by the European Consumer Centers Network (ECC-Net), 70% of Europeans use the internet regularly, and 45% shop online, indicating a significant increase in internet use in this region. Organizations in this region deploy DDoS protection and mitigation solutions to tackle advanced DDoS and cyberattacks. In July 2022, Akamai detected and mitigated the largest DDoS attack ever launched against European customers on the Prolexic platform, with globally distributed attack traffic peaking at 853.7 Gbps and 659.6 Gbps over a 14-hour period. The attack had targeted a swath of customer IP addresses. Factors such as data security and data sovereignty are compelling enterprises in Europe to adopt DDoS protection and mitigation solutions. Furthermore, the strong involvement of European governments in strengthening organizations' data security is driving the adoption of DDoS protection and mitigation solutions.

TABLE 169 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	550.5	647.0	755.7	875.4	1,007.2	1,172.4	16.3%
Services	167.3	199.2	235.8	276.7	322.5	380.3	17.9%
Total	717.7	846.3	991.5	1,152.1	1,329.6	1,552.7	16.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 170 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	1,338.1	1,523.2	1,729.2	1,958.0	2,209.2	2,503.4	13.3%
Services	439.6	506.7	582.6	668.0	763.2	875.6	14.8%
Total	1,777.7	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 171 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	236.9	277.2	322.3	371.5	425.4	492.9	15.8%
Software/Platforms	313.6	369.8	433.5	503.9	581.7	679.5	16.7%
Total	550.5	647.0	755.7	875.4	1,007.2	1,172.4	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 172 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	559.9	634.2	716.5	807.3	906.4	1,022.2	12.8%
Software/Platforms	778.3	889.0	1,012.7	1,150.7	1,302.8	1,481.2	13.7%
Total	1,338.1	1,523.2	1,729.2	1,958.0	2,209.2	2,503.4	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 173 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	96.8	114.9	135.7	158.8	184.6	217.1	17.5%
Managed Services	70.5	84.3	100.1	117.9	137.9	163.1	18.3%
Total	167.3	199.2	235.8	276.7	322.5	380.3	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 174 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	250.3	287.8	330.0	377.4	430.1	492.1	14.5%
Managed Services	189.2	218.9	252.5	290.6	333.1	383.5	15.2%
Total	439.6	506.7	582.6	668.0	763.2	875.6	14.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 175 EUROPE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	26.8	31.7	37.2	43.3	50.1	58.6	16.9%
Consulting & Advisory	23.5	28.2	33.7	40.0	47.0	56.0	19.0%
Training & Education	15.9	19.0	22.6	26.6	31.1	36.8	18.3%
Support & Maintenance	19.0	22.3	25.9	30.0	34.4	39.9	16.0%
DDoS Testing & Validation	11.5	13.7	16.2	18.9	22.0	25.9	17.5%
Total	96.8	114.9	135.7	158.8	184.6	217.1	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 176 EUROPE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	67.1	76.8	87.5	99.5	112.8	128.3	13.8%
Consulting & Advisory	65.3	75.9	88.0	101.8	117.3	135.7	15.8%
Training & Education	42.7	49.4	57.0	65.6	75.1	86.5	15.1%
Support & Maintenance	45.4	51.4	58.2	65.6	73.6	83.0	12.8%
DDoS Testing & Validation	29.8	34.3	39.3	45.0	51.3	58.7	14.5%
Total	250.3	287.8	330.0	377.4	430.1	492.1	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 177 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	181.9	213.8	249.6	289.1	332.4	386.8	16.3%
Threat Mitigation Systems	167.6	197.3	230.8	267.8	308.7	360.1	16.5%
Botnet Detection & Management	108.5	128.1	150.3	174.8	201.9	236.0	16.8%
Other Solution Types	92.5	107.9	125.0	143.7	164.1	189.6	15.4%
Total	550.5	647.0	755.7	875.4	1,007.2	1,172.4	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 178 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	441.2	501.9	569.3	644.1	726.1	821.9	13.2%
Threat Mitigation Systems	411.9	469.9	534.7	606.8	686.4	779.8	13.6%
Botnet Detection & Management	270.3	308.8	351.8	399.8	452.6	514.4	13.7%
Other Solution Types	214.7	242.6	273.4	307.3	344.2	387.2	12.5%
Total	1,338.1	1,523.2	1,729.2	1,958.0	2,209.2	2,503.4	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 179 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	250.8	296.3	347.7	404.7	467.9	547.4	16.9%
Web Applications & APIs	228.1	272.5	323.3	380.5	444.7	525.8	18.2%
DNS Infrastructure	238.8	277.5	320.4	366.8	417.0	479.6	15.0%
Total	717.7	846.3	991.5	1,152.1	1,329.6	1,552.7	16.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 180 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	627.8	718.0	819.2	932.1	1,056.9	1,203.6	13.9%
Web Applications & APIs	609.4	704.3	811.7	933.0	1,068.4	1,228.7	15.1%
DNS Infrastructure	540.6	607.6	680.9	760.9	847.1	946.8	11.9%
Total	1,777.7	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 181 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	227.0	266.0	309.7	357.7	410.2	476.1	16.0%
Cloud	438.1	518.1	608.9	709.7	821.5	962.3	17.0%
Hybrid	52.7	62.2	72.9	84.8	97.9	114.3	16.8%
Total	717.7	846.3	991.5	1,152.1	1,329.6	1,552.7	16.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 182 EUROPE: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	541.8	614.8	695.9	785.6	883.7	998.4	13.0%
Cloud	1,105.1	1,265.7	1,445.9	1,647.4	1,870.5	2,149.7	14.2%
Hybrid	130.9	149.4	170.0	193.0	218.2	230.8	12.0%
Total	1,777.7	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 183 EUROPE: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	449.3	526.4	612.7	707.4	811.1	940.9	15.9%
SMEs	268.4	319.9	378.8	444.7	518.6	611.8	17.9%
Total	717.7	846.3	991.5	1,152.1	1,329.6	1,552.7	16.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 184 EUROPE: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	1,070.2	1,213.9	1,373.2	1,549.3	1,741.8	1,966.6	12.9%
SMEs	707.5	816.0	938.6	1,076.6	1,230.6	1,412.4	14.8%
Total	1,777.7	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 185 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	142.0	170.8	204.2	241.9	284.6	338.6	19.0%
Government & Defense	101.7	117.3	134.5	152.7	172.2	196.4	14.1%
Healthcare	57.6	68.1	80.0	93.1	107.8	126.1	17.0%
IT & ITeS	52.1	62.2	73.9	87.1	101.9	120.6	18.3%
Telecommunications	74.8	87.2	101.0	116.1	132.4	152.9	15.4%
Manufacturing	36.8	42.7	49.2	56.2	63.8	73.2	14.7%
Energy & Utilities	95.3	113.2	133.5	156.2	181.5	213.4	17.5%
Retail	79.6	93.6	109.5	127.0	146.3	170.5	16.5%
Education	32.5	38.0	44.3	51.1	58.6	67.9	15.9%
Other Verticals	45.4	53.0	61.4	70.6	80.6	93.1	15.4%
Total	717.7	846.3	991.5	1,152.1	1,329.6	1,552.7	16.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 186 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	394.9	459.1	532.2	615.1	708.3	818.9	15.7%
Government & Defense	219.5	244.5	271.4	300.3	330.9	366.0	10.8%
Healthcare	144.7	165.7	189.1	215.3	244.3	278.3	14.0%
IT & ITeS	139.8	161.8	186.6	214.6	246.0	283.1	15.1%
Telecommunications	173.0	195.2	219.7	246.6	275.7	309.5	12.3%
Manufacturing	82.3	92.3	103.2	115.0	127.7	142.3	11.6%
Energy & Utilities	246.0	282.8	324.3	370.8	422.5	483.5	14.5%
Retail	194.8	222.0	252.4	286.2	323.4	366.8	13.5%
Education	77.2	87.5	99.0	111.6	125.4	141.6	12.9%
Other Verticals	105.4	118.9	133.9	150.3	168.2	188.9	12.4%
Total	1,777.7	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 187 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)

Country	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
UK	153.9	178.5	206.0	235.8	268.1	308.4	14.9%
Germany	173.0	202.2	234.8	270.3	308.9	357.2	15.6%
France	87.2	105.1	125.9	149.6	176.5	210.6	19.3%
Italy	64.3	76.7	90.9	106.9	124.8	147.5	18.1%
Rest of Europe	239.4	283.7	333.9	389.5	451.3	529.0	17.2%
Total	717.7	846.3	991.5	1,152.1	1,329.6	1,552.7	16.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 188 EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
UK	347.7	391.0	438.3	489.9	545.5	609.5	11.9%
Germany	404.9	457.6	515.8	579.7	649.1	730.9	12.5%
France	246.5	287.6	334.7	387.0	446.6	517.7	16.0%
Italy	170.9	197.5	227.6	261.7	299.9	345.1	15.1%
Rest of Europe	607.7	696.2	795.4	907.7	1,031.3	1,175.8	14.1%
Total	1,777.7	2,029.9	2,311.8	2,626.0	2,972.4	3,379.0	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.3.1 UK

15.3.1.1 Increasing demand for monitoring solutions among SMEs to drive market

The UK is expected to be the largest contributor to the European DDoS protection and mitigation market, as it is one of the developed economies in the region. It has a dynamic demography, a robust IT infrastructure, and a strong economy. The UK comprises major growing verticals, which offer significant growth opportunities for DDoS protection and mitigation solution providers. Cybercrime in Europe is becoming increasingly aggressive and confrontational, driven by the growing use of extortion through DDoS attacks, ransomware, and data extortion. Cybercriminals and hackers in the region are using advanced techniques to attack organizations' confidential information. The urgent need to prevent the increasing spear-phishing attacks, security breaches, and incidents is the major factor expected to drive the growth of the UK's DDoS protection and mitigation market. The UK, being well-connected across Europe, has long been a prime target for cyberattacks. Recently, multiple Voice over Internet Protocol (VoIP) services in the UK witnessed a massive and coordinated attack. Comms Council UK announced that several members were impacted by the DDoS attack, which was suspected to be an extortion scheme against VoIP providers across the region. The growing need for comprehensive technologies to manage network infrastructure has made the UK a more lucrative market for vendors offering DDoS protection and mitigation solutions. The adoption trend is expected to rise in the future due to the increasing demand for DDoS protection and mitigation solutions among SMEs.

TABLE 189 UK: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	118.0	136.5	157.0	179.2	203.1	232.9	14.6%
Services	35.9	42.0	49.0	56.6	65.0	75.5	16.1%
Total	153.9	178.5	206.0	235.8	268.1	308.4	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 190 UK: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	261.8	293.4	327.8	365.3	405.4	451.6	11.5%
Services	86.0	97.6	110.4	124.6	140.1	157.9	12.9%
Total	347.7	391.0	438.3	489.9	545.5	609.5	11.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 191 UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	50.0	57.5	65.9	74.9	84.4	96.4	14.0%
Software/Platforms	68.0	78.9	91.1	104.3	118.7	136.5	15.0%
Total	118.0	136.5	157.0	179.2	203.1	232.9	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 192 UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	107.8	120.3	133.7	148.3	163.8	181.6	11.0%
Software/Platforms	153.9	173.1	194.1	217.0	241.6	270.0	11.9%
Total	261.8	293.4	327.8	365.3	405.4	451.6	11.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 193 UK: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	20.7	24.2	28.2	32.5	37.2	43.1	15.8%
Managed Services	15.1	17.8	20.8	24.1	27.8	32.4	16.5%
Total	35.9	42.0	49.0	56.6	65.0	75.5	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 194 UK: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	49.0	55.4	62.6	70.4	78.9	88.8	12.6%
Managed Services	37.0	42.2	47.9	54.2	61.1	69.2	13.3%
Total	86.0	97.6	110.4	124.6	140.1	157.9	12.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 195 UK: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	5.7	6.7	7.7	8.9	10.1	11.6	15.1%
Consulting & Advisory	5.0	6.0	7.0	8.2	9.5	11.1	17.2%
Training & Education	3.4	4.0	4.7	5.5	6.3	7.3	16.5%
Support & Maintenance	4.1	4.7	5.4	6.1	6.9	7.9	14.3%
DDoS Testing & Validation	2.5	2.9	3.4	3.9	4.4	5.1	15.8%
Total	20.7	24.2	28.2	32.5	37.2	43.1	15.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 196 UK: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	13.1	14.8	16.6	18.6	20.7	23.1	12.0%
Consulting & Advisory	12.8	14.6	16.7	19.0	21.5	24.5	13.9%
Training & Education	8.4	9.5	10.8	12.2	13.8	15.6	13.3%
Support & Maintenance	8.9	9.9	11.0	12.2	13.5	15.0	11.0%
DDoS Testing & Validation	5.8	6.6	7.5	8.4	9.4	10.6	12.6%
Total	49.0	55.4	62.6	70.4	78.9	88.8	12.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 197 UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	39.1	45.4	52.3	59.8	67.9	78.1	14.8%
Threat Mitigation Systems	34.0	39.2	45.0	51.3	58.0	66.3	14.3%
Botnet Detection & Management	25.6	29.8	34.6	39.7	45.4	52.4	15.4%
Other Solution Types	19.3	22.1	25.1	28.3	31.8	36.1	13.3%
Total	118.0	136.5	157.0	179.2	203.1	232.9	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 198 UK: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	87.9	98.7	110.6	123.5	137.3	153.3	11.8%
Threat Mitigation Systems	74.4	83.1	92.7	103.0	114.1	126.7	11.2%
Botnet Detection & Management	59.4	67.1	75.5	84.7	94.8	106.3	12.3%
Other Solution Types	40.1	44.4	49.1	54.1	59.3	65.3	10.3%
Total	261.8	293.4	327.8	365.3	405.4	451.6	11.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 199 UK: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	53.8	62.5	72.2	82.8	94.4	108.7	15.1%
Web Applications & APIs	48.9	57.5	67.2	77.9	89.7	104.4	16.4%
DNS Infrastructure	51.2	58.5	66.6	75.1	84.1	95.3	13.2%
Total	153.9	178.5	206.0	235.8	268.1	308.4	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 200 UK: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	122.8	138.3	155.3	173.9	194.0	217.1	12.1%
Web Applications & APIs	119.2	135.6	153.9	174.1	196.1	221.6	13.2%
DNS Infrastructure	105.7	117.0	129.1	141.9	155.5	170.8	10.1%
Total	347.7	391.0	438.3	489.9	545.5	609.5	11.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 201 UK: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	48.7	56.1	64.3	73.2	82.7	94.6	14.2%
Cloud	93.9	109.3	126.5	145.3	165.7	191.1	15.3%
Hybrid	11.3	13.1	15.1	17.4	19.7	22.7	15.0%
Total	153.9	178.5	206.0	235.8	268.1	308.4	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 202 UK: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	106.0	118.4	131.9	146.6	162.2	180.1	11.2%
Cloud	216.2	243.8	274.1	307.3	343.3	387.7	12.4%
Hybrid	25.6	28.8	32.2	36.0	40.0	41.6	10.2%
Total	347.7	391.0	438.3	489.9	545.5	609.5	11.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 203 UK: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	96.3	111.0	127.3	144.8	163.6	186.9	14.2%
SMEs	57.5	67.5	78.7	91.0	104.6	121.5	16.1%
Total	153.9	178.5	206.0	235.8	268.1	308.4	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 204 UK: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	209.3	233.8	260.3	289.0	319.7	354.7	11.1%
SMEs	138.4	157.2	177.9	200.9	225.8	254.8	13.0%
Total	347.7	391.0	438.3	489.9	545.5	609.5	11.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 205 UK: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	30.4	36.0	42.4	49.5	57.4	67.3	17.2%
Government & Defense	21.8	24.7	27.9	31.3	34.7	39.0	12.4%
Healthcare	12.4	14.4	16.6	19.1	21.7	25.1	15.2%
IT & ITeS	11.2	13.1	15.4	17.8	20.5	23.9	16.5%
Telecommunications	16.0	18.4	21.0	23.8	26.7	30.4	13.6%
Manufacturing	7.9	9.0	10.2	11.5	12.9	14.5	13.0%
Energy & Utilities	20.4	23.9	27.7	32.0	36.6	42.4	15.7%
Retail	17.1	19.7	22.7	26.0	29.5	33.9	14.7%
Education	7.0	8.0	9.2	10.5	11.8	13.5	14.1%
Other Verticals	9.7	11.2	12.8	14.5	16.3	18.5	13.7%
Total	153.9	178.5	206.0	235.8	268.1	308.4	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 206 UK: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	77.2	88.4	100.9	114.8	130.0	147.7	13.8%
Government & Defense	42.9	47.1	51.5	56.0	60.7	66.0	9.0%
Healthcare	28.3	31.9	35.9	40.2	44.8	50.2	12.1%
IT & ITeS	27.4	31.2	35.4	40.0	45.1	51.1	13.3%
Telecommunications	33.8	37.6	41.7	46.0	50.6	55.8	10.5%
Manufacturing	16.1	17.8	19.6	21.5	23.4	25.7	9.8%
Energy & Utilities	48.1	54.5	61.5	69.2	77.5	87.2	12.6%
Retail	38.1	42.8	47.9	53.4	59.3	66.2	11.7%
Education	15.1	16.9	18.8	20.8	23.0	25.5	11.1%
Other Verticals	20.6	22.9	25.4	28.0	30.9	34.1	10.6%
Total	347.7	391.0	438.3	489.9	545.5	609.5	11.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.3.2 GERMANY

15.3.2.1 Increasing investments in DDoS protection and mitigation solutions to drive market

Germany is the second-largest market for DDoS protection and mitigation in Europe. Organizations in Germany are planning to increase their investments in DDoS protection and mitigation solutions. Businesses and citizens in Germany are dependent on the reliable functioning of ICT and the internet. Hence, the confidentiality of sensitive data and information has become a vital question of the 21st century. The country's Federal Ministry of the Interior has established an expert team to address IT security. The increasing number of cybercrimes indicates that Germany is a potential market for DDoS protection and mitigation vendors.

TABLE 207 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	132.7	154.6	179.0	205.4	234.0	269.7	15.2%
Services	40.3	47.6	55.8	64.9	74.9	87.5	16.8%
Total	173.0	202.2	234.8	270.3	308.9	357.2	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 208 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	304.8	343.4	385.8	432.3	482.4	541.5	12.2%
Services	100.1	114.2	130.0	147.5	166.7	189.4	13.6%
Total	404.9	457.6	515.8	579.7	649.1	730.9	12.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 209 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	58.9	68.4	78.8	90.0	102.0	117.1	14.7%
Software/Platforms	73.8	86.3	100.2	115.4	132.0	152.7	15.7%
Total	132.7	154.6	179.0	205.4	234.0	269.7	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 210 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	131.7	147.6	165.1	184.0	204.4	228.3	11.6%
Software/Platforms	173.1	195.8	220.8	248.2	278.1	313.2	12.6%
Total	304.8	343.4	385.8	432.3	482.4	541.5	12.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 211 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	23.3	27.5	32.1	37.3	42.9	50.0	16.5%
Managed Services	17.0	20.1	23.7	27.7	32.0	37.5	17.2%
Total	40.3	47.6	55.8	64.9	74.9	87.5	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 212 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	57.0	64.9	73.6	83.3	93.9	106.4	13.3%
Managed Services	43.1	49.4	56.3	64.1	72.7	82.9	14.0%
Total	100.1	114.2	130.0	147.5	166.7	189.4	13.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 213 GERMANY: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	6.5	7.6	8.8	10.2	11.6	13.5	15.8%
Consulting & Advisory	5.7	6.7	8.0	9.4	10.9	12.9	17.9%
Training & Education	3.8	4.6	5.4	6.2	7.2	8.5	17.2%
Support & Maintenance	4.6	5.3	6.1	7.0	8.0	9.2	14.9%
DDoS Testing & Validation	2.8	3.3	3.8	4.4	5.1	6.0	16.5%
Total	23.3	27.5	32.1	37.3	42.9	50.0	16.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 214 GERMANY: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	15.3	17.3	19.5	22.0	24.6	27.7	12.7%
Consulting & Advisory	14.9	17.1	19.6	22.5	25.6	29.3	14.6%
Training & Education	9.7	11.1	12.7	14.5	16.4	18.7	14.0%
Support & Maintenance	10.3	11.6	13.0	14.5	16.1	18.0	11.7%
DDoS Testing & Validation	6.8	7.7	8.8	9.9	11.2	12.7	13.3%
Total	57.0	64.9	73.6	83.3	93.9	106.4	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 215 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	43.7	51.1	59.3	68.1	77.8	89.9	15.5%
Threat Mitigation Systems	37.5	43.5	50.3	57.5	65.4	75.2	15.0%
Botnet Detection & Management	28.1	33.0	38.5	44.5	51.1	59.4	16.2%
Other Solution Types	23.4	27.0	30.9	35.2	39.7	45.3	14.1%
Total	132.7	154.6	179.0	205.4	234.0	269.7	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 216 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	101.8	114.9	129.4	145.2	162.4	182.7	12.4%
Threat Mitigation Systems	84.8	95.3	106.8	119.3	132.8	148.7	11.9%
Botnet Detection & Management	67.6	76.8	86.9	98.1	110.3	124.8	13.0%
Other Solution Types	50.6	56.5	62.8	69.6	76.9	85.3	11.0%
Total	304.8	343.4	385.8	432.3	482.4	541.5	12.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 217 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	60.5	70.8	82.3	94.9	108.7	125.9	15.8%
Web Applications & APIs	55.0	65.1	76.6	89.3	103.3	121.0	17.1%
DNS Infrastructure	57.6	66.3	75.9	86.1	96.9	110.3	13.9%
Total	173.0	202.2	234.8	270.3	308.9	357.2	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 218 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	143.0	161.9	182.8	205.8	230.8	260.3	12.7%
Web Applications & APIs	138.8	158.8	181.1	206.0	233.3	265.8	13.9%
DNS Infrastructure	123.1	137.0	151.9	168.0	185.0	204.8	10.7%
Total	404.9	457.6	515.8	579.7	649.1	730.9	12.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 219 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	54.7	63.6	73.3	83.9	95.3	109.5	14.9%
Cloud	105.6	123.8	144.2	166.5	190.9	221.4	16.0%
Hybrid	12.7	14.9	17.3	19.9	22.7	26.3	15.7%
Total	173.0	202.2	234.8	270.3	308.9	357.2	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 220 GERMANY: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	123.4	138.6	155.3	173.4	193.0	216.0	11.8%
Cloud	251.7	285.4	322.6	363.7	408.5	465.0	13.1%
Hybrid	29.8	33.7	37.9	42.6	47.7	49.9	10.9%
Total	404.9	457.6	515.8	579.7	649.1	730.9	12.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 221 GERMANY: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	108.3	125.8	145.1	165.9	188.4	216.5	14.9%
SMEs	64.7	76.4	89.7	104.3	120.5	140.7	16.8%
Total	173.0	202.2	234.8	270.3	308.9	357.2	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 222 GERMANY: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	243.7	273.7	306.4	342.0	380.4	425.4	11.8%
SMEs	161.1	184.0	209.4	237.7	268.7	305.5	13.6%
Total	404.9	457.6	515.8	579.7	649.1	730.9	12.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 223 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	34.2	40.8	48.4	56.8	66.1	77.9	17.9%
Government & Defense	24.5	28.0	31.8	35.8	40.0	45.2	13.0%
Healthcare	13.9	16.3	18.9	21.9	25.0	29.0	15.9%
IT & ITeS	12.5	14.9	17.5	20.4	23.7	27.7	17.2%
Telecommunications	18.0	20.8	23.9	27.2	30.8	35.2	14.3%
Manufacturing	8.9	10.2	11.7	13.2	14.8	16.8	13.6%
Energy & Utilities	23.0	27.0	31.6	36.6	42.2	49.1	16.4%
Retail	19.2	22.4	25.9	29.8	34.0	39.2	15.4%
Education	7.8	9.1	10.5	12.0	13.6	15.6	14.8%
Other Verticals	10.9	12.7	14.5	16.6	18.7	21.4	14.4%
Total	173.0	202.2	234.8	270.3	308.9	357.2	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 224 GERMANY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	89.9	103.5	118.7	135.8	154.7	177.1	14.5%
Government & Defense	50.0	55.1	60.6	66.3	72.3	79.2	9.6%
Healthcare	33.0	37.4	42.2	47.5	53.3	60.2	12.8%
IT & ITeS	31.9	36.5	41.6	47.4	53.7	61.2	14.0%
Telecommunications	39.4	44.0	49.0	54.4	60.2	67.0	11.2%
Manufacturing	18.7	20.8	23.0	25.4	27.9	30.8	10.4%
Energy & Utilities	56.0	63.8	72.4	81.9	92.3	104.6	13.3%
Retail	44.4	50.1	56.3	63.2	70.6	79.3	12.3%
Education	17.6	19.7	22.1	24.6	27.4	30.6	11.7%
Other Verticals	24.0	26.8	29.9	33.2	36.7	40.9	11.2%
Total	404.9	457.6	515.8	579.7	649.1	730.9	12.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.3.3 FRANCE

15.3.3.1 Market is driven by the growing exposure of critical sectors to cyber threats

France represents a significant market for DDoS protection and mitigation, driven by the growing exposure of government, enterprises, telecommunications, and critical infrastructure to cyber threats. The country's highly digitalized economy and expanding dependence on online services are increasing the importance of maintaining network and application availability. According to France's cybersecurity agency ANSSI, DDoS attacks targeting French entities doubled in 2024, with heightened activity observed during the Paris Olympic Games. ANSSI also explicitly recommends the use of dedicated DDoS protection services to reduce the risk of service unavailability. Increasing geopolitical tensions, hacktivist activity, regulatory developments such as NIS2, and the protection of critical infrastructure are expected to further drive demand for advanced DDoS mitigation solutions and services in France.

TABLE 225 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	66.9	80.4	96.0	113.7	133.7	159.1	18.9%
Services	20.3	24.7	29.9	35.9	42.8	51.6	20.5%
Total	87.2	105.1	125.9	149.6	176.5	210.6	19.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 226 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	185.5	215.8	250.3	288.5	331.9	383.5	15.6%
Services	60.9	71.8	84.3	98.4	114.7	134.1	17.1%
Total	246.5	287.6	334.7	387.0	446.6	517.7	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 227 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	28.3	33.9	40.3	47.5	55.6	65.8	18.4%
Software/Platforms	38.5	46.5	55.7	66.2	78.1	93.2	19.3%
Total	66.9	80.4	96.0	113.7	133.7	159.1	18.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 228 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	76.4	88.5	102.1	117.1	134.1	154.2	15.1%
Software/Platforms	109.1	127.3	148.2	171.4	197.8	229.3	16.0%
Total	185.5	215.8	250.3	288.5	331.9	383.5	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 229 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	11.8	14.3	17.2	20.6	24.5	29.5	20.2%
Managed Services	8.6	10.5	12.7	15.3	18.3	22.1	20.9%
Total	20.3	24.7	29.9	35.9	42.8	51.6	20.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 230 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	34.7	40.8	47.8	55.6	64.6	75.4	16.8%
Managed Services	26.2	31.0	36.6	42.8	50.1	58.8	17.5%
Total	60.9	71.8	84.3	98.4	114.7	134.1	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 231 FRANCE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	3.3	3.9	4.7	5.6	6.6	7.9	19.5%
Consulting & Advisory	2.9	3.5	4.3	5.2	6.2	7.6	21.6%
Training & Education	1.9	2.4	2.9	3.5	4.1	5.0	20.9%
Support & Maintenance	2.3	2.8	3.3	3.9	4.6	5.4	18.6%
DDoS Testing & Validation	1.4	1.7	2.1	2.5	2.9	3.5	20.2%
Total	11.8	14.3	17.2	20.6	24.5	29.5	20.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 232 FRANCE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	9.3	10.9	12.7	14.7	16.9	19.7	16.1%
Consulting & Advisory	9.0	10.8	12.7	15.0	17.6	20.8	18.1%
Training & Education	5.9	7.0	8.3	9.7	11.3	13.2	17.5%
Support & Maintenance	6.3	7.3	8.4	9.7	11.1	12.7	15.1%
DDoS Testing & Validation	4.1	4.9	5.7	6.6	7.7	9.0	16.8%
Total	34.7	40.8	47.8	55.6	64.6	75.4	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 233 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	22.1	26.4	31.3	36.7	42.8	50.5	17.9%
Threat Mitigation Systems	25.8	31.3	37.6	44.9	53.2	63.8	19.8%
Botnet Detection & Management	8.5	10.1	12.0	14.2	16.6	19.6	18.4%
Other Solution Types	10.5	12.6	15.1	17.9	21.1	25.2	19.2%
Total	66.9	80.4	96.0	113.7	133.7	159.1	18.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 234 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	58.3	67.2	77.3	88.3	100.6	115.2	14.6%
Threat Mitigation Systems	75.0	87.8	102.6	119.2	138.1	160.7	16.5%
Botnet Detection & Management	22.8	26.4	30.4	34.9	40.0	45.9	15.1%
Other Solution Types	29.5	34.4	40.0	46.2	53.2	61.7	15.9%
Total	185.5	215.8	250.3	288.5	331.9	383.5	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 235 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	30.5	36.8	44.2	52.6	62.1	74.3	19.5%
Web Applications & APIs	27.7	33.8	41.1	49.4	59.0	71.3	20.8%
DNS Infrastructure	29.0	34.5	40.7	47.6	55.4	65.1	17.5%
Total	87.2	105.1	125.9	149.6	176.5	210.6	19.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 236 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	87.0	101.7	118.6	137.4	158.8	184.4	16.2%
Web Applications & APIs	84.5	99.8	117.5	137.5	160.5	188.2	17.4%
DNS Infrastructure	75.0	86.1	98.6	112.1	127.3	145.1	14.1%
Total	246.5	287.6	334.7	387.0	446.6	517.7	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 237 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	27.6	33.0	39.3	46.4	54.5	64.6	18.6%
Cloud	53.2	64.4	77.3	92.1	109.0	130.5	19.7%
Hybrid	6.4	7.7	9.3	11.0	13.0	15.5	19.4%
Total	87.2	105.1	125.9	149.6	176.5	210.6	19.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 238 FRANCE: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	75.1	87.1	100.7	115.8	132.8	153.0	15.3%
Cloud	153.2	179.3	209.3	242.8	281.0	329.4	16.5%
Hybrid	18.1	21.2	24.6	28.4	32.8	35.4	14.3%
Total	246.5	287.6	334.7	387.0	446.6	517.7	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 239 FRANCE: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	54.6	65.4	77.8	91.9	107.7	127.7	18.5%
SMEs	32.6	39.7	48.1	57.7	68.8	83.0	20.5%
Total	87.2	105.1	125.9	149.6	176.5	210.6	19.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 240 FRANCE: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	148.4	172.0	198.8	228.3	261.7	301.3	15.2%
SMEs	98.1	115.6	135.9	158.7	184.9	216.4	17.1%
Total	246.5	287.6	334.7	387.0	446.6	517.7	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 241 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	17.2	21.2	25.9	31.4	37.8	45.9	21.6%
Government & Defense	12.4	14.6	17.1	19.8	22.9	26.6	16.6%
Healthcare	7.0	8.5	10.2	12.1	14.3	17.1	19.6%
IT & ITeS	6.3	7.7	9.4	11.3	13.5	16.4	20.9%
Telecommunications	9.1	10.8	12.8	15.1	17.6	20.7	18.0%
Manufacturing	4.5	5.3	6.3	7.3	8.5	9.9	17.3%
Energy & Utilities	11.6	14.1	17.0	20.3	24.1	29.0	20.1%
Retail	9.7	11.6	13.9	16.5	19.4	23.1	19.1%
Education	3.9	4.7	5.6	6.6	7.8	9.2	18.5%
Other Verticals	5.5	6.6	7.8	9.2	10.7	12.6	18.0%
Total	87.2	105.1	125.9	149.6	176.5	210.6	19.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 242 FRANCE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	54.8	65.0	77.0	90.6	106.4	125.5	18.0%
Government & Defense	30.4	34.6	39.3	44.3	49.7	56.1	13.0%
Healthcare	20.1	23.5	27.4	31.7	36.7	42.6	16.3%
IT & ITeS	19.4	22.9	27.0	31.6	37.0	43.4	17.5%
Telecommunications	24.0	27.7	31.8	36.3	41.4	47.4	14.6%
Manufacturing	11.4	13.1	14.9	16.9	19.2	21.8	13.8%
Energy & Utilities	34.1	40.1	46.9	54.6	63.5	74.1	16.8%
Retail	27.0	31.5	36.5	42.2	48.6	56.2	15.8%
Education	10.7	12.4	14.3	16.4	18.8	21.7	15.2%
Other Verticals	14.6	16.9	19.4	22.1	25.3	28.9	14.7%
Total	246.5	287.6	334.7	387.0	446.6	517.7	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.3.4 ITALY

15.3.4.1 The market is driven by increasing cyber threats in critical infrastructure

Italy represents a growing market for DDoS protection and mitigation, driven by increasing cyber threats targeting public administration, telecommunications, financial services, and other critical infrastructure. Geopolitical tensions and hacktivist activity have contributed to a rise in DDoS campaigns against Italian organizations. According to Italy's National Cybersecurity Agency (ACN), cyber events increased by 38% in 2025, with major peaks linked to four DDoS campaigns targeting national entities. Additionally, TIM's Cyber Security Report 2025 reported a 36% increase in DDoS attacks in Italy during 2024, reaching an average of 18 incidents per day. The growing frequency and scale of attacks are expected to drive investments in advanced DDoS detection, mitigation, and resilience solutions.

TABLE 243 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	49.3	58.6	69.3	81.2	94.5	111.4	17.7%
Services	15.0	18.1	21.6	25.7	30.3	36.1	19.2%
Total	64.3	76.7	90.9	106.9	124.8	147.5	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 244 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	128.6	148.2	170.3	195.1	222.9	255.7	14.7%
Services	42.3	49.3	57.4	66.6	77.0	89.4	16.2%
Total	170.9	197.5	227.6	261.7	299.9	345.1	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 245 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	21.9	25.9	30.5	35.6	41.2	48.3	17.2%
Software/Platforms	27.4	32.7	38.8	45.6	53.3	63.0	18.1%
Total	49.3	58.6	69.3	81.2	94.5	111.4	17.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 246 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	55.6	63.7	72.8	83.1	94.4	107.8	14.2%
Software/Platforms	73.1	84.5	97.4	112.1	128.5	147.9	15.1%
Total	128.6	148.2	170.3	195.1	222.9	255.7	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 247 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	8.7	10.4	12.4	14.7	17.3	20.6	18.9%
Managed Services	6.3	7.6	9.2	10.9	12.9	15.5	19.7%
Total	15.0	18.1	21.6	25.7	30.3	36.1	19.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 248 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	24.1	28.0	32.5	37.6	43.4	50.3	15.9%
Managed Services	18.2	21.3	24.9	29.0	33.6	39.2	16.6%
Total	42.3	49.3	57.4	66.6	77.0	89.4	16.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 249 ITALY: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	2.4	2.9	3.4	4.0	4.7	5.6	18.3%
Consulting & Advisory	2.1	2.6	3.1	3.7	4.4	5.3	20.4%
Training & Education	1.4	1.7	2.1	2.5	2.9	3.5	19.6%
Support & Maintenance	1.7	2.0	2.4	2.8	3.2	3.8	17.4%
DDoS Testing & Validation	1.0	1.2	1.5	1.8	2.1	2.5	18.9%
Total	8.7	10.4	12.4	14.7	17.3	20.6	18.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 250 ITALY: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	6.5	7.5	8.6	9.9	11.4	13.1	15.2%
Consulting & Advisory	6.3	7.4	8.7	10.1	11.8	13.9	17.2%
Training & Education	4.1	4.8	5.6	6.5	7.6	8.8	16.5%
Support & Maintenance	4.4	5.0	5.7	6.5	7.4	8.5	14.2%
DDoS Testing & Validation	2.9	3.3	3.9	4.5	5.2	6.0	15.9%
Total	24.1	28.0	32.5	37.6	43.4	50.3	15.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 251 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	16.3	19.3	22.6	26.2	30.2	35.3	16.7%
Threat Mitigation Systems	19.0	22.8	27.2	32.1	37.6	44.7	18.6%
Botnet Detection & Management	6.2	7.4	8.7	10.1	11.7	13.7	17.1%
Other Solution Types	7.7	9.2	10.9	12.8	14.9	17.6	18.0%
Total	49.3	58.6	69.3	81.2	94.5	111.4	17.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 252 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	40.4	46.2	52.6	59.7	67.6	76.8	13.7%
Threat Mitigation Systems	52.0	60.3	69.8	80.6	92.7	107.1	15.6%
Botnet Detection & Management	15.8	18.1	20.7	23.6	26.8	30.6	14.2%
Other Solution Types	20.4	23.6	27.2	31.2	35.8	41.1	15.0%
Total	128.6	148.2	170.3	195.1	222.9	255.7	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 253 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	22.5	26.8	31.9	37.5	43.9	52.0	18.3%
Web Applications & APIs	20.4	24.7	29.6	35.3	41.7	49.9	19.6%
DNS Infrastructure	21.4	25.1	29.4	34.0	39.1	45.5	16.3%
Total	64.3	76.7	90.9	106.9	124.8	147.5	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 254 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	60.3	69.9	80.7	92.9	106.6	122.9	15.3%
Web Applications & APIs	58.6	68.5	79.9	93.0	107.8	125.5	16.5%
DNS Infrastructure	52.0	59.1	67.0	75.8	85.5	96.7	13.2%
Total	170.9	197.5	227.6	261.7	299.9	345.1	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 255 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	20.3	24.1	28.4	33.2	38.5	45.2	17.3%
Cloud	39.2	46.9	55.8	65.8	77.1	91.4	18.4%
Hybrid	4.7	5.6	6.7	7.9	9.2	10.9	18.1%
Total	64.3	76.7	90.9	106.9	124.8	147.5	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 256 ITALY: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	52.1	59.8	68.5	78.3	89.2	102.0	14.4%
Cloud	106.2	123.1	142.4	164.2	188.7	219.6	15.6%
Hybrid	12.6	14.5	16.7	19.2	22.0	23.6	13.4%
Total	170.9	197.5	227.6	261.7	299.9	345.1	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 257 ITALY: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	40.2	47.7	56.2	65.6	76.1	89.4	17.3%
SMEs	24.0	29.0	34.7	41.3	48.7	58.1	19.3%
Total	64.3	76.7	90.9	106.9	124.8	147.5	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 258 ITALY: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	102.9	118.1	135.2	154.4	175.7	200.9	14.3%
SMEs	68.0	79.4	92.4	107.3	124.2	144.3	16.2%
Total	170.9	197.5	227.6	261.7	299.9	345.1	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 259 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	12.7	15.5	18.7	22.4	26.7	32.2	20.4%
Government & Defense	9.1	10.6	12.3	14.2	16.2	18.7	15.4%
Healthcare	5.2	6.2	7.3	8.6	10.1	12.0	18.3%
IT & ITeS	4.7	5.6	6.8	8.1	9.6	11.5	19.7%
Telecommunications	6.7	7.9	9.3	10.8	12.4	14.5	16.7%
Manufacturing	3.3	3.9	4.5	5.2	6.0	6.9	16.1%
Energy & Utilities	8.5	10.3	12.2	14.5	17.0	20.3	18.9%
Retail	7.1	8.5	10.0	11.8	13.7	16.2	17.8%
Education	2.9	3.4	4.1	4.7	5.5	6.4	17.3%
Other Verticals	4.1	4.8	5.6	6.5	7.6	8.8	16.8%
Total	64.3	76.7	90.9	106.9	124.8	147.5	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 260 ITALY: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	38.0	44.7	52.4	61.3	71.5	83.6	17.1%
Government & Defense	21.1	23.8	26.7	29.9	33.4	37.4	12.1%
Healthcare	13.9	16.1	18.6	21.5	24.6	28.4	15.4%
IT & ITeS	13.4	15.7	18.4	21.4	24.8	28.9	16.6%
Telecommunications	16.6	19.0	21.6	24.6	27.8	31.6	13.7%
Manufacturing	7.9	9.0	10.2	11.5	12.9	14.5	12.9%
Energy & Utilities	23.6	27.5	31.9	37.0	42.6	49.4	15.9%
Retail	18.7	21.6	24.9	28.5	32.6	37.5	14.9%
Education	7.4	8.5	9.7	11.1	12.7	14.5	14.3%
Other Verticals	10.1	11.6	13.2	15.0	17.0	19.3	13.8%
Total	170.9	197.5	227.6	261.7	299.9	345.1	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.3.5 REST OF EUROPE

This section includes countries like the Netherlands, the Czech Republic, and Ireland. Strong economic infrastructure and high internet penetration make these countries lucrative markets for DDoS protection and mitigation solutions, representing the fastest-growing revenue sectors. Public and private organizations in Europe are focusing on protecting the sensitive data of their employees and customers. European governments have begun taking initiatives to provide training and education programs for security professionals throughout the rest of Europe. The rest of Europe is expected to witness increased investment in DDoS protection and mitigation, as well as associated services, over the next five years.

TABLE 261 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	183.6	216.9	254.5	296.0	341.9	399.4	16.8%
Services	55.8	66.8	79.4	93.6	109.5	129.5	18.4%
Total	239.4	283.7	333.9	389.5	451.3	529.0	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 262 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	457.5	522.4	595.0	676.8	766.5	871.2	13.7%
Services	150.3	173.8	200.4	230.9	264.8	304.7	15.2%
Total	607.7	696.2	795.4	907.7	1,031.3	1,175.8	14.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 263 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	77.8	91.5	106.8	123.7	142.1	165.3	16.3%
Software/Platforms	105.8	125.5	147.7	172.3	199.7	234.1	17.2%
Total	183.6	216.9	254.5	296.0	341.9	399.4	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 264 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	188.4	214.1	242.7	274.8	309.7	350.3	13.2%
Software/Platforms	269.0	308.3	352.2	402.0	456.8	520.9	14.1%
Total	457.5	522.4	595.0	676.8	766.5	871.2	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 265 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	32.3	38.5	45.7	53.7	62.7	74.0	18.0%
Managed Services	23.5	28.3	33.7	39.9	46.8	55.6	18.8%
Total	55.8	66.8	79.4	93.6	109.5	129.5	18.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 266 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	85.6	98.7	113.6	130.4	149.2	171.2	14.9%
Managed Services	64.7	75.1	86.9	100.4	115.6	133.5	15.6%
Total	150.3	173.8	200.4	230.9	264.8	304.7	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 267 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	8.9	10.6	12.5	14.6	17.0	19.9	17.4%
Consulting & Advisory	7.8	9.5	11.4	13.5	16.0	19.1	19.5%
Training & Education	5.3	6.4	7.6	9.0	10.6	12.6	18.8%
Support & Maintenance	6.3	7.5	8.7	10.1	11.7	13.6	16.5%
DDoS Testing & Validation	3.8	4.6	5.4	6.4	7.5	8.8	18.0%
Total	32.3	38.5	45.7	53.7	62.7	74.0	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 268 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	23.0	26.3	30.1	34.4	39.1	44.6	14.2%
Consulting & Advisory	22.3	26.0	30.3	35.2	40.7	47.2	16.2%
Training & Education	14.6	16.9	19.6	22.7	26.1	30.1	15.5%
Support & Maintenance	15.5	17.6	20.0	22.7	25.5	28.9	13.2%
DDoS Testing & Validation	10.2	11.8	13.5	15.5	17.8	20.4	14.9%
Total	85.6	98.7	113.6	130.4	149.2	171.2	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 269 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	60.5	71.7	84.3	98.2	113.7	133.1	17.1%
Threat Mitigation Systems	51.3	60.4	70.7	82.0	94.5	110.2	16.5%
Botnet Detection & Management	40.2	47.8	56.5	66.2	77.1	90.7	17.7%
Other Solution Types	31.6	37.0	43.0	49.5	56.6	65.4	15.6%
Total	183.6	216.9	254.5	296.0	341.9	399.4	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 270 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	152.7	174.8	199.5	227.4	258.1	293.9	14.0%
Threat Mitigation Systems	125.8	143.4	162.8	184.8	208.7	236.6	13.5%
Botnet Detection & Management	104.7	120.5	138.2	158.4	180.7	206.8	14.6%
Other Solution Types	74.2	83.8	94.4	106.3	119.0	133.8	12.5%
Total	457.5	522.4	595.0	676.8	766.5	871.2	13.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 271 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	83.7	99.3	117.1	136.8	158.8	186.5	17.4%
Web Applications & APIs	76.1	91.3	108.9	128.7	150.9	179.1	18.7%
DNS Infrastructure	79.7	93.1	107.9	124.0	141.5	163.4	15.5%
Total	239.4	283.7	333.9	389.5	451.3	529.0	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 272 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	214.6	246.3	281.8	322.2	366.7	418.8	14.3%
Web Applications & APIs	208.3	241.6	279.3	322.5	370.7	427.6	15.5%
DNS Infrastructure	184.8	208.4	234.3	263.0	293.9	329.5	12.3%
Total	607.7	696.2	795.4	907.7	1,031.3	1,175.8	14.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 273 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	75.7	89.2	104.3	120.9	139.2	162.2	16.5%
Cloud	146.1	173.7	205.1	240.0	278.9	327.8	17.5%
Hybrid	17.6	20.8	24.6	28.7	33.2	38.9	17.3%
Total	239.4	283.7	333.9	389.5	451.3	529.0	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 274 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	185.2	210.9	239.4	271.5	306.6	347.4	13.4%
Cloud	377.8	434.1	497.5	569.4	649.0	748.1	14.6%
Hybrid	44.7	51.2	58.5	66.7	75.7	80.3	12.4%
Total	607.7	696.2	795.4	907.7	1,031.3	1,175.8	14.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 275 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	149.9	176.5	206.4	239.2	275.3	320.6	16.4%
SMEs	89.5	107.3	127.6	150.4	176.0	208.4	18.4%
Total	239.4	283.7	333.9	389.5	451.3	529.0	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 276 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	365.9	416.3	472.5	535.5	604.3	684.3	13.3%
SMEs	241.9	279.9	322.9	372.1	427.0	491.5	15.2%
Total	607.7	696.2	795.4	907.7	1,031.3	1,175.8	14.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 277 REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	47.4	57.3	68.8	81.8	96.6	115.4	19.5%
Government & Defense	33.9	39.3	45.3	51.6	58.5	66.9	14.6%
Healthcare	19.2	22.8	26.9	31.5	36.6	43.0	17.5%
IT & ITeS	17.4	20.9	24.9	29.5	34.6	41.1	18.8%
Telecommunications	24.9	29.2	34.0	39.2	45.0	52.1	15.9%
Manufacturing	12.3	14.3	16.6	19.0	21.6	24.9	15.2%
Energy & Utilities	31.8	37.9	45.0	52.8	61.6	72.7	18.0%
Retail	26.5	31.4	36.9	42.9	49.6	58.1	17.0%
Education	10.8	12.8	14.9	17.3	19.9	23.1	16.4%
Other Verticals	15.2	17.8	20.7	23.9	27.4	31.7	15.9%
Total	239.4	283.7	333.9	389.5	451.3	529.0	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 278 **REST OF EUROPE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)**

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	135.0	157.5	183.1	212.6	245.7	285.0	16.1%
Government & Defense	75.0	83.9	93.4	103.8	114.8	127.4	11.2%
Healthcare	49.5	56.8	65.1	74.4	84.8	96.9	14.4%
IT & ITeS	47.8	55.5	64.2	74.2	85.4	98.5	15.6%
Telecommunications	59.1	67.0	75.6	85.2	95.7	107.7	12.7%
Manufacturing	28.1	31.6	35.5	39.8	44.3	49.5	12.0%
Energy & Utilities	84.1	97.0	111.6	128.2	146.6	168.2	14.9%
Retail	66.6	76.2	86.8	98.9	112.2	127.7	13.9%
Education	26.4	30.0	34.1	38.6	43.5	49.3	13.3%
Other Verticals	36.0	40.8	46.1	52.0	58.4	65.7	12.8%
Total	607.7	696.2	795.4	907.7	1,031.3	1,175.8	14.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.4 ASIA PACIFIC

The Asia Pacific region is the fastest-growing market for DDoS protection and mitigation. Within this region, several prosperous economies, such as India, China, Australia, and New Zealand, have well-developed cyber ecosystems. These countries are rapidly adopting DDoS protection and mitigation solutions to enhance visibility into their networks. Large enterprises and SMEs in Asia Pacific are recognizing the significance of data security. They are now more receptive toward adopting dedicated DDoS protection and mitigation solutions to protect their critical and sensitive business data from commercial espionage, cyber threats, and computer hackers. Additionally, the increasing advancements in mobility and rising cloud adoption, coupled with mandatory compliance with certain government regulations for resolving data security issues, have compelled companies in the region to adopt DDoS protection and mitigation solutions. With the rising intensity and complexity of cyberattacks, the data security concerns of businesses in the region have further heightened. According to a NETSCOUT threat intelligence report, attacks in Asia Pacific increased by 7% as other regions subsided. Amid the ongoing geopolitical tensions in China, Hong Kong, and Taiwan, the Asia Pacific region saw the most significant increase in attacks year over year compared to other regions.

FIGURE 41 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET SNAPSHOT

Source: Interviews with Experts and MarketsandMarkets Analysis

TABLE 279 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	410.6	495.2	594.0	707.3	838.3	1,005.7	19.6%
Services	124.8	152.5	185.3	223.6	268.4	326.2	21.2%
Total	535.4	647.7	779.3	930.9	1,106.8	1,331.9	20.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 280 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	1,161.4	1,337.9	1,537.6	1,763.1	2,016.9	2,302.2	14.7%
Services	381.5	445.1	518.0	601.5	696.7	805.2	16.1%
Total	1,542.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 281 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	180.2	216.3	258.1	305.9	360.7	430.6	19.0%
Software/Platforms	230.4	278.9	335.8	401.4	477.6	575.1	20.1%
Total	410.6	495.2	594.0	707.3	838.3	1,005.7	19.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 282 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	494.7	567.0	648.3	739.5	841.5	955.7	14.1%
Software/Platforms	666.7	770.9	889.4	1,023.6	1,175.4	1,346.5	15.1%
Total	1,161.4	1,337.9	1,537.6	1,763.1	2,016.9	2,302.2	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 283 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	72.2	88.0	106.6	128.3	153.7	186.3	20.9%
Managed Services	52.6	64.5	78.7	95.2	114.8	139.9	21.6%
Total	124.8	152.5	185.3	223.6	268.4	326.2	21.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 284 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	217.3	252.8	293.5	339.8	392.6	452.5	15.8%
Managed Services	164.2	192.3	224.6	261.6	304.1	352.7	16.5%
Total	381.5	445.1	518.0	601.5	696.7	805.2	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 285 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	20.0	24.3	29.2	35.0	41.7	50.2	20.2%
Consulting & Advisory	17.5	21.6	26.5	32.3	39.1	48.0	22.3%
Training & Education	11.9	14.6	17.8	21.5	25.9	31.6	21.6%
Support & Maintenance	14.2	17.0	20.4	24.2	28.6	34.2	19.3%
DDoS Testing & Validation	8.6	10.5	12.7	15.3	18.3	22.2	20.9%
Total	72.2	88.0	106.6	128.3	153.7	186.3	20.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 286 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	58.3	67.4	77.8	89.6	102.9	118.0	15.2%
Consulting & Advisory	56.6	66.7	78.3	91.7	107.1	124.8	17.1%
Training & Education	37.1	43.4	50.7	59.0	68.6	79.5	16.5%
Support & Maintenance	39.4	45.2	51.7	59.0	67.2	76.3	14.2%
DDoS Testing & Validation	25.9	30.1	35.0	40.5	46.8	53.9	15.8%
Total	217.3	252.8	293.5	339.8	392.6	452.5	15.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 287 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	136.0	164.4	197.5	235.6	279.7	336.1	19.8%
Threat Mitigation Systems	118.2	142.1	170.0	202.0	238.8	285.7	19.3%
Botnet Detection & Management	88.7	107.8	130.4	156.5	186.9	226.0	20.6%
Other Solution Types	67.7	80.9	96.1	113.3	133.0	157.9	18.5%
Total	410.6	495.2	594.0	707.3	838.3	1,005.7	19.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 288 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	388.8	448.7	516.7	593.5	680.2	777.9	14.9%
Threat Mitigation Systems	329.2	378.3	433.7	496.1	566.1	644.6	14.4%
Botnet Detection & Management	263.0	305.3	353.6	408.5	470.8	541.5	15.5%
Other Solution Types	180.4	205.6	233.7	265.0	299.7	338.3	13.4%
Total	1,161.4	1,337.9	1,537.6	1,763.1	2,016.9	2,302.2	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 289 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	187.1	226.7	273.3	327.0	389.5	469.5	20.2%
Web Applications & APIs	170.1	208.5	254.1	307.5	370.2	451.0	21.5%
DNS Infrastructure	178.1	212.4	251.8	296.4	347.1	411.4	18.2%
Total	535.4	647.7	779.3	930.9	1,106.8	1,331.9	20.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 290 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	544.8	630.7	728.4	839.3	964.9	1,106.8	15.2%
Web Applications & APIs	528.9	618.6	721.8	840.1	975.4	1,129.9	16.4%
DNS Infrastructure	469.2	533.7	605.5	685.1	773.3	870.7	13.2%
Total	1,542.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 291 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	169.3	203.6	243.4	289.0	341.5	408.4	19.3%
Cloud	326.8	396.5	478.6	573.4	683.8	825.5	20.4%
Hybrid	39.3	47.6	57.3	68.5	81.5	98.0	20.1%
Total	535.4	647.7	779.3	930.9	1,106.8	1,331.9	20.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 292 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	470.2	540.0	618.8	707.4	806.8	918.2	14.3%
Cloud	959.1	1,111.8	1,285.7	1,483.4	1,707.6	1,976.9	15.6%
Hybrid	113.6	131.2	151.2	173.8	199.2	212.3	13.3%
Total	1,542.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 293 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	335.1	402.9	481.6	571.6	675.1	807.1	19.2%
SMEs	200.2	244.8	297.7	359.3	431.6	524.8	21.3%
Total	535.4	647.7	779.3	930.9	1,106.8	1,331.9	20.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 294 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	928.8	1,066.2	1,221.1	1,395.1	1,590.2	1,808.5	14.3%
SMEs	614.1	716.8	834.6	969.5	1,123.5	1,298.9	16.2%
Total	1,542.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 295 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	105.9	130.8	160.5	195.5	236.9	290.5	22.4%
Government & Defense	75.8	89.8	105.7	123.4	143.4	168.5	17.3%
Healthcare	43.0	52.1	62.9	75.3	89.7	108.2	20.3%
IT & ITeS	38.8	47.6	58.1	70.4	84.8	103.4	21.6%
Telecommunications	55.8	66.7	79.4	93.8	110.2	131.1	18.6%
Manufacturing	27.5	32.7	38.7	45.4	53.1	62.8	18.0%
Energy & Utilities	71.1	86.6	104.9	126.2	151.1	183.1	20.8%
Retail	59.4	71.7	86.1	102.6	121.7	146.2	19.8%
Education	24.2	29.1	34.8	41.3	48.7	58.3	19.2%
Other Verticals	33.9	40.6	48.3	57.1	67.1	79.8	18.7%
Total	535.4	647.7	779.3	930.9	1,106.8	1,331.9	20.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 296 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	342.7	403.3	473.2	553.9	646.6	753.1	17.1%
Government & Defense	190.5	214.8	241.4	270.4	302.1	336.6	12.1%
Healthcare	125.6	145.5	168.2	193.9	223.0	256.0	15.3%
IT & ITeS	121.4	142.1	165.9	193.3	224.6	260.3	16.5%
Telecommunications	150.1	171.5	195.4	222.0	251.7	284.7	13.6%
Manufacturing	71.4	81.1	91.7	103.6	116.6	130.9	12.9%
Energy & Utilities	213.5	248.5	288.4	333.9	385.7	444.6	15.8%
Retail	169.1	195.0	224.5	257.7	295.2	337.3	14.8%
Education	67.0	76.9	88.0	100.5	114.5	130.2	14.2%
Other Verticals	91.4	104.5	119.1	135.3	153.5	173.7	13.7%
Total	1,542.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 297 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)

Country	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
China	187.1	221.7	261.1	305.3	355.0	417.7	17.4%
India	53.6	66.1	81.0	98.5	119.2	145.9	22.2%
Japan	84.6	105.3	130.4	160.2	195.9	242.5	23.5%
Rest of Asia Pacific	210.1	254.7	306.8	366.9	436.6	525.8	20.1%
Total	535.4	647.7	779.3	930.9	1,106.8	1,331.9	20.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 298 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
China	476.7	542.7	616.3	698.3	789.5	890.5	13.3%
India	171.9	202.1	236.9	276.9	322.9	375.7	16.9%
Japan	288.8	343.1	406.7	480.8	563.6	661.0	18.0%
Rest of Asia Pacific	605.5	695.1	795.8	908.5	1,037.7	1,180.2	14.3%
Total	1,542.9	1,783.0	2,055.7	2,364.6	2,713.7	3,107.4	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.4.1 CHINA

15.4.1.1 Development of cybersecurity safeguard system to fuel market

China plays a key role in the technology and manufacturing landscape of Asia Pacific. It is heavily dependent on the internet for technological innovations, making business-critical applications more vulnerable to DDoS, cyber, and bot attacks. China's internet sector has experienced significant growth in recent years, which has also brought about increased cybersecurity risks. For example, cybersecurity risks on cloud platforms have increased, with the majority being Denial of Service attacks. There are numerous vulnerabilities, loopholes, and rogue programs in China's mobile internet, industrial internet, and blockchain systems. Understanding these risks, China's government has built a cybersecurity safeguard system. Several laws have been introduced in recent years, including those related to data security and key information infrastructure security. China also carries out data security investigations on several domestic companies. As a result, securing websites and applications is becoming a serious issue faced by Chinese organizations. Cybercriminals in this country use advanced attack techniques to penetrate an organization's IT environment. Organizations in China are increasingly adopting DDoS protection and mitigation solutions to secure their networks, mobile applications, APIs, and websites from sophisticated DDoS attacks and cyber threats.

TABLE 299 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	143.5	169.5	199.0	232.0	268.9	315.4	17.1%
Services	43.6	52.2	62.1	73.3	86.1	102.3	18.6%
Total	187.1	221.7	261.1	305.3	355.0	417.7	17.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 300 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	358.8	407.2	461.0	520.7	586.8	659.8	13.0%
Services	117.9	135.5	155.3	177.6	202.7	230.8	14.4%
Total	476.7	542.7	616.3	698.3	789.5	890.5	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 301 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	63.7	74.9	87.6	101.6	117.3	136.9	16.5%
Software/Platforms	79.8	94.6	111.4	130.3	151.7	178.5	17.5%
Total	143.5	169.5	199.0	232.0	268.9	315.4	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 302 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	155.0	175.1	197.2	221.7	248.6	278.2	12.4%
Software/Platforms	203.8	232.1	263.8	299.0	338.2	381.6	13.4%
Total	358.8	407.2	461.0	520.7	586.8	659.8	13.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 303 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	25.2	30.1	35.7	42.1	49.3	58.4	18.3%
Managed Services	18.4	22.1	26.4	31.2	36.8	43.9	19.0%
Total	43.6	52.2	62.1	73.3	86.1	102.3	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 304 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	67.1	76.9	88.0	100.4	114.2	129.7	14.1%
Managed Services	50.7	58.5	67.3	77.3	88.5	101.1	14.8%
Total	117.9	135.5	155.3	177.6	202.7	230.8	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 305 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	7.0	8.3	9.8	11.5	13.4	15.8	17.6%
Consulting & Advisory	6.1	7.4	8.9	10.6	12.6	15.1	19.7%
Training & Education	4.2	5.0	6.0	7.1	8.3	9.9	19.0%
Support & Maintenance	4.9	5.8	6.8	7.9	9.2	10.7	16.7%
DDoS Testing & Validation	3.0	3.6	4.3	5.0	5.9	7.0	18.3%
Total	25.2	30.1	35.7	42.1	49.3	58.4	18.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 306 CHINA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	18.0	20.5	23.3	26.5	29.9	33.8	13.4%
Consulting & Advisory	17.5	20.3	23.5	27.1	31.1	35.8	15.4%
Training & Education	11.5	13.2	15.2	17.4	20.0	22.8	14.7%
Support & Maintenance	12.2	13.8	15.5	17.4	19.6	21.9	12.5%
DDoS Testing & Validation	8.0	9.2	10.5	12.0	13.6	15.5	14.1%
Total	67.1	76.9	88.0	100.4	114.2	129.7	14.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 307 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	49.2	58.2	68.5	80.0	92.9	109.2	17.3%
Threat Mitigation Systems	42.2	49.8	58.3	67.8	78.4	91.7	16.8%
Botnet Detection & Management	31.1	37.0	43.8	51.4	60.1	71.0	18.0%
Other Solution Types	21.0	24.5	28.4	32.8	37.5	43.5	15.7%
Total	143.5	169.5	199.0	232.0	268.9	315.4	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 308 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	124.5	141.5	160.6	181.7	205.2	231.2	13.2%
Threat Mitigation Systems	104.1	117.8	133.1	150.0	168.6	189.1	12.7%
Botnet Detection & Management	81.4	93.1	106.2	120.8	137.1	155.3	13.8%
Other Solution Types	48.8	54.7	61.2	68.2	75.9	84.2	11.5%
Total	358.8	407.2	461.0	520.7	586.8	659.8	13.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 309 CHINA: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	65.4	77.6	91.6	107.2	124.9	147.3	17.6%
Web Applications & APIs	59.4	71.4	85.2	100.8	118.7	141.5	18.9%
DNS Infrastructure	62.2	72.7	84.4	97.2	111.3	129.0	15.7%
Total	187.1	221.7	261.1	305.3	355.0	417.7	17.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 310 CHINA: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	168.3	192.0	218.4	247.9	280.7	317.2	13.5%
Web Applications & APIs	163.4	188.3	216.4	248.1	283.8	323.8	14.7%
DNS Infrastructure	145.0	162.4	181.5	202.3	225.0	249.5	11.5%
Total	476.7	542.7	616.3	698.3	789.5	890.5	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 311 CHINA: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	59.2	69.7	81.6	94.8	109.5	128.1	16.7%
Cloud	114.2	135.7	160.4	188.0	219.4	258.9	17.8%
Hybrid	13.7	16.3	19.2	22.5	26.1	30.8	17.5%
Total	187.1	221.7	261.1	305.3	355.0	417.7	17.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 312 CHINA: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	145.3	164.4	185.5	208.9	234.7	263.1	12.6%
Cloud	296.3	338.4	385.5	438.1	496.8	566.6	13.8%
Hybrid	35.1	39.9	45.3	51.3	58.0	60.8	11.6%
Total	476.7	542.7	616.3	698.3	789.5	890.5	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 313 CHINA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	117.1	137.9	161.4	187.4	216.6	253.2	16.7%
SMEs	70.0	83.8	99.8	117.8	138.5	164.6	18.7%
Total	187.1	221.7	261.1	305.3	355.0	417.7	17.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 314 CHINA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	287.0	324.5	366.1	412.0	462.6	518.3	12.6%
SMEs	189.7	218.2	250.2	286.3	326.8	372.2	14.4%
Total	476.7	542.7	616.3	698.3	789.5	890.5	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 315 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	37.0	44.8	53.8	64.1	76.0	91.1	19.7%
Government & Defense	26.5	30.7	35.4	40.5	46.0	52.9	14.8%
Healthcare	15.0	17.8	21.1	24.7	28.8	33.9	17.7%
IT & ITeS	13.6	16.3	19.5	23.1	27.2	32.4	19.0%
Telecommunications	19.5	22.8	26.6	30.8	35.4	41.1	16.1%
Manufacturing	9.6	11.2	13.0	14.9	17.0	19.7	15.4%
Energy & Utilities	24.8	29.6	35.2	41.4	48.5	57.4	18.2%
Retail	20.7	24.5	28.8	33.6	39.1	45.9	17.2%
Education	8.5	10.0	11.7	13.5	15.6	18.3	16.6%
Other Verticals	11.8	13.9	16.2	18.7	21.5	25.0	16.2%
Total	187.1	221.7	261.1	305.3	355.0	417.7	17.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 316 CHINA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	105.9	122.7	141.9	163.6	188.1	215.8	15.3%
Government & Defense	58.9	65.4	72.4	79.9	87.9	96.5	10.4%
Healthcare	38.8	44.3	50.4	57.3	64.9	73.4	13.6%
IT & ITeS	37.5	43.2	49.7	57.1	65.3	74.6	14.8%
Telecommunications	46.4	52.2	58.6	65.6	73.2	81.6	12.0%
Manufacturing	22.1	24.7	27.5	30.6	33.9	37.5	11.2%
Energy & Utilities	66.0	75.6	86.5	98.6	112.2	127.4	14.1%
Retail	52.2	59.4	67.3	76.1	85.9	96.7	13.1%
Education	20.7	23.4	26.4	29.7	33.3	37.3	12.5%
Other Verticals	28.3	31.8	35.7	40.0	44.7	49.8	12.0%
Total	476.7	542.7	616.3	698.3	789.5	890.5	13.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.4.2 JAPAN

15.4.2.1 Stringent laws and regulations for cybersecurity to drive market

Japan is one of the most advanced countries in terms of ICT development. DDoS protection and mitigation solutions have garnered increasing attention in Japan as the number and sophistication of cyberattacks have escalated. Such attacks raise significant concerns about the safety of infrastructure sectors such as railroads and data-dependent Internet of Things (IoT) networks and systems. Japan is a technological powerhouse and pioneer, but it, too, has faced cybercrime, threats, and attacks. During the Tokyo Olympics 2020, Japan heavily relied on digital infrastructure, including AI-enabled face-to-face live translation devices, face-recognition technology, and ZMP's Robot Taxi, a driverless taxi. According to the UK National Cyber Security Centre, the Russian military was an alleged threat to Japan during the preparations for the Tokyo 2020 Olympics, where journalists, foreign officials, spectators, and athletes joined Japan's 117 million active internet users. Japan was prepared for attacks because it had already collaborated with the US Department of Homeland Security to enhance its cybersecurity and with Israel's power provider, Israel Electric Corporation (IEC), to tackle cybersecurity risks for key infrastructure during the Olympics.

TABLE 317 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	41.1	50.5	61.7	74.8	90.3	110.2	21.8%
Services	12.5	15.5	19.2	23.7	28.9	35.7	23.4%
Total	53.6	66.1	81.0	98.5	119.2	145.9	22.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 318 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	129.4	151.6	177.2	206.5	240.0	278.3	16.6%
Services	42.5	50.4	59.7	70.4	82.9	97.3	18.0%
Total	171.9	202.1	236.9	276.9	322.9	375.7	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 319 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	17.4	21.3	25.9	31.3	37.6	45.6	21.2%
Software/Platforms	23.7	29.2	35.8	43.6	52.8	64.6	22.2%
Total	41.1	50.5	61.7	74.8	90.3	110.2	21.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 320 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	53.3	62.2	72.3	83.8	97.0	111.9	16.0%
Software/Platforms	76.1	89.5	104.9	122.6	143.0	166.4	16.9%
Total	129.4	151.6	177.2	206.5	240.0	278.3	16.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 321 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	7.2	9.0	11.1	13.6	16.6	20.4	23.1%
Managed Services	5.3	6.6	8.2	10.1	12.4	15.3	23.8%
Total	12.5	15.5	19.2	23.7	28.9	35.7	23.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 322 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	24.2	28.7	33.8	39.8	46.7	54.7	17.7%
Managed Services	18.3	21.8	25.9	30.6	36.2	42.6	18.4%
Total	42.5	50.4	59.7	70.4	82.9	97.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 323 JAPAN: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	2.0	2.5	3.0	3.7	4.5	5.5	22.4%
Consulting & Advisory	1.8	2.2	2.8	3.4	4.2	5.3	24.6%
Training & Education	1.2	1.5	1.8	2.3	2.8	3.5	23.8%
Support & Maintenance	1.4	1.7	2.1	2.6	3.1	3.7	21.5%
DDoS Testing & Validation	0.9	1.1	1.3	1.6	2.0	2.4	23.1%
Total	7.2	9.0	11.1	13.6	16.6	20.4	23.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 324 JAPAN: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	6.5	7.6	9.0	10.5	12.3	14.3	17.0%
Consulting & Advisory	6.3	7.6	9.0	10.7	12.7	15.1	19.0%
Training & Education	4.1	4.9	5.8	6.9	8.2	9.6	18.4%
Support & Maintenance	4.4	5.1	6.0	6.9	8.0	9.2	16.0%
DDoS Testing & Validation	2.9	3.4	4.0	4.7	5.6	6.5	17.7%
Total	24.2	28.7	33.8	39.8	46.7	54.7	17.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 325 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	13.7	16.8	20.6	25.1	30.3	37.0	22.1%
Threat Mitigation Systems	11.7	14.4	17.5	21.2	25.5	31.0	21.5%
Botnet Detection & Management	8.9	11.0	13.6	16.6	20.2	24.8	22.7%
Other Solution Types	6.8	8.3	10.0	12.0	14.3	17.3	20.5%
Total	41.1	50.5	61.7	74.8	90.3	110.2	21.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 326 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	43.6	51.2	59.9	70.0	81.5	94.7	16.8%
Threat Mitigation Systems	36.4	42.5	49.6	57.6	66.8	77.3	16.3%
Botnet Detection & Management	29.4	34.7	40.8	47.9	56.1	65.5	17.4%
Other Solution Types	20.1	23.3	26.9	31.0	35.6	40.8	15.2%
Total	129.4	151.6	177.2	206.5	240.0	278.3	16.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 327 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	18.7	23.1	28.4	34.6	42.0	51.4	22.4%
Web Applications & APIs	17.0	21.3	26.4	32.5	39.9	49.4	23.7%
DNS Infrastructure	17.8	21.7	26.2	31.4	37.4	45.1	20.4%
Total	53.6	66.1	81.0	98.5	119.2	145.9	22.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 328 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	60.7	71.5	83.9	98.3	114.8	133.8	17.1%
Web Applications & APIs	58.9	70.1	83.2	98.4	116.1	136.6	18.3%
DNS Infrastructure	52.3	60.5	69.8	80.2	92.0	105.3	15.0%
Total	171.9	202.1	236.9	276.9	322.9	375.7	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 329 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	16.9	20.8	25.3	30.6	36.8	44.7	21.4%
Cloud	32.7	40.4	49.7	60.7	73.7	90.4	22.6%
Hybrid	3.9	4.9	6.0	7.2	8.8	10.7	22.3%
Total	53.6	66.1	81.0	98.5	119.2	145.9	22.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 330 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	52.4	61.2	71.3	82.8	96.0	111.0	16.2%
Cloud	106.9	126.0	148.1	173.7	203.2	239.0	17.5%
Hybrid	12.7	14.9	17.4	20.3	23.7	25.7	15.2%
Total	171.9	202.1	236.9	276.9	322.9	375.7	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 331 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	33.5	41.1	50.0	60.5	72.7	88.4	21.4%
SMEs	20.0	25.0	30.9	38.0	46.5	57.5	23.5%
Total	53.6	66.1	81.0	98.5	119.2	145.9	22.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 332 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	103.5	120.8	140.7	163.4	189.2	218.6	16.1%
SMEs	68.4	81.2	96.2	113.5	133.7	157.0	18.1%
Total	171.9	202.1	236.9	276.9	322.9	375.7	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 333 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	10.6	13.3	16.7	20.7	25.5	31.8	24.6%
Government & Defense	7.6	9.2	11.0	13.1	15.4	18.5	19.4%
Healthcare	4.3	5.3	6.5	8.0	9.7	11.9	22.5%
IT & ITeS	3.9	4.9	6.0	7.4	9.1	11.3	23.9%
Telecommunications	5.6	6.8	8.2	9.9	11.9	14.4	20.8%
Manufacturing	2.8	3.3	4.0	4.8	5.7	6.9	20.1%
Energy & Utilities	7.1	8.8	10.9	13.4	16.3	20.1	23.0%
Retail	5.9	7.3	8.9	10.9	13.1	16.0	21.9%
Education	2.4	3.0	3.6	4.4	5.3	6.4	21.4%
Other Verticals	3.4	4.1	5.0	6.0	7.2	8.7	20.9%
Total	53.6	66.1	81.0	98.5	119.2	145.9	22.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 334 JAPAN: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	38.2	45.7	54.5	64.9	76.9	91.0	19.0%
Government & Defense	21.2	24.3	27.8	31.7	36.0	40.7	13.9%
Healthcare	14.0	16.5	19.4	22.7	26.5	30.9	17.2%
IT & ITeS	13.5	16.1	19.1	22.6	26.7	31.5	18.4%
Telecommunications	16.7	19.4	22.5	26.0	30.0	34.4	15.5%
Manufacturing	8.0	9.2	10.6	12.1	13.9	15.8	14.7%
Energy & Utilities	23.8	28.2	33.2	39.1	45.9	53.8	17.7%
Retail	18.8	22.1	25.9	30.2	35.1	40.8	16.7%
Education	7.5	8.7	10.1	11.8	13.6	15.7	16.1%
Other Verticals	10.2	11.8	13.7	15.9	18.3	21.0	15.6%
Total	171.9	202.1	236.9	276.9	322.9	375.7	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.4.3 INDIA

15.4.3.1 Increasing DDoS attacks leading to adoption of DDoS protection and mitigation solutions

India is one of the leading markets for DDoS protection and mitigation in Asia Pacific. The widespread proliferation of broadband connectivity, the penetration of advanced technologies across organizations, the presence of massive network infrastructure, and the increased frequency of cyberattacks on enterprise networks are the major factors driving enterprises to implement DDoS protection and mitigation equipment and software. India has been facing cybersecurity issues due to inadequate security infrastructure and a lack of security awareness. Another reason for DDoS attacks in India is the tight and low security budgets. Companies often lack security measures, such as web application firewalls, to monitor details. India is the second country with the highest number of internet users globally; this directly contributes to the enhanced number of DDoS attacks. Over the years, India has been helping organizations embrace innovative technologies. The country has implemented DDoS protection and mitigation solutions to secure confidential information exchanged through various channels. The primary objective of organizations in India is to overcome persistent challenges, including regulatory compliance and outdated legacy IT infrastructures. SMEs and large enterprises in India are continually adopting innovative technologies to enhance their productivity, driven by the increasing use of cloud and mobile applications. The increased implementation of smart city initiatives and the growth of IoT trends in India have led to more sophisticated DDoS, bot, and cyberattacks. Security vendors in the country are developing enhanced DDoS protection and mitigation solutions, which will help consumers effectively tackle the increasing DDoS attack vectors.

TABLE 335 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	64.9	80.5	99.4	121.7	148.4	183.1	23.1%
Services	19.7	24.8	31.0	38.5	47.5	59.4	24.7%
Total	84.6	105.3	130.4	160.2	195.9	242.5	23.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 336 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	217.4	257.5	304.2	358.5	418.9	489.7	17.6%
Services	71.4	85.7	102.5	122.3	144.7	171.3	19.1%
Total	288.8	343.1	406.7	480.8	563.6	661.0	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 337 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	27.5	33.9	41.7	50.9	61.7	75.8	22.5%
Software/Platforms	37.4	46.6	57.7	70.9	86.7	107.3	23.5%
Total	64.9	80.5	99.4	121.7	148.4	183.1	23.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 338 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	89.5	105.5	124.1	145.5	169.2	196.9	17.1%
Software/Platforms	127.9	151.9	180.1	212.9	249.6	292.8	18.0%
Total	217.4	257.5	304.2	358.5	418.9	489.7	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 339 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	11.4	14.3	17.8	22.1	27.2	33.9	24.4%
Managed Services	8.3	10.5	13.2	16.4	20.3	25.5	25.1%
Total	19.7	24.8	31.0	38.5	47.5	59.4	24.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 340 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	40.7	48.7	58.1	69.1	81.5	96.3	18.8%
Managed Services	30.7	37.0	44.4	53.2	63.2	75.0	19.5%
Total	71.4	85.7	102.5	122.3	144.7	171.3	19.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 341 INDIA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	3.2	3.9	4.9	6.0	7.4	9.1	23.7%
Consulting & Advisory	2.8	3.5	4.4	5.6	6.9	8.7	25.9%
Training & Education	1.9	2.4	3.0	3.7	4.6	5.8	25.1%
Support & Maintenance	2.2	2.8	3.4	4.2	5.1	6.2	22.7%
DDoS Testing & Validation	1.4	1.7	2.1	2.6	3.2	4.0	24.4%
Total	11.4	14.3	17.8	22.1	27.2	33.9	24.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 342 INDIA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	10.9	13.0	15.4	18.2	21.4	25.1	18.1%
Consulting & Advisory	10.6	12.8	15.5	18.6	22.2	26.5	20.1%
Training & Education	6.9	8.4	10.0	12.0	14.2	16.9	19.5%
Support & Maintenance	7.4	8.7	10.2	12.0	14.0	16.2	17.1%
DDoS Testing & Validation	4.8	5.8	6.9	8.2	9.7	11.5	18.8%
Total	40.7	48.7	58.1	69.1	81.5	96.3	18.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 343 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	20.9	26.0	32.1	39.4	48.2	59.5	23.3%
Threat Mitigation Systems	19.0	23.6	29.0	35.4	43.1	53.1	22.8%
Botnet Detection & Management	14.6	18.2	22.7	28.0	34.4	42.7	24.0%
Other Solution Types	10.4	12.8	15.6	18.9	22.8	27.8	21.7%
Total	64.9	80.5	99.4	121.7	148.4	183.1	23.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 344 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	70.9	84.1	99.6	117.6	137.7	161.3	17.9%
Threat Mitigation Systems	62.9	74.3	87.5	102.9	119.9	139.9	17.3%
Botnet Detection & Management	51.1	60.9	72.5	86.0	101.2	119.2	18.5%
Other Solution Types	32.6	38.2	44.6	52.0	60.0	69.3	16.3%
Total	217.4	257.5	304.2	358.5	418.9	489.7	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 345 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	29.6	36.9	45.7	56.3	68.9	85.5	23.7%
Web Applications & APIs	26.9	33.9	42.5	52.9	65.5	82.1	25.0%
DNS Infrastructure	28.1	34.5	42.1	51.0	61.5	74.9	21.6%
Total	84.6	105.3	130.4	160.2	195.9	242.5	23.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 346 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	102.0	121.4	144.1	170.7	200.4	235.4	18.2%
Web Applications & APIs	99.0	119.1	142.8	170.8	202.6	240.4	19.4%
DNS Infrastructure	87.8	102.7	119.8	139.3	160.6	185.2	16.1%
Total	288.8	343.1	406.7	480.8	563.6	661.0	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 347 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	26.7	33.1	40.7	49.7	60.4	74.4	22.7%
Cloud	51.6	64.5	80.1	98.7	121.1	150.3	23.8%
Hybrid	6.2	7.7	9.6	11.8	14.4	17.9	23.5%
Total	84.6	105.3	130.4	160.2	195.9	242.5	23.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 348 INDIA: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	88.0	103.9	122.4	143.8	167.6	195.3	17.3%
Cloud	179.6	214.0	254.3	301.6	354.7	420.5	18.6%
Hybrid	21.3	25.2	29.9	35.3	41.4	45.2	16.3%
Total	288.8	343.1	406.7	480.8	563.6	661.0	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 349 INDIA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	52.9	65.5	80.6	98.4	119.5	147.0	22.7%
SMEs	31.6	39.8	49.8	61.8	76.4	95.5	24.7%
Total	84.6	105.3	130.4	160.2	195.9	242.5	23.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 350 INDIA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	173.9	205.2	241.6	283.7	330.3	384.7	17.2%
SMEs	115.0	137.9	165.1	197.1	233.3	276.3	19.2%
Total	288.8	343.1	406.7	480.8	563.6	661.0	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 351 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	16.7	21.3	26.8	33.6	41.9	52.9	25.9%
Government & Defense	12.0	14.6	17.7	21.2	25.4	30.7	20.7%
Healthcare	6.8	8.5	10.5	13.0	15.9	19.7	23.7%
IT & ITeS	6.1	7.7	9.7	12.1	15.0	18.8	25.1%
Telecommunications	8.8	10.8	13.3	16.1	19.5	23.9	22.1%
Manufacturing	4.3	5.3	6.5	7.8	9.4	11.4	21.4%
Energy & Utilities	11.2	14.1	17.6	21.7	26.7	33.3	24.3%
Retail	9.4	11.7	14.4	17.7	21.6	26.6	23.2%
Education	3.8	4.7	5.8	7.1	8.6	10.6	22.6%
Other Verticals	5.4	6.6	8.1	9.8	11.9	14.5	22.1%
Total	84.6	105.3	130.4	160.2	195.9	242.5	23.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 352 INDIA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	64.2	77.6	93.6	112.6	134.3	160.2	20.1%
Government & Defense	35.7	41.3	47.7	55.0	62.8	71.6	15.0%
Healthcare	23.5	28.0	33.3	39.4	46.3	54.5	18.3%
IT & ITeS	22.7	27.3	32.8	39.3	46.6	55.4	19.5%
Telecommunications	28.1	33.0	38.6	45.1	52.3	60.6	16.6%
Manufacturing	13.4	15.6	18.1	21.1	24.2	27.8	15.8%
Energy & Utilities	40.0	47.8	57.0	67.9	80.1	94.6	18.8%
Retail	31.7	37.5	44.4	52.4	61.3	71.8	17.8%
Education	12.5	14.8	17.4	20.4	23.8	27.7	17.2%
Other Verticals	17.1	20.1	23.6	27.5	31.9	37.0	16.6%
Total	288.8	343.1	406.7	480.8	563.6	661.0	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.4.4 REST OF ASIA PACIFIC

The rest of Asia Pacific includes South Korea and the remaining countries. These countries have large untapped markets and significant growth potential for DDoS protection and mitigation solutions and services. The small and large-scale organizations in these countries have become more aware of government regulations and compliance and have started adopting proactive DDoS protection and mitigation solutions. Countries in the rest of Asia Pacific have seen digital transformation initiatives in various business areas. These initiatives are expected to further propel the adoption of DDoS protection and mitigation solutions and services.

TABLE 353 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	161.2	194.7	233.9	278.8	330.7	397.0	19.8%
Services	49.0	59.9	73.0	88.1	105.9	128.8	21.3%
Total	210.1	254.7	306.8	366.9	436.6	525.8	20.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 354 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	455.8	521.6	595.3	677.4	771.2	874.4	13.9%
Services	149.7	173.5	200.6	231.1	266.4	305.8	15.4%
Total	605.5	695.1	795.8	908.5	1,037.7	1,180.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 355 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	71.6	86.1	102.9	122.1	144.2	172.3	19.2%
Software/Platforms	89.6	108.6	130.9	156.7	186.5	224.7	20.2%
Total	161.2	194.7	233.9	278.8	330.7	397.0	19.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 356 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	196.9	224.2	254.7	288.4	326.7	368.7	13.4%
Software/Platforms	258.9	297.4	340.6	389.0	444.5	505.7	14.3%
Total	455.8	521.6	595.3	677.4	771.2	874.4	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 357 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	28.3	34.6	42.0	50.6	60.6	73.5	21.0%
Managed Services	20.6	25.4	31.0	37.5	45.3	55.2	21.8%
Total	49.0	59.9	73.0	88.1	105.9	128.8	21.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 358 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	85.3	98.6	113.6	130.6	150.1	171.9	15.0%
Managed Services	64.5	75.0	86.9	100.5	116.3	133.9	15.8%
Total	149.7	173.5	200.6	231.1	266.4	305.8	15.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 359 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	7.9	9.5	11.5	13.8	16.4	19.8	20.4%
Consulting & Advisory	6.9	8.5	10.4	12.7	15.4	18.9	22.5%
Training & Education	4.7	5.7	7.0	8.5	10.2	12.5	21.7%
Support & Maintenance	5.6	6.7	8.0	9.5	11.3	13.5	19.4%
DDoS Testing & Validation	3.4	4.1	5.0	6.0	7.2	8.8	21.0%
Total	28.3	34.6	42.0	50.6	60.6	73.5	21.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 360 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	22.9	26.3	30.1	34.4	39.4	44.8	14.4%
Consulting & Advisory	22.2	26.0	30.3	35.2	40.9	47.4	16.3%
Training & Education	14.6	16.9	19.6	22.7	26.2	30.2	15.7%
Support & Maintenance	15.4	17.6	20.0	22.7	25.7	29.0	13.4%
DDoS Testing & Validation	10.2	11.7	13.5	15.6	17.9	20.5	15.0%
Total	85.3	98.6	113.6	130.6	150.1	171.9	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 361 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	52.3	63.4	76.3	91.1	108.3	130.3	20.0%
Threat Mitigation Systems	45.2	54.4	65.2	77.6	91.8	109.9	19.5%
Botnet Detection & Management	34.1	41.6	50.3	60.4	72.3	87.4	20.7%
Other Solution Types	29.5	35.4	42.1	49.7	58.4	69.4	18.6%
Total	161.2	194.7	233.9	278.8	330.7	397.0	19.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 362 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	149.9	171.9	196.6	224.2	255.8	290.6	14.2%
Threat Mitigation Systems	125.8	143.7	163.5	185.6	210.8	238.4	13.6%
Botnet Detection & Management	101.1	116.6	134.1	153.8	176.4	201.5	14.8%
Other Solution Types	78.9	89.4	101.0	113.8	128.3	143.9	12.8%
Total	455.8	521.6	595.3	677.4	771.2	874.4	13.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 363 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	73.4	89.2	107.6	128.9	153.6	185.3	20.3%
Web Applications & APIs	66.8	82.0	100.1	121.2	146.0	178.0	21.7%
DNS Infrastructure	69.9	83.5	99.2	116.8	136.9	162.4	18.4%
Total	210.1	254.7	306.8	366.9	436.6	525.8	20.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 364 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	213.8	245.9	282.0	322.5	369.0	420.4	14.5%
Web Applications & APIs	207.5	241.2	279.4	322.8	373.0	429.1	15.6%
DNS Infrastructure	184.1	208.1	234.4	263.2	295.7	330.7	12.4%
Total	605.5	695.1	795.8	908.5	1,037.7	1,180.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 365 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	66.5	80.0	95.8	113.9	134.7	161.2	19.4%
Cloud	128.3	155.9	188.4	226.0	269.7	325.9	20.5%
Hybrid	15.4	18.7	22.6	27.0	32.1	38.7	20.2%
Total	210.1	254.7	306.8	366.9	436.6	525.8	20.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 366 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	184.5	210.5	239.6	271.8	308.5	348.7	13.6%
Cloud	376.4	433.4	497.8	570.0	653.0	750.8	14.8%
Hybrid	44.6	51.2	58.5	66.8	76.2	80.6	12.6%
Total	605.5	695.1	795.8	908.5	1,037.7	1,180.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 367 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	131.5	158.4	189.6	225.3	266.3	318.6	19.4%
SMEs	78.6	96.3	117.2	141.6	170.3	207.2	21.4%
Total	210.1	254.7	306.8	366.9	436.6	525.8	20.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 368 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	364.5	415.7	472.7	536.0	608.1	686.9	13.5%
SMEs	241.0	279.4	323.1	372.5	429.6	493.3	15.4%
Total	605.5	695.1	795.8	908.5	1,037.7	1,180.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 369 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	41.6	51.4	63.2	77.0	93.4	114.7	22.5%
Government & Defense	29.8	35.3	41.6	48.6	56.6	66.5	17.4%
Healthcare	16.9	20.5	24.7	29.7	35.4	42.7	20.4%
IT & ITeS	15.2	18.7	22.9	27.7	33.5	40.8	21.8%
Telecommunications	21.9	26.2	31.3	37.0	43.5	51.8	18.8%
Manufacturing	10.8	12.9	15.2	17.9	20.9	24.8	18.1%
Energy & Utilities	27.9	34.1	41.3	49.8	59.6	72.3	21.0%
Retail	23.3	28.2	33.9	40.4	48.0	57.7	19.9%
Education	9.5	11.4	13.7	16.3	19.2	23.0	19.3%
Other Verticals	13.3	15.9	19.0	22.5	26.5	31.5	18.8%
Total	210.1	254.7	306.8	366.9	436.6	525.8	20.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 370 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	134.5	157.2	183.2	212.8	247.3	286.0	16.3%
Government & Defense	74.8	83.7	93.4	103.9	115.5	127.8	11.3%
Healthcare	49.3	56.7	65.1	74.5	85.3	97.2	14.5%
IT & ITeS	47.6	55.4	64.2	74.3	85.9	98.9	15.7%
Telecommunications	58.9	66.9	75.6	85.3	96.3	108.1	12.9%
Manufacturing	28.0	31.6	35.5	39.8	44.6	49.7	12.1%
Energy & Utilities	83.8	96.9	111.6	128.3	147.5	168.9	15.0%
Retail	66.4	76.0	86.9	99.0	112.9	128.1	14.1%
Education	26.3	30.0	34.1	38.6	43.8	49.4	13.5%
Other Verticals	35.9	40.7	46.1	52.0	58.7	66.0	13.0%
Total	605.5	695.1	795.8	908.5	1,037.7	1,180.2	14.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.5 MIDDLE EAST & AFRICA

The Middle East & Africa region includes the GCC countries, South Africa, Egypt, Nigeria, and the remaining countries. The region has been relatively cautious in adopting DDoS protection and mitigation solutions and services, although its DDoS protection and mitigation market is expected to grow rapidly during the forecast period. According to a NETSCOUT DDoS threat intelligence report, in 1H 2022, attacks increased or peaked unusually in several nations, including Saudi Arabia (51%), South Africa (41%), Finland (249%), and Ireland (200%). According to a survey by A10 Networks, in the Middle East, more than half of service providers focus on increasing their security investments, with DDoS mitigation being their highest priority. Currently, the financial services and healthcare enterprises in the Middle East & Africa are investing in the adoption of data security solutions, thereby driving the adoption of DDoS protection and mitigation solutions. Major investments are flowing in enterprise mobility, cloud computing, broadband networks, LTE, and LTE-Advanced technologies in Arab countries, North African countries, Nigeria, Egypt, and South Africa. Several domestic players, as well as global companies, are expanding their network coverage across the region.

TABLE 371 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	223.1	264.8	312.3	365.7	425.6	501.6	17.6%
Services	67.8	81.5	97.4	115.6	136.3	162.7	19.1%
Total	290.9	346.3	409.8	481.2	561.9	664.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 372 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	579.8	668.7	764.7	872.5	993.1	1,128.0	14.2%
Services	190.5	222.5	257.6	297.6	343.1	394.5	15.7%
Total	770.3	891.1	1,022.3	1,170.1	1,336.2	1,522.5	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 373 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	96.2	113.7	133.5	155.6	180.2	211.4	17.0%
Software/Platforms	126.9	151.1	178.8	210.1	245.4	290.2	18.0%
Total	223.1	264.8	312.3	365.7	425.6	501.6	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 374 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	243.2	279.2	317.8	360.8	408.7	462.0	13.7%
Software/Platforms	336.6	389.5	446.9	511.7	584.4	665.9	14.6%
Total	579.8	668.7	764.7	872.5	993.1	1,128.0	14.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 375 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	38.8	46.5	55.5	65.6	77.1	91.8	18.8%
Managed Services	29.0	35.0	42.0	50.0	59.2	70.9	19.6%
Total	67.8	81.5	97.4	115.6	136.3	162.7	19.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 376 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	107.1	124.7	144.0	165.9	190.6	218.5	15.3%
Managed Services	83.4	97.7	113.6	131.8	152.5	176.0	16.1%
Total	190.5	222.5	257.6	297.6	343.1	394.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 377 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	10.8	12.8	15.2	17.9	20.9	24.7	18.1%
Consulting & Advisory	9.4	11.4	13.8	16.5	19.6	23.6	20.2%
Training & Education	6.4	7.7	9.2	11.0	13.0	15.6	19.5%
Support & Maintenance	7.6	9.0	10.6	12.4	14.4	16.9	17.2%
DDoS Testing & Validation	4.6	5.5	6.6	7.8	9.2	10.9	18.8%
Total	38.8	46.5	55.5	65.6	77.1	91.8	18.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 378 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	28.7	33.3	38.2	43.7	50.0	57.0	14.7%
Consulting & Advisory	27.9	32.9	38.4	44.7	52.0	60.2	16.6%
Training & Education	18.3	21.4	24.9	28.8	33.3	38.4	16.0%
Support & Maintenance	19.4	22.3	25.4	28.8	32.6	36.9	13.7%
DDoS Testing & Validation	12.8	14.9	17.2	19.8	22.7	26.0	15.3%
Total	107.1	124.7	144.0	165.9	190.6	218.5	15.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 379 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	73.6	86.8	101.8	118.5	137.2	160.8	16.9%
Threat Mitigation Systems	80.4	95.9	113.7	133.8	156.5	185.3	18.2%
Botnet Detection & Management	33.6	39.9	47.2	55.3	64.4	76.0	17.7%
Other Solution Types	35.6	42.2	49.7	58.1	67.5	79.5	17.5%
Total	223.1	264.8	312.3	365.7	425.6	501.6	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 380 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	184.8	211.9	241.0	273.4	309.5	349.6	13.6%
Threat Mitigation Systems	215.2	249.4	286.6	328.5	375.6	428.6	14.8%
Botnet Detection & Management	88.0	101.6	116.3	132.9	151.6	172.4	14.4%
Other Solution Types	91.8	105.7	120.8	137.6	156.4	177.4	14.1%
Total	579.8	668.7	764.7	872.5	993.1	1,128.0	14.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 381 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	101.7	121.2	143.7	169.1	197.7	234.2	18.2%
Web Applications & APIs	92.4	111.5	133.6	158.9	187.9	224.9	19.5%
DNS Infrastructure	96.8	113.6	132.4	153.2	176.2	205.2	16.2%
Total	290.9	346.3	409.8	481.2	561.9	664.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 382 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	272.0	315.2	362.3	415.3	475.1	542.3	14.8%
Web Applications & APIs	264.1	309.2	359.0	415.7	480.3	553.6	16.0%
DNS Infrastructure	234.2	266.7	301.1	339.0	380.8	426.6	12.7%
Total	770.3	891.1	1,022.3	1,170.1	1,336.2	1,522.5	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 383 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	92.0	108.8	128.0	149.4	173.4	203.7	17.2%
Cloud	177.5	212.0	251.7	296.4	347.2	411.7	18.3%
Hybrid	21.3	25.4	30.1	35.4	41.4	48.9	18.0%
Total	290.9	346.3	409.8	481.2	561.9	664.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 384 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	234.7	269.9	307.7	350.0	397.3	449.9	13.9%
Cloud	478.9	555.7	639.4	734.1	840.8	968.6	15.1%
Hybrid	56.7	65.6	75.2	86.0	98.1	104.0	12.9%
Total	770.3	891.1	1,022.3	1,170.1	1,336.2	1,522.5	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 385 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	182.1	215.4	253.2	295.5	342.8	402.5	17.2%
SMEs	108.8	130.9	156.5	185.8	219.1	261.7	19.2%
Total	290.9	346.3	409.8	481.2	561.9	664.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 386 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	463.7	532.9	607.3	690.4	783.0	886.1	13.8%
SMEs	306.6	358.2	415.1	479.7	553.2	636.4	15.7%
Total	770.3	891.1	1,022.3	1,170.1	1,336.2	1,522.5	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 387 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	57.5	69.9	84.4	101.1	120.3	144.9	20.3%
Government & Defense	41.2	48.0	55.6	63.8	72.8	84.0	15.3%
Healthcare	23.4	27.9	33.1	38.9	45.5	54.0	18.2%
IT & ITeS	21.1	25.5	30.6	36.4	43.1	51.6	19.6%
Telecommunications	30.3	35.7	41.8	48.5	56.0	65.4	16.6%
Manufacturing	14.9	17.5	20.3	23.5	27.0	31.3	16.0%
Energy & Utilities	38.6	46.3	55.2	65.3	76.7	91.3	18.8%
Retail	32.3	38.3	45.3	53.0	61.8	72.9	17.7%
Education	13.2	15.6	18.3	21.3	24.7	29.1	17.2%
Other Verticals	18.4	21.7	25.4	29.5	34.1	39.8	16.7%
Total	290.9	346.3	409.8	481.2	561.9	664.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 388 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	171.1	201.6	235.4	274.1	318.4	369.0	16.6%
Government & Defense	95.1	107.3	120.0	133.8	148.8	164.9	11.6%
Healthcare	62.7	72.7	83.6	95.9	109.8	125.4	14.9%
IT & ITeS	60.6	71.0	82.5	95.6	110.6	127.6	16.1%
Telecommunications	75.0	85.7	97.2	109.9	123.9	139.5	13.2%
Manufacturing	35.7	40.5	45.6	51.2	57.4	64.1	12.5%
Energy & Utilities	106.6	124.2	143.4	165.2	189.9	217.8	15.4%
Retail	84.4	97.5	111.6	127.5	145.4	165.3	14.4%
Education	33.5	38.4	43.8	49.7	56.4	63.8	13.8%
Other Verticals	45.7	52.2	59.2	67.0	75.6	85.1	13.3%
Total	770.3	891.1	1,022.3	1,170.1	1,336.2	1,522.5	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 389 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)

Country	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
GCC	169.8	202.4	239.9	282.0	329.8	390.3	18.1%
South Africa	27.4	33.1	39.6	47.2	55.8	66.8	19.5%
Rest of Middle East & Africa	93.7	110.8	130.3	152.0	176.3	207.1	17.2%
Total	290.9	346.3	409.8	481.2	561.9	664.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 390 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
GCC	453.2	525.0	603.0	691.0	790.1	901.4	14.7%
South Africa	78.5	92.0	107.0	124.1	143.3	165.3	16.1%
Rest of Middle East & Africa	238.6	274.1	312.4	355.0	402.8	455.8	13.8%
Total	770.3	891.1	1,022.3	1,170.1	1,336.2	1,522.5	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.5.1 GCC

The Gulf Cooperation Council (GCC) DDoS protection and mitigation market comprises Saudi Arabia, the United Arab Emirates (UAE), Qatar, Kuwait, Oman, and Bahrain. The region represents a growing market, driven by rapid digital transformation, expanding cloud adoption, increasing deployment of 5G networks, and the growing dependence of government and enterprises on digital services. Critical sectors such as government, BFSI, energy and utilities, telecommunications, and healthcare are increasingly exposed to

large-scale and sophisticated cyberattacks, including DDoS attacks. The region's geopolitical significance and concentration of critical infrastructure further elevate the risk of disruptive cyber campaigns. Additionally, national cybersecurity strategies and investments in smart cities and digital economies, such as Saudi Vision 2030 and the UAE's digital transformation initiatives, are encouraging organizations to strengthen network resilience, service availability, and business continuity, thereby driving demand for advanced DDoS protection and mitigation solutions and managed services.

TABLE 391 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	130.2	154.8	182.8	214.3	249.8	294.7	17.7%
Services	39.6	47.7	57.0	67.7	80.0	95.6	19.3%
Total	169.8	202.4	239.9	282.0	329.8	390.3	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 392 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	341.1	393.9	451.0	515.2	587.3	667.8	14.4%
Services	112.1	131.0	151.9	175.8	202.9	233.6	15.8%
Total	453.2	525.0	603.0	691.0	790.1	901.4	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 393 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	56.9	67.3	79.1	92.3	107.1	125.8	17.2%
Software/Platforms	73.4	87.5	103.7	122.0	142.7	168.9	18.2%
Total	130.2	154.8	182.8	214.3	249.8	294.7	17.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 394 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	144.9	166.6	189.8	215.8	244.7	277.0	13.8%
Software/Platforms	196.2	227.4	261.2	299.4	342.5	390.8	14.8%
Total	341.1	393.9	451.0	515.2	587.3	667.8	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 395 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	22.5	27.0	32.2	38.1	44.9	53.5	18.9%
Managed Services	17.1	20.7	24.8	29.6	35.1	42.1	19.8%
Total	39.6	47.7	57.0	67.7	80.0	95.6	19.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 396 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	62.5	72.8	84.1	97.0	111.6	128.1	15.4%
Managed Services	49.6	58.2	67.8	78.8	91.3	105.5	16.3%
Total	112.1	131.0	151.9	175.8	202.9	233.6	15.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 397 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	6.2	7.4	8.8	10.4	12.2	14.4	18.3%
Consulting & Advisory	5.5	6.6	8.0	9.6	11.4	13.8	20.3%
Training & Education	3.7	4.5	5.4	6.4	7.6	9.1	19.6%
Support & Maintenance	4.4	5.2	6.2	7.2	8.4	9.8	17.3%
DDoS Testing & Validation	2.7	3.2	3.8	4.5	5.3	6.4	18.9%
Total	22.5	27.0	32.2	38.1	44.9	53.5	18.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 398 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	16.8	19.4	22.3	25.6	29.3	33.4	14.8%
Consulting & Advisory	16.3	19.2	22.4	26.2	30.4	35.3	16.7%
Training & Education	10.7	12.5	14.5	16.9	19.5	22.5	16.1%
Support & Maintenance	11.3	13.0	14.8	16.9	19.1	21.6	13.8%
DDoS Testing & Validation	7.4	8.7	10.0	11.6	13.3	15.3	15.4%
Total	62.5	72.8	84.1	97.0	111.6	128.1	15.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 399 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	42.8	50.7	59.7	69.7	80.9	95.2	17.3%
Threat Mitigation Systems	44.5	53.1	62.9	74.0	86.5	102.3	18.1%
Botnet Detection & Management	21.9	26.1	30.9	36.4	42.6	50.5	18.2%
Other Solution Types	21.0	24.9	29.3	34.2	39.8	46.7	17.3%
Total	130.2	154.8	182.8	214.3	249.8	294.7	17.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 400 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	109.8	126.3	144.2	164.1	186.5	211.3	14.0%
Threat Mitigation Systems	118.8	137.6	158.0	180.9	206.8	235.8	14.7%
Botnet Detection & Management	58.7	68.0	78.2	89.7	102.7	117.3	14.9%
Other Solution Types	53.9	62.0	70.7	80.4	91.3	103.4	13.9%
Total	341.1	393.9	451.0	515.2	587.3	667.8	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 401 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	59.3	70.9	84.1	99.1	116.0	137.6	18.3%
Web Applications & APIs	54.0	65.2	78.2	93.2	110.3	132.2	19.6%
DNS Infrastructure	56.5	66.4	77.5	89.8	103.4	120.6	16.4%
Total	169.8	202.4	239.9	282.0	329.8	390.3	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 402 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	160.0	185.7	213.7	245.3	280.9	321.1	14.9%
Web Applications & APIs	155.4	182.1	211.7	245.5	284.0	327.8	16.1%
DNS Infrastructure	137.8	157.1	177.6	200.2	225.2	252.6	12.9%
Total	453.2	525.0	603.0	691.0	790.1	901.4	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 403 GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	53.7	63.6	74.9	87.6	101.7	119.7	17.4%
Cloud	103.7	123.9	147.3	173.7	203.7	241.9	18.5%
Hybrid	12.5	14.9	17.6	20.8	24.3	28.7	18.2%
Total	169.8	202.4	239.9	282.0	329.8	390.3	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 404 GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	138.1	159.0	181.5	206.7	234.9	266.3	14.0%
Cloud	281.7	327.3	377.1	433.5	497.2	573.5	15.3%
Hybrid	33.4	38.6	44.3	50.8	58.0	61.6	13.0%
Total	453.2	525.0	603.0	691.0	790.1	901.4	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 405 GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	106.3	125.9	148.2	173.2	201.1	236.5	17.3%
SMEs	63.5	76.5	91.6	108.9	128.6	153.8	19.3%
Total	169.8	202.4	239.9	282.0	329.8	390.3	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 406 GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	272.8	313.9	358.2	407.7	463.0	524.6	14.0%
SMEs	180.4	211.0	244.8	283.3	327.1	376.8	15.9%
Total	453.2	525.0	603.0	691.0	790.1	901.4	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 407 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	33.6	40.9	49.4	59.2	70.6	85.1	20.4%
Government & Defense	24.1	28.1	32.5	37.4	42.7	49.4	15.5%
Healthcare	13.6	16.3	19.3	22.8	26.7	31.7	18.4%
IT & ITeS	12.3	14.9	17.9	21.3	25.3	30.3	19.7%
Telecommunications	17.7	20.9	24.4	28.4	32.8	38.4	16.8%
Manufacturing	8.7	10.2	11.9	13.8	15.8	18.4	16.1%
Energy & Utilities	22.5	27.1	32.3	38.2	45.0	53.7	18.9%
Retail	18.8	22.4	26.5	31.1	36.3	42.9	17.9%
Education	7.7	9.1	10.7	12.5	14.5	17.1	17.3%
Other Verticals	10.7	12.7	14.9	17.3	20.0	23.4	16.8%
Total	169.8	202.4	239.9	282.0	329.8	390.3	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 408 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	100.7	118.7	138.8	161.9	188.3	218.5	16.8%
Government & Defense	56.0	63.2	70.8	79.0	88.0	97.6	11.8%
Healthcare	36.9	42.8	49.3	56.7	64.9	74.3	15.0%
IT & ITeS	35.7	41.8	48.7	56.5	65.4	75.5	16.2%
Telecommunications	44.1	50.5	57.3	64.9	73.3	82.6	13.4%
Manufacturing	21.0	23.9	26.9	30.3	34.0	38.0	12.6%
Energy & Utilities	62.7	73.1	84.6	97.6	112.3	129.0	15.5%
Retail	49.7	57.4	65.8	75.3	86.0	97.9	14.5%
Education	19.7	22.6	25.8	29.4	33.3	37.8	13.9%
Other Verticals	26.9	30.8	34.9	39.5	44.7	50.4	13.4%
Total	453.2	525.0	603.0	691.0	790.1	901.4	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 409 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)

Country	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
KSA	79.0	94.5	112.5	132.8	155.9	185.3	18.6%
UAE	60.8	72.4	85.7	100.6	117.4	138.7	17.9%
Rest of GCC	30.1	35.5	41.7	48.7	56.5	66.3	17.1%
Total	169.8	202.4	239.9	282.0	329.8	390.3	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 410 GCC: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
KSA	216.1	251.3	289.9	333.6	383.2	438.8	15.2%
UAE	160.7	185.8	213.0	243.6	278.0	316.7	14.5%
Rest of GCC	76.4	87.8	100.0	113.7	128.9	145.9	13.8%
Total	453.2	525.0	603.0	691.0	790.1	901.4	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.5.1.1 KSA

15.5.1.1.1 Increasing investments in mitigation and growth in number of startups to drive market

Cities such as Riyadh, Jeddah, Mecca, and Medina are among those in the Kingdom of Saudi Arabia (KSA) that are experiencing rapid expansion in their digital economies and the telecommunications sector. These cities are witnessing rapid improvements in their IT sector and overall digital economic growth. DDoS protection and mitigation is an emerging technology trend in Saudi Arabia, where the government is focused on implementing digital transformation initiatives and stringent regulatory compliance. As organizations in various sectors, including telecommunications, government, finance, and ecommerce, face rising vulnerabilities, there is a growing demand for advanced DDoS protection solutions. The adoption of cloud-based services, the integration of AI and machine learning for real-time threat detection, and compliance with local cybersecurity regulations are among the key factors driving the market in KSA. Leading global vendors, such as Akamai Technologies and Cloudflare, along with local providers, are actively offering services in the country. Despite challenges such as cost concerns and a shortage of skilled professionals, the market outlook remains positive, with continued investments in cybersecurity and government initiatives driving expansion.

TABLE 411 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	60.6	72.3	85.7	100.9	118.1	139.9	18.2%
Services	18.4	22.3	26.7	31.9	37.8	45.4	19.8%
Total	79.0	94.5	112.5	132.8	155.9	185.3	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 412 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	162.7	188.6	216.9	248.8	284.8	325.1	14.9%
Services	53.4	62.7	73.1	84.9	98.4	113.7	16.3%
Total	216.1	251.3	289.9	333.6	383.2	438.8	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 413 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	26.9	32.0	37.7	44.2	51.5	60.7	17.7%
Software/Platforms	33.7	40.3	48.0	56.7	66.6	79.2	18.7%
Total	60.6	72.3	85.7	100.9	118.1	139.9	18.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 414 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	70.3	81.1	92.8	105.9	120.6	137.1	14.3%
Software/Platforms	92.4	107.5	124.1	142.9	164.1	188.0	15.3%
Total	162.7	188.6	216.9	248.8	284.8	325.1	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 415 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	10.5	12.6	15.1	18.0	21.3	25.5	19.5%
Managed Services	7.9	9.6	11.6	13.9	16.5	19.9	20.2%
Total	18.4	22.3	26.7	31.9	37.8	45.4	19.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 416 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	29.9	35.1	40.7	47.2	54.5	62.9	16.0%
Managed Services	23.5	27.7	32.3	37.7	43.8	50.8	16.7%
Total	53.4	62.7	73.1	84.9	98.4	113.7	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 417 KSA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	2.9	3.5	4.2	4.9	5.8	6.9	18.8%
Consulting & Advisory	2.5	3.1	3.8	4.5	5.4	6.6	20.9%
Training & Education	1.7	2.1	2.5	3.0	3.6	4.3	20.2%
Support & Maintenance	2.1	2.4	2.9	3.4	4.0	4.7	17.9%
DDoS Testing & Validation	1.2	1.5	1.8	2.1	2.5	3.0	19.5%
Total	10.5	12.6	15.1	18.0	21.3	25.5	19.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 418 KSA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	8.0	9.4	10.8	12.4	14.3	16.4	15.3%
Consulting & Advisory	7.8	9.2	10.9	12.7	14.9	17.3	17.3%
Training & Education	5.1	6.0	7.0	8.2	9.5	11.0	16.7%
Support & Maintenance	5.4	6.3	7.2	8.2	9.3	10.6	14.3%
DDoS Testing & Validation	3.6	4.2	4.9	5.6	6.5	7.5	16.0%
Total	29.9	35.1	40.7	47.2	54.5	62.9	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 419 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	19.7	23.6	28.0	33.1	38.8	46.1	18.5%
Threat Mitigation Systems	17.6	21.0	24.8	29.2	34.1	40.3	18.0%
Botnet Detection & Management	13.1	15.7	18.8	22.3	26.3	31.4	19.2%
Other Solution Types	10.1	12.0	14.0	16.4	19.0	22.2	17.0%
Total	60.6	72.3	85.7	100.9	118.1	139.9	18.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 420 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	53.7	62.4	71.8	82.6	94.7	108.4	15.1%
Threat Mitigation Systems	46.7	54.0	62.0	70.9	81.0	92.2	14.6%
Botnet Detection & Management	36.7	42.9	49.7	57.5	66.3	76.2	15.7%
Other Solution Types	25.6	29.3	33.3	37.8	42.8	48.3	13.6%
Total	162.7	188.6	216.9	248.8	284.8	325.1	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 421 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	27.6	33.1	39.4	46.7	54.9	65.3	18.8%
Web Applications & APIs	25.1	30.4	36.7	43.9	52.1	62.8	20.1%
DNS Infrastructure	26.3	31.0	36.3	42.3	48.9	57.2	16.9%
Total	79.0	94.5	112.5	132.8	155.9	185.3	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 422 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	76.3	88.9	102.7	118.4	136.2	156.3	15.4%
Web Applications & APIs	74.1	87.2	101.8	118.5	137.7	159.6	16.6%
DNS Infrastructure	65.7	75.2	85.4	96.7	109.2	123.0	13.4%
Total	216.1	251.3	289.9	333.6	383.2	438.8	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 423 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	25.0	29.7	35.1	41.2	48.1	56.8	17.9%
Cloud	48.2	57.9	69.1	81.8	96.3	114.9	19.0%
Hybrid	5.8	6.9	8.3	9.8	11.5	13.6	18.7%
Total	79.0	94.5	112.5	132.8	155.9	185.3	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 424 KSA: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	65.9	76.1	87.3	99.8	113.9	129.7	14.5%
Cloud	134.3	156.7	181.3	209.3	241.1	279.2	15.8%
Hybrid	15.9	18.5	21.3	24.5	28.1	30.0	13.5%
Total	216.1	251.3	289.9	333.6	383.2	438.8	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 425 KSA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	49.4	58.8	69.5	81.5	95.1	112.3	17.8%
SMEs	29.5	35.7	43.0	51.3	60.8	73.0	19.8%
Total	79.0	94.5	112.5	132.8	155.9	185.3	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 426 KSA: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	130.1	150.3	172.2	196.8	224.5	255.4	14.4%
SMEs	86.0	101.0	117.7	136.8	158.6	183.4	16.4%
Total	216.1	251.3	289.9	333.6	383.2	438.8	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 427 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	15.6	19.1	23.2	27.9	33.4	40.4	20.9%
Government & Defense	11.2	13.1	15.3	17.6	20.2	23.4	16.0%
Healthcare	6.3	7.6	9.1	10.7	12.6	15.1	18.9%
IT & ITeS	5.7	7.0	8.4	10.0	11.9	14.4	20.2%
Telecommunications	8.2	9.7	11.5	13.4	15.5	18.2	17.3%
Manufacturing	4.1	4.8	5.6	6.5	7.5	8.7	16.6%
Energy & Utilities	10.5	12.6	15.1	18.0	21.3	25.5	19.4%
Retail	8.8	10.5	12.4	14.6	17.2	20.3	18.4%
Education	3.6	4.2	5.0	5.9	6.9	8.1	17.8%
Other Verticals	5.0	5.9	7.0	8.1	9.5	11.1	17.3%
Total	79.0	94.5	112.5	132.8	155.9	185.3	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 428 KSA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	48.0	56.8	66.7	78.2	91.3	106.3	17.2%
Government & Defense	26.7	30.3	34.0	38.2	42.7	47.5	12.2%
Healthcare	17.6	20.5	23.7	27.4	31.5	36.1	15.5%
IT & ITeS	17.0	20.0	23.4	27.3	31.7	36.8	16.7%
Telecommunications	21.0	24.2	27.6	31.3	35.5	40.2	13.8%
Manufacturing	10.0	11.4	12.9	14.6	16.5	18.5	13.1%
Energy & Utilities	29.9	35.0	40.7	47.1	54.5	62.8	16.0%
Retail	23.7	27.5	31.7	36.4	41.7	47.6	15.0%
Education	9.4	10.8	12.4	14.2	16.2	18.4	14.4%
Other Verticals	12.8	14.7	16.8	19.1	21.7	24.5	13.9%
Total	216.1	251.3	289.9	333.6	383.2	438.8	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.5.1.2 UAE

15.5.1.2.1 Growing reliance on cloud-based applications to boost market

The UAE is one of the leading countries in the region when it comes to adopting DDoS protection and mitigation. The DDoS protection and mitigation market in the UAE is experiencing significant growth, driven by the rising frequency of cyber threats and the rapid adoption of digital services. The increasing reliance on cloud-based applications, along with government initiatives to enhance cybersecurity, has fueled demand for robust DDoS protection solutions. Both global players, such as Akamai, Cloudflare, and Radware, as well as regional providers, offer a range of solutions, including on-premises and cloud-based deployments in the UAE. The market is experiencing trends like AI integration for real-time threat detection and an increase in managed security services. However, challenges like the high cost of implementation and the constantly evolving threat remain a concern.

TABLE 429 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	46.6	55.4	65.3	76.4	88.9	104.7	17.6%
Services	14.2	17.1	20.4	24.2	28.5	34.0	19.1%
Total	60.8	72.4	85.7	100.6	117.4	138.7	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 430 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	121.0	139.4	159.3	181.6	206.6	234.6	14.2%
Services	39.7	46.4	53.7	62.0	71.4	82.1	15.6%
Total	160.7	185.8	213.0	243.6	278.0	316.7	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 431 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	19.7	23.4	27.4	31.9	37.0	43.3	17.0%
Software/Platforms	26.9	32.0	37.9	44.5	51.9	61.4	18.0%
Total	46.6	55.4	65.3	76.4	88.9	104.7	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 432 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	49.8	57.2	65.0	73.7	83.5	94.3	13.6%
Software/Platforms	71.1	82.3	94.3	107.9	123.1	140.3	14.5%
Total	121.0	139.4	159.3	181.6	206.6	234.6	14.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 433 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	8.0	9.5	11.3	13.4	15.7	18.7	18.6%
Managed Services	6.2	7.5	9.0	10.8	12.7	15.3	19.8%
Total	14.2	17.1	20.4	24.2	28.5	34.0	19.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 434 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	21.8	25.3	29.1	33.5	38.4	43.9	15.1%
Managed Services	18.0	21.1	24.6	28.5	33.0	38.1	16.2%
Total	39.7	46.4	53.7	62.0	71.4	82.1	15.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 435 UAE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	2.2	2.6	3.1	3.7	4.3	5.0	17.9%
Consulting & Advisory	1.9	2.3	2.8	3.4	4.0	4.8	20.0%
Training & Education	1.3	1.6	1.9	2.2	2.7	3.2	19.3%
Support & Maintenance	1.6	1.8	2.2	2.5	2.9	3.4	17.0%
DDoS Testing & Validation	0.9	1.1	1.4	1.6	1.9	2.2	18.6%
Total	8.0	9.5	11.3	13.4	15.7	18.7	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 436 UAE: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	5.8	6.7	7.7	8.8	10.1	11.5	14.4%
Consulting & Advisory	5.7	6.7	7.8	9.0	10.5	12.1	16.4%
Training & Education	3.7	4.3	5.0	5.8	6.7	7.7	15.8%
Support & Maintenance	3.9	4.5	5.1	5.8	6.6	7.4	13.5%
DDoS Testing & Validation	2.6	3.0	3.5	4.0	4.6	5.2	15.1%
Total	21.8	25.3	29.1	33.5	38.4	43.9	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 437 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	15.4	18.2	21.3	24.7	28.4	33.2	16.6%
Threat Mitigation Systems	18.0	21.5	25.6	30.2	35.4	42.0	18.5%
Botnet Detection & Management	5.9	7.0	8.2	9.5	11.0	12.9	17.0%
Other Solution Types	7.3	8.7	10.3	12.0	14.0	16.6	17.9%
Total	46.6	55.4	65.3	76.4	88.9	104.7	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 438 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	38.0	43.4	49.2	55.6	62.7	70.5	13.1%
Threat Mitigation Systems	48.9	56.7	65.3	75.0	86.0	98.3	15.0%
Botnet Detection & Management	14.9	17.0	19.4	22.0	24.9	28.1	13.6%
Other Solution Types	19.2	22.2	25.4	29.1	33.1	37.7	14.5%
Total	121.0	139.4	159.3	181.6	206.6	234.6	14.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 439 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	21.2	25.4	30.0	35.3	41.3	48.9	18.1%
Web Applications & APIs	19.3	23.3	27.9	33.2	39.3	47.0	19.4%
DNS Infrastructure	20.2	23.8	27.7	32.0	36.8	42.8	16.2%
Total	60.8	72.4	85.7	100.6	117.4	138.7	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 440 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	56.8	65.7	75.5	86.5	98.9	112.8	14.7%
Web Applications & APIs	55.1	64.5	74.8	86.6	99.9	115.1	15.9%
DNS Infrastructure	48.9	55.6	62.7	70.6	79.2	88.7	12.7%
Total	160.7	185.8	213.0	243.6	278.0	316.7	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 441 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	19.2	22.8	26.8	31.2	36.2	42.5	17.2%
Cloud	37.1	44.3	52.6	61.9	72.5	85.9	18.3%
Hybrid	4.5	5.3	6.3	7.4	8.6	10.2	18.0%
Total	60.8	72.4	85.7	100.6	117.4	138.7	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 442 UAE: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	49.0	56.3	64.1	72.9	82.7	93.6	13.8%
Cloud	99.9	115.9	133.2	152.8	175.0	201.5	15.1%
Hybrid	11.8	13.7	15.7	17.9	20.4	21.6	12.8%
Total	160.7	185.8	213.0	243.6	278.0	316.7	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 443 UAE: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	38.0	45.1	52.9	61.7	71.6	84.0	17.2%
SMEs	22.7	27.4	32.7	38.8	45.8	54.6	19.2%
Total	60.8	72.4	85.7	100.6	117.4	138.7	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 444 UAE: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	96.7	111.1	126.5	143.7	162.9	184.3	13.8%
SMEs	64.0	74.7	86.5	99.9	115.1	132.4	15.7%
Total	160.7	185.8	213.0	243.6	278.0	316.7	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 445 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	12.0	14.6	17.6	21.1	25.1	30.2	20.3%
Government & Defense	8.6	10.0	11.6	13.3	15.2	17.5	15.3%
Healthcare	4.9	5.8	6.9	8.1	9.5	11.3	18.2%
IT & ITeS	4.4	5.3	6.4	7.6	9.0	10.8	19.6%
Telecommunications	6.3	7.5	8.7	10.1	11.7	13.7	16.6%
Manufacturing	3.1	3.7	4.3	4.9	5.6	6.5	15.9%
Energy & Utilities	8.1	9.7	11.5	13.6	16.0	19.1	18.8%
Retail	6.7	8.0	9.5	11.1	12.9	15.2	17.7%
Education	2.7	3.3	3.8	4.5	5.2	6.1	17.1%
Other Verticals	3.8	4.5	5.3	6.2	7.1	8.3	16.7%
Total	60.8	72.4	85.7	100.6	117.4	138.7	17.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 446 UAE: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	35.7	42.0	49.0	57.1	66.2	76.7	16.5%
Government & Defense	19.8	22.4	25.0	27.9	31.0	34.3	11.6%
Healthcare	13.1	15.2	17.4	20.0	22.8	26.1	14.8%
IT & ITeS	12.6	14.8	17.2	19.9	23.0	26.5	16.0%
Telecommunications	15.6	17.9	20.2	22.9	25.8	29.0	13.2%
Manufacturing	7.4	8.4	9.5	10.7	11.9	13.3	12.4%
Energy & Utilities	22.2	25.9	29.9	34.4	39.5	45.3	15.3%
Retail	17.6	20.3	23.3	26.6	30.2	34.4	14.3%
Education	7.0	8.0	9.1	10.4	11.7	13.3	13.7%
Other Verticals	9.5	10.9	12.3	13.9	15.7	17.7	13.2%
Total	160.7	185.8	213.0	243.6	278.0	316.7	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.5.1.3 Rest of GCC

The Rest of GCC DDoS protection and mitigation market, comprising Qatar, Kuwait, Oman, and Bahrain, is expected to grow steadily, driven by accelerating digital transformation, cloud adoption, expansion of data center infrastructure, and increasing dependence on digital government and financial services. While these markets are smaller than Saudi Arabia and the UAE, they are developing specialized digital ecosystems supported by national transformation strategies and investments in connectivity and cybersecurity. Qatar's National Cybersecurity Strategy 2024–2030, Kuwait Vision 2035, Oman Vision 2040, and Bahrain's cloud-first initiatives are strengthening cybersecurity requirements across critical sectors. Furthermore, the GCC Cybersecurity Strategy (2024–2028) emphasizes regional cooperation and cyber resilience. The growing attack surface across government, BFSI, telecommunications, energy, and cloud infrastructure is expected to drive demand for advanced DDoS detection, mitigation, testing, and managed security services.

TABLE 447 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	23.1	27.1	31.8	37.0	42.8	50.1	16.8%
Services	7.0	8.4	9.9	11.7	13.7	16.2	18.3%
Total	30.1	35.5	41.7	48.7	56.5	66.3	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 448 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	57.5	65.9	74.8	84.8	95.8	108.1	13.5%
Services	18.9	21.9	25.2	28.9	33.1	37.8	14.9%
Total	76.4	87.8	100.0	113.7	128.9	145.9	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 449 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	10.3	12.0	14.0	16.2	18.7	21.7	16.2%
Software/Platforms	12.8	15.1	17.8	20.8	24.1	28.3	17.2%
Total	23.1	27.1	31.8	37.0	42.8	50.1	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 450 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	24.8	28.3	32.0	36.1	40.6	45.6	12.9%
Software/Platforms	32.7	37.6	42.8	48.7	55.2	62.5	13.9%
Total	57.5	65.9	74.8	84.8	95.8	108.1	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 451 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	4.1	4.8	5.7	6.7	7.8	9.3	18.0%
Managed Services	3.0	3.5	4.2	5.0	5.9	7.0	18.7%
Total	7.0	8.4	9.9	11.7	13.7	16.2	18.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 452 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	10.8	12.5	14.3	16.3	18.7	21.2	14.6%
Managed Services	8.1	9.5	10.9	12.6	14.5	16.6	15.3%
Total	18.9	21.9	25.2	28.9	33.1	37.8	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 453 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	1.1	1.3	1.6	1.8	2.1	2.5	17.3%
Consulting & Advisory	1.0	1.2	1.4	1.7	2.0	2.4	19.4%
Training & Education	0.7	0.8	1.0	1.1	1.3	1.6	18.7%
Support & Maintenance	0.8	0.9	1.1	1.3	1.5	1.7	16.4%
DDoS Testing & Validation	0.5	0.6	0.7	0.8	0.9	1.1	18.0%
Total	4.1	4.8	5.7	6.7	7.8	9.3	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 454 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	2.9	3.3	3.8	4.3	4.9	5.5	13.9%
Consulting & Advisory	2.8	3.3	3.8	4.4	5.1	5.9	15.9%
Training & Education	1.8	2.1	2.5	2.8	3.3	3.7	15.2%
Support & Maintenance	1.9	2.2	2.5	2.8	3.2	3.6	13.0%
DDoS Testing & Validation	1.3	1.5	1.7	1.9	2.2	2.5	14.6%
Total	10.8	12.5	14.3	16.3	18.7	21.2	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 455 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	7.6	8.9	10.4	11.9	13.7	15.9	15.8%
Threat Mitigation Systems	8.9	10.6	12.5	14.6	17.0	20.1	17.7%
Botnet Detection & Management	2.9	3.4	4.0	4.6	5.3	6.2	16.2%
Other Solution Types	3.6	4.3	5.0	5.8	6.8	7.9	17.1%
Total	23.1	27.1	31.8	37.0	42.8	50.1	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 456 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	18.1	20.5	23.1	25.9	29.1	32.5	12.4%
Threat Mitigation Systems	23.2	26.8	30.7	35.0	39.9	45.3	14.3%
Botnet Detection & Management	7.1	8.1	9.1	10.3	11.5	13.0	12.9%
Other Solution Types	9.1	10.5	11.9	13.6	15.4	17.4	13.7%
Total	57.5	65.9	74.8	84.8	95.8	108.1	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 457 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	10.5	12.4	14.6	17.1	19.9	23.4	17.3%
Web Applications & APIs	9.6	11.4	13.6	16.1	18.9	22.5	18.6%
DNS Infrastructure	10.0	11.6	13.5	15.5	17.7	20.5	15.4%
Total	30.1	35.5	41.7	48.7	56.5	66.3	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 458 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	27.0	31.1	35.4	40.4	45.8	52.0	14.0%
Web Applications & APIs	26.2	30.5	35.1	40.4	46.4	53.1	15.2%
DNS Infrastructure	23.2	26.3	29.5	32.9	36.7	40.9	12.0%
Total	76.4	87.8	100.0	113.7	128.9	145.9	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 459 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	9.5	11.2	13.0	15.1	17.4	20.3	16.4%
Cloud	18.4	21.7	25.6	30.0	34.9	41.1	17.5%
Hybrid	2.2	2.6	3.1	3.6	4.2	4.9	17.2%
Total	30.1	35.5	41.7	48.7	56.5	66.3	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 460 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	23.3	26.6	30.1	34.0	38.3	43.1	13.1%
Cloud	47.5	54.8	62.6	71.3	81.1	92.8	14.3%
Hybrid	5.6	6.5	7.4	8.4	9.5	10.0	12.1%
Total	76.4	87.8	100.0	113.7	128.9	145.9	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 461 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	18.8	22.1	25.8	29.9	34.5	40.2	16.4%
SMEs	11.3	13.4	15.9	18.8	22.0	26.1	18.4%
Total	30.1	35.5	41.7	48.7	56.5	66.3	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 462 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	46.0	52.5	59.4	67.1	75.6	84.9	13.0%
SMEs	30.4	35.3	40.6	46.6	53.4	61.0	14.9%
Total	76.4	87.8	100.0	113.7	128.9	145.9	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 463 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	6.0	7.2	8.6	10.2	12.1	14.5	19.4%
Government & Defense	4.3	4.9	5.7	6.5	7.3	8.4	14.5%
Healthcare	2.4	2.9	3.4	3.9	4.6	5.4	17.4%
IT & ITeS	2.2	2.6	3.1	3.7	4.3	5.2	18.7%
Telecommunications	3.1	3.7	4.3	4.9	5.6	6.5	15.8%
Manufacturing	1.5	1.8	2.1	2.4	2.7	3.1	15.1%
Energy & Utilities	4.0	4.7	5.6	6.6	7.7	9.1	17.9%
Retail	3.3	3.9	4.6	5.4	6.2	7.3	16.9%
Education	1.4	1.6	1.9	2.2	2.5	2.9	16.3%
Other Verticals	1.9	2.2	2.6	3.0	3.4	4.0	15.9%
Total	30.1	35.5	41.7	48.7	56.5	66.3	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 464 REST OF GCC: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	17.0	19.9	23.0	26.6	30.7	35.4	15.8%
Government & Defense	9.4	10.6	11.7	13.0	14.4	15.8	10.9%
Healthcare	6.2	7.2	8.2	9.3	10.6	12.0	14.1%
IT & ITeS	6.0	7.0	8.1	9.3	10.7	12.2	15.3%
Telecommunications	7.4	8.4	9.5	10.7	12.0	13.4	12.4%
Manufacturing	3.5	4.0	4.5	5.0	5.5	6.1	11.7%
Energy & Utilities	10.6	12.2	14.0	16.1	18.3	20.9	14.6%
Retail	8.4	9.6	10.9	12.4	14.0	15.8	13.6%
Education	3.3	3.8	4.3	4.8	5.4	6.1	13.0%
Other Verticals	4.5	5.1	5.8	6.5	7.3	8.2	12.5%
Total	76.4	87.8	100.0	113.7	128.9	145.9	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.5.2 SOUTH AFRICA

15.5.2.1 Government initiatives and substantial foreign investments to drive market

South Africa is at the forefront of technological advancements and the mobile economy in the African region. The DDoS protection and mitigation market in South Africa is experiencing significant growth due to the increasing frequency and sophistication of cyberattacks targeting businesses and public services. Key factors driving this market include the rising number of cyber threats, government regulations around data protection, and the rapid adoption of cloud services. As companies allocate more budget toward cybersecurity, there is a growing demand for advanced DDoS mitigation solutions that incorporate AI and machine learning for better detection and response. Additionally, many organizations are opting for managed security services to handle DDoS attacks, leveraging the expertise of specialized providers. Furthermore, government initiatives and substantial foreign investments are encouraging an increasing number of entrepreneurs, tech ventures, and innovation centers, which are expected to create growth opportunities for DDoS protection and mitigation vendors in the coming years. This could be the perfect time for vendors to develop innovative solutions.

TABLE 465 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	21.0	25.3	30.2	35.8	42.3	50.5	19.1%
Services	6.4	7.8	9.4	11.3	13.5	16.4	20.7%
Total	27.4	33.1	39.6	47.2	55.8	66.8	19.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 466 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	59.1	69.1	80.0	92.5	106.5	122.5	15.7%
Services	19.4	23.0	27.0	31.6	36.8	42.8	17.1%
Total	78.5	92.0	107.0	124.1	143.3	165.3	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 467 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	8.9	10.7	12.7	15.0	17.6	20.9	18.6%
Software/Platforms	12.1	14.6	17.5	20.9	24.7	29.6	19.5%
Total	21.0	25.3	30.2	35.8	42.3	50.5	19.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 468 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	24.3	28.3	32.7	37.6	43.0	49.2	15.1%
Software/Platforms	34.8	40.8	47.4	55.0	63.5	73.2	16.1%
Total	59.1	69.1	80.0	92.5	106.5	122.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 469 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	3.7	4.5	5.4	6.5	7.7	9.3	20.4%
Managed Services	2.7	3.3	4.0	4.8	5.8	7.0	21.1%
Total	6.4	7.8	9.4	11.3	13.5	16.4	20.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 470 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	11.1	13.1	15.3	17.8	20.7	24.1	16.8%
Managed Services	8.4	9.9	11.7	13.7	16.1	18.8	17.6%
Total	19.4	23.0	27.0	31.6	36.8	42.8	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 471 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	1.0	1.2	1.5	1.8	2.1	2.5	19.7%
Consulting & Advisory	0.9	1.1	1.3	1.6	2.0	2.4	21.8%
Training & Education	0.6	0.7	0.9	1.1	1.3	1.6	21.1%
Support & Maintenance	0.7	0.9	1.0	1.2	1.4	1.7	18.8%
DDoS Testing & Validation	0.4	0.5	0.6	0.8	0.9	1.1	20.4%
Total	3.7	4.5	5.4	6.5	7.7	9.3	20.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 472 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	3.0	3.5	4.1	4.7	5.4	6.3	16.2%
Consulting & Advisory	2.9	3.4	4.1	4.8	5.7	6.6	18.2%
Training & Education	1.9	2.2	2.6	3.1	3.6	4.2	17.5%
Support & Maintenance	2.0	2.3	2.7	3.1	3.5	4.1	15.2%
DDoS Testing & Validation	1.3	1.6	1.8	2.1	2.5	2.9	16.8%
Total	11.1	13.1	15.3	17.8	20.7	24.1	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 473 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	7.0	8.3	9.8	11.6	13.5	16.0	18.1%
Threat Mitigation Systems	8.1	9.8	11.8	14.2	16.8	20.2	20.0%
Botnet Detection & Management	2.7	3.2	3.8	4.5	5.2	6.2	18.6%
Other Solution Types	3.3	4.0	4.7	5.6	6.7	8.0	19.4%
Total	21.0	25.3	30.2	35.8	42.3	50.5	19.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 474 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	18.6	21.5	24.7	28.3	32.3	36.8	14.6%
Threat Mitigation Systems	23.9	28.1	32.8	38.2	44.3	51.3	16.5%
Botnet Detection & Management	7.3	8.4	9.7	11.2	12.8	14.7	15.1%
Other Solution Types	9.4	11.0	12.8	14.8	17.1	19.7	16.0%
Total	59.1	69.1	80.0	92.5	106.5	122.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 475 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	9.6	11.6	13.9	16.6	19.6	23.6	19.7%
Web Applications & APIs	8.7	10.6	12.9	15.6	18.7	22.6	21.0%
DNS Infrastructure	9.1	10.8	12.8	15.0	17.5	20.6	17.7%
Total	27.4	33.1	39.6	47.2	55.8	66.8	19.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 476 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	27.7	32.6	37.9	44.1	51.0	58.9	16.3%
Web Applications & APIs	26.9	31.9	37.6	44.1	51.5	60.1	17.4%
DNS Infrastructure	23.9	27.5	31.5	36.0	40.8	46.3	14.2%
Total	78.5	92.0	107.0	124.1	143.3	165.3	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 477 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	8.7	10.4	12.4	14.6	17.2	20.5	18.8%
Cloud	16.7	20.2	24.3	29.0	34.5	41.4	19.9%
Hybrid	2.0	2.4	2.9	3.5	4.1	4.9	19.6%
Total	27.4	33.1	39.6	47.2	55.8	66.8	19.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 478 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	23.9	27.9	32.2	37.1	42.6	48.8	15.3%
Cloud	48.8	57.4	66.9	77.9	90.2	105.2	16.6%
Hybrid	5.8	6.8	7.9	9.1	10.5	11.3	14.3%
Total	78.5	92.0	107.0	124.1	143.3	165.3	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 479 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	17.2	20.6	24.5	29.0	34.0	40.5	18.7%
SMEs	10.3	12.5	15.1	18.2	21.8	26.3	20.8%
Total	27.4	33.1	39.6	47.2	55.8	66.8	19.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 480 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	47.3	55.0	63.6	73.2	84.0	96.2	15.3%
SMEs	31.2	37.0	43.4	50.9	59.3	69.1	17.2%
Total	78.5	92.0	107.0	124.1	143.3	165.3	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 481 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	5.4	6.7	8.2	9.9	11.9	14.6	21.9%
Government & Defense	3.9	4.6	5.4	6.3	7.2	8.5	16.8%
Healthcare	2.2	2.7	3.2	3.8	4.5	5.4	19.8%
IT & ITeS	2.0	2.4	3.0	3.6	4.3	5.2	21.1%
Telecommunications	2.9	3.4	4.0	4.8	5.6	6.6	18.2%
Manufacturing	1.4	1.7	2.0	2.3	2.7	3.1	17.5%
Energy & Utilities	3.6	4.4	5.3	6.4	7.6	9.2	20.3%
Retail	3.0	3.7	4.4	5.2	6.1	7.3	19.3%
Education	1.2	1.5	1.8	2.1	2.5	2.9	18.7%
Other Verticals	1.7	2.1	2.5	2.9	3.4	4.0	18.2%
Total	27.4	33.1	39.6	47.2	55.8	66.8	19.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 482 SOUTH AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	17.4	20.8	24.6	29.1	34.1	40.1	18.1%
Government & Defense	9.7	11.1	12.6	14.2	16.0	17.9	13.1%
Healthcare	6.4	7.5	8.8	10.2	11.8	13.6	16.3%
IT & ITeS	6.2	7.3	8.6	10.1	11.9	13.8	17.5%
Telecommunications	7.6	8.9	10.2	11.7	13.3	15.1	14.7%
Manufacturing	3.6	4.2	4.8	5.4	6.2	7.0	13.9%
Energy & Utilities	10.9	12.8	15.0	17.5	20.4	23.7	16.8%
Retail	8.6	10.1	11.7	13.5	15.6	17.9	15.8%
Education	3.4	4.0	4.6	5.3	6.0	6.9	15.2%
Other Verticals	4.7	5.4	6.2	7.1	8.1	9.2	14.7%
Total	78.5	92.0	107.0	124.1	143.3	165.3	16.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.5.3 REST OF MIDDLE EAST & AFRICA

Israel, Turkey, and the remaining countries are considered in the rest of Middle East & Africa. The DDoS protection and mitigation market in these countries is witnessing significant growth, driven by the rising frequency and sophistication of DDoS attacks, as well as a heightened awareness of cybersecurity needs. In Israel, a hub for cybersecurity innovation, the market is propelled by key players such as Radware and NETSCOUT, alongside government initiatives that promote cybersecurity advancements. In Turkey, the demand for DDoS protection services is increasing due to a rise in cyber threats, with local firms and international companies such as Cloudflare and Akamai leading the way. These countries are experiencing a shift toward cloud-based solutions and integrated security services, although challenges such as skill shortages and an evolving threat landscape remain significant hurdles.

TABLE 483 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	71.8	84.7	99.3	115.5	133.6	156.4	16.8%
Services	21.8	26.1	31.0	36.5	42.8	50.7	18.4%
Total	93.7	110.8	130.3	152.0	176.3	207.1	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 484 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	179.6	205.7	233.6	264.7	299.4	337.7	13.5%
Services	59.0	68.4	78.7	90.3	103.4	118.1	14.9%
Total	238.6	274.1	312.4	355.0	402.8	455.8	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 485 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	30.4	35.7	41.7	48.3	55.5	64.7	16.3%
Software/Platforms	41.4	49.0	57.6	67.3	78.0	91.7	17.2%
Total	71.8	84.7	99.3	115.5	133.6	156.4	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 486 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	74.0	84.3	95.3	107.5	121.0	135.8	12.9%
Software/Platforms	105.6	121.4	138.3	157.2	178.4	201.9	13.8%
Total	179.6	205.7	233.6	264.7	299.4	337.7	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 487 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	12.6	15.1	17.8	21.0	24.5	29.0	18.1%
Managed Services	9.2	11.0	13.2	15.6	18.3	21.8	18.8%
Total	21.8	26.1	31.0	36.5	42.8	50.7	18.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 488 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	33.6	38.9	44.6	51.0	58.3	66.4	14.6%
Managed Services	25.4	29.6	34.1	39.3	45.1	51.7	15.3%
Total	59.0	68.4	78.7	90.3	103.4	118.1	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 489 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	3.5	4.1	4.9	5.7	6.6	7.8	17.4%
Consulting & Advisory	3.1	3.7	4.4	5.3	6.2	7.5	19.5%
Training & Education	2.1	2.5	3.0	3.5	4.1	4.9	18.8%
Support & Maintenance	2.5	2.9	3.4	4.0	4.6	5.3	16.5%
DDoS Testing & Validation	1.5	1.8	2.1	2.5	2.9	3.5	18.1%
Total	12.6	15.1	17.8	21.0	24.5	29.0	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 490 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	9.0	10.4	11.8	13.5	15.3	17.3	13.9%
Consulting & Advisory	8.8	10.3	11.9	13.8	15.9	18.3	15.9%
Training & Education	5.7	6.7	7.7	8.9	10.2	11.7	15.3%
Support & Maintenance	6.1	6.9	7.9	8.9	10.0	11.2	13.0%
DDoS Testing & Validation	4.0	4.6	5.3	6.1	6.9	7.9	14.6%
Total	33.6	38.9	44.6	51.0	58.3	66.4	14.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 491 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	23.8	27.8	32.3	37.3	42.7	49.6	15.8%
Threat Mitigation Systems	27.7	33.0	38.9	45.6	53.2	62.7	17.7%
Botnet Detection & Management	9.1	10.7	12.4	14.4	16.6	19.3	16.3%
Other Solution Types	11.2	13.3	15.6	18.2	21.1	24.8	17.1%
Total	71.8	84.7	99.3	115.5	133.6	156.4	16.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 492 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	56.5	64.1	72.1	81.0	90.8	101.4	12.4%
Threat Mitigation Systems	72.6	83.7	95.8	109.3	124.5	141.5	14.3%
Botnet Detection & Management	22.1	25.1	28.4	32.0	36.0	40.5	12.9%
Other Solution Types	28.5	32.7	37.3	42.4	48.0	54.3	13.7%
Total	179.6	205.7	233.6	264.7	299.4	337.7	13.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 493 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	32.7	38.8	45.7	53.4	62.1	73.0	17.4%
Web Applications & APIs	29.8	35.7	42.5	50.2	59.0	70.1	18.7%
DNS Infrastructure	31.2	36.3	42.1	48.4	55.3	64.0	15.5%
Total	93.7	110.8	130.3	152.0	176.3	207.1	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 494 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	84.2	97.0	110.7	126.0	143.2	162.3	14.0%
Web Applications & APIs	81.8	95.1	109.7	126.1	144.8	165.7	15.2%
DNS Infrastructure	72.5	82.1	92.0	102.9	114.8	127.7	12.0%
Total	238.6	274.1	312.4	355.0	402.8	455.8	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 495 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	29.6	34.8	40.7	47.2	54.4	63.5	16.5%
Cloud	57.2	67.8	80.0	93.6	109.0	128.4	17.6%
Hybrid	6.9	8.1	9.6	11.2	13.0	15.2	17.3%
Total	93.7	110.8	130.3	152.0	176.3	207.1	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 496 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	72.7	83.0	94.0	106.2	119.7	134.7	13.1%
Cloud	148.3	170.9	195.4	222.7	253.5	290.0	14.3%
Hybrid	17.6	20.2	23.0	26.1	29.6	31.1	12.1%
Total	238.6	274.1	312.4	355.0	402.8	455.8	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 497 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	58.6	68.9	80.5	93.3	107.6	125.5	16.4%
SMEs	35.0	41.9	49.8	58.7	68.8	81.6	18.4%
Total	93.7	110.8	130.3	152.0	176.3	207.1	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 498 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	143.6	163.9	185.5	209.5	236.0	265.3	13.1%
SMEs	95.0	110.2	126.8	145.6	166.7	190.5	14.9%
Total	238.6	274.1	312.4	355.0	402.8	455.8	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 499 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	18.5	22.4	26.8	31.9	37.7	45.2	19.5%
Government & Defense	13.3	15.4	17.7	20.2	22.8	26.2	14.6%
Healthcare	7.5	8.9	10.5	12.3	14.3	16.8	17.5%
IT & ITeS	6.8	8.2	9.7	11.5	13.5	16.1	18.8%
Telecommunications	9.8	11.4	13.3	15.3	17.6	20.4	15.9%
Manufacturing	4.8	5.6	6.5	7.4	8.5	9.8	15.2%
Energy & Utilities	12.4	14.8	17.5	20.6	24.1	28.5	18.0%
Retail	10.4	12.3	14.4	16.8	19.4	22.7	17.0%
Education	4.2	5.0	5.8	6.7	7.8	9.1	16.4%
Other Verticals	5.9	6.9	8.1	9.3	10.7	12.4	15.9%
Total	93.7	110.8	130.3	152.0	176.3	207.1	17.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 500 REST OF THE MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	53.0	62.0	71.9	83.2	96.0	110.5	15.8%
Government & Defense	29.5	33.0	36.7	40.6	44.8	49.4	10.9%
Healthcare	19.4	22.4	25.6	29.1	33.1	37.5	14.1%
IT & ITeS	18.8	21.8	25.2	29.0	33.3	38.2	15.3%
Telecommunications	23.2	26.4	29.7	33.3	37.4	41.8	12.5%
Manufacturing	11.0	12.5	13.9	15.5	17.3	19.2	11.7%
Energy & Utilities	33.0	38.2	43.8	50.1	57.3	65.2	14.6%
Retail	26.1	30.0	34.1	38.7	43.8	49.5	13.6%
Education	10.4	11.8	13.4	15.1	17.0	19.1	13.0%
Other Verticals	14.1	16.1	18.1	20.3	22.8	25.5	12.5%
Total	238.6	274.1	312.4	355.0	402.8	455.8	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.6 LATIN AMERICA

The increasing global competition has prompted DDoS protection and mitigation solution providers to enter emerging markets in search of new business models and services. Latin America is an attractive market for DDoS protection and mitigation solution providers. The region is expected to make social and economic progress. Companies in the region are considering adopting DDoS protection and mitigation solutions to enhance data privacy and prevent sensitive data breaches from traversing networks. The surge in cloud adoption for data storage and ease of access from anywhere adds to data security concerns. The need to protect organizational data from DDoS attacks, cyberattacks, misuse due to unauthorized access, and theft-related losses has driven the adoption of DDoS protection and mitigation solutions in the region. Nexusguard significantly expanded its footprint in Latin America by partnering with leading telecommunications providers and Internet Service Providers (ISPs) in Brazil. This strategic collaboration led to the deployment of 8 DDoS scrubbing centers across the country, a direct response to the escalating demand for robust cybersecurity infrastructure within the region.

The driving factors, including the rise in broadband networks, cloud services, Managed Service Providers (MSPs), the IT sector, and the limited availability of legacy infrastructure, are expected to drive the growth of the DDoS protection and mitigation market in Latin America. Enterprises are not only demanding the maintenance of their network activities, but also the stability of their network operations. SMEs are the early adopters of network traffic tools to survive in the fast-paced business process. In addition, the rising complexities in network infrastructure and the increasing need to maintain network devices and secure network operations have compelled businesses to opt for DDoS protection and mitigation solutions.

TABLE 501 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	94.0	112.0	132.4	154.9	179.6	202.3	16.6%
Services	28.6	34.5	41.3	49.0	57.5	65.6	18.1%
Total	122.5	146.5	173.7	203.9	237.1	267.9	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 502 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	231.5	264.0	304.6	350.2	403.4	446.1	14.0%
Services	76.1	87.8	102.6	119.5	139.4	156.0	15.5%
Total	307.6	351.9	407.2	469.7	542.7	602.1	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 503 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	40.6	48.2	56.7	66.0	76.1	85.3	16.0%
Software/Platforms	53.4	63.8	75.8	88.9	103.5	117.0	17.0%
Total	94.0	112.0	132.4	154.9	179.6	202.3	16.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 504 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	97.2	110.3	126.6	144.8	166.0	182.7	13.5%
Software/Platforms	134.4	153.8	178.0	205.4	237.4	263.4	14.4%
Total	231.5	264.0	304.6	350.2	403.4	446.1	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 505 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	16.5	19.9	23.8	28.1	32.9	37.5	17.8%
Managed Services	12.0	14.6	17.5	20.9	24.6	28.1	18.5%
Total	28.6	34.5	41.3	49.0	57.5	65.6	18.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 506 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	43.3	49.9	58.1	67.5	78.5	87.7	15.1%
Managed Services	32.7	37.9	44.5	52.0	60.8	68.3	15.9%
Total	76.1	87.8	102.6	119.5	139.4	156.0	15.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 507 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	4.6	5.5	6.5	7.7	8.9	10.1	17.2%
Consulting & Advisory	4.0	4.9	5.9	7.1	8.4	9.7	19.2%
Training & Education	2.7	3.3	4.0	4.7	5.6	6.4	18.5%
Support & Maintenance	3.2	3.9	4.5	5.3	6.1	6.9	16.3%
DDoS Testing & Validation	2.0	2.4	2.8	3.4	3.9	4.5	17.8%
Total	16.5	19.9	23.8	28.1	32.9	37.5	17.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 508 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	11.6	13.3	15.4	17.8	20.6	22.9	14.5%
Consulting & Advisory	11.3	13.2	15.5	18.2	21.4	24.2	16.4%
Training & Education	7.4	8.6	10.0	11.7	13.7	15.4	15.8%
Support & Maintenance	7.8	8.9	10.2	11.7	13.4	14.8	13.5%
DDoS Testing & Validation	5.2	5.9	6.9	8.0	9.4	10.5	15.1%
Total	43.3	49.9	58.1	67.5	78.5	87.7	15.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 509 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	30.3	36.2	42.9	50.3	58.5	66.0	16.8%
Threat Mitigation Systems	26.3	31.2	36.8	43.0	49.7	55.9	16.3%
Botnet Detection & Management	20.1	24.1	28.8	33.9	39.6	45.0	17.5%
Other Solution Types	17.3	20.4	23.9	27.7	31.8	35.4	15.5%
Total	94.0	112.0	132.4	154.9	179.6	202.3	16.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 510 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	75.7	86.6	100.1	115.3	133.1	147.5	14.3%
Threat Mitigation Systems	63.8	72.5	83.5	95.7	110.0	121.3	13.7%
Botnet Detection & Management	51.9	59.6	69.3	80.2	93.1	103.7	14.9%
Other Solution Types	40.2	45.4	51.8	59.0	67.2	73.6	12.9%
Total	231.5	264.0	304.6	350.2	403.4	446.1	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 511 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	42.8	51.3	60.9	71.6	83.4	94.5	17.1%
Web Applications & APIs	38.9	47.2	56.7	67.3	79.3	90.7	18.4%
DNS Infrastructure	40.8	48.0	56.1	64.9	74.4	82.8	15.2%
Total	122.5	146.5	173.7	203.9	237.1	267.9	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 512 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	108.6	124.5	144.3	166.7	193.0	214.5	14.6%
Web Applications & APIs	105.4	122.1	143.0	166.9	195.1	218.9	15.7%
DNS Infrastructure	93.5	105.3	119.9	136.1	154.7	168.7	12.5%
Total	307.6	351.9	407.2	469.7	542.7	602.1	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 513 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	38.8	46.0	54.3	63.3	73.1	82.2	16.2%
Cloud	74.8	89.7	106.7	125.6	146.5	166.1	17.3%
Hybrid	9.0	10.8	12.8	15.0	17.4	19.7	17.0%
Total	122.5	146.5	173.7	203.9	237.1	267.9	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 514 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	93.7	106.6	122.6	140.5	161.4	177.9	13.7%
Cloud	191.2	219.4	254.7	294.7	341.5	383.0	14.9%
Hybrid	22.6	25.9	29.9	34.5	39.8	41.1	12.7%
Total	307.6	351.9	407.2	469.7	542.7	602.1	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 515 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	76.7	91.1	107.4	125.2	144.6	162.4	16.2%
SMEs	45.8	55.4	66.4	78.7	92.5	105.6	18.2%
Total	122.5	146.5	173.7	203.9	237.1	267.9	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 516 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	185.2	210.4	241.9	277.1	318.0	350.4	13.6%
SMEs	122.4	141.5	165.3	192.6	224.7	251.7	15.5%
Total	307.6	351.9	407.2	469.7	542.7	602.1	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 517 LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	24.2	29.6	35.8	42.8	50.7	58.4	19.2%
Government & Defense	17.4	20.3	23.6	27.0	30.7	33.9	14.3%
Healthcare	9.8	11.8	14.0	16.5	19.2	21.8	17.2%
IT & ITeS	8.9	10.8	13.0	15.4	18.2	20.8	18.5%
Telecommunications	12.8	15.1	17.7	20.5	23.6	26.4	15.6%
Manufacturing	6.3	7.4	8.6	9.9	11.4	12.6	15.0%
Energy & Utilities	16.3	19.6	23.4	27.6	32.4	36.8	17.8%
Retail	13.6	16.2	19.2	22.5	26.1	29.4	16.7%
Education	5.5	6.6	7.8	9.0	10.4	11.7	16.1%
Other Verticals	7.8	9.2	10.8	12.5	14.4	16.1	15.7%
Total	122.5	146.5	173.7	203.9	237.1	267.9	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 518 **LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)**

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	68.3	79.6	93.8	110.0	129.3	145.9	16.4%
Government & Defense	38.0	42.4	47.8	53.7	60.4	65.2	11.4%
Healthcare	25.0	28.7	33.3	38.5	44.6	49.6	14.6%
IT & ITeS	24.2	28.0	32.9	38.4	44.9	50.4	15.8%
Telecommunications	29.9	33.8	38.7	44.1	50.3	55.2	13.0%
Manufacturing	14.2	16.0	18.2	20.6	23.3	25.4	12.2%
Energy & Utilities	42.6	49.0	57.1	66.3	77.1	86.2	15.1%
Retail	33.7	38.5	44.5	51.2	59.0	65.4	14.2%
Education	13.4	15.2	17.4	20.0	22.9	25.2	13.6%
Other Verticals	18.2	20.6	23.6	26.9	30.7	33.7	13.0%
Total	307.6	351.9	407.2	469.7	542.7	602.1	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 519 **LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2020–2025 (USD MILLION)**

Country	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Brazil	50.3	59.6	69.9	81.2	93.4	104.5	15.7%
Mexico	41.4	50.2	59.9	70.9	83.0	94.5	18.0%
Rest of Latin America	30.8	36.8	43.9	51.8	60.6	68.9	17.5%
Total	122.5	146.5	173.7	203.9	237.1	267.9	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 520 **LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY COUNTRY, 2026–2031 (USD MILLION)**

Country	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Brazil	119.5	136.1	156.9	180.2	207.4	229.7	14.0%
Mexico	109.3	126.0	147.0	170.8	198.8	222.2	15.2%
Rest of Latin America	78.8	89.7	103.4	118.7	136.5	150.1	13.8%
Total	307.6	351.9	407.2	469.7	542.7	602.1	14.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.6.1 BRAZIL

15.6.1.1 Increasing focus on establishing effective cybersecurity strategies to drive market

Brazil is one of the major countries responsible for shaping the technology landscape of Latin America. Most of the DDoS attacks in this region are targeted toward Brazil, and so the country needs to take special precautions against such threats. According to the International Monetary Fund (IMF), despite the country's declining economic performance over the past few years, it is expected to grow in the coming years. Brazil has witnessed the entry of major tech companies, leading to digital transformation initiatives across various sectors, including BFSI, retail, manufacturing, and healthcare. To mitigate the DDoS attacks and spear-phishing attacks that have been witnessed in recent years, organizations in Brazil are expected to adopt DDoS protection and mitigation services. In this context, DDoS attacks have become a significant issue in Brazil, leading to an increasing demand for legislative measures. Brazil is attempting to enhance cybersecurity legislation by forcing regulated firms to establish effective cybersecurity strategies. However, due to the internet's global reach and transnational nature, Brazilian authorities' ability to investigate cybercrime is increasingly seen as a major concern for the future.

TABLE 521 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	38.6	45.6	53.3	61.7	70.8	78.9	15.4%
Services	11.7	14.0	16.6	19.5	22.7	25.6	16.9%
Total	50.3	59.6	69.9	81.2	93.4	104.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 522 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	89.9	102.1	117.3	134.4	154.1	170.2	13.6%
Services	29.5	34.0	39.5	45.8	53.2	59.5	15.0%
Total	119.5	136.1	156.9	180.2	207.4	229.7	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 523 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	17.1	20.1	23.5	27.0	30.9	34.2	14.8%
Software/Platforms	21.5	25.4	29.8	34.7	39.9	44.7	15.8%
Total	38.6	45.6	53.3	61.7	70.8	78.9	15.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 524 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	38.8	43.9	50.2	57.2	65.3	71.8	13.1%
Software/Platforms	51.1	58.2	67.1	77.2	88.8	98.4	14.0%
Total	89.9	102.1	117.3	134.4	154.1	170.2	13.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 525 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	6.8	8.1	9.6	11.2	13.0	14.6	16.6%
Managed Services	4.9	5.9	7.1	8.3	9.7	11.0	17.3%
Total	11.7	14.0	16.6	19.5	22.7	25.6	16.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 526 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	16.8	19.3	22.4	25.9	30.0	33.5	14.7%
Managed Services	12.7	14.7	17.1	19.9	23.2	26.1	15.4%
Total	29.5	34.0	39.5	45.8	53.2	59.5	15.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 527 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	1.9	2.2	2.6	3.1	3.5	3.9	15.9%
Consulting & Advisory	1.6	2.0	2.4	2.8	3.3	3.8	18.0%
Training & Education	1.1	1.3	1.6	1.9	2.2	2.5	17.3%
Support & Maintenance	1.3	1.6	1.8	2.1	2.4	2.7	15.1%
DDoS Testing & Validation	0.8	1.0	1.1	1.3	1.5	1.7	16.6%
Total	6.8	8.1	9.6	11.2	13.0	14.6	16.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 528 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	4.5	5.1	5.9	6.8	7.9	8.7	14.1%
Consulting & Advisory	4.4	5.1	6.0	7.0	8.2	9.2	16.0%
Training & Education	2.9	3.3	3.9	4.5	5.2	5.9	15.4%
Support & Maintenance	3.0	3.4	3.9	4.5	5.1	5.6	13.1%
DDoS Testing & Validation	2.0	2.3	2.7	3.1	3.6	4.0	14.7%
Total	16.8	19.3	22.4	25.9	30.0	33.5	14.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 529 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	12.4	14.6	17.2	19.9	22.9	25.6	15.6%
Threat Mitigation Systems	10.8	12.7	14.8	17.1	19.6	21.8	15.1%
Botnet Detection & Management	8.3	9.9	11.7	13.6	15.7	17.7	16.3%
Other Solution Types	7.1	8.3	9.6	11.1	12.6	13.9	14.3%
Total	38.6	45.6	53.3	61.7	70.8	78.9	15.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 530 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	29.2	33.3	38.3	43.9	50.5	55.9	13.9%
Threat Mitigation Systems	24.7	28.0	32.1	36.7	42.0	46.2	13.3%
Botnet Detection & Management	20.3	23.2	26.9	31.0	35.9	39.9	14.5%
Other Solution Types	15.7	17.6	20.0	22.7	25.8	28.2	12.5%
Total	89.9	102.1	117.3	134.4	154.1	170.2	13.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 531 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	17.6	20.9	24.5	28.5	32.9	36.8	15.9%
Web Applications & APIs	16.0	19.2	22.8	26.8	31.3	35.4	17.2%
DNS Infrastructure	16.7	19.5	22.6	25.9	29.3	32.3	14.0%
Total	50.3	59.6	69.9	81.2	93.4	104.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 532 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET,
BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	42.2	48.1	55.6	64.0	73.7	81.8	14.2%
Web Applications & APIs	41.0	47.2	55.1	64.0	74.5	83.5	15.3%
DNS Infrastructure	36.3	40.7	46.2	52.2	59.1	64.4	12.1%
Total	119.5	136.1	156.9	180.2	207.4	229.7	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 533 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	15.9	18.7	21.8	25.2	28.8	32.0	15.0%
Cloud	30.7	36.5	42.9	50.0	57.7	64.8	16.1%
Hybrid	3.7	4.4	5.1	6.0	6.9	7.7	15.8%
Total	50.3	59.6	69.9	81.2	93.4	104.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 534 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	36.4	41.2	47.2	53.9	61.7	67.9	13.3%
Cloud	74.3	84.9	98.1	113.1	130.5	146.2	14.5%
Hybrid	8.8	10.0	11.5	13.2	15.2	15.7	12.3%
Total	119.5	136.1	156.9	180.2	207.4	229.7	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 535 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	31.5	37.1	43.2	49.9	57.0	63.3	15.0%
SMEs	18.8	22.5	26.7	31.4	36.4	41.2	16.9%
Total	50.3	59.6	69.9	81.2	93.4	104.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 536 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	71.9	81.4	93.2	106.3	121.5	133.7	13.2%
SMEs	47.5	54.7	63.7	73.9	85.9	96.0	15.1%
Total	119.5	136.1	156.9	180.2	207.4	229.7	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 537 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	10.0	12.0	14.4	17.1	20.0	22.8	18.0%
Government & Defense	7.1	8.3	9.5	10.8	12.1	13.2	13.1%
Healthcare	4.0	4.8	5.6	6.6	7.6	8.5	16.0%
IT & ITeS	3.7	4.4	5.2	6.1	7.2	8.1	17.3%
Telecommunications	5.2	6.1	7.1	8.2	9.3	10.3	14.4%
Manufacturing	2.6	3.0	3.5	4.0	4.5	4.9	13.8%
Energy & Utilities	6.7	8.0	9.4	11.0	12.8	14.4	16.5%
Retail	5.6	6.6	7.7	9.0	10.3	11.5	15.5%
Education	2.3	2.7	3.1	3.6	4.1	4.6	14.9%
Other Verticals	3.2	3.7	4.3	5.0	5.7	6.3	14.5%
Total	50.3	59.6	69.9	81.2	93.4	104.5	15.7%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 538 BRAZIL: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	26.5	30.8	36.1	42.2	49.4	55.7	16.0%
Government & Defense	14.8	16.4	18.4	20.6	23.1	24.9	11.0%
Healthcare	9.7	11.1	12.8	14.8	17.0	18.9	14.2%
IT & ITeS	9.4	10.8	12.7	14.7	17.2	19.2	15.4%
Telecommunications	11.6	13.1	14.9	16.9	19.2	21.0	12.6%
Manufacturing	5.5	6.2	7.0	7.9	8.9	9.7	11.8%
Energy & Utilities	16.5	19.0	22.0	25.4	29.5	32.9	14.7%
Retail	13.1	14.9	17.1	19.6	22.6	24.9	13.8%
Education	5.2	5.9	6.7	7.7	8.7	9.6	13.2%
Other Verticals	7.1	8.0	9.1	10.3	11.7	12.8	12.6%
Total	119.5	136.1	156.9	180.2	207.4	229.7	14.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.6.2 MEXICO

15.6.2.1 Rising adoption of cloud-based services to drive market

Mexico is increasingly adopting cloud-based services. The country can become digitally advanced in terms of technical expertise due to its proximity to the US. Moreover, various tech companies have opened their data centers in Mexico to cater to Latin America. The DDoS protection and mitigation market in Mexico has experienced moderate adoption. However, this adoption is expected to increase in the coming years as organizations become more aware of phishing scams, data thefts, and data breaches. The Mexican government has been using sophisticated surveillance devices. Civil society organizations and independent media in Mexico have observed a rise in DDoS attacks.

TABLE 539 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	31.7	38.4	45.7	53.8	62.9	71.4	17.6%
Services	9.6	11.8	14.3	17.0	20.1	23.2	19.1%
Total	41.4	50.2	59.9	70.9	83.0	94.5	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 540 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	82.3	94.6	109.9	127.3	147.8	164.6	14.9%
Services	27.0	31.5	37.0	43.4	51.0	57.6	16.3%
Total	109.3	126.0	147.0	170.8	198.8	222.2	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 541 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	13.4	16.2	19.2	22.5	26.1	29.5	17.1%
Software/Platforms	18.3	22.2	26.5	31.4	36.7	41.8	18.0%
Total	31.7	38.4	45.7	53.8	62.9	71.4	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 542 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	33.9	38.8	44.8	51.7	59.7	66.2	14.3%
Software/Platforms	48.4	55.8	65.1	75.6	88.1	98.4	15.3%
Total	82.3	94.6	109.9	127.3	147.8	164.6	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 543 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	5.6	6.8	8.2	9.8	11.5	13.2	18.8%
Managed Services	4.1	5.0	6.0	7.3	8.6	9.9	19.6%
Total	9.6	11.8	14.3	17.0	20.1	23.2	19.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 544 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	15.4	17.9	21.0	24.5	28.8	32.4	16.0%
Managed Services	11.6	13.6	16.1	18.9	22.3	25.2	16.7%
Total	27.0	31.5	37.0	43.4	51.0	57.6	16.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 545 MEXICO: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	1.5	1.9	2.2	2.7	3.1	3.6	18.2%
Consulting & Advisory	1.4	1.7	2.0	2.5	2.9	3.4	20.3%
Training & Education	0.9	1.1	1.4	1.6	1.9	2.2	19.5%
Support & Maintenance	1.1	1.3	1.6	1.8	2.1	2.4	17.3%
DDoS Testing & Validation	0.7	0.8	1.0	1.2	1.4	1.6	18.8%
Total	5.6	6.8	8.2	9.8	11.5	13.2	18.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 546 MEXICO: DDOS PROTECTION AND MITIGATION MARKET,
BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	4.1	4.8	5.6	6.5	7.5	8.4	15.4%
Consulting & Advisory	4.0	4.7	5.6	6.6	7.8	8.9	17.3%
Training & Education	2.6	3.1	3.6	4.3	5.0	5.7	16.7%
Support & Maintenance	2.8	3.2	3.7	4.3	4.9	5.5	14.4%
DDoS Testing & Validation	1.8	2.1	2.5	2.9	3.4	3.9	16.0%
Total	15.4	17.9	21.0	24.5	28.8	32.4	16.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 547 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE,
2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	10.3	12.5	14.9	17.6	20.6	23.4	17.9%
Threat Mitigation Systems	8.9	10.7	12.7	15.0	17.5	19.8	17.3%
Botnet Detection & Management	6.7	8.2	9.8	11.7	13.7	15.7	18.5%
Other Solution Types	5.8	7.0	8.2	9.6	11.1	12.5	16.5%
Total	31.7	38.4	45.7	53.8	62.9	71.4	17.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 548 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	27.1	31.2	36.3	42.1	49.0	54.7	15.1%
Threat Mitigation Systems	22.7	26.0	30.2	34.9	40.4	44.9	14.6%
Botnet Detection & Management	18.3	21.1	24.8	28.9	33.8	37.9	15.7%
Other Solution Types	14.2	16.2	18.7	21.4	24.6	27.1	13.7%
Total	82.3	94.6	109.9	127.3	147.8	164.6	14.9%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 549 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	14.5	17.6	21.0	24.9	29.2	33.3	18.2%
Web Applications & APIs	13.1	16.1	19.5	23.4	27.8	32.0	19.5%
DNS Infrastructure	13.8	16.5	19.4	22.6	26.0	29.2	16.2%
Total	41.4	50.2	59.9	70.9	83.0	94.5	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 550 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	38.6	44.6	52.1	60.6	70.7	79.1	15.4%
Web Applications & APIs	37.5	43.7	51.6	60.7	71.5	80.8	16.6%
DNS Infrastructure	33.3	37.7	43.3	49.5	56.7	62.3	13.4%
Total	109.3	126.0	147.0	170.8	198.8	222.2	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 551 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	13.1	15.8	18.7	22.0	25.6	29.0	17.2%
Cloud	25.3	30.7	36.8	43.7	51.3	58.6	18.3%
Hybrid	3.0	3.7	4.4	5.2	6.1	7.0	18.0%
Total	41.4	50.2	59.9	70.9	83.0	94.5	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 552 MEXICO: DDOS PROTECTION AND MITIGATION MARKET,
BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	33.3	38.2	44.2	51.1	59.1	65.7	14.5%
Cloud	68.0	78.6	91.9	107.1	125.1	141.4	15.8%
Hybrid	8.0	9.3	10.8	12.5	14.6	15.2	13.5%
Total	109.3	126.0	147.0	170.8	198.8	222.2	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 553 MEXICO: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	25.9	31.2	37.0	43.5	50.6	57.3	17.2%
SMEs	15.5	19.0	22.9	27.4	32.4	37.2	19.2%
Total	41.4	50.2	59.9	70.9	83.0	94.5	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 554 MEXICO: DDOS PROTECTION AND MITIGATION MARKET,
BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	65.8	75.4	87.3	100.8	116.5	129.3	14.5%
SMEs	43.5	50.7	59.7	70.0	82.3	92.9	16.4%
Total	109.3	126.0	147.0	170.8	198.8	222.2	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 555 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL,
2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	8.2	10.1	12.3	14.9	17.8	20.6	20.3%
Government & Defense	5.9	7.0	8.1	9.4	10.8	12.0	15.3%
Healthcare	3.3	4.0	4.8	5.7	6.7	7.7	18.2%
IT & ITeS	3.0	3.7	4.5	5.4	6.4	7.3	19.6%
Telecommunications	4.3	5.2	6.1	7.1	8.3	9.3	16.6%
Manufacturing	2.1	2.5	3.0	3.5	4.0	4.5	16.0%
Energy & Utilities	5.5	6.7	8.1	9.6	11.3	13.0	18.8%
Retail	4.6	5.6	6.6	7.8	9.1	10.4	17.7%
Education	1.9	2.3	2.7	3.1	3.7	4.1	17.2%
Other Verticals	2.6	3.1	3.7	4.3	5.0	5.7	16.7%
Total	41.4	50.2	59.9	70.9	83.0	94.5	18.0%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 556 MEXICO: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	24.3	28.5	33.8	40.0	47.4	53.9	17.3%
Government & Defense	13.5	15.2	17.3	19.5	22.1	24.1	12.3%
Healthcare	8.9	10.3	12.0	14.0	16.3	18.3	15.5%
IT & ITeS	8.6	10.0	11.9	14.0	16.5	18.6	16.7%
Telecommunications	10.6	12.1	14.0	16.0	18.4	20.4	13.9%
Manufacturing	5.1	5.7	6.6	7.5	8.5	9.4	13.1%
Energy & Utilities	15.1	17.6	20.6	24.1	28.3	31.8	16.0%
Retail	12.0	13.8	16.0	18.6	21.6	24.1	15.0%
Education	4.7	5.4	6.3	7.3	8.4	9.3	14.4%
Other Verticals	6.5	7.4	8.5	9.8	11.2	12.4	13.9%
Total	109.3	126.0	147.0	170.8	198.8	222.2	15.2%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

15.6.3 REST OF LATIN AMERICA

The rest of Latin America includes Argentina, Peru, Chile, and the remaining countries. The DDoS protection and mitigation market in these countries is evolving in response to rising cyber threats and increasing awareness of cybersecurity needs. Argentina has experienced a surge in DDoS attacks, prompting organizations in the country to invest more in robust cybersecurity solutions, driven by factors such as the increasing digitalization of services and the growth of the ecommerce sector. Chile is considered one of the most advanced countries in Latin America in terms of cybersecurity infrastructure. The government is strongly promoting digital transformation, and with high internet penetration, the country faces increasing vulnerability to cyber threats. Peru, while still developing its DDoS protection market, faces a growing number of cyber incidents targeting critical infrastructure, prompting businesses to enhance their cybersecurity measures. However, challenges remain, including a lack of awareness among many businesses regarding the risks of DDoS attacks and budget constraints for smaller companies. Additionally, as businesses and organizations in these countries become more digital, they are becoming increasingly vulnerable to DDoS attacks, which can disrupt operations, damage their reputation, and lead to financial losses.

TABLE 557 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2020–2025 (USD MILLION)

Offering	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Solution	23.6	28.1	33.4	39.4	45.9	52.0	17.1%
Services	7.2	8.7	10.4	12.4	14.7	16.9	18.6%
Total	30.8	36.8	43.9	51.8	60.6	68.9	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 558 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY OFFERING, 2026–2031 (USD MILLION)

Offering	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Solution	59.3	67.3	77.3	88.5	101.5	111.2	13.4%
Services	19.5	22.4	26.1	30.2	35.1	38.9	14.8%
Total	78.8	89.7	103.4	118.7	136.5	150.1	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 559 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2020–2025 (USD MILLION)

Solution	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Hardware	10.0	11.9	14.0	16.4	19.1	21.5	16.5%
Software/Platforms	13.6	16.3	19.4	22.9	26.8	30.5	17.5%
Total	23.6	28.1	33.4	39.4	45.9	52.0	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 560 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION, 2026–2031 (USD MILLION)

Solution	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Hardware	24.4	27.6	31.6	35.9	41.0	44.7	12.9%
Software/Platforms	34.9	39.7	45.8	52.6	60.5	66.5	13.8%
Total	59.3	67.3	77.3	88.5	101.5	111.2	13.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 561 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2020–2025 (USD MILLION)

Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Professional Services	4.2	5.0	6.0	7.1	8.4	9.6	18.3%
Managed Services	3.0	3.7	4.4	5.3	6.3	7.2	19.1%
Total	7.2	8.7	10.4	12.4	14.7	16.9	18.6%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 562 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SERVICE, 2026–2031 (USD MILLION)

Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Professional Services	11.1	12.7	14.8	17.1	19.8	21.9	14.5%
Managed Services	8.4	9.7	11.3	13.1	15.3	17.0	15.2%
Total	19.5	22.4	26.1	30.2	35.1	38.9	14.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 563 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2020–2025 (USD MILLION)

Professional Service	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Design & Implementation	1.2	1.4	1.6	1.9	2.3	2.6	17.7%
Consulting & Advisory	1.0	1.2	1.5	1.8	2.1	2.5	19.8%
Training & Education	0.7	0.8	1.0	1.2	1.4	1.6	19.0%
Support & Maintenance	0.8	1.0	1.1	1.3	1.6	1.8	16.8%
DDoS Testing & Validation	0.5	0.6	0.7	0.9	1.0	1.1	18.3%
Total	4.2	5.0	6.0	7.1	8.4	9.6	18.3%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 564 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY PROFESSIONAL SERVICE, 2026–2031 (USD MILLION)

Professional Service	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Design & Implementation	3.0	3.4	3.9	4.5	5.2	5.7	13.9%
Consulting & Advisory	2.9	3.4	3.9	4.6	5.4	6.0	15.8%
Training & Education	1.9	2.2	2.5	3.0	3.5	3.8	15.2%
Support & Maintenance	2.0	2.3	2.6	3.0	3.4	3.7	12.9%
DDoS Testing & Validation	1.3	1.5	1.8	2.0	2.4	2.6	14.5%
Total	11.1	12.7	14.8	17.1	19.8	21.9	14.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 565 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2020–2025 (USD MILLION)

Solution Type	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network Traffic Analyzers	7.7	9.1	10.9	12.8	15.0	17.0	17.3%
Threat Mitigation Systems	6.6	7.8	9.3	10.9	12.7	14.4	16.8%
Botnet Detection & Management	5.1	6.1	7.3	8.6	10.1	11.6	18.0%
Other Solution Types	4.3	5.1	6.0	7.0	8.1	9.1	16.0%
Total	23.6	28.1	33.4	39.4	45.9	52.0	17.1%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 566 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY SOLUTION TYPE, 2026–2031 (USD MILLION)

Solution Type	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network Traffic Analyzers	19.4	22.1	25.5	29.2	33.6	36.9	13.6%
Threat Mitigation Systems	16.3	18.5	21.2	24.2	27.6	30.2	13.1%
Botnet Detection & Management	13.3	15.2	17.6	20.3	23.4	25.9	14.3%
Other Solution Types	10.3	11.5	13.1	14.9	16.9	18.3	12.3%
Total	59.3	67.3	77.3	88.5	101.5	111.2	13.4%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 567 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2020–2025 (USD MILLION)

Application Area	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Network & IP Infrastructure	10.8	12.9	15.4	18.2	21.3	24.3	17.7%
Web Applications & APIs	9.8	11.8	14.3	17.1	20.3	23.3	19.0%
DNS Infrastructure	10.3	12.1	14.2	16.5	19.0	21.3	15.7%
Total	30.8	36.8	43.9	51.8	60.6	68.9	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 568 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY APPLICATION AREA, 2026–2031 (USD MILLION)

Application Area	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Network & IP Infrastructure	27.8	31.7	36.6	42.1	48.6	53.5	14.0%
Web Applications & APIs	27.0	31.1	36.3	42.2	49.1	54.6	15.1%
DNS Infrastructure	24.0	26.9	30.5	34.4	38.9	42.1	11.9%
Total	78.8	89.7	103.4	118.7	136.5	150.1	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 569 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2020–2025 (USD MILLION)

Deployment Mode	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
On-premises	9.7	11.6	13.7	16.1	18.7	21.1	16.7%
Cloud	18.8	22.5	26.9	31.9	37.4	42.7	17.8%
Hybrid	2.3	2.7	3.2	3.8	4.5	5.1	17.5%
Total	30.8	36.8	43.9	51.8	60.6	68.9	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 570 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY DEPLOYMENT MODE, 2026–2031 (USD MILLION)

Deployment Mode	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
On-premises	24.0	27.2	31.1	35.5	40.6	44.4	13.1%
Cloud	49.0	56.0	64.7	74.5	85.9	95.5	14.3%
Hybrid	5.8	6.6	7.6	8.7	10.0	10.3	12.1%
Total	78.8	89.7	103.4	118.7	136.5	150.1	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 571 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2020–2025 (USD MILLION)

Organization Size	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
Large Enterprises	19.3	22.9	27.1	31.8	37.0	41.8	16.7%
SMEs	11.5	13.9	16.8	20.0	23.6	27.2	18.7%
Total	30.8	36.8	43.9	51.8	60.6	68.9	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 572 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY ORGANIZATION SIZE, 2026–2031 (USD MILLION)

Organization Size	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
Large Enterprises	47.4	53.7	61.4	70.0	80.0	87.4	13.0%
SMEs	31.4	36.1	42.0	48.7	56.5	62.8	14.9%
Total	78.8	89.7	103.4	118.7	136.5	150.1	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 573 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2020–2025 (USD MILLION)

Vertical	2020	2021	2022	2023	2024	2025	CAGR (2020–2025)
BFSI	6.1	7.4	9.0	10.9	13.0	15.0	19.8%
Government & Defense	4.4	5.1	5.9	6.9	7.9	8.7	14.8%
Healthcare	2.5	3.0	3.5	4.2	4.9	5.6	17.7%
IT & ITeS	2.2	2.7	3.3	3.9	4.6	5.4	19.1%
Telecommunications	3.2	3.8	4.5	5.2	6.0	6.8	16.1%
Manufacturing	1.6	1.9	2.2	2.5	2.9	3.2	15.5%
Energy & Utilities	4.1	4.9	5.9	7.0	8.3	9.5	18.3%
Retail	3.4	4.1	4.8	5.7	6.7	7.6	17.2%
Education	1.4	1.7	2.0	2.3	2.7	3.0	16.7%
Other Verticals	2.0	2.3	2.7	3.2	3.7	4.1	16.2%
Total	30.8	36.8	43.9	51.8	60.6	68.9	17.5%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 574 **REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION MARKET, BY VERTICAL, 2026–2031 (USD MILLION)**

Vertical	2026	2027	2028	2029	2030	2031	CAGR (2026–2031)
BFSI	17.5	20.3	23.8	27.8	32.5	36.4	15.8%
Government & Defense	9.7	10.8	12.1	13.6	15.2	16.3	10.8%
Healthcare	6.4	7.3	8.5	9.7	11.2	12.4	14.0%
IT & ITeS	6.2	7.2	8.3	9.7	11.3	12.6	15.2%
Telecommunications	7.7	8.6	9.8	11.1	12.7	13.8	12.4%
Manufacturing	3.6	4.1	4.6	5.2	5.9	6.3	11.6%
Energy & Utilities	10.9	12.5	14.5	16.8	19.4	21.5	14.5%
Retail	8.6	9.8	11.3	12.9	14.9	16.3	13.6%
Education	3.4	3.9	4.4	5.0	5.8	6.3	13.0%
Other Verticals	4.7	5.3	6.0	6.8	7.7	8.4	12.4%
Total	78.8	89.7	103.4	118.7	136.5	150.1	13.8%

Source: Secondary Research, Interviews with Experts, and MarketsandMarkets Analysis

16 COMPETITIVE LANDSCAPE

16.1 INTRODUCTION

The competitive landscape provides an overview of the prevailing competitive scenario in the DDoS protection and mitigation market. It includes a trend analysis based on the revenue of various business segments of key market players. Additionally, it benchmarks the growth strategies adopted by key players. This section also comprehensively analyzes developments, such as contracts, partnerships, expansions, agreements, and product launches.

16.2 KEY PLAYER STRATEGIES/RIGHT TO WIN, 2022–2025

Key players have adopted organic and inorganic growth strategies to expand their global presence, helping them increase market share. Major market players generate significant revenues from North America, followed by Europe and Asia Pacific. A few key player strategies are as follows:

TABLE 575 DDOS PROTECTION AND MITIGATION MARKET: OVERVIEW OF STRATEGIES DEPLOYED BY KEY PLAYERS

KEY PLAYER	PRODUCT TYPE	STRATEGIC DEVELOPMENT/ PARTNERSHIP	MERGER & ACQUISITION/ PRODUCT LAUNCH	REGION
NETSCOUT (US)	Arbor Sightline Network Visibility Software	NETSCOUT collaborated with NTT Communications on Threat Intelligence and DDoS Attack Resilience Research. The aim was to detect and mitigate large DDoS attacks, implement defenses against application attacks, and identify new attacks before they became an issue.	NETSCOUT announced that it expanded its Arbor Cloud DDoS attack mitigation network to 16 scrubbing centers worldwide with the recent addition of a new Toronto facility. This network offers ISPs and enterprise customers more than 15 terabits per second (Tbps) of dedicated attack capacity.	The US contributes more than 55% to the company's revenue.
Akamai Technologies (US)	Prolexic	Akamai Technologies announced a global partnership with Corero Network Security, a specialist in distributed denial-of-service (DDoS) protection solutions. Akamai offered Corero's on-premises DDoS protection to extend Akamai Prolexic.	Akamai Technologies announced the launch of its Prolexic Network Cloud Firewall. This new Akamai Prolexic capability lets customers define and manage their own access control lists (ACLs) while giving them greater flexibility to secure their network edge.	The US contributes about 51% to the company's revenue.
Radware (Israel)	DefensePro X	Radware signed a managed security service provider partnership with Lightpath, an all-fiber, infrastructure-based connectivity provider. Based on the agreement, Lightpath was leveraging Radware's AI-powered	Radware introduced a new Cloud Web DDoS Protection solution, designed to minimize the growing gap between standard DDoS mitigation and an emerging generation of more aggressive, layer 7 (L7) HTTPS Flood attacks, also known as Web DDoS Tsunami attacks. Radware's advanced	The Americas contribute about 38% to the company's revenue.

		DefensePro DDoS Protection to offer customers a DDoS scrubbing service designed to combat today's increasingly complex threats.	solution could combat these encrypted, high-volume, multi-vector threats that evade standard web application firewalls (WAFs) and network-based DDoS tools, essentially rendering them ineffective.	
Cloudflare (US)	Cloudflare DDoS Protection, Cloudflare Spectrum, Magic Transit	Cloudflare and Booz Allen Hamilton established a collaboration to provide Under Attack as a Service (UAaaS), enabling Booz Allen's commercial clients facing active cyberattacks to receive expedited access to Cloudflare's incident response capabilities and 30-day Rapid Response DDoS Mitigation service, including continuous monitoring and protection.	Cloudflare introduced Programmable Flow Protection for Magic Transit Enterprise customers. The capability enabled customers to implement and deploy custom, stateful DDoS mitigation logic across Cloudflare's global network, specifically supporting protection for custom and proprietary UDP-based protocols. The capability was made available in beta to eligible Magic Transit Enterprise customers.	Asia Pacific contributes more than 40% of the overall revenue
Nexusguard (Singapore)	Nexusguard DDoS Protection	Nexusguard collaborated with Eastern Communications, a telecom provider in the Philippines. This strategic collaboration combines Nexusguard's cloud-based DDoS protection with Eastern Communications' robust infrastructure to provide scalable cybersecurity solutions. The partnership aims to safeguard Philippine enterprises and government agencies through the "DDoS-Protected Eastern IDS," ensuring reliable connectivity and business continuity.	NA	Asia Pacific contributes more than 40% of the overall revenue

Source: Annual Reports, Press Releases, and MarketsandMarkets Analysis

Strategies of various DDoS protection and mitigation vendors have been assessed, along with the strategies they have adopted:

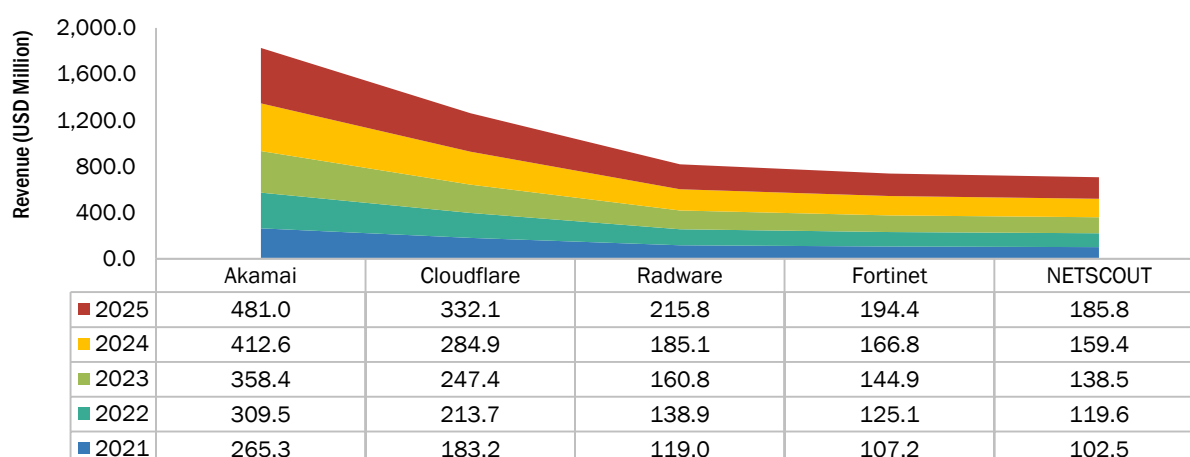
- **Product Type:** Key players in the DDoS protection and mitigation market offer a comprehensive product portfolio that includes DDoS protection and mitigation hardware solutions, software solutions, and services for end users.
- **Regional Focus:** Players in this market have a well-diversified presence across the globe.
- **Partnerships:** Players primarily deploy inorganic development strategies; they leverage partnerships focused on technology enhancements to grow their revenue.

- **Acquisitions:** Players in the market have been relatively less active on the M&A front or investing in startups.

16.3 REVENUE ANALYSIS, 2021–2025

Players in the DDoS protection and mitigation market were identified through secondary research. In terms of value, each market player's share was inferred from annual reports, presentations, and secondary research sources. Primary research interviews were conducted with key opinion leaders, such as CEOs, directors, industry experts, and other executives, to validate revenues and market shares.

FIGURE 42 DDoS PROTECTION AND MITIGATION MARKET: REVENUE ANALYSIS OF FIVE KEY PLAYERS, 2021–2025



Source: Company Websites and Annual Reports

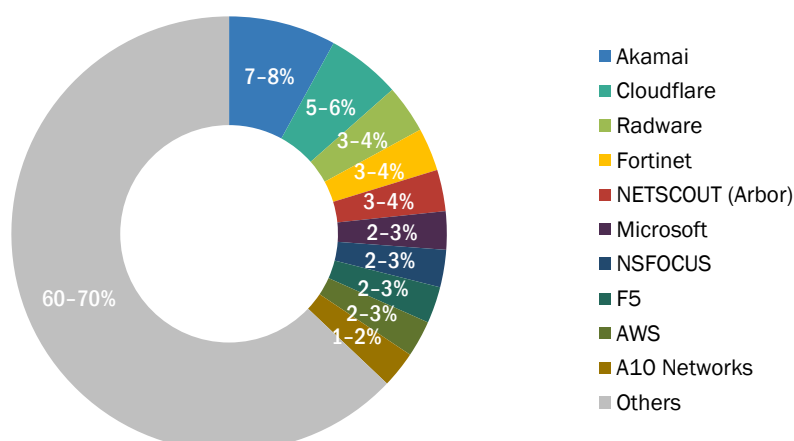
The revenue analysis of five key players in the DDoS protection and mitigation market from 2020 to 2025 highlights sustained growth and strengthening market positions among leading vendors. Akamai remains a prominent player, supported by its comprehensive DDoS protection portfolio, global infrastructure, and strong enterprise presence. Cloudflare demonstrates strong market momentum, driven by its cloud-native security platform, globally distributed network, and growing adoption of DDoS-as-a-Service solutions. Radware maintains a strong position through its advanced behavioral detection, automated mitigation, and multi-layer DDoS protection capabilities. Fortinet benefits from its established cybersecurity portfolio and purpose-built DDoS protection solutions, while NETSCOUT maintains a significant presence through its Arbor DDoS protection portfolio, network visibility, and threat intelligence capabilities. Overall, the performance of these key players reflects increasing demand for scalable, automated, and resilient DDoS protection solutions as organizations face increasingly frequent and sophisticated cyber threats.

16.4 MARKET SHARE ANALYSIS, 2025

Key players in the DDoS protection and mitigation market were identified through secondary research, and their market share, in terms of value, was inferred from their annual reports, presentations, and other secondary sources. Primary research interviews were conducted with key opinion leaders in the industry, such as CEOs, directors, industry experts, and other executives, to validate revenue and market share.

The following table illustrates the market share of the top five players in the DDoS protection and mitigation market in 2025.

FIGURE 43 SHARE ANALYSIS OF LEADING COMPANIES IN DDOS PROTECTION AND MITIGATION MARKET, 2025



Source: Annual Reports, Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

TABLE 576 DDOS PROTECTION AND MITIGATION MARKET: DEGREE OF COMPETITION, 2025

DEGREE OF COMPETITION	COMPETITIVE
Total Market Share of Top 5 players	30-40%
Akamai	7%-8%
Cloudflare	5%-6%
Radware	3%-4%
Fortinet	3%-4%
NETSCOUT (Arbor)	3%-4%
Microsoft	2%-3%
NSFOCUS	2%-3%
F5	2%-3%
AWS	2%-3%
A10 Networks	1%-2%
Other Players	60-70%

THE DEGREE OF COMPETITION IS DEFINED AS BELOW:

- Fragmented: When the top five players have a total market share of <25%.
- Competitive: When the top five players have 25-50% market share.
- Consolidated: When the top five players have a total market share of >50%.

Note: The market share of the above companies is calculated based on the relevant segment revenues generated by companies.

Source: Annual Reports, Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

The market is fragmented, with the top five players collectively accounting for less than 25% of the global DDoS protection and mitigation market. The market includes many established vendors, specialized providers, and emerging players, resulting in a highly dispersed competitive landscape. While leading players such as Akamai, Cloudflare, Radware, Fortinet, and NETSCOUT maintain strong positions through their extensive capabilities, global presence, and established customer bases, their combined market share remains relatively limited. This fragmented structure creates opportunities for both established and emerging vendors to expand through differentiated solutions, cloud-based protection, automated mitigation, and advanced threat detection.

AKAMAI

Akamai Technologies is a global provider of cloud, cybersecurity, content delivery, and edge computing solutions. Its security portfolio includes application and API protection, bot management, web application security, DNS security, and DDoS protection. In the DDoS protection and mitigation market, Akamai provides solutions such as Prolexic, which protects internet-facing infrastructure against large-scale and sophisticated DDoS attacks, along with application and DNS security capabilities. Its DDoS protection portfolio supports cloud, on-premises, and hybrid environments, enabling organizations to protect applications, infrastructure, and critical services from network- and application-layer attacks.

Akamai's DDoS protection capabilities are supported by dedicated infrastructure and a globally distributed edge network, allowing it to mitigate attacks before they reach customers' applications and internal infrastructure. Its solutions are designed to maintain business continuity, protect network resources, and provide visibility and control over malicious traffic. Akamai serves organizations across financial services, healthcare, retail, government, media, gaming, and other industries that require scalable, resilient cybersecurity solutions.

NETSCOUT

NETSCOUT is a leading provider of network and application performance management, cybersecurity, and DDoS protection solutions. Its portfolio includes solutions for network visibility, service assurance, security, and business assurance across enterprises, service providers, government, and other industry environments. In the DDoS protection and mitigation market, NETSCOUT offers the Arbor security portfolio, including Arbor Edge Defense (AED), Arbor Cloud, and other Arbor DDoS protection solutions. These solutions automatically detect and mitigate volumetric, network-layer, and application-layer attacks, supported by NETSCOUT's global visibility and threat intelligence capabilities. Arbor Edge Defense provides on-premises protection against DDoS attacks and other threats before they reach stateful network security devices, while Arbor Cloud provides cloud-based DDoS mitigation capabilities.

NETSCOUT's DDoS protection capabilities are supported by its extensive network visibility and ATLAS threat intelligence, enabling organizations to identify attack sources and emerging threats. Its solutions are designed to reduce the impact of DDoS attacks, protect network infrastructure and applications, and maintain service availability. The company serves telecommunications providers, enterprises, government organizations, and other large-scale network environments requiring continuous monitoring and automated threat mitigation.

CLOUDFLARE

Cloudflare is a global connectivity, cloud, performance, and cybersecurity provider offering solutions for websites, applications, networks, and enterprise infrastructure. Its security portfolio includes DDoS protection, web application firewall, bot management, API security, network firewall, and Zero Trust solutions. In the DDoS protection and mitigation market, Cloudflare provides always-on protection across network and application layers, including Layer 3, Layer 4, and Layer 7 attacks. Its portfolio includes DDoS protection for websites and applications, Magic Transit for network infrastructure, and Spectrum for TCP/UDP applications.

Cloudflare's DDoS protection runs on its globally distributed network and autonomous, edge-based detection and mitigation systems. The platform automatically detects and mitigates attacks while allowing legitimate traffic to continue reaching protected applications and services. Its solutions use managed rulesets, adaptive protection, advanced TCP and DNS protection, and programmable traffic controls to address evolving attack techniques. Cloudflare serves enterprises, public-sector organizations, developers, and businesses across a broad range of industries seeking scalable, cloud-based security and network resilience.

RADWARE

Radware provides application delivery, cybersecurity, and DDoS protection solutions designed to protect digital services and applications from increasingly sophisticated cyber threats. Its DDoS protection portfolio provides multi-layered protection across on-premises, cloud, and hybrid environments. Radware uses behavior-based detection and automated mitigation technologies to identify and block advanced DDoS attacks, including volumetric, DNS, Web, IoT botnet, and ransom DDoS attacks. Its portfolio also protects web and API applications against sophisticated HTTP and application-layer DDoS attacks.

Radware's DDoS protection capabilities combine behavioral algorithms, real-time threat intelligence, and automated mitigation to distinguish legitimate traffic from malicious activity. Its cloud DDoS protection service is supported by a global network of scrubbing centers designed to absorb and mitigate large-scale attacks while maintaining service availability and user experience. The company serves enterprises, telecommunications providers, financial institutions, government organizations, and other industries requiring continuous availability of digital services.

FORTINET

Fortinet is a global cybersecurity provider offering network security, cloud security, secure networking, and security operations solutions. Its cybersecurity portfolio includes firewalls, intrusion prevention, secure access, endpoint security, security operations, and DDoS protection. In the DDoS protection and mitigation market, Fortinet offers FortiDDoS, a purpose-built, inline DDoS protection solution designed to protect networks, applications, and services from attacks that overwhelm network resources with malicious traffic. FortiDDoS provides automated detection and mitigation of multiple simultaneous attacks without requiring manual intervention.

FortiDDoS uses extensive traffic monitoring and packet inspection to identify abnormal traffic patterns and mitigate attacks before they cause service disruption. The solution monitors a large number of traffic parameters and performs mitigation in real time, supporting protection against both known and emerging DDoS attack techniques. Fortinet serves enterprises, service providers, government organizations, and other industries requiring high-performance network security and resilient infrastructure protection.

16.5 BRAND COMPARISON

FIGURE 44 DDOS PROTECTION AND MITIGATION MARKET: COMPARISON OF VENDOR BRANDS

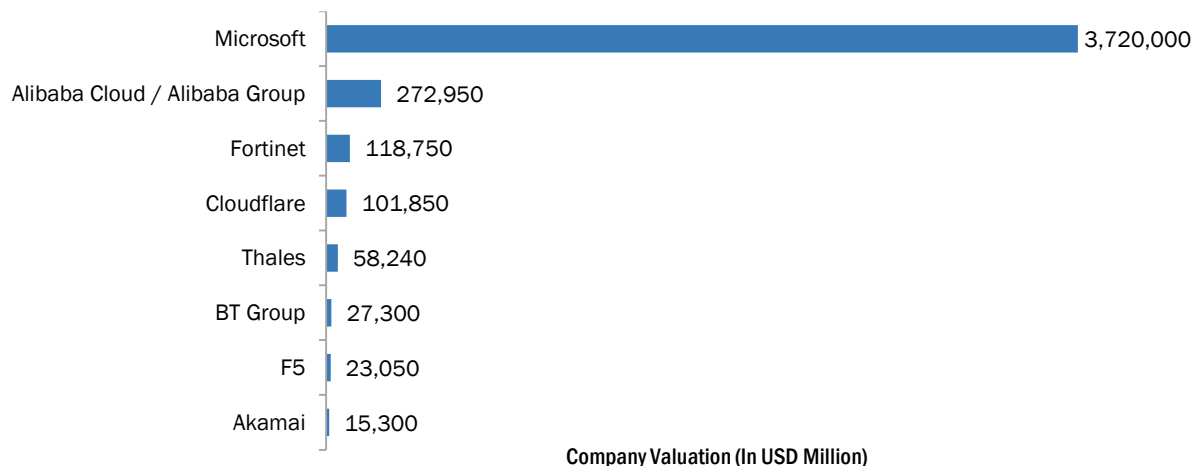
PARAMETER					NETSCOUT
PRODUCT PORTFOLIO	●	●	●	●	●
INNOVATION READINESS	●	●	●	●	●
CUSTOMER FEEDBACK/ RATING	●	●	●	●	●
Geographic Presence	Global presence with extensive coverage across North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa	Extensive global presence supported by a large distributed network spanning major markets worldwide	Broad global presence across North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America	Strong global presence across North America, Europe, Asia Pacific, Latin America, and the Middle East & Africa	Strong presence across North America, Europe, Asia Pacific, and other major global markets
STRENGTHS	Dedicated DDoS infrastructure, multi-layer protection, cloud, on-premises and hybrid deployment, strong threat intelligence, and 24/7 mitigation capabilities	Highly scalable cloud-native DDoS protection, extensive global network, automated mitigation, and strong L3/L4/L7 protection capabilities	Advanced behavioral detection, automated mitigation, multi-layer protection, strong application and API DDoS defense, and flexible cloud, on-premises, and hybrid deployment	Purpose-built DDoS protection, autonomous mitigation, machine-learning-based anomaly detection, granular traffic monitoring, and rapid mitigation	Strong network visibility, DDoS-focused expertise, automated detection and mitigation, extensive threat intelligence, and strong service-provider capabilities
WEAKNESSES	Premium positioning and relatively complex deployment for organizations requiring highly customized protection architectures	Enterprise-oriented network protection capabilities can involve greater configuration complexity; some advanced capabilities are available primarily through enterprise offerings	Strong enterprise focus and specialized architecture may result in higher deployment and operational complexity	Greater emphasis on purpose-built network protection and appliance-based deployments may provide less breadth than cloud-native DDoS specialists	More focused on network and service-provider environments, with comparatively narrower application-security breadth than diversified cloud security platforms
 EXCELLENT  GOOD  FAIR  POOR					

Source: Annual Reports, Press Releases, and MarketsandMarkets Analysis

16.6 COMPANY VALUATION AND FINANCIAL METRICS, 2025

16.6.1 COMPANY VALUATION

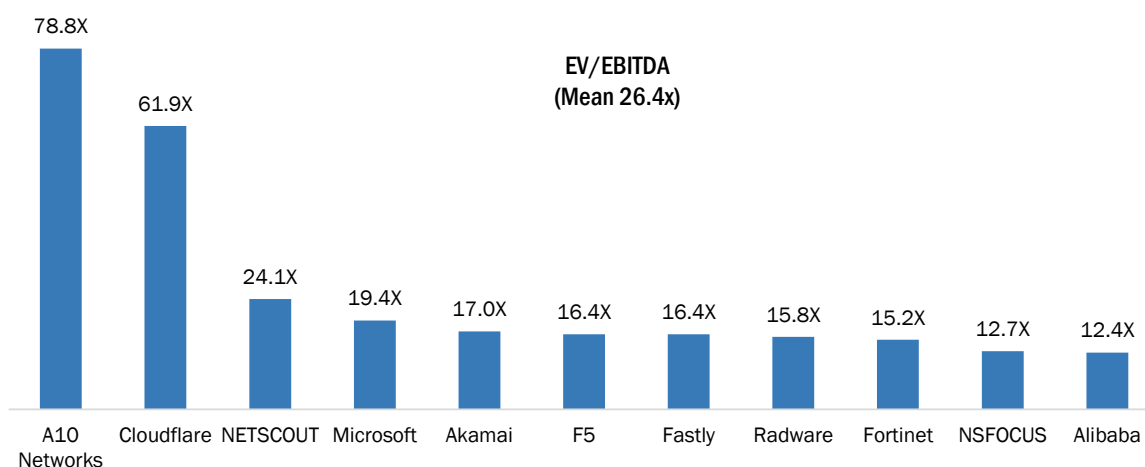
FIGURE 45 COMPANY VALUATION, 2025 (USD BILLION)



Source: Dealroom.co

16.6.2 FINANCIAL METRICS

FIGURE 46 FINANCIAL METRICS, 2025



Note: EV/EBITDA for all companies as of October 2025.

Source: Finbox.com

16.7 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2025

The company evaluation matrix provides information about the major players offering DDoS protection and mitigation solutions and services. It also outlines the findings and analysis of how well each market vendor performs within the predefined competitive leadership mapping criteria. The vendor evaluations are based on two broad categories: product footprint and market share/rank. Each category carries various criteria based on which vendors have been evaluated. The evaluation criteria considered under the product footprint include the breadth and depth of product offerings, product features and functionality, and estimated product revenue.

Based on a questionnaire, extensive secondary and primary research was conducted to gather critical information about the vendor's strength of product portfolio and market share/rank. A scale of 0–10 was formulated for each question, after which each criterion for every vendor was scored based on the collected information. After data gathering and verification, the scores and weightage for shortlisted vendors against each parameter were finalized. A comparison scorecard was prepared after evaluating all vendors, and they were then placed into four categories based on their performance in each criterion. These are Stars, Emerging Leaders, Pervasive Players, and Participants.

- Stars (companies with large market share, wider application, and geographical use cases and footprint).
- Emerging leaders (companies with large market share, low application, and geographical penetration).
- Pervasive players are companies with small market share, high application, and regional availability). These players' products are available for multiple application/end-use industries and in most regions worldwide.
- Participants have a small footprint in the market at a global level but may have a strong presence in one or more regions and/or customer segments.

16.7.1 STARS

Star players are the leading key players in the market, with a wide product portfolio, strong market presence, and effective business strategies. Their wide product portfolio enables them to serve most regions worldwide. Star players primarily focus on acquiring the leading market position through their strong financial capabilities and well-established brand equity. Akamai, Cloudflare, Radware, Fortinet, NETSCOUT, Microsoft, AWS, NSFOCUS, F5, NexuGuard, A10 Networks, Corero are the vendors in this category.

16.7.2 EMERGING LEADERS

The key players involved in the development and innovation of new products in the DDoS protection and mitigation market have been included in this quadrant. Emerging leaders demonstrate substantial product innovations as compared with their competitors. These players have a broad product portfolio and robust potential to build strong business strategies to expand their businesses and stay on par with the star players. However, they have not adopted effective growth strategies for their overall business. Thales (Imperva), Alibaba Cloud, Fastly, Link11 fall under this category.

16.7.3 PERVASIVE PLAYERS

Pervasive players are well-established companies with effective business strategies. They offer innovative solutions, services, and hardware portfolios and have an extensive network of channel partners and resellers to increase the deployment of their solutions across a multitude of vertical markets. They generally focus on a specific type of technology related to the product. Huawei, BT, Lumen Technologies under this category.

16.7.4 PARTICIPANTS

Participants are companies that offer niche products and have gradually started gaining a position in the market. Unlike other established players, they lack effective business strategies. These players are mostly new entrants in the market and require more time to gain significant traction. Allot, Stratacore, Sucuri (GoDaddy) are placed in this quadrant.

FIGURE 47 DDOS PROTECTION AND MITIGATION MARKET:
COMPANY EVALUATION MATRIX (KEY PLAYERS), 2025



Source: Press Releases, Interviews with Experts, and MarketsandMarkets Analysis

16.7.5 COMPANY FOOTPRINT: KEY PLAYERS, 2025

16.7.5.1 Company footprint

FIGURE 48 DDOS PROTECTION AND MITIGATION MARKET: COMPANY FOOTPRINT, 2025

COMPANY NAME	REGIONAL FOOTPRINT	OFFERING FOOTPRINT	VERTICAL FOOTPRINT	OVERALL FOOTPRINT
NETSCOUT	○○○○	○○○○	○○○	○○○○
Akamai	○○○○	○○○○	○○○○	○○○
Radware	○○○○	○○○○	○○○	○○○○
Huawei	○○○○	○○○○	○○○	○○○
Fortinet	○○○○	○○○○	○○○○	○○○○
Nexusguard	○○○○	○○○○	○○○	○○○
Link11	○○○○	○○○○	○○○	○○○○
Thales (Imperva)	○○○○	○○○○	○○○○	○○○
NSFocus	○○○○	○○○○	○○○○	○○○○
Cloudflare	○○○○	○○○○	○○○○	○○○
BT	○○○○	○○○○	○○○○	○○○○
A10 Networks	○○○○	○○○○	○○○	○○○○
F5	○○○○	○○○	○○○○	○○○
Fastly	○○○	○○○	○○○	○○○
Corero	○○○○	○○○○	○○○○	○○○○
Microsoft	○○○○	○○○○	○○○○	○○○○
AWS	○○○○	○○○○	○○○○	○○○○
Alibaba Cloud	○○○○	○○○○	○○○○	○○○○
Sucuri (GoDaddy)	○○○	○○○○	○○○	○○○
Allot	○○	○○○○	○○○○	○○○
Stratacore	○○○	○○○○	○○○○	○○○
Lumen Technologies	○○○	○○○○	○○○○	○○○
RATING : ○○○○ EXCELLENT ○○○ GOOD ○○ AVERAGE ○ BELOW AVERAGE NOT APPLICABLE				

Source: Company Websites and MarketsandMarkets Analysis

16.7.5.2 Regional footprint

TABLE 577 DDOS PROTECTION AND MITIGATION MARKET: REGIONAL FOOTPRINT, 2025

COMPANY	NORTH AMERICA	EUROPE	ASIA PACIFIC	MIDDLE EAST & AFRICA	LATIN AMERICA	REGION FOOTPRINT
Microsoft	Y	Y	Y	Y	Y	4.00
AWS	Y	Y	Y	Y	Y	4.00
Alibaba Cloud	Y	Y	Y	Y	Y	4.00
NETSCOUT	Y	Y	Y	Y	Y	4.00
Akamai	Y	Y	Y	Y	Y	4.00
Radware	Y	Y	Y	Y	Y	4.00
Huawei	Y	Y	Y	Y	Y	4.00
Fortinet	Y	Y	Y	Y	Y	4.00
Nexusguard	Y	Y	Y	Y	Y	4.00
Link11	Y	Y	Y	Y	Y	4.00
Thales (Imperva)	Y	Y	Y	Y	Y	4.00
NSFOCUS	Y	Y	Y	Y	Y	4.00
Cloudflare	Y	Y	Y	Y	Y	4.00
BT	Y	Y	Y	Y	Y	4.00
A10 Networks	Y	Y	Y	Y	Y	4.00
F5	Y	Y	Y	Y	Y	4.00
Fastly	Y	N	Y	N	N	1.60
Corero	Y	Y	Y	Y	Y	4.00
Allot	Y	N	N	N	N	0.80
StrataCore	Y	Y	Y	N	N	2.40
Sucuri (GoDaddy)	Y	Y	Y	Y	Y	4.00
Lumen Technologies	Y	Y	Y	Y	N	3.20

Source: Company Websites and MarketsandMarkets Analysis

16.7.5.3 Offering footprint

TABLE 578 DDOS PROTECTION AND MITIGATION MARKET: OFFERING FOOTPRINT, 2025

COMPANY	HARDWARE SOLUTIONS	SOFTWARE SOLUTIONS	SERVICES	OFFERING FOOTPRINT
Microsoft	N	Y	Y	2.7
AWS	N	Y	Y	2.7
Alibaba Cloud	N	Y	Y	2.7
NETSCOUT	N	Y	Y	2.7
Akamai	N	Y	N	1.3
Radware	N	Y	Y	2.7
Huawei Technology	Y	N	N	1.3
Fortinet	Y	Y	N	2.7
Nexusguard	Y	Y	Y	4.0
Link11	N	Y	Y	2.7
Thales (Imperva)	N	Y	N	1.3
NSFOCUS	Y	Y	Y	4.0
Cloudflare	N	Y	Y	2.7
BT	N	Y	N	1.3
A10 Networks	N	Y	Y	2.7
F5	N	N	Y	1.3
Fastly	N	Y	Y	2.7
Corero	Y	Y	Y	4.0
Allot	N	Y	N	1.3
StrataCore	N	Y	N	1.3
Sucuri (GoDaddy)	N	Y	Y	2.7
Lumen Technologies	N	Y	N	1.3

Source: Company Websites and MarketsandMarkets Analysis

16.7.5.4 Vertical footprint

TABLE 579 DDOS PROTECTION AND MITIGATION MARKET: VERTICAL FOOTPRINT, 2025

COMPANY	BFSI	HEALTHCARE	IT & ITES	VERTICAL FOOTPRINT
Microsoft	Y	Y	Y	4.00
AWS	Y	Y	Y	4.00
Alibaba Cloud	Y	Y	Y	4.00
NETSCOUT	Y	Y	Y	4.00
Akamai	Y	Y	Y	4.00
Radware	Y	Y	Y	4.00
Huawei Technology	Y	Y	Y	4.00
Fortinet	Y	Y	Y	4.00
Nexusguard	Y	Y	Y	4.00
Link11	Y	N	N	1.33
Thales (Imperva)	Y	Y	Y	4.00
NSFOCUS	Y	Y	Y	4.00
Cloudflare	Y	Y	Y	4.00
BT	Y	Y	Y	4.00
A10 Networks	Y	Y	Y	4.00
F5	Y	N	Y	2.67
Fastly	Y	N	N	1.33
Corero	Y	Y	Y	4.00
Allot	N	N	Y	1.33
StrataCore	Y	N	Y	2.67
Sucuri (GoDaddy)	Y	Y	N	2.67
Lumen Technologies	Y	Y	Y	4.00

Source: Company Websites and MarketsandMarkets Analysis

16.8 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2025

The Company Evaluation Matrix for Startups and SMEs identifies and profiles companies with commercial blockchain offerings globally, regardless of their development stage (seed, early-stage, mid-stage, etc.). Companies are classified into startups and SMEs based on defined parameters:

SMEs (Small & Medium-sized Enterprises):

- Companies with an annual revenue of less than USD 1 billion.

Startups:

- The annual revenue is less than USD 50 million
- The employee count is less than 100
- Company valuation is less than USD 500 million
- The age of the company is less than 10 years, and any of the above conditions is met

The startups/SMEs evaluation matrix features emerging and innovative DDoS protection and mitigation market companies. The startups selected for the matrix were chosen based on their founding years, revenues, and employee count. Overall vendor evaluations are based on the strength of the product portfolio and market shares/rank:

- **Progressive Companies:** Vendors that have been marking their presence in the market by offering innovative solutions as per customer requirements and adopting various strategies to achieve growth in the market
- **Responsive Companies:** These companies have a robust potential to build strong business strategies to expand their product footprint and stay on par with progressive companies
- **Dynamic Companies:** Dynamic companies offer innovative solution portfolios and have competent distribution to increase their market presence
- **Starting Blocks:** Most starting blocks have been undertaking multiple product developments and launches to cater to a broader range of clients

The competitive evaluation matrix includes the company evaluation matrix of startups operating in the market to understand each player's performance. It features the analysis of startups in the DDoS protection and mitigation market based on their offerings.

16.8.1 PROGRESSIVE COMPANIES

Gcore, Mlytics, Seceon, Xcitium, and Haltdos are progressive companies. They offer strong solution portfolios in the market. These vendors have been marking their presence by providing innovative solutions as per customer requirements and adopting various strategies to achieve growth in the DDoS protection and mitigation market.

16.8.2 RESPONSIVE COMPANIES

MazeBolt, Indusface, and RioRey are recognized as responsive companies in the DDoS protection and mitigation market. Responsive companies provide innovative solutions to cater to future DDoS protection and mitigation demands. These companies have a robust potential to build strong business strategies to expand their business and stay on par with progressive companies. These vendors have been offering DDoS protection and mitigation products and solutions to their customers to fulfill their demands.

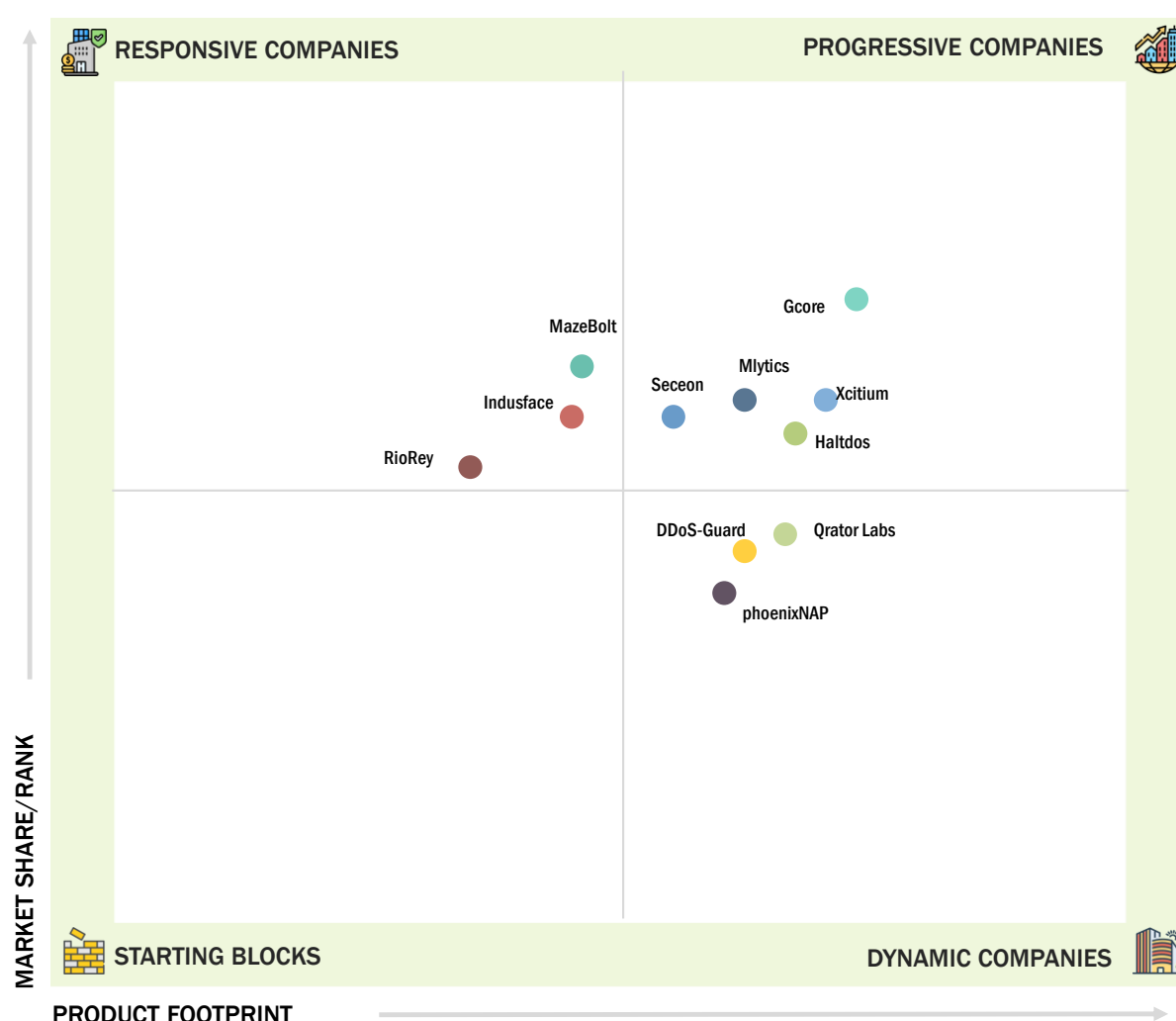
16.8.3 DYNAMIC COMPANIES

Dynamic companies such as DDoS-Guard, Qrator Labs, and phoenixNAP offer innovative solution portfolios and have an extensive network of channel partners and resellers to increase the deployment of their solutions across a multitude of vertical markets. Dynamic companies have been consistently generating positive revenue growth in the DDoS protection and mitigation market, and organic and inorganic ventures have boosted their market position.

16.8.4 STARTING BLOCKS

Most of the starting blocks have been undertaking multiple product developments and launches to boost their sales capabilities across regions to offer integrated solutions and services to a wide range of clients.

FIGURE 49 DDoS PROTECTION AND MITIGATION MARKET:
COMPANY EVALUATION MATRIX (STARTUPS/SMES), 2025



Source: Secondary Research and MarketsandMarkets Analysis

16.8.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2025

16.8.5.1 Detailed list of key startups/SMEs

TABLE 580 DDOS PROTECTION AND MITIGATION MARKET: KEY STARTUPS/SMES, 2025

COMPANY	TYPE	CATEGORY	OWNERSHIP STATUS	HQ LOCATION	FOUNDED	EMPLOYEES	FINANCING STATUS	LATEST FUNDING ROUND	TOTAL FUNDING (USD MILLION)
Seceon	SME	Solution/ Services	Private	Massachusetts, US	2014	51–200	Equity	Debt	2.2
HaltDos	SME	Solution/ Services	Private	Noida, India	2015	11–50	Venture Capital	Grant	0.01
DDoS-Guard	SME	Solution/ Services	Private	Russia	2011	51–200	Venture Capital	NA	NA
Indusface	SME	Solution/ Services	Private	Gujarat, India	2012	51–200	Venture Capital	Venture	5
Mlytics	SME	Solution/ Services	Private	Singapore	2017	51–200	Venture Capital	NA	NA
RioRey	SME	Solution	Private	Maryland, US	2006	11–50	Venture Capital	Debt	0.29
PhoenixNAP	SME	Solution	Private	Phoenix, US	2009	201–500	Venture Capital	NA	NA
MazeBolt	SME	Solution	Private	Ramat Gan, Israel	2013	11–50	Venture Capital	Undisclosed Round	NA
Gcore	SME	Solution	Private	Contern, Luxembourg	2014	501–1,000	Venture Capital	Series A	60
Xcitium	SME	Solution	Private	Bloomfield, New Jersey, US	2018	501–1,000	Venture Capital	NA	NA
Qrator Labs	SME	Solution	Private	Prague, Czech Republic	2009	51–200	NA	NA	NA

Note: As the above companies are SMEs, the funding data is not available for all the companies.

Source: Secondary Research and MarketsandMarkets Analysis

16.8.5.2 Competitive benchmarking of key startups/SMEs

TABLE 581 DDOS PROTECTION AND MITIGATION MARKET: COMPETITIVE BENCHMARKING OF KEY STARTUPS/SMES, 2025

COMPANY	OFFERING			VERTICAL			REGION				
	HARDWARE	SOFTWARE	SERVICES	BFSI	HEALTHCARE	IT & ITES	NORTH AMERICA	EUROPE	ASIA PACIFIC	MIDDLE EAST & AFRICA	LATIN AMERICA
Seceon	N	Y	Y	Y	N	N	Y	Y	Y	N	N
HaltDos	N	Y	Y	N	N	Y	Y	N	Y	N	N
DDoS-Guard	N	Y	Y	Y	Y	N	Y	N	N	N	N
Indusface	N	Y	Y	Y	Y	Y	N	Y	Y	N	N
Activereach	N	Y	N	N	N	Y	Y	Y	Y	Y	Y
Mlytics	N	Y	N	N	N	Y	Y	Y	Y	Y	Y
RioRey	N	Y	N	N	N	Y	Y	Y	Y	N	N
PhoenixNAP	N	Y	Y	N	N	Y	Y	Y	N	Y	Y
MazeBolt	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Gcore	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Xcitium	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Qrator Labs	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Source: Secondary Research and MarketsandMarkets Analysis

16.9 COMPETITIVE SCENARIO & TRENDS

This section studies the growth strategies adopted by players between January 2024–August 2026. Major players are adopting strategies to increase market share, such as product/solution launches, product enhancements, partnerships, collaborations, and acquisitions.

16.9.1 PRODUCT LAUNCHES & ENHANCEMENTS

TABLE 582 DDOS PROTECTION AND MITIGATION MARKET: PRODUCT LAUNCHES AND ENHANCEMENTS, JANUARY 2024–AUGUST 2026

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (TYPE)	DESCRIPTION
July 2026	Product enhancement	Radware (Israel)	DefensePro X – Cloud-Augmented Protection (Hardware/Platform)	Radware introduced a cloud-augmented protection architecture for DefensePro X, extending its on-premises DDoS protection platform with AI-powered cloud algorithms. The enhancement debuted with Web DDoS Defense and enables additional protection against

				sophisticated application-layer attacks while retaining local traffic inspection and mitigation capabilities.
March 2026	Hardware expansion	Fortinet (US)	FortiDDoS 3000G (Hardware Appliance)	Fortinet added the FortiDDoS 3000G to its FortiDDoS hardware portfolio. The official Fortinet documentation published in March 2026 lists the new model, expanding the company's purpose-built appliance portfolio for protecting network infrastructure against DDoS attacks. FortiDDoS provided autonomous detection and mitigation using behavioral analysis and full packet inspection.
March 2026	Product launch	Radware (Israel)	Web DDoS Protection for Encrypted Traffic (Cloud-based Platform)	Radware launched a cloud-based Web DDoS Protection capability designed to detect and mitigate encrypted application-layer DDoS attacks without requiring SSL/TLS certificate sharing or traffic decryption. The solution used behavioral analysis to identify malicious traffic while preserving encrypted communications.
March 2026	Product launch	Cloudflare (US)	Programmable Flow Protection (DDoS Protection Capability)	Cloudflare introduced Programmable Flow Protection for Magic Transit Enterprise customers. The capability enabled customers to implement and deploy custom, stateful DDoS mitigation logic across Cloudflare's global network, specifically supporting protection for custom and proprietary UDP-based protocols. The capability was made available in beta to eligible Magic Transit Enterprise customers.
January 2026	Network Infrastructure enhancement	Radware (Israel)	Cloud DDoS Protection Service (Cloud Service)	Radware doubled the mitigation capacity of its global cloud security service network from 15 Tbps to 30 Tbps, strengthening its ability to absorb and mitigate large-scale volumetric DDoS attacks.
September 2025	Product enhancement	Fortinet (US)	FortiAppSec Cloud (Cloud-based WAAP Platform)	Fortinet expanded its cloud application security portfolio and made FortiAppSec Cloud available through AWS Marketplace. The platform combined web application firewall, bot management, API security, and DDoS mitigation capabilities, extending Fortinet's application-layer DDoS protection availability for cloud environments.
April 2025	Product enhancement	Radware (Israel)	DefensePro X Version 10.9 (Hardware/Platform)	Radware released DefensePro X version 10.9, introducing TLS Fingerprint Reputation Feed for Web DDoS Protection, ASN-based protection, enhanced geo-based rate limiting, standard DNS and HTTPS protection capabilities, and new DefensePro X110, X220, and X380 high-end platforms.
March 2025	Product launch	NETSCOUT (US)	Arbor Threat Mitigation System (TMS)	NETSCOUT launched its enhanced Arbor Threat Mitigation System (TMS), featuring advanced AI- and ML-driven capabilities for adaptive DDoS protection. The upgraded solution leveraged global threat intelligence from the ATLAS

				Intelligence Feed to detect, analyze, and mitigate complex attacks more effectively, enabling service providers and enterprises to ensure stronger network resilience and minimize downtime.
November 2024	Product launch	Radware (Israel)	AI SOC Xpert (Security Management Platform)	Radware launched AI SOC Xpert, a cloud security service that uses AI to support investigation, remediation, and response to DDoS and application security incidents. The service automated analysis of security events and assists SOC teams in accelerating incident response.
October 2024	Product enhancement	Akamai (US)	Behavioral DDoS Engine for App & API Protector (Software/Platform)	Akamai made its Behavioral DDoS Engine available for App & API Protector. The capability used machine learning, anomaly analysis, and multidimensional traffic correlation to automatically detect and mitigate sophisticated application-layer DDoS attacks. It provided customized protection based on customer traffic baselines and risk sensitivities while reducing false positives and manual intervention.
September 2024	Product enhancement	Radware (Israel)	DefensePro X Version 10.7 (Hardware/Platform)	Radware enhanced DefensePro X with improvements to network and encrypted Web DDoS protection. The release reduced network DDoS time-to-mitigation to below 10 seconds and introduced enhancements for behavioral DDoS detection, DNS protection, encrypted Web DDoS protection, and hybrid deployments.
April 2024	Product launch	Radware (Israel)	AI-Powered Rule-Free DNS DDoS Protection (Software/Platform)	Radware introduced a new AI-powered, rule-free edition of its DNS DDoS Protection solution. The capability used behavioral algorithms and automated detection to identify and mitigate DNS DDoS attacks without requiring manually configured rules or signatures.
April 2024	Product launch	Akamai (US)	Shield NS53 (DNS Security Platform)	Akamai launched Shield NS53 to protect on-premises and hybrid DNS infrastructure against resource-exhaustion attacks that can overwhelm DNS servers and disrupt legitimate queries. The solution complemented Akamai Edge DNS and Prolexic and expanded the company's protection capabilities for DNS-focused DDoS and availability threats.
March 2024	Product enhancement	Akamai (US)	App & API Protector (Application Security Platform)	Akamai enhanced App & API Protector with advanced Layer 7 DDoS defenses, including improved detection and mitigation of short DDoS attack bursts and client reputation-based rate limiting. The update also introduced URL Protection, which prioritizes legitimate traffic to help maintain the availability of critical URLs, APIs, and microservices during highly distributed attacks.
March 2024	Product launch	Cloudflare (US)	Advanced DNS Protection (DDoS)	Cloudflare introduced Advanced DNS Protection, a distributed and software-defined DDoS defense system designed to detect and mitigate sophisticated DNS-based DDoS attacks. The

			Protection Capability)	capability complemented Cloudflare's existing DDoS defense systems and used stateful traffic analysis to identify anomalous DNS attack patterns.
March 2024	Product enhancement	Cloudflare (US)	Express Cloudflare Network Interconnect (Network Interconnect Service)	Cloudflare introduced Express CNI, a major enhancement to Cloudflare Network Interconnect that simplifies and accelerates enterprise connectivity to Cloudflare services, including Magic Transit. The enhancement enabled enterprises to establish faster connectivity between their networks and Cloudflare's infrastructure supporting network-layer security and DDoS protection deployments.

Source: Press Releases

16.9.2 DEALS

TABLE 583 DDOS PROTECTION AND MITIGATION MARKET: DEALS, JANUARY 2024– AUGUST 2026

MONTH & YEAR	DEAL TYPE	COMPANY 1 NAME	COMPANY 2 NAME	DESCRIPTION	DEAL SIZE
August 2026	Strategic alliance	Akamai (US)	Deloitte Canada (Canada)	Akamai established a strategic alliance with Deloitte Canada to deliver platform-based cyber resilience capabilities. The joint security approach included Akamai's Application Protection Platform, with Akamai App & API Protector and Akamai Prolexic specifically incorporated for WAF and DDoS protection and mitigation of high-volume infrastructure attacks. The alliance combined Deloitte's cybersecurity advisory and managed services with Akamai's security technologies.	NA
May 2026	Partnership	Radware (Israel)	Chief Telecom (Taiwan)	Radware partnered with Chief Telecom to power Godshield Pro, a DDoS protection service in Taiwan. The service combined Radware's DDoS mitigation technology with Chief Telecom's network infrastructure to provide low-latency protection against large-scale and sophisticated DDoS attacks.	NA
December 2025	Customer deal	Radware (Israel)	A NYSE-traded US Enterprise Software Company (US)	Radware secured a significant multi-year customer win with a leading US enterprise software company. The agreement covers Radware's cloud security capabilities, including protection for the customer's large-scale IT platform and digital infrastructure.	NA
April 2025	Partnership	Radware (Israel)	EPIC Cloud Company (Taiwan)	Radware announced a strategic partnership with EPIC Cloud Company in Taiwan to provide AI-driven cloud application and DDoS protection services. The collaboration enabled EPIC Cloud to integrate Radware's WAF, bot management, and DDoS defense into its managed security portfolio.	NA

December 2024	Agreement expansion	Radware (Israel)	Top 5 Bank in Italy (Italy)	Radware expanded its agreement with one of Italy's top five banks to provide an end-to-end suite of AI-driven network and application security solutions. The expanded deployment includes DDoS protection capabilities designed to protect the bank's critical digital infrastructure.	NA
November 2024	Customer agreement	Radware (Israel)	Top 10 Airport in India (India)	Radware signed an agreement with a top 10 airport in India to deliver Cloud DDoS Protection and Cloud Application Protection. The deployment is intended to protect the airport's digital infrastructure and online services against network- and application-layer cyberattacks.	NA
November 2024	Contract expansion	Radware (Israel)	Leading US CPaaS Provider (US)	Radware expanded its relationship with a prominent US-based communications platform-as-a-service provider through a multimillion-dollar agreement that added Hybrid Cloud DDoS Protection to the customer's security deployment.	NA
April 2024	Strategic collaboration	Cloudflare (US)	Booz Allen Hamilton (US)	Cloudflare and Booz Allen Hamilton established a collaboration to provide Under Attack as a Service (UAaaS), enabling Booz Allen's commercial clients facing active cyberattacks to receive expedited access to Cloudflare's incident response capabilities and 30-day Rapid Response DDoS Mitigation service, including continuous monitoring and protection.	NA

Source: Press Releases

16.9.3 EXPANSIONS

TABLE 584 DDOS PROTECTION AND MITIGATION MARKET: EXPANSIONS, JANUARY 2024–AUGUST 2026

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
June 2024	Expansion	Facility	Canada	NETSCOUT (US)	NETSCOUT announced that it expanded its Arbor Cloud DDoS attack mitigation network to 16 scrubbing centers worldwide with the recent addition of a new Toronto facility. This network offered ISPs and enterprise customers more than 15 terabits per second (Tbps) of dedicated attack capacity.

Source: Press Releases

17 COMPANY PROFILES

17.1 KEY PLAYERS

17.1.1 AKAMAI

17.1.1.1 Business overview

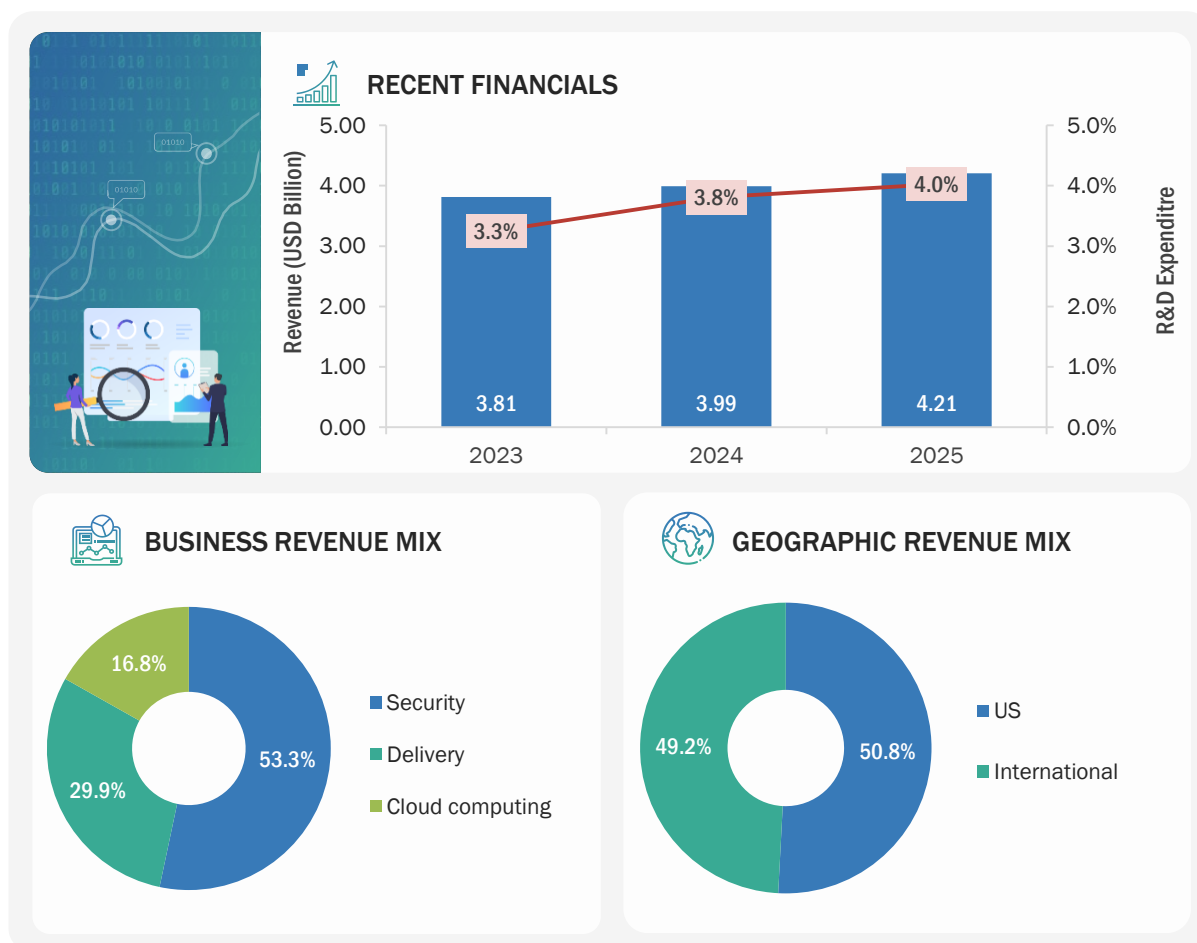
Akamai Technologies (Akamai) specializes in web and mobile acceleration, DNS and traffic management, media delivery, cloud security, and CDN. It offers security solutions, media delivery solutions, and network operator solutions. Its cloud security portfolio includes application protection, bot management, DDoS mitigation, and threat protection products. The company is a key player in the DDoS protection and mitigation market, with a portfolio that includes Kona Site Defender, Web Application Protector, Fast DNS, and Prolexic. Kona Site Defender protects websites and applications from advanced DDoS attacks. It offers features such as site shield, adaptive caching, site failover, access control, net storage, log delivery service, security information and event management (SIEM) integration, and ISO 27002 compliance management module. Prolexic helps protect enterprises from network-layer and application-layer DDoS attacks. It offers features such as a customizable protection model, global network support, DDoS monitoring, attack support, and SOC support.

Akamai helps enterprises reduce network and infrastructure costs while increasing their throughput over time. Its security solution protects enterprises' websites, applications, and users from ever-rising threats. Its intelligent platform is a network of more than 240,000 servers deployed over 1,700 networks in over 139 countries. The platform anticipates the traffic, secures against attacks, and is scalable with the growing traffic. As enterprises need highly secure, good-quality, and fast data delivered to their devices, the company accelerates application performance and delivers high-end software solutions while reducing infrastructure costs. The company offers its products to almost all verticals, including healthcare and life sciences, business services, BFSI, automotive, hotel and travel, manufacturing, media and entertainment, public sector, gaming, retail and consumer goods, and software technology. It offers its products to large enterprises and startups. Some of the significant security customers of the company include Alliant Credit Union, Fidor Bank, Nuance Healthcare, and Red Hat.

TABLE 585 AKAMAI: COMPANY OVERVIEW

AKAMAI	
Founded	1998
Country	US
City	Cambridge, Massachusetts
Ownership	Public (NASDAQ: AKAM)

Source: Company Website

FIGURE 50 AKAMAI: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.1.2 Products/Solutions/Services offered**TABLE 586** AKAMAI: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/SOLUTION/SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Prolexic	Prolexic is Akamai's purpose-built DDoS protection platform for internet-facing infrastructure. It provides automated detection and mitigation of DDoS attacks across cloud, on-premises, and hybrid environments, with in-cloud scrubbing, on-premises protection, hybrid deployment options, and Network Cloud Firewall capabilities.	Software/platform & services	Telecommunications, BFSI, government, healthcare, retail & eCommerce, technology, gaming, media & entertainment, manufacturing
App & API Protector	App & API Protector is an integrated application and API security solution that combines web application firewall (WAF), API security, bot management, and Layer 7 DDoS/DoS protection. It uses adaptive and behavioral protections to detect and mitigate attacks targeting websites, web applications, and APIs across edge, hybrid cloud, and multicloud environments.	Software/platform	BFSI, retail & eCommerce, technology, media & entertainment, gaming, healthcare, government

Edge DNS	Edge DNS is a cloud-based authoritative DNS solution that provides DNS availability, performance, and resilience against high-volume DDoS attacks. It supports cloud, on-premises, and hybrid DNS environments and can be combined with other Akamai security offerings for multilayered infrastructure protection.	Software/ platform	Telecommunications, BFSI, government, technology, retail & eCommerce, media & entertainment, healthcare
----------	---	-----------------------	---

Source: Company Website

17.1.1.3 Recent developments

17.1.1.3.1 Product launches & enhancements

TABLE 587 AKAMAI: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
October 2024	Product enhancement	Akamai (US)	Behavioral DDoS Engine for App & API Protector (Software/Platform)	Akamai made its Behavioral DDoS Engine available for App & API Protector. The capability used machine learning, anomaly analysis, and multidimensional traffic correlation to automatically detect and mitigate sophisticated application-layer DDoS attacks. It provided customized protection based on customer traffic baselines and risk sensitivities while reducing false positives and manual intervention.
April 2024	Product launch	Akamai (US)	Shield NS53 (DNS Security Platform)	Akamai launched Shield NS53 to protect on-premises and hybrid DNS infrastructure against resource-exhaustion attacks that can overwhelm DNS servers and disrupt legitimate queries. The solution complemented Akamai Edge DNS and Prolexic and expanded the company's protection capabilities for DNS-focused DDoS and availability threats.
March 2024	Product enhancement	Akamai (US)	App & API Protector (Application Security Platform)	Akamai enhanced App & API Protector with advanced Layer 7 DDoS defenses, including improved detection and mitigation of short DDoS attack bursts and client reputation-based rate limiting. The update also introduced URL Protection, which prioritizes legitimate traffic to help maintain the availability of critical URLs, APIs, and microservices during highly distributed attacks.

Source: Press Releases

17.1.1.3.2 Deals

TABLE 588 AKAMAI: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
August 2026	Strategic alliance	Akamai (US)	Deloitte Canada (Canada)	Akamai established a strategic alliance with Deloitte Canada to deliver platform-based cyber resilience capabilities. The joint security approach included Akamai's Application Protection Platform, with Akamai App & API Protector and Akamai Prolexic specifically incorporated for WAF and DDoS protection and mitigation of high-volume infrastructure attacks. The alliance combined Deloitte's cybersecurity advisory and managed services with Akamai's security technologies.

Source: Press Releases

17.1.1.4 MnM view

17.1.1.4.1 Right to win

Akamai protects websites and applications with its robust range of products and services. Holding exclusive rights to over 300 patents, the company has a strong customer base that includes many of the world's leading corporations and public sector organizations.

17.1.1.4.2 Strategic choices

Akamai operates in three segments: Security, Delivery, and Compute solutions. The company's DDoS protection and mitigation are part of the performance and security solutions business, which generates around half of the company's revenue. The company also focuses on inorganic growth, either through partnerships with prominent players or acquisitions of other competitors.

17.1.1.4.3 Weaknesses and competitive threats

The company's primary revenue comes mainly from the US market. To ensure long-term sustainability, the company needs to prioritize diversification. Its current focus is on inorganic growth strategies, which means that the effectiveness of its business operations could be impacted if it does not fully leverage the potential of the acquired companies.

17.1.2 CLOUDFLARE

17.1.2.1 Business overview

Cloudflare is a connectivity cloud and cybersecurity company providing network, application, cloud, and Internet security solutions. The company offers a broad portfolio spanning application security, network security, Zero Trust services, connectivity, developer services, and performance solutions. Its overall product portfolio includes DDoS Protection, Magic Transit, Cloudflare Spectrum, Web Application Firewall (WAF), API Security, Bot Management, DNS Security, Zero Trust, Cloudflare One, CDN, and application performance services. Cloudflare delivers these capabilities through its globally distributed cloud network, which supports organizations in securing and connecting applications, networks, and infrastructure.

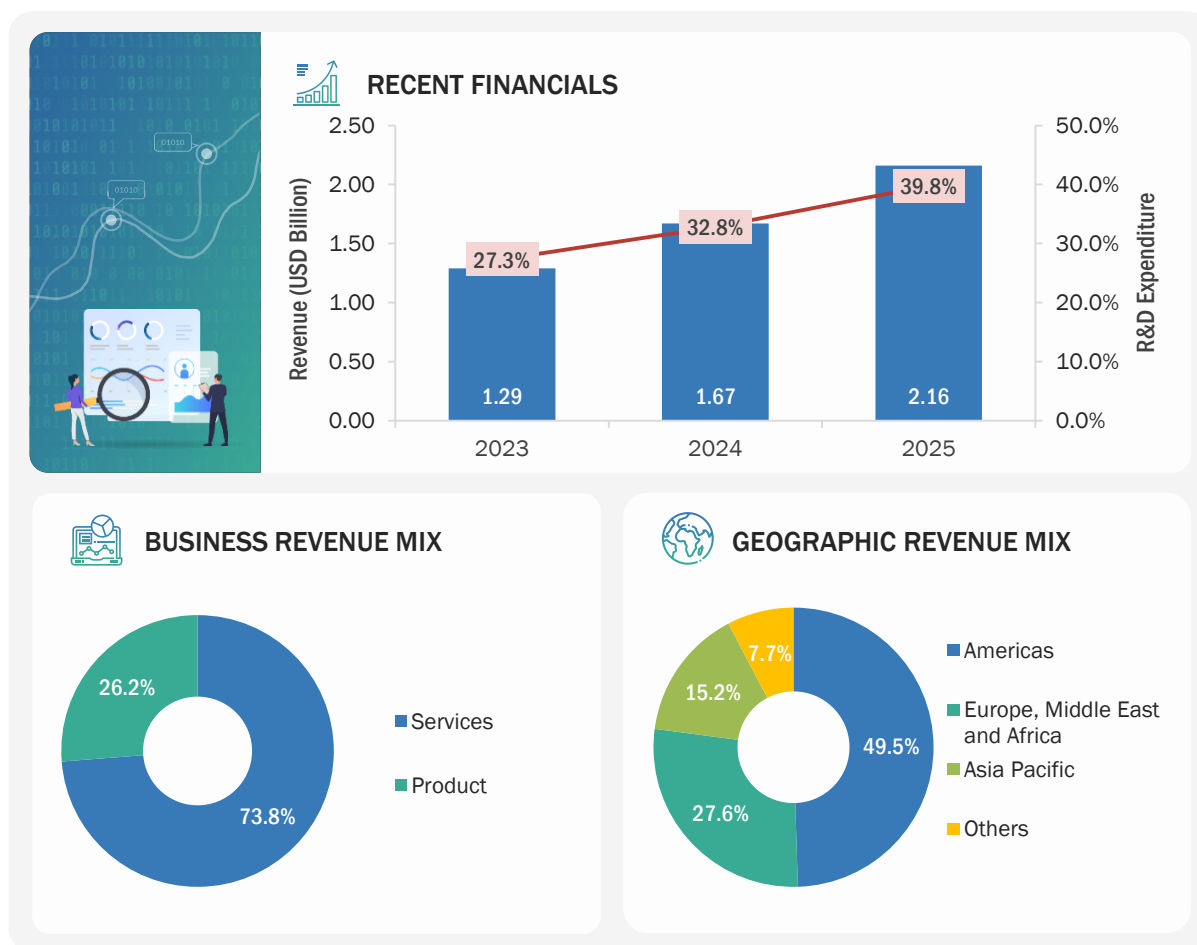
Cloudflare provides DDoS protection across network, transport, and application layers through its Cloudflare DDoS Protection portfolio, including Magic Transit for network and infrastructure protection and Cloudflare Spectrum for TCP/UDP applications. Its Autonomous DDoS Protection Edge automatically detects and mitigates attacks across Layers 3, 4, and 7 using dynamic managed rulesets, adaptive traffic analysis, and stateful protection capabilities. Magic Transit uses BGP routing and Cloudflare's Anycast network to absorb and filter malicious traffic close to its source, while Spectrum protects TCP- and UDP-based applications against Layer 3 and Layer 4 attacks. Cloudflare currently states that its network has 534 Tbps of capacity and can mitigate most attacks in under three seconds.

Cloudflare serves organizations across industries including financial services, government, healthcare, telecommunications, technology, retail, media, and gaming. Its global customer base includes enterprises and digital platforms such as Shopify, Canva, Japan Airlines, Wikimedia Foundation, and Delivery Hero. The company operates a geographically distributed network spanning 335+ cities worldwide, enabling localized traffic inspection, mitigation, and delivery services. Its offices are in North America, South America, Europe, Asia Pacific, and MEA.

TABLE 589 CLOUDFLARE: COMPANY OVERVIEW

CLOUDFLARE	
Founded	2009
Country	US
City	San Francisco, California
Ownership	Public (NYSE: NET)

Source: Company Website

FIGURE 51 CLOUDFLARE: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and MarketsandMarkets Analysis

17.1.2.2 Products/Solutions/Services offered

TABLE 590 CLOUDFLARE: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	PRODUCT TYPE	DESCRIPTION	APPLICATION
Cloudflare DDoS Protection	Software/ platform	Cloudflare DDoS Protection provides automated DDoS detection and mitigation across Layers 3, 4, and 7 through Cloudflare's global network and Autonomous DDoS Protection systems. The offering protects websites and HTTP/HTTPS applications using managed rulesets and adaptive mitigation capabilities.	▪ BFSI ▪ retail & eCommerce ▪ media & entertainment ▪ technology, government ▪ healthcare
Cloudflare Spectrum	Software/ platform	Cloudflare Spectrum provides DDoS protection and traffic acceleration for TCP- and UDP-based applications. Operating as a Layer 4 reverse proxy, it protects applications against network- and transport-layer DDoS attacks while concealing origin infrastructure.	▪ Gaming ▪ financial services ▪ technology ▪ telecommunications ▪ media & entertainment
Magic Transit	Software/ platform	Magic Transit provides hardware-free DDoS protection for enterprise networks, data centers, and on-premises, cloud-hosted, and hybrid infrastructure. The solution uses Cloudflare's global	▪ BFSI ▪ telecommunications ▪ government

Anycast network and BGP routing to absorb and filter malicious traffic. Its DDoS protection capabilities include managed network-layer rulesets, Advanced TCP Protection, Advanced DNS Protection, Programmable Flow Protection for UDP-based protocols, and Network Firewall.

- healthcare
- technology
- critical infrastructure

Source: Company Website

17.1.2.3 Recent developments

17.1.2.3.1 Product launches & enhancements

TABLE 591 CLOUDFLARE: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
March 2026	Product launch	Cloudflare (US)	Programmable Flow Protection (DDoS Protection Capability)	Cloudflare introduced Programmable Flow Protection for Magic Transit Enterprise customers. The capability enabled customers to implement and deploy custom, stateful DDoS mitigation logic across Cloudflare's global network, specifically supporting protection for custom and proprietary UDP-based protocols. The capability was made available in beta to eligible Magic Transit Enterprise customers.
March 2024	Product launch	Cloudflare (US)	Advanced DNS Protection (DDoS Protection Capability)	Cloudflare introduced Advanced DNS Protection, a distributed and software-defined DDoS defense system designed to detect and mitigate sophisticated DNS-based DDoS attacks. The capability complemented Cloudflare's existing DDoS defense systems and used stateful traffic analysis to identify anomalous DNS attack patterns.
March 2024	Product enhancement	Cloudflare (US)	Express Cloudflare Network Interconnect (Network Interconnect Service)	Cloudflare introduced Express CNl, a major enhancement to Cloudflare Network Interconnect that simplifies and accelerates enterprise connectivity to Cloudflare services, including Magic Transit. The enhancement enabled enterprises to establish faster connectivity between their networks and Cloudflare's infrastructure supporting network-layer security and DDoS protection deployments.

Source: Press Releases

17.1.2.3.2 Deals

TABLE 592 CLOUDFLARE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
April 2024	Strategic collaboration	Cloudflare (US)	Booz Allen Hamilton (US)	Cloudflare and Booz Allen Hamilton established a collaboration to provide Under Attack as a Service (UAaaS), enabling Booz Allen's commercial clients facing active cyberattacks to receive expedited access to Cloudflare's incident response capabilities and 30-day Rapid Response DDoS Mitigation service, including continuous monitoring and protection.

Source: Press Releases

17.1.2.4 MnM view

17.1.2.4.1 Key strengths

Cloudflare operates one of the world's largest DDoS mitigation networks, spanning more than 335+ cities in across 125 countries. With more than 238,000 paying customers and strong enterprise adoption, it leverages real-time automation and global telemetry to mitigate multi-terabit attacks effectively.

17.1.2.4.2 Strategic choices

Cloudflare continues to expand network capacity and invest in AI-driven detection and integrated DDoS solutions within its security platform. Its rising R&D spend (USD 421 million approx. in 2024) and focus on enterprise clients strengthen its competitive positioning and long-term scalability.

17.1.2.4.3 Weaknesses and competitive threats

Heavy investment in infrastructure and R&D pressures margins, with the company still posting GAAP losses despite revenue growth. Intense competition from established players and regional compliance barriers could challenge expansion and profitability.

17.1.3 RADWARE

17.1.3.1 Business overview

Radware is a global cybersecurity and application delivery solutions provider specializing in infrastructure, application, and network protection. The company offers a broad portfolio spanning cloud security, application protection, network security, application delivery, bot management, API security, and threat intelligence. Its overall product portfolio includes Cloud DDoS Protection Services, DefensePro X, Web DDoS Protection, Cyber Controller, Cloud Web Application Firewall, Bot Manager, API Security, Alteon Application Delivery Controllers, and AI-powered SOC services. Radware serves more than 12,500 enterprise and carrier customers globally and has over 1,200 employees worldwide.

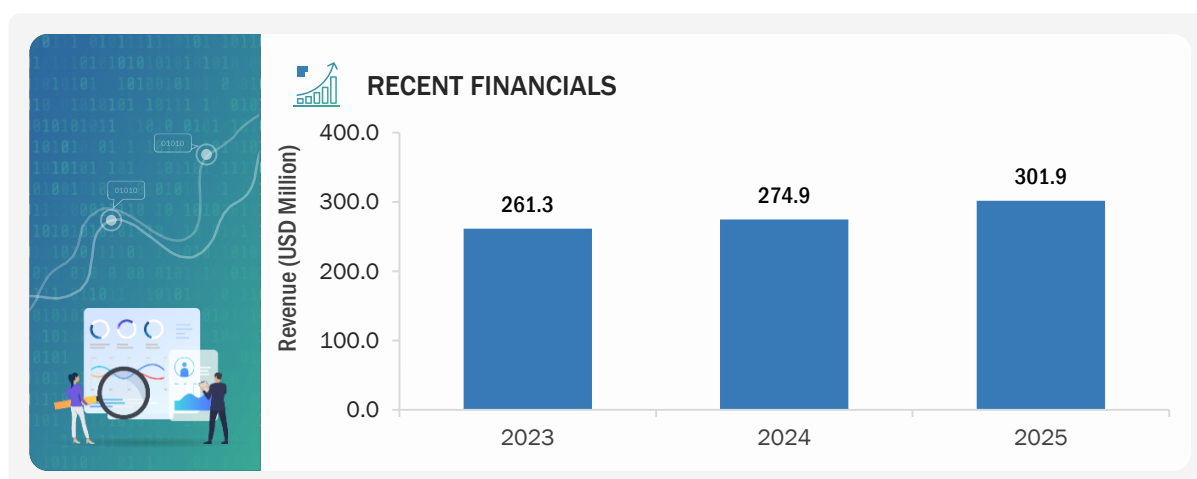
Radware's DDoS protection portfolio provides automated protection against network- and application-layer attacks across cloud, on-premises, and hybrid environments. Its key offerings include Cloud DDoS Protection Services, DefensePro X, Web DDoS Protection, and Cyber Controller. The solutions use behavioral-based detection, machine learning, automated signature generation, and threat intelligence to identify and mitigate volumetric, protocol, DNS, encrypted, and application-layer DDoS attacks. Radware's cloud DDoS infrastructure comprises 25 globally distributed scrubbing centers with 30 Tbps of mitigation capacity, while its hybrid architecture enables coordinated mitigation between on-premises and cloud environments. Cyber Controller further provides centralized visibility, analytics, policy management, and automated mitigation orchestration across DDoS protection deployments.

Radware serves enterprises, carriers, service providers, and public-sector organizations across industries including financial services, telecommunications, cloud and hosting, eCommerce, government, healthcare, and critical infrastructure. Radware has a global reach, with offices in all the major geographies, such as North America, EMEA, Asia Pacific, and Latin America. It also has scrubbing centers at various locations across the globe.

TABLE 593 RADWARE: COMPANY OVERVIEW

RADWARE	
Founded	1996
Country	Israel
City	Tel Aviv
Ownership	Public (NASDAQ: RDWR)

Source: Company Website

FIGURE 52 RADWARE: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.3.2 Products/Solutions/Services offered

TABLE 594 RADWARE: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/SOLUTION/SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Cloud DDoS Protection Service	Radware Cloud DDoS Protection Service uses advanced behavioral algorithms to detect and mitigate DDoS attacks at any level. It includes Infrastructure DDoS Protection and Web DDoS Protection.	Service	Security
DefensePro X	DefensePro, part of Radware's attack mitigation solution, provides automated DDoS protection from fast-moving, high-volume, encrypted, or very short-duration threats. It defends against IoT-based, Burst, DNS, and TLS/SSL attacks to secure organizations against emerging network multi-vector attacks, ransom DDoS campaigns, IoT botnets, phantom floods, and other types of cyberattacks. Radware's line-up of DefensePro platforms includes the following: - DefensePro 6 Series - DefensePro 20 Series - DefensePro 60 Series - DefensePro 110 and 220 Series - DefensePro 200 and 400 Series Radware's line-up of DefensePro X platforms includes the following: - DefensePro X10 & X20 - DefensePro X40 - DefensePro X80 - DefensePro X100 & X200 - DefensePro X800 & X400	Solution	Security & mitigation
Threat Intelligence Subscriptions	Radware's Threat Intelligence Subscriptions immunize the DDoS protection system. They provide real-time intelligence for preemptive protection and enable multilayered protection against known and unknown vectors and actors, as well as ongoing and emergency filters. Radware's Threat Intelligence Subscriptions	Service	Analysis & security

	enhance DDoS protection and extend its automated, real-time behavioral threat analysis for preemptive protection.		
DNS DDoS Protection	Radware's DDoS Protection solutions use behavior-based detection and automatic real-time signatures to identify and automatically block today's most advanced DNS DDoS attacks. These DNS DDoS defenses leverage adaptive and multilayered protection that can be flexibly deployed, such as via cloud or as a hybrid deployment to suit every customer's needs and deployment architecture.	Solution	Detection & security
Web DDoS Protection	Radware's patented Cloud Web DDoS Protection does what network-based DDoS protection and standard WAF solutions cannot. It overcomes the scale, complexity, and dynamic nature of these Web DDoS Tsunami attacks without affecting legitimate traffic.	Solution	Security

Source: Company Website

17.1.3.3 Recent developments

17.1.3.3.1 Product launches & enhancements

TABLE 595 RADWARE: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
July 2026	Product enhancement	Radware (Israel)	DefensePro X – Cloud-Augmented Protection (Hardware/Platform)	Radware introduced a cloud-augmented protection architecture for DefensePro X, extending its on-premises DDoS protection platform with AI-powered cloud algorithms. The enhancement debuted with Web DDoS Defense and enables additional protection against sophisticated application-layer attacks while retaining local traffic inspection and mitigation capabilities.
March 2026	Product launch	Radware (Israel)	Web DDoS Protection for Encrypted Traffic (Cloud-based Platform)	Radware launched a cloud-based Web DDoS Protection capability designed to detect and mitigate encrypted application-layer DDoS attacks without requiring SSL/TLS certificate sharing or traffic decryption. The solution used behavioral analysis to identify malicious traffic while preserving encrypted communications.
January 2026	Network Infrastructure enhancement	Radware (Israel)	Cloud DDoS Protection Service (Cloud Service)	Radware doubled the mitigation capacity of its global cloud security service network from 15 Tbps to 30 Tbps, strengthening its ability to absorb and mitigate large-scale volumetric DDoS attacks.
April 2025	Product enhancement	Radware (Israel)	DefensePro X Version 10.9 (Hardware/Platform)	Radware released DefensePro X version 10.9, introducing TLS Fingerprint Reputation Feed for Web DDoS Protection, ASN-based protection, enhanced geo-based rate limiting,

				standard DNS and HTTPS protection capabilities, and new DefensePro X110, X220, and X380 high-end platforms.
November 2024	Product launch	Radware (Israel)	AI SOC Xpert (Security Management Platform)	Radware launched AI SOC Xpert, a cloud security service that uses AI to support investigation, remediation, and response to DDoS and application security incidents. The service automated analysis of security events and assists SOC teams in accelerating incident response.
September 2024	Product enhancement	Radware (Israel)	DefensePro X Version 10.7 (Hardware/Platform)	Radware enhanced DefensePro X with improvements to network and encrypted Web DDoS protection. The release reduced network DDoS time-to-mitigation to below 10 seconds and introduced enhancements for behavioral DDoS detection, DNS protection, encrypted Web DDoS protection, and hybrid deployments.
April 2024	Product launch	Radware (Israel)	AI-Powered Rule-Free DNS DDoS Protection (Software/Platform)	Radware introduced a new AI-powered, rule-free edition of its DNS DDoS Protection solution. The capability used behavioral algorithms and automated detection to identify and mitigate DNS DDoS attacks without requiring manually configured rules or signatures.

Source: Press Releases

17.1.3.3.2 Deals

TABLE 596 RADWARE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
May 2026	Partnership	Radware (Israel)	Chief Telecom (Taiwan)	Radware partnered with Chief Telecom to power Godshield Pro, a DDoS protection service in Taiwan. The service combined Radware's DDoS mitigation technology with Chief Telecom's network infrastructure to provide low-latency protection against large-scale and sophisticated DDoS attacks.
December 2025	Customer deal	Radware (Israel)	A NYSE-traded US Enterprise Software Company (US)	Radware secured a significant multi-year customer win with a leading US enterprise software company. The agreement covers Radware's cloud security capabilities, including protection for the customer's large-scale IT platform and digital infrastructure.
April 2025	Partnership	Radware (Israel)	EPIC Cloud Company (Taiwan)	Radware announced a strategic partnership with EPIC Cloud Company in Taiwan to provide AI-driven cloud application and DDoS protection services. The collaboration enabled EPIC Cloud to integrate Radware's WAF, bot management, and DDoS defense into its managed security portfolio.

December 2024	Agreement expansion	Radware (Israel)	Top 5 Bank in Italy (Italy)	Radware expanded its agreement with one of Italy's top five banks to provide an end-to-end suite of AI-driven network and application security solutions. The expanded deployment includes DDoS protection capabilities designed to protect the bank's critical digital infrastructure.
November 2024	Customer agreement	Radware (Israel)	Top 10 Airport in India (India)	Radware signed an agreement with a top 10 airport in India to deliver Cloud DDoS Protection and Cloud Application Protection. The deployment is intended to protect the airport's digital infrastructure and online services against network- and application-layer cyberattacks.
November 2024	Contract expansion	Radware (Israel)	Leading US CPaaS Provider (US)	Radware expanded its relationship with a prominent US-based communications platform-as-a-service provider through a multimillion-dollar agreement that added Hybrid Cloud DDoS Protection to the customer's security deployment.

Source: Press Releases

17.1.3.4 MnM view

17.1.3.4.1 Right to win

Radware is a pioneer in launching the industry's first hybrid cloud-based web application firewall service. Its strong DDoS protection, application delivery, and load-balancing solutions optimize the operations of over 10,000 customers worldwide, providing support capabilities.

17.1.3.4.2 Strategic choices

Radware is highly focused on its R&D expenditure. With its strong R&D, the company focuses on the organic growth strategy of product development and product enhancement. Radware's attack mitigation capabilities are integrated with ML, big data analytics, and threat analysis techniques, and it focuses on improving them. Its strategic partnerships with other leading vendors such as Cisco, Check Point, HP, and IBM will help the company increase its customer reach and revenues.

17.1.3.4.3 Weaknesses and competitive threats

The company's product sales figures could be impacted due to the adoption of the subscription sales format, which might create challenges in business conditions. Other factors, like political and economic stability in Israel, can affect the operations in Radware's headquarters.

17.1.4 FORTINET

17.1.4.1 Business overview

Fortinet is a cybersecurity company specializing in integrated network security, cloud security, security operations, and secure networking. The company delivers its offerings through the Fortinet Security Fabric, which integrates security technologies across enterprise networks, cloud environments, endpoints, applications, and operational technology environments. Its broad portfolio includes FortiGate Next-Generation Firewall, FortiDDoS, FortiWeb, FortiADC, FortiSASE, FortiSIEM, FortiEDR/XDR, FortiNDR, FortiManager, FortiAnalyzer, and FortiGuard AI-Powered Security Services, addressing cybersecurity requirements across organizations of different sizes and industries.

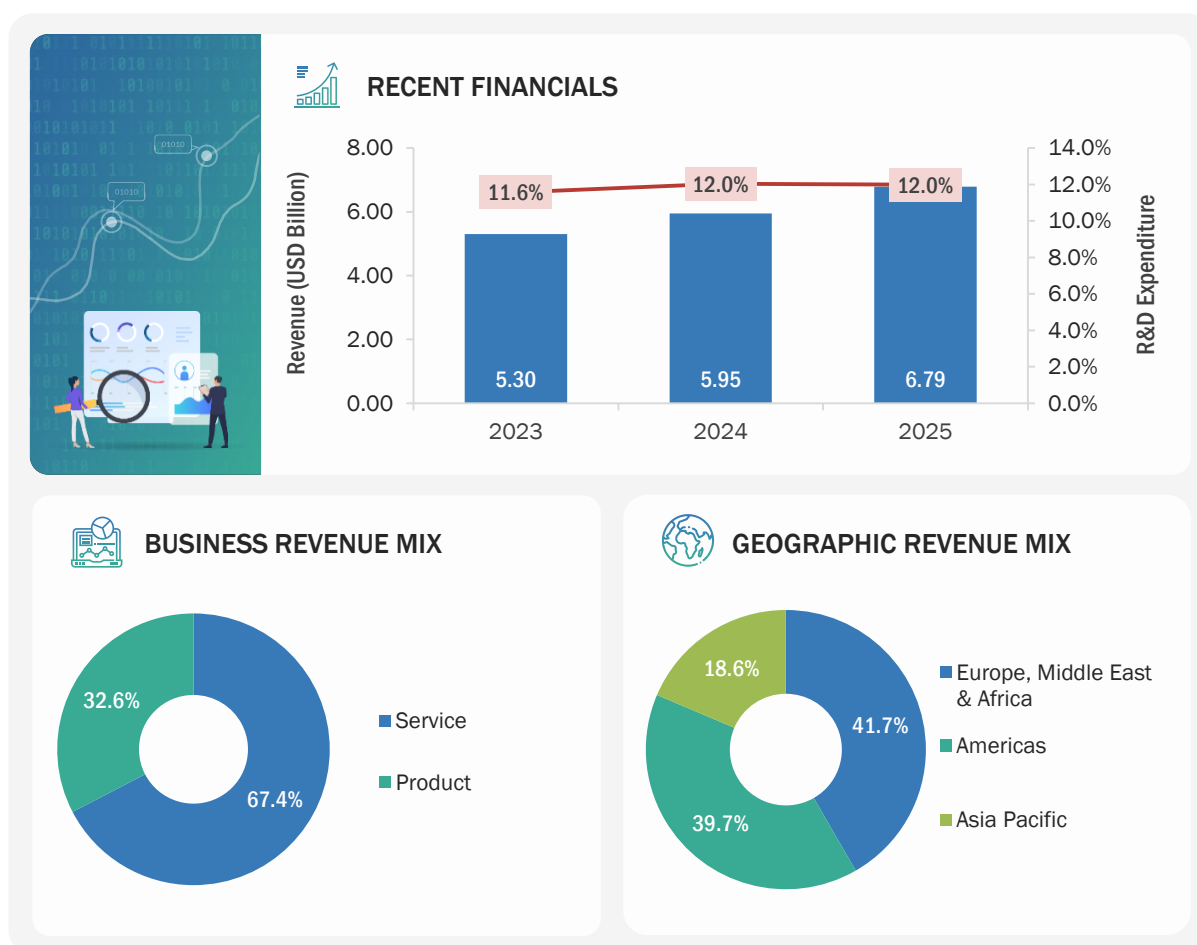
Fortinet's DDoS protection offering, FortiDDoS, is a purpose-built solution available as hardware appliances and virtual machines for protecting enterprise data centers and network infrastructure against DDoS attacks. The solution uses autonomous machine learning, behavioral anomaly detection, and statistical techniques to establish baselines of legitimate traffic and identify deviations associated with known and zero-day attacks. FortiDDoS provides automated mitigation across Layers 3, 4, and 7, with capabilities for mitigating SYN, DNS, NTP, TCP, UDP reflection, QUIC, and other direct or reflected attacks. It continuously monitors a large number of traffic parameters and performs full packet inspection to enable rapid, autonomous mitigation without requiring manual intervention during attacks.

Fortinet serves hundreds of thousands of customers globally across industries including financial services, government, healthcare, manufacturing, retail, telecommunications, energy and utilities, transportation, education, technology, and media and entertainment. With over 330,000 customers in 180 countries, the company has a broad customer base across the Americas, EMEA, and Asia Pacific.

TABLE 597 FORTINET: COMPANY OVERVIEW

FORTINET	
Founded	2000
Country	US
City	Sunnyvale, California
Ownership	Public (NASDAQ: FTNT)

Source: Company Website

FIGURE 53 FORTINET: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.4.2 Products/Solutions/Services offered**TABLE 598** FORTINET: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
FortiDDoS	It uses a machine learning architecture to provide solutions against DDoS attacks.	Software	DDoS attacks protection
Next-Generation Firewall (NGFW)	FortiGate Next-Generation Firewalls (NGFWs) protect data, assets, and users across today's hybrid environments. Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications. FortiGate NGFWs, backed by FortiGuard AI-Powered Security Services, help to prevent cyberattacks and mitigate security risks with consistent, real-time protection and responses against even the newest and most sophisticated threats.	Hardware	Firewall

Source: Company Website

17.1.4.3 Recent developments

17.1.4.3.1 Product launches & enhancements

TABLE 599 FORTINET: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
March 2026	Hardware expansion	Fortinet (US)	FortiDDoS 3000G (Hardware Appliance)	Fortinet added the FortiDDoS 3000G to its FortiDDoS hardware portfolio. The official Fortinet documentation published in March 2026 lists the new model, expanding the company's purpose-built appliance portfolio for protecting network infrastructure against DDoS attacks. FortiDDoS provided autonomous detection and mitigation using behavioral analysis and full packet inspection.
September 2025	Product enhancement	Fortinet (US)	FortiAppSec Cloud (Cloud-based WAAP Platform)	Fortinet expanded its cloud application security portfolio and made FortiAppSec Cloud available through AWS Marketplace. The platform combined web application firewall, bot management, API security, and DDoS mitigation capabilities, extending Fortinet's application-layer DDoS protection availability for cloud environments.

Source: Press Releases

17.1.4.4 MnM view

17.1.4.4.1 Key strengths

Fortinet has developed a robust product portfolio over the years, offering a diverse range of solutions to its customers. This variety enables the company to cater to different segments within the software and programming industry. Additionally, Fortinet's global offerings allow it to reach a broader market, solidifying its position as a key player in the DDoS protection and mitigation market.

17.1.4.4.2 Strategic choices

Fortinet takes its R&D investments seriously and focuses on consumer-driven innovation, which helps it sustain strong competition. Increasing government regulations have restricted unorganized players from entering the market, which gives Fortinet a chance to grow.

17.1.4.4.3 Weaknesses and competitive threats

Companies continuously launch new products in the market. Additionally, due to its large customer base, Fortinet may take time to respond to niche customer needs. This can lead to competitive disadvantages for Fortinet, thereby affecting the overall growth of the company in the DDoS protection & mitigation market.

17.1.5 NETSCOUT

17.1.5.1 Business overview

NETSCOUT is a US-based cybersecurity and network observability company specializing in network detection and response, deep packet inspection, performance management, and DDoS protection. The company provides solutions for enterprises, service providers, and public-sector organizations to improve network visibility, availability, security, and operational resilience. Its overall portfolio includes the Arbor DDoS Protection portfolio, Omnis network visibility and cybersecurity solutions, nGenius service assurance solutions, and threat intelligence capabilities powered by NETSCOUT's ATLAS platform.

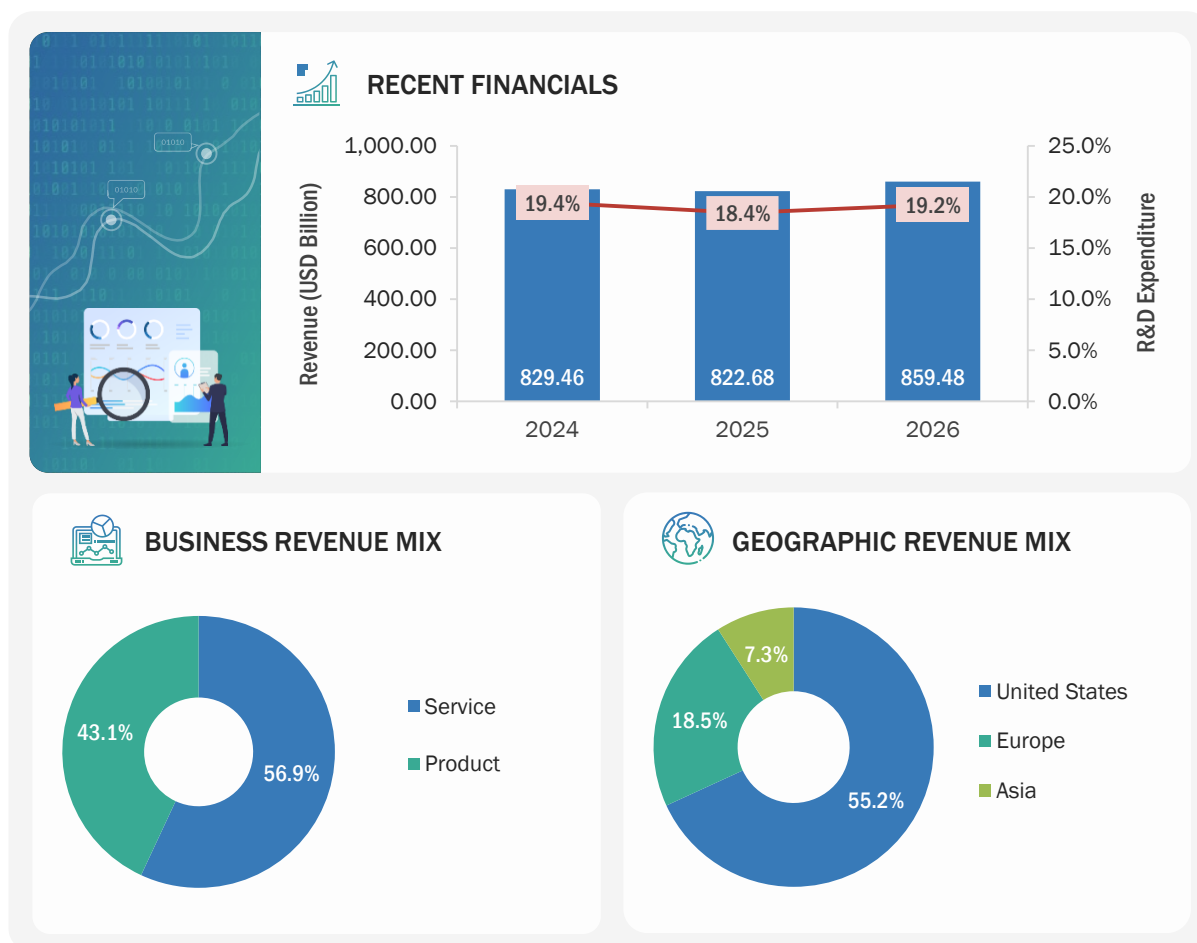
NETSCOUT's Arbor DDoS Protection portfolio provides multi-layered protection across on-premises, cloud, and hybrid environments. Key offerings include Arbor Edge Defense (AED) for always-on inline protection, Arbor Cloud for cloud-based traffic scrubbing, Arbor Threat Mitigation System (TMS) for high-capacity mitigation, and Arbor Sightline for network-wide DDoS detection and visibility. These solutions leverage AI-driven analytics and the ATLAS Intelligence Feed to identify and mitigate volumetric, protocol, application-layer, and multi-vector attacks. Arbor Cloud currently provides 33 Tbps of mitigation capacity across 16 global scrubbing centers, while Arbor TMS can scale to 50 Tbps in a single deployment.

NETSCOUT serves organizations across industries including telecommunications, financial services, government, healthcare, education, manufacturing, retail, transportation, and utilities. The company supports a global ecosystem of enterprises, service providers, technology partners, and public-sector organizations, with technology partnerships including AWS, Cisco, F5, Google Cloud, Microsoft, Palo Alto Networks, and Splunk. Its DDoS capabilities are further supported by global threat intelligence and the ATLAS data-sharing ecosystem.

TABLE 600 **NETSCOUT: COMPANY OVERVIEW**

NETSCOUT	
Founded	1984
Country	US
City	Westford, Massachusetts
Ownership	Public (NASDAQ: NTCT)

Source: Company Website

FIGURE 54 NETSCOUT: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and MarketsandMarkets Analysis

17.1.5.2 Products/Solutions/Services offered

TABLE 601 NETSCOUT: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/SOLUTION/SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Arbor Sightline Network Visibility Software	It provides robust capabilities, from network-wide capacity planning to identifying and managing the mitigation and detection of DDoS and other threats to the network.	Solution	Identification & mitigation
Arbor Sightline with Sentinel for Mitigating DDoS Attacks	Sightline with Sentinel integrates network infrastructure defense functionality and orchestrated mitigation support to deliver unparalleled protection at a lower cost than any other solution.	Solution	DDoS mitigation
Arbor Edge Defense	It is an inline defense application that automatically detects and stops inbound DDoS threats.	Solution	Security
Arbor Threat Mitigation Systems	This system removes DDoS attack traffic from the network without any disruption in network services.	Solution	Mitigation
Arbor Managed DDoS Protection Services	It is fully managed DDoS protection backed by a world-class Security Operations Center (SOC).	Service	Security

Arbor Cloud	Arbor Cloud is a fully managed DDoS attack protection service that provides 33 Tbps of mitigation capacity through 16 worldwide scrubbing centers, delivering global protection against large-scale DDoS attacks.	Service	Security & mitigation
-------------	---	---------	-----------------------

Source: Company Website

17.1.5.3 Recent developments

17.1.5.3.1 Product launches & enhancements

TABLE 602 NETSCOUT: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
March 2025	Product launch	NETSCOUT (US)	Arbor Threat Mitigation System (TMS)	NETSCOUT launched its enhanced Arbor Threat Mitigation System (TMS), featuring advanced AI- and ML-driven capabilities for adaptive DDoS protection. The upgraded solution leveraged global threat intelligence from the ATLAS Intelligence Feed to detect, analyze, and mitigate complex attacks more effectively, enabling service providers and enterprises to ensure stronger network resilience and minimize downtime.

Source: Press Releases

17.1.5.3.2 Expansions

TABLE 603 NETSCOUT: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
June 2024	Expansion	Facility	Canada	NETSCOUT (US)	NETSCOUT announced that it expanded its Arbor Cloud DDoS attack mitigation network to 16 scrubbing centers worldwide with the recent addition of a new Toronto facility. This network offered ISPs and enterprise customers more than 15 terabits per second (Tbps) of dedicated attack capacity.

Source: Press Releases

17.1.5.4 MnM view

17.1.5.4.1 Right to win

NETSCOUT is a key market player catering to more than 20,000 enterprise customers across the globe. It provides DDoS protection and mitigation solutions for various environments, including on-premises, cloud, and hybrid systems. This has enabled the company to maintain a large customer base across significant sectors such as healthcare, manufacturing, retail, insurance, education, transportation, and government. The proliferation in demand for cloud-based DDoS protection has been in favor of NETSCOUT for years.

17.1.5.4.2 Strategic choices

NETSCOUT is expanding its reach into adjacent complementary markets by expanding, enhancing, and integrating its product portfolio. Partnerships have helped the company strengthen its product capabilities and enabled it to stay competitive in the market. The company invests in R&D and leverages its strong technical and domain expertise across organizations.

17.1.5.4.3 Weaknesses and competitive threats

NETSCOUT faces problems while moving to other segments. Intense competition from competitors, rapidly changing cybersecurity demands, and the development of similar products from competitors are some problems the company faces from time to time. NETSCOUT focuses more on monitoring solutions than on traffic analysis. However, its solutions do not have the ability to retrieve data. The company faces strong competition from other market players offering similar products in the market.

17.1.6 NEXUSGUARD

17.1.6.1 Business overview

Nexusguard is a leader in cloud-based Distributed Denial of Service (DDoS) security, primarily serving as a specialized Managed Security Service Provider (MSSP) for communication service providers (CSPs) and large enterprises. Its core business model centers on ensuring uninterrupted internet service and infrastructure availability through a multi-layered defense architecture. The company's comprehensive solution suite includes Application Protection for securing websites and APIs, Origin Protection for backend infrastructure, and DNS Protection to safeguard critical naming services. A key offering is Nexusguard Bastions, a carrier-grade, multi-tenant DDoS protection platform designed to serve a dual role: enabling Communications Service Providers to protect their own network and infrastructure at scale, while also acting as a fully productized, turnkey foundation for delivering managed security services to end customers. Bastions supports sovereign-grade deployment models and can be operated directly by Nexusguard or by partners as part of their own managed security offerings. Additionally, the company provides managed Security Operations Center (SOC) services.

Geographically, Nexusguard maintains a robust global footprint with a massive, distributed scrubbing network comprising over 60 dedicated centers and a total mitigation capacity exceeding 3 Tbps. While headquartered in Singapore, it operates major regional offices in San Francisco and Hong Kong, with a physical and operational presence spanning across the globe. Its growth is heavily driven by its Transformational Alliance Partner (TAP) program, a strategic initiative designed to help traditional Managed Service Providers (MSPs) and Telcos transition into MSSPs. This partnership strategy focuses on "DDoS productization," enabling partners to offer co-branded or white-labeled security services with minimal capital expenditure.

TABLE 604 NEXUSGUARD: COMPANY OVERVIEW

NEXUSGUARD	
Founded	2008
Country	Singapore
City	Singapore
Ownership	Private

Source: Company Website

17.1.6.2 Products/Solutions/Services offered

TABLE 605 NEXUSGUARD: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Nexusguard DDoS Protection	The Nexusguard DDoS Solution is a unified, cloud-based mitigation platform that provides a multi-layered defense to ensure 24/7 availability and performance. It integrates Application Protection for Layer 7 web threats, Origin Protection for Layer 3/4 network infrastructure, and DNS Protection to safeguard domain resolution. By leveraging a global scrubbing network, it neutralizes both volumetric floods and sophisticated targeted attacks before they can impact your services.	Platform	DDoS protection & mitigation

Nexusguard Bastions	Nexusguard Bastions is a carrier-grade, DDoS mitigation platform designed specifically for Communications Service Providers (CSPs) and ISPs. It integrates on-premises hardware with Nexusguard's global scrubbing cloud, allowing providers to secure their own infrastructure while simultaneously offering branded security services to their customers.	Platform	DDoS mitigation
---------------------	---	----------	-----------------

Source: Company Website

17.1.6.3 Recent developments

17.1.6.3.1 Product launches & enhancements

TABLE 606 NEXUSGUARD: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
February 2025	Product enhancement	Nexusguard (Singapore)	TCP Connection Flood Protection (DDoS Protection Capability)	Nexusguard introduced and documented enhanced TCP Connection Flood Protection capabilities designed to safeguard server resources and service availability against TCP connection flood attacks. The capability strengthened Nexusguard's behavioral and protocol-level DDoS mitigation approach by identifying and filtering malicious connection attempts while allowing legitimate traffic to continue reaching protected infrastructure.
May 2024	Product enhancement	Nexusguard (Singapore)	Nexusguard On-Net (DDoS Protection Service)	Nexusguard enhanced its On-Net DDoS protection approach for network infrastructure by combining segregated Internet uplinks, automated route announcements, and rapid traffic diversion. The solution is designed to improve resilience against volumetric attacks and provide more efficient cloud diversion and routing policy management for protected infrastructure.

Source: Press Releases

17.1.6.3.2 Deals

TABLE 607 NEXUSGUARD: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
September 2025	Collaboration	Nexusguard (Singapore)	Eastern Communications (Philippines)	Nexusguard collaborated with Eastern Communications, a telecom provider in the Philippines. This strategic collaboration combined Nexusguard's cloud-based DDoS protection with Eastern Communications' robust infrastructure to provide scalable cybersecurity solutions. The partnership aimed to safeguard Philippine enterprises and government agencies through the "DDoS-Protected Eastern IDS," ensuring reliable connectivity and business continuity.
April 2025	Partnership	Nexusguard (Singapore)	Cellcard (Cambodia)	Nexusguard partnered with Cellcard to introduce enterprise-grade DDoS protection featuring Cambodia's first local scrubbing center. This "true hybrid" defense model optimized performance and reduced latency, providing high-level security tailored specifically for the country's financial and public sectors.
September 2024	Partnership	Nexusguard (Singapore)	Wind Telecom (Dominican Republic)	Nexusguard partnered with Wind Telecom, a telecom company, to offer advanced cybersecurity tools, including DDoS protection and DNS security. This initiative is designed to empower Dominican businesses with robust solutions to mitigate data vulnerabilities and enhance digital resilience.

Source: Press Releases

17.1.7 HUAWEI

17.1.7.1 Business overview

Huawei is a global provider of information and communications technology (ICT) infrastructure, cloud services, smart devices, and digital solutions. Founded in 1987, the company operates across enterprise, carrier, consumer, cloud, and digital power businesses. Its broad portfolio includes telecommunications network equipment, data center and cloud infrastructure, networking, storage, AI platforms, cybersecurity solutions, and smart devices. Within cybersecurity, Huawei offers solutions across network security, firewalls, endpoint security, anti-DDoS, advanced threat protection, security operations, and security management.

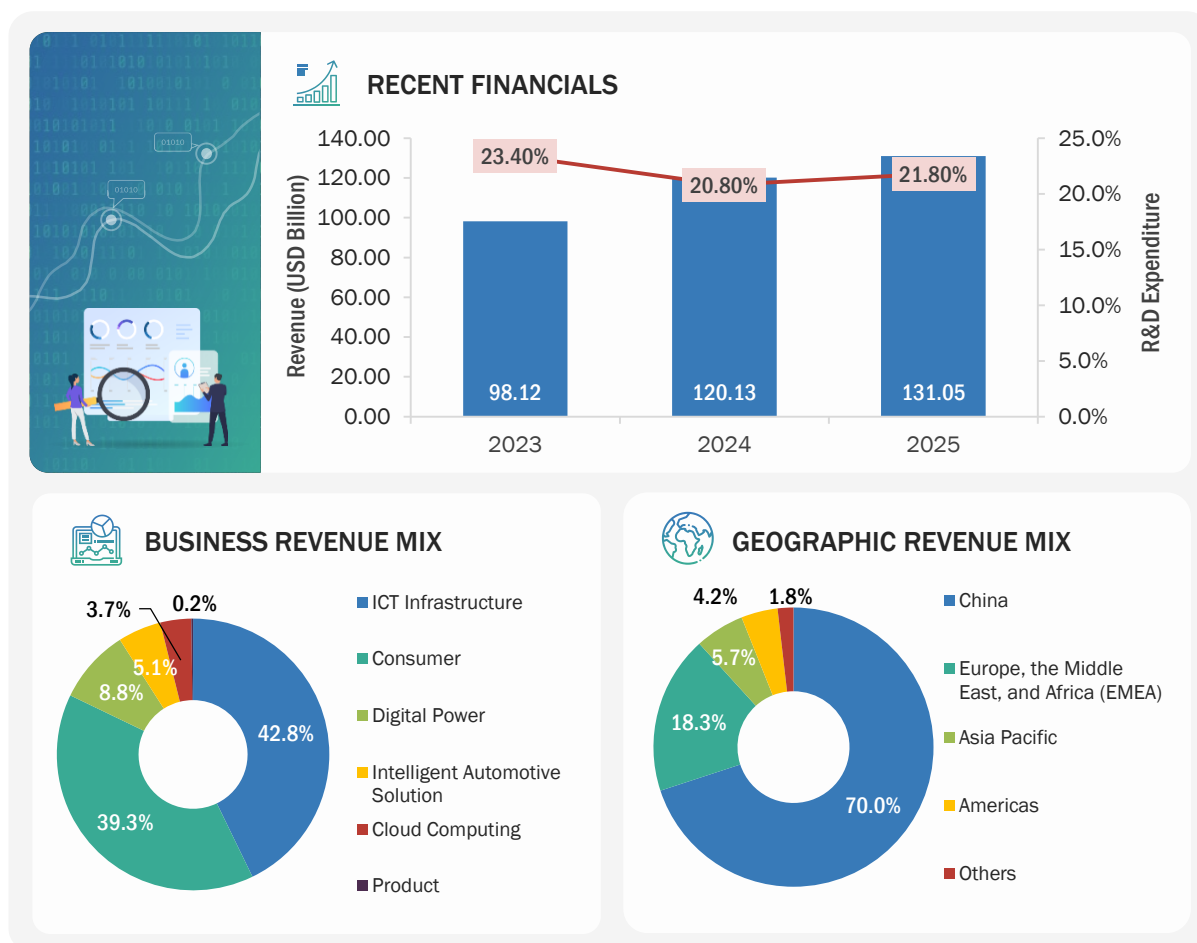
Huawei's DDoS protection portfolio includes the AntiDDoS1000 Series, AntiDDoS8000 DDoS Protection System, and HiSecEngine AntiDDoS12000 Series DDoS Defense System. These solutions provide carrier- and enterprise-grade protection against volumetric, protocol, and application-layer DDoS attacks through traffic analysis, behavioral modeling, per-packet inspection, and automated mitigation. The AntiDDoS8000 supports modeling for 60+ traffic types and defense against 100+ attack types, while integrating with cloud scrubbing centers for multi-layered protection. The AntiDDoS12000 Series provides up to 2.4 Tbps protection performance per device and supports millisecond-level response to high-volume attacks. Huawei's portfolio supports on-premises and hybrid defense architectures for protecting network links and online services.

Huawei serves telecommunications carriers, enterprises, governments, data centers, and large Internet content providers globally. Its cybersecurity and DDoS solutions support industries including telecommunications, government, financial services, energy and utilities, transportation, manufacturing, and other critical infrastructure sectors. Huawei operates in more than 170 countries and has offices in Asia Pacific, Europe, Latin America, the Middle East & Africa, and North America.

TABLE 608 HUAWEI: COMPANY OVERVIEW

HUAWEI	
Founded	1987
Country	China
City	Shenzhen
Ownership	Private

Source: Company Website

FIGURE 55 HUAWEI: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and MarketsandMarkets Analysis

17.1.7.2 Products/Solutions/Services offered

TABLE 609 HUAWEI: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Huawei AntiDDoS8000 DDoS Protection System	Huawei AntiDDoS8000 DDoS Protection System provides carrier-grade, multi-layer DDoS protection with Terabit-level defense capacity and second-level attack response. The system uses big data analysis and traffic modeling across 60+ traffic types to detect and mitigate 100+ attack types across Layers 3, 4, and 7. It supports protection for network links and online services, including web, DNS, DHCP, and VoIP, and can integrate with cloud scrubbing centers for hybrid DDoS defense.	Hardware	- Telecommunications - ISPs - large enterprises - data centers - internet content providers
Huawei HiSecEngine AntiDDoS12000 Series DDoS Defense System	Huawei HiSecEngine AntiDDoS12000 Series DDoS Defense System provides high-capacity DDoS defense for heavy-traffic attacks, with up to 2.4 Tbps protection performance per device. The solution combines per-packet traffic inspection, network processor-	Hardware	- Telecommunications - ISPs - large enterprises - data centers - internet content providers

accelerated defense, behavioral analysis, machine learning, automated policy tuning, and Layer 7 intelligent filtering to mitigate complex network-, protocol-, and application-layer DDoS attacks, including zero-day threats.

Huawei
AntiDDoS1000
Series DDoS
Protection Systems

Huawei AntiDDoS1000 Series DDoS Protection Systems provide dedicated anti-DDoS protection for enterprise networks and online services, enabling organizations to detect and mitigate DDoS attacks targeting network infrastructure. The appliance-based solution is designed to protect business-critical services and IT infrastructure through dedicated DDoS defense capabilities.

Hardware

- Enterprises
- financial institutions
- ISPs

Source: Company Website

17.1.7.3 Recent developments

17.1.7.3.1 Product launches & enhancements

TABLE 610 HUAWEI: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
May 2024	Product launch	Huawei (China)	HiSecEngine Anti-DDoS Series System (Hardware)	Huawei launched the HiSecEngine Anti-DDoS series system as part of its intelligent Anti-DDoS portfolio. The system combined high-performance NP and CPU collaborative acceleration, defense against concurrent carpet-bombing attacks, and decryption-less protection against encrypted application-layer attacks. Huawei stated that a single device can provide up to 2.4 Tbps of defense performance and protect more than 2,000 address segments concurrently.

Source: Press Releases

17.1.8 LINK11

17.1.8.1 Business overview

Link11 is a cloud cybersecurity company specializing in DDoS protection, web application and API security, and application performance. Founded in 2005, the company focuses on strengthening the cyber resilience and availability of networks and critical digital services. Its overall portfolio includes Network DDoS Protection, Web Application & API Protection (WAAP), Secure CDN, Secure DNS, Web Application Firewall, Bot Management, API Security, and Web DDoS Protection. Link11 delivers its services through a globally distributed cloud platform and serves organizations requiring continuous protection of network infrastructure, web applications, and digital services.

Link11's DDoS protection portfolio comprises Network DDoS Protection and Web DDoS Protection, with the latter integrated into its WAAP platform. Network DDoS Protection provides cloud-based Layer 3 and Layer 4 mitigation using adaptive behavioral and protocol-based analysis, automated thresholds, and granular filtering. Web DDoS Protection safeguards web applications and APIs against Layer 7 attacks, including HTTP floods and other application-layer attack methods, using AI-driven traffic analysis and fingerprinting technology. The company's DDoS platform provides patented, self-learning protection across Layers 3, 4, and 7, with automated mitigation, Always-On deployment options, and SLA-backed protection bandwidths.

Link11 serves organizations in regulated and critical sectors, including financial services, logistics, healthcare, government, telecommunications, and other critical infrastructure environments. Its customer references include companies such as Hermes, Bank-Verlag, Beiersdorf, and Scalable Press. The company operates globally, with offices and operations across Europe, North America, Asia, and the Middle East, and supports customers through a partner ecosystem offering network security, web protection, and application performance solutions.

TABLE 611 LINK11: COMPANY OVERVIEW

LINK11	
Founded	2005
Country	Germany
City	Frankfurt
Ownership	Private

Source: Company Website

17.1.8.2 Products/Solutions/Services offered

TABLE 612 LINK11: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Network DDoS Protection	Network DDoS Protection is a cloud-based Layer 3/4 DDoS mitigation service that uses adaptive behavioral and protocol-based analysis, auto-learning thresholds, granular filtering, and automated mitigation to protect networks and infrastructure from volumetric and protocol attacks. The solution provides real-time visibility into mitigation actions and supports protection of critical infrastructure, network devices, APIs, and web applications against network-layer floods.	Software/ platform	Financial services, logistics, healthcare, government, telecommunications, critical infrastructure

Web DDoS Protection	Web DDoS Protection is cloud-based Layer 7 DDoS protection integrated within Link11's Web Application & API Protection (WAAP) platform. It uses behavioral techniques, AI-driven analysis, traffic fingerprinting, global load balancing, and automated scaling to detect and mitigate HTTP floods, Slowloris, protocol abuse, and other application-layer attacks while maintaining availability of web applications and APIs.	Software/ platform	Financial services, eCommerce, logistics, healthcare, government, technology
Secure CDN	Secure CDN is a secure content delivery network designed to improve content availability and performance while incorporating Layer 3/4 DDoS protection across CDN nodes. The solution supports content caching, origin load reduction, load balancing, and delivery of streaming and video-on-demand services, with integration into Link11's broader security portfolio for additional application protection.	Software/ platform	Media & entertainment, streaming, eCommerce, technology, gaming, digital services

Source: Company Website

17.1.8.3 Recent developments

17.1.8.3.1 Product launches & enhancements

TABLE 613 LINK11: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
July 2026	Product launch	Link11 (Germany)	Next-Gen Network DDoS Protection (Software/Platform)	Link11 launched its next-generation Network DDoS Protection solution after rebuilding its Layer 3/4 mitigation architecture. The platform combined behavior-based detection, deep learning, full IPv4 and IPv6 coverage, deeper state tracking, protocol awareness, and auto-learning thresholds. It provided targeted mitigation for individual attack vectors and reduced mitigation time for unknown vectors to under three seconds
May 2025	Product Launch	Link11 (Germany)	Link11 WAAP (Web Application & API Protection) SaaS (Platform)	Link11 GmbH introduced its newly branded unified platform by combining the three brands (Link11, DOSarrest, and Reblaze) into one integrated offering.

Source: Press Releases

17.1.8.3.2 Deals

TABLE 614 LINK11: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
May 2025	Strategic partnership	Link11 (Germany)	evoila (Germany)	Link11 and evoila established a strategic partnership to expand evoila's cybersecurity portfolio with Link11's DDoS protection, WAF, and API security solutions. The collaboration followed the integration of Link11 services into evoila's Security Operations Center and Security 360° approach and targeted critical infrastructure and international markets.
January 2024	Acquisition	Link11 (Germany)	Reblaze Technologies (Israel)	Link11 completed the acquisition of Reblaze Technologies, a provider of cloud-native WAAP solutions. The acquisition expanded Link11's international presence and strengthened its portfolio across web application and API security, complementing its existing Network and Web DDoS Protection capabilities. Financial terms of the transaction were not disclosed.

Source: Press Releases

17.1.9 THALES (IMPERVA)

17.1.9.1 Business overview

Thales is a global technology and cybersecurity company providing solutions across defense, aerospace, cyber and digital technologies. Within cybersecurity, the company focuses on protecting applications, data, identities, AI, and software through an integrated portfolio of security platforms. Its broader cybersecurity portfolio includes the Imperva Application Security Platform, CipherTrust Data Security Platform, SafeNet Trusted Access, hardware security modules, encryption, key management, identity and access management, and cybersecurity services. Thales significantly expanded its application security portfolio through the completed acquisition of Imperva in December 2023, integrating Imperva's capabilities into its cybersecurity business.

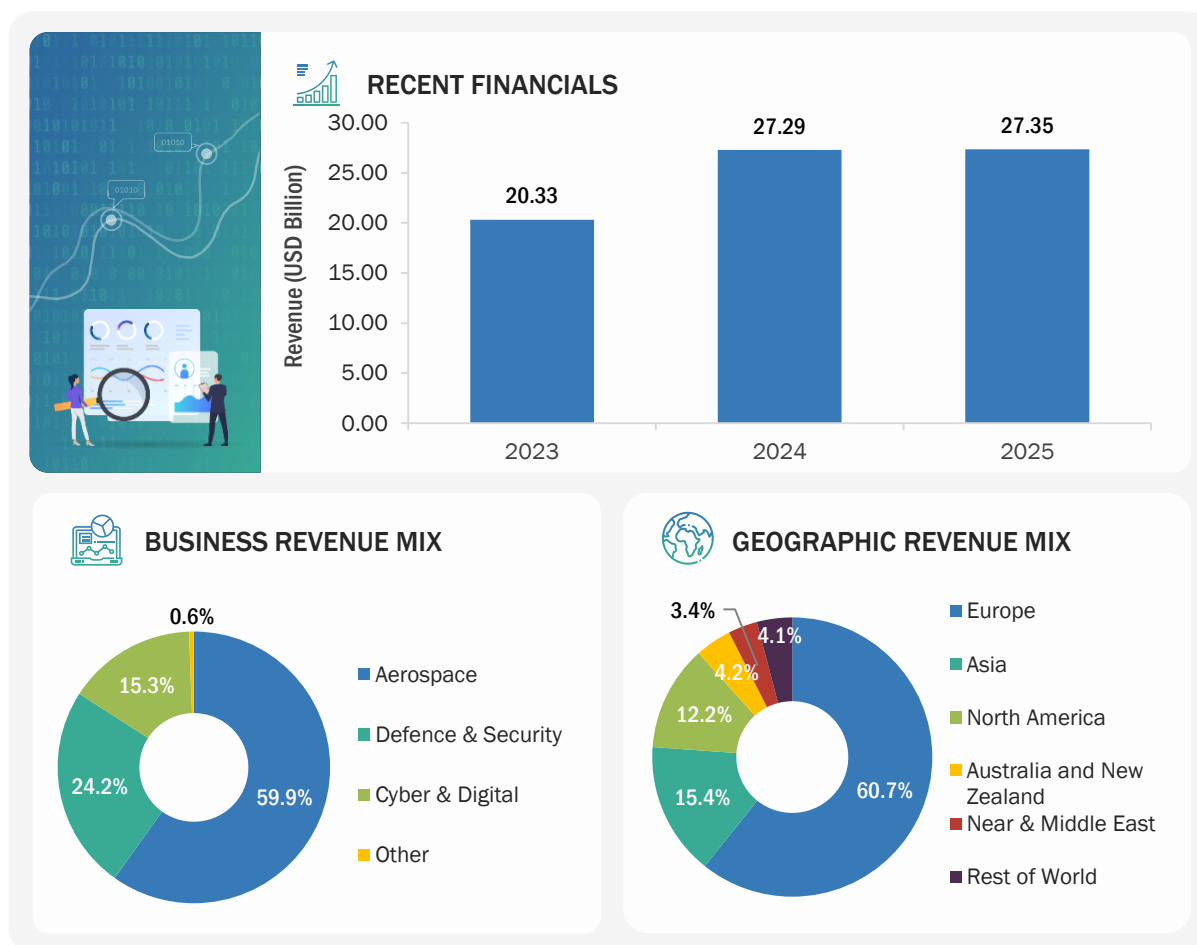
For the DDoS protection and mitigation market, Thales offers Imperva DDoS Protection, part of the Imperva Application Security Platform. The platform provides protection against volumetric, protocol-based, and application-layer attacks across Layers 3, 4, and 7. Imperva DDoS Protection supports automated, always-on mitigation for websites, networks, DNS infrastructure, and individual IP addresses, using a globally distributed mitigation network and proprietary detection techniques. The offering is backed by a 3-second mitigation SLA for Layer 3 and Layer 4 DDoS attacks, along with 24/7 security operations and threat intelligence from Imperva Research Labs.

Thales serves more than 30,000 organizations globally, with cybersecurity solutions deployed across 148 countries. Its customer base spans industries including financial services, telecommunications, government, energy, healthcare, retail, eCommerce, and other critical infrastructure sectors. The company supports customers through its global cybersecurity operations and partner ecosystem, combining application, data, and identity security capabilities to protect complex digital environments.

TABLE 615 THALES (IMPERVA): COMPANY OVERVIEW

THALES (IMPERVA)	
Founded	2000
Country	France
City	La Défense
Ownership	Public (EPA: H0)

Source: Company Website

FIGURE 56 THALES (IMPERVA): COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and MarketsandMarkets Analysis

17.1.9.2 Products/Solutions/Services offered

TABLE 616 THALES (IMPERVA): PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Imperva DDoS Protection for Websites	Imperva DDoS Protection for Websites provides always-on protection for websites, web applications, and APIs against application-layer DDoS attacks. The service routes HTTP/S traffic through Imperva's secure proxy and global mitigation network to filter malicious traffic, protect origin infrastructure, and maintain application availability.	Software/ platform	BFSI, retail & eCommerce, technology, healthcare, media & entertainment, government
Imperva DDoS Protection for Networks	Imperva DDoS Protection for Networks provides always-on and on-demand protection for enterprise networks and subnets against volumetric and multi-vector Layer 3 and Layer 4 DDoS attacks. It uses Imperva's global scrubbing infrastructure, high-capacity packet processing, flow-based monitoring, and automated or manual traffic diversion to protect network infrastructure.	Software/ platform	Telecommunications, BFSI, government, energy & utilities, data centers, critical infrastructure

Imperva DDoS Protection for Individual IPs	Imperva DDoS Protection for Individual IPs provides always-on protection for Internet-facing services hosted on individual public IP addresses across on-premises and cloud environments. The service mitigates Layer 3 and Layer 4 attacks and is designed for organizations that need to protect specific non-HTTP assets or services without routing an entire network through a cloud-based security platform.	Software/ platform	Cloud & hosting, technology, BFSI, telecommunications, government, digital services
Imperva DNS Protection	Imperva DNS Protection provides always-on protection for authoritative DNS infrastructure against volumetric, protocol-based, amplification, and other DNS-targeted DDoS attacks. The service uses Imperva's globally distributed Anycast network to scrub malicious queries before they reach authoritative DNS servers while providing DNS traffic visibility, analytics, and policy controls.	Software/ platform	BFSI, government, telecommunications, eCommerce, technology, critical infrastructure

Source: Company Website

17.1.9.3 Recent developments

17.1.9.3.1 Product launches & enhancements

TABLE 617 THALES (IMPERVA): PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
April 2026	Product launch	Thales (France)	Imperva for Google Cloud (Cloud Application Security Platform)	Thales introduced Imperva for Google Cloud in Controlled Availability, enabling Imperva's application security capabilities to operate directly within Google Cloud infrastructure through integration with Google Cloud Load Balancing and Private Service Connect. The offering supported protection of web applications and APIs while maintaining cloud-native traffic flows and centralized security management. As Imperva's Application Security platform incorporates DDoS protection capabilities, the launch expanded deployment options for its broader application-layer protection portfolio.
June 2025	Product enhancement	Thales (France)	Imperva Application Security (Software/Platform)	Thales enhanced the Imperva Application Security platform with integrated API detection and response capabilities, enabling real-time detection and automated mitigation of API threats. While the enhancement was primarily API-security focused, it strengthened Imperva's unified application security architecture, which also incorporated protection against application-layer DDoS attacks across web applications and APIs.

Source: Press Releases

17.1.10 BT

17.1.10.1 Business overview

Formerly known as British Telecom (BT), BT Group is a telecommunications and technology company providing connectivity, networking, cloud, managed services, and cybersecurity solutions to consumers, businesses, public-sector organizations, and multinational enterprises. Its business portfolio spans fixed and mobile communications, IP voice, unified communications, networking, cloud services, IoT, managed services, and cybersecurity. Within its security portfolio, BT offers DDoS Security, Managed Firewall, Cloud Security, SASE, EDR & XDR Security, SIEM, Threat Intelligence, and Cyber Threat Management services.

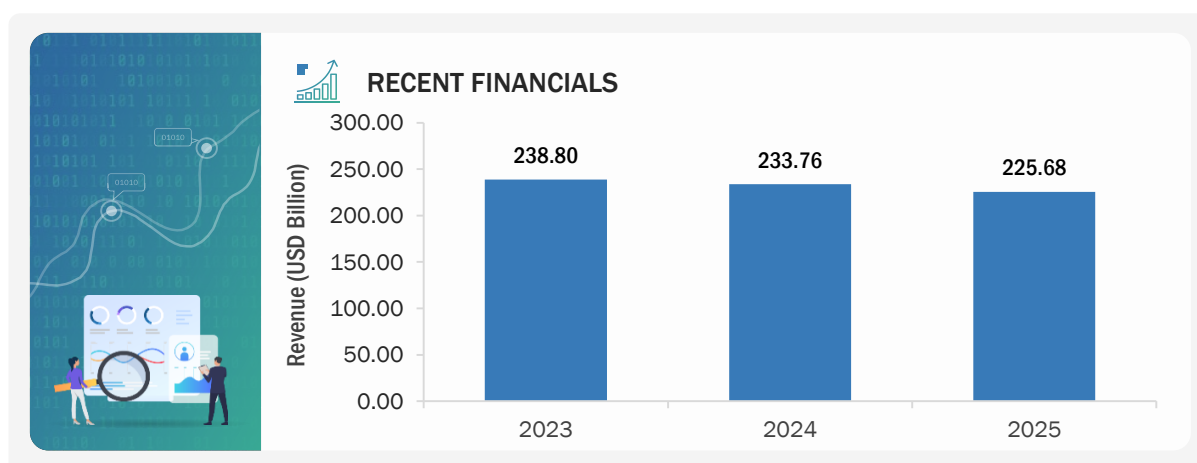
For the DDoS protection and mitigation market, BT offers DDoS Protection & Mitigation (Managed DDoS) as part of its managed security controls portfolio. The cloud-based service provides automated detection and mitigation of DDoS attacks before malicious traffic reaches an organization's network, helping maintain service availability during large-scale attacks. BT's offering is designed to address multiple DDoS attack types and provides centralized protection and mitigation capabilities supported by its security operations expertise. BT also states that its DDoS offering is developed in collaboration with Arbor, combining BT's managed security capabilities with DDoS protection technology and expertise.

BT serves organizations ranging from SMEs to large enterprises, government bodies, public-sector institutions, and multinational corporations. Its cybersecurity services support customers across industries including financial services, government, healthcare, telecommunications, retail, manufacturing, and critical infrastructure. BT supports its security portfolio through a global team of cybersecurity specialists and security operations centers, while partnering with technology providers to deliver managed security services. Its international infrastructure and service capabilities enable the company to support organizations internationally across approximately 180 countries in the UK, Europe, the Americas, and Asia-Pacific, Middle East, and Africa regions.

TABLE 618 BT: COMPANY OVERVIEW

BT	
Founded	1980
Country	England
City	London
Ownership	Public (LON: BT.A)

Source: Company Website

FIGURE 57 BT: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and Investor Presentations

17.1.10.2 Products/Solutions/Services offered

TABLE 619 BT: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
BT Managed DDoS Security	BT Managed DDoS Security is a cloud-based managed service that provides automated detection and mitigation of DDoS attacks before malicious traffic reaches the customer's network. The service profiles normal Internet traffic, monitors anomalous behavior, and supports automated alerts, traffic analysis, pre-approved or SOC-assisted mitigation, 24/7 service support, and reporting through a management portal. It is available for both on-net and off-net deployments, with Managed DDoS Edge Defence providing additional protection against application-layer attacks.	Service	DDoS protection & mitigation

Source: Company Website

17.1.11 A10 NETWORKS

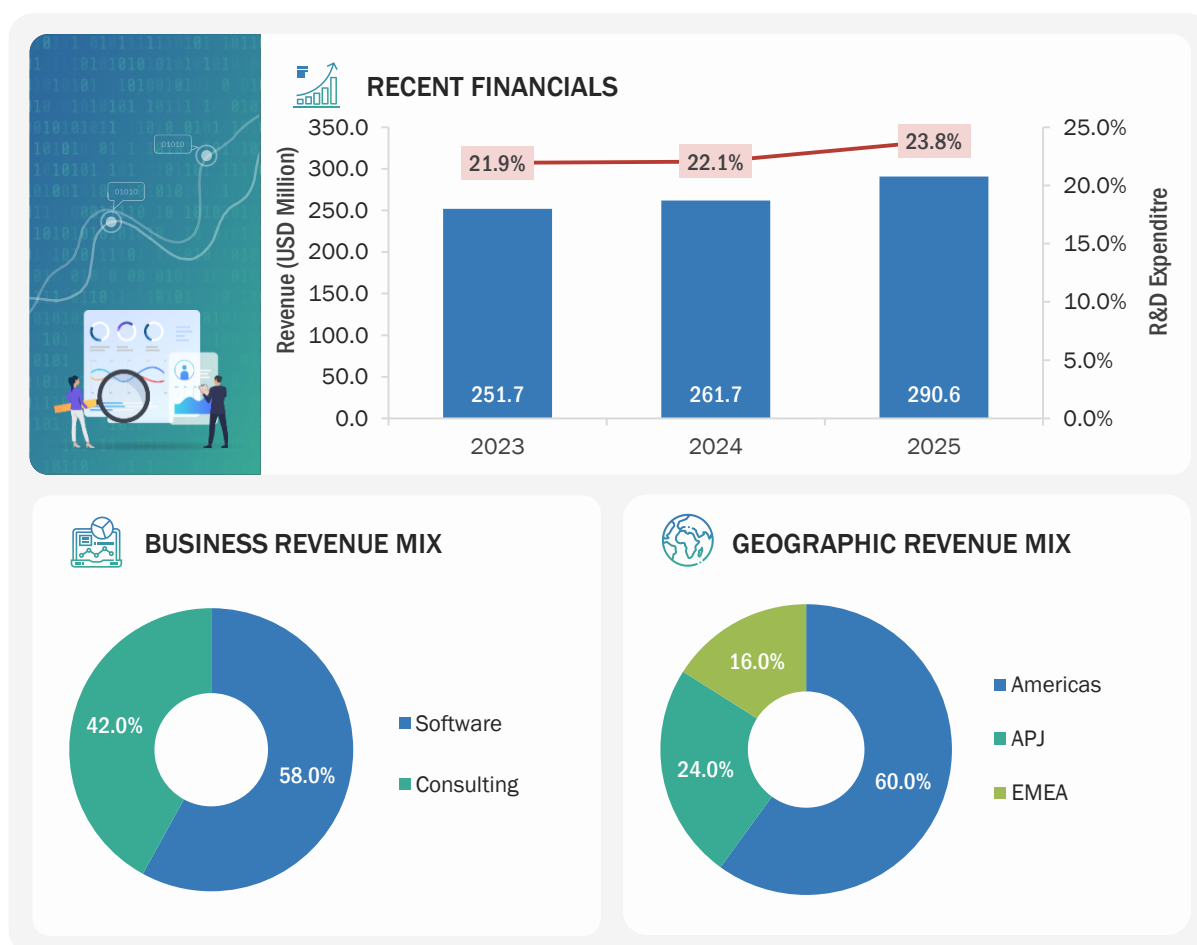
17.1.11.1 Business overview

A10 Networks is a cybersecurity company specializing in networking solutions. It offers a range of products, including Application Delivery Controllers (ADCs) for optimizing performance and security, DDoS protection through its Thunder Threat Protection System, and solutions for managing SSL/TLS traffic and Carrier-Grade NAT (CGNAT). A10 caters to industries like telecommunications, financial services, and government, with a global presence spanning the Americas, EMEA, and Asia Pacific. The company's strategy focuses on enhancing security for cloud and hybrid environments, driving security-driven networking, and leveraging automation and AI for optimized traffic management. Revenue is generated through a mix of product sales and recurring services, with a shift toward subscription-based models. A10 Networks competes with major players like F5 Networks and Cloudflare and is continually evolving its portfolio to meet the demands of 5G networks, edge computing, and cloud migration, ensuring high performance and security for modern data centers. A10 Networks has integrated intelligence and automation in its product portfolio and services. It promises to enable intelligent automation with deep ML to ensure that business-critical applications are protected, reliable, and always available. A10 Networks offers solutions for accelerating web application delivery, bandwidth management, and network identity issues.

TABLE 620 A10 NETWORKS: COMPANY OVERVIEW

A10 NETWORKS	
Founded	2004
Country	US
City	San Jose, California
Ownership	Public (NYSE: ATEN)

Source: Company Website

FIGURE 58 A10 NETWORKS: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.11.2 Products/Solutions/Services offered**TABLE 621** A10 NETWORKS: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
A10 Defend	A10's integrated DDoS defense portfolio designed to provide network-wide detection, mitigation, orchestration, and threat intelligence. The portfolio includes A10 Defend DDoS Detector, A10 Defend DDoS Mitigator, A10 Defend DDoS Orchestrator, and A10 Defend Threat Control, enabling automated detection and mitigation of volumetric, protocol, resource-exhaustion, and application-layer DDoS attacks. The solutions use behavioral profiling, machine learning, heuristic analysis, packet-level visibility, and automated mitigation policies to protect against known and zero-day attack vectors.	Software/ platform	Telecommunications, service providers, cloud & hosting providers, data centers, enterprises, gaming
A10 DDoS Security Incident Response Team (DSIRT)	A10 DDoS Security Incident Response Team (DSIRT) provides 24/7 incident response and technical support services to help organizations investigate and mitigate active DDoS attacks, restore service availability, and strengthen DDoS defense operations. The service is	Services	Telecommunications, service providers, cloud & hosting providers, data centers, enterprises

supported by A10's DDoS protection and threat intelligence capabilities.

Source: Company Website

17.1.11.3 Recent developments

17.1.11.3.1 Product launches & enhancements

TABLE 622 A10 NETWORKS: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
March 2024	Product launch	A10 Networks (US)	A10 Defend Threat Control (SaaS Platform)	A10 Networks launched A10 Defend Threat Control, a proactive DDoS threat intelligence SaaS platform and an addition to the A10 Defend suite. The platform provided actionable intelligence and insights on DDoS threats to support proactive defense, including information that can help organizations identify evolving attack trends and strengthen their overall DDoS protection posture.

Source: Press Releases

17.1.11.3.2 Deals

TABLE 623 A10 NETWORKS: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
February 2025	Acquisition	A10 Networks (US)	ThreatX Protect (US)	A10 Networks completed the acquisition of certain assets and key personnel of ThreatX Protect, including its WAAP solution. The acquisition expanded A10's security portfolio and complemented its A10 Defend platform, which combines hybrid DDoS protection and threat intelligence with web application and bot protection. The acquired platform also strengthens A10's application-layer security capabilities.

Source: Press Releases

17.1.12 NSFOCUS

17.1.12.1 Business overview

NSFOCUS was founded in 2000 and is headquartered in Beijing, with an international headquarters in Santa Clara, California. It is one of the global leaders in holistic, carrier-grade cybersecurity, specializing in a hybrid defense model that integrates on-premises appliances with a globally distributed cloud scrubbing network. Its core business focuses on maintaining service availability for many of the world's largest telecommunications companies, financial institutions, and data center operators. The company's flagship DDoS protection suite consists of the Anti-DDoS System (ADS) for real-time mitigation, the Network Traffic Analyzer (NTA) for multi-stage detection, and the Anti-DDoS System Manager (ADS-M) for centralized multi-tenant management. To address large-scale volumetric threats, NSFOCUS offers its Cloud DPS (Distributed Protection Service) and the Active Defense Business Operating System (ADBOS), a smart traffic-scrubbing scheduling platform that allows organizations to seamlessly transition between local and cloud-based mitigation.

TABLE 624 NSFOCUS: COMPANY OVERVIEW

NSFOCUS	
Founded	2000
Country	China
City	Beijing
Ownership	Public (SHE: 300369)

Source: Company Website

17.1.12.2 Products/Solutions/Services offered

TABLE 625 NSFOCUS: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Cloud DDoS Protection Service (Cloud DPS)	It is a subscription-based cloud scrubbing service with over 7 Tbps of global capacity that provides sub-second detection and AI-powered mitigation for volumetric and application-layer attacks. It utilizes BGP or DNS diversion to mask origin IPs and clean traffic at the source, ensuring business continuity for enterprises and service providers without requiring on-site hardware. It also offers Managed Security Services, which include 24/7 monitoring, attack response, mitigation tuning, SLA-backed services, reporting, and dedicated SOC support.	Service	DDoS protection & mitigation
On-Premises DDoS Defenses (Anti-DDoS System – ADS)	It is a high-performance appliance-based suite that comprises ADS, NTA, and ADS-M, mitigating malicious traffic in real-time with scalable capacities ranging from 200 Mbps to 400 Gbps. It leverages multi-stage inspection engines and behavioral analysis to accurately block sophisticated DDoS threats while maintaining extremely low latency for legitimate user traffic. Network Traffic Analyzer (NTA): On-premises traffic monitoring and DDoS detection system that analyzes network flows to identify abnormal traffic patterns. Anti-DDoS System (ADS): On-premises mitigation appliance that blocks malicious traffic locally, protecting data centers and	Solution	DDoS protection & mitigation



	enterprise networks from DDoS attacks. Anti-DDoS System Manager (ADS-M): Centralized management platform that controls and orchestrates NTA and ADS devices, with support for hybrid cloud integration.		
Services	NSFOCUS offers various services, such as product support services, professional services, and managed security services.	Services	NA

Source: Company Website

17.1.13 MICROSOFT

17.1.13.1 Business overview

Microsoft is a global technology company providing cloud computing, enterprise software, cybersecurity, productivity, AI, data, and infrastructure solutions. Its broad portfolio includes Microsoft Azure, Microsoft 365, Dynamics 365, Windows, Microsoft Defender, Microsoft Sentinel, Microsoft Entra, Power Platform, GitHub, and Azure networking and security services. Through Azure, Microsoft delivers cloud infrastructure, application hosting, networking, data, analytics, AI, and security capabilities for organizations operating across public cloud, hybrid, and multicloud environments.

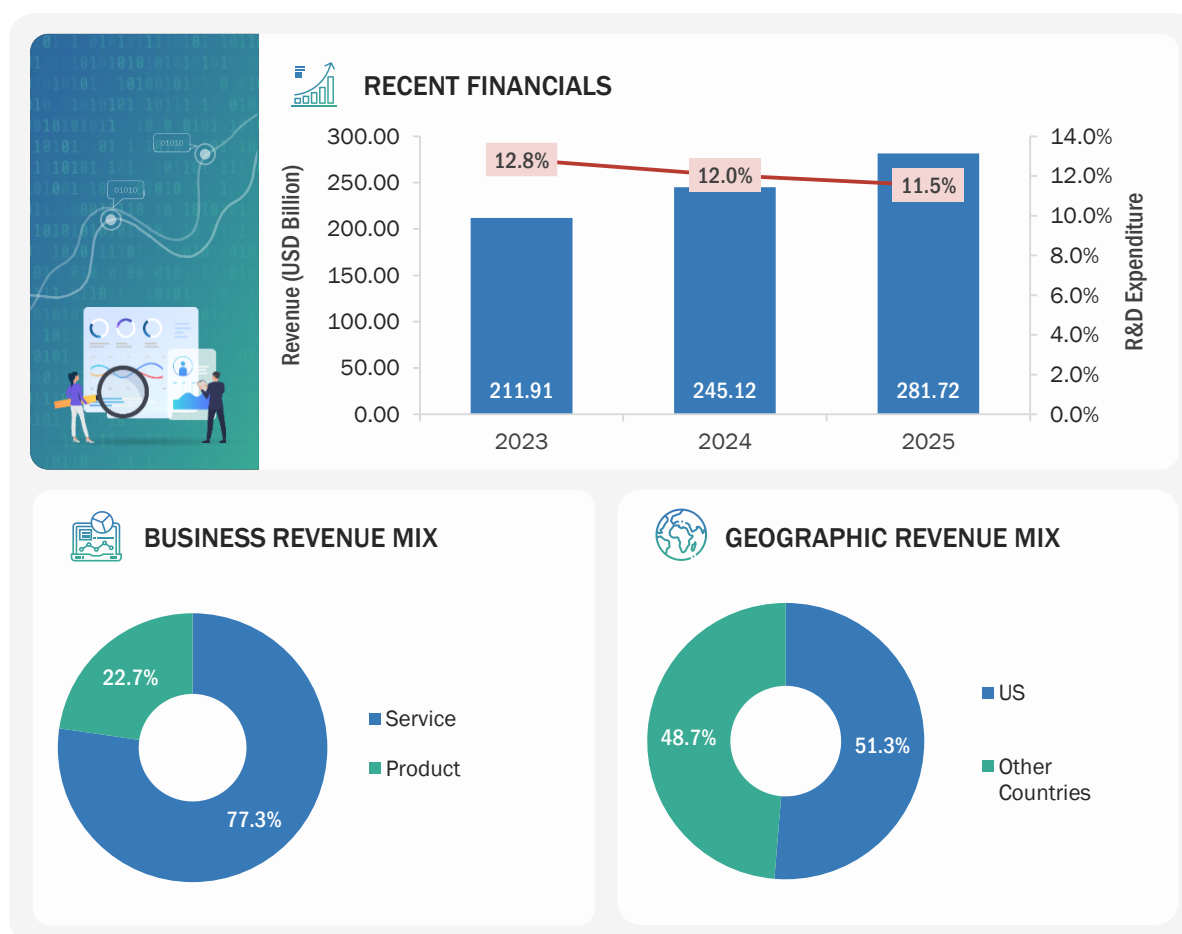
For the DDoS protection and mitigation market, Microsoft offers Azure DDoS Protection, comprising DDoS Network Protection and DDoS IP Protection. The service provides always-on traffic monitoring, adaptive real-time tuning, machine learning-based traffic profiling, automated detection, and mitigation of volumetric and protocol attacks targeting Azure resources. DDoS Network Protection secures public IP resources deployed within protected virtual networks, while DDoS IP Protection enables protection at an individual public IP level. The platform primarily provides Layer 3 and Layer 4 mitigation and can be combined with Azure Web Application Firewall for multilayer protection against application-layer attacks. Network Protection additionally provides DDoS Rapid Response support, cost protection, and WAF-related benefits.

Microsoft serves organizations across industries including BFSI, government, healthcare, retail, manufacturing, telecommunications, education, energy and utilities, media and entertainment, and technology. The company has a strong presence in North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America.

TABLE 626 MICROSOFT: COMPANY OVERVIEW

MICROSOFT	
Founded	1975
Country	US
City	Redmond, Washington
Ownership	Public (NASDAQ: MSFT)

Source: Company Website

FIGURE 59 MICROSOFT: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.13.2 Products/Solutions/Services offered**TABLE 627** MICROSOFT: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Azure DDoS Network Protection	Azure DDoS Network Protection provides enhanced DDoS mitigation for Azure resources deployed within protected virtual networks. The service uses always-on traffic monitoring, adaptive real-time tuning, machine learning-based traffic profiling, automated attack detection and mitigation, and telemetry and alerting capabilities to protect against volumetric and protocol-based attacks. It also includes value-added capabilities such as DDoS Rapid Response support, cost protection, and Web Application Firewall discounts.	Software/ platform	BFSI, government, healthcare, retail, manufacturing, telecommunications, energy & utilities, technology
Azure DDoS IP Protection	Azure DDoS IP Protection provides DDoS protection for individual Azure public IP resources through a pay-per-protected-IP model. It includes the same core detection and mitigation capabilities as Azure DDoS Network Protection, including always-on monitoring and adaptive traffic profiling, and is designed for organizations requiring protection for a smaller number of public-facing Azure resources.	Software/ platform	BFSI, government, healthcare, retail, manufacturing, telecommunications, technology, digital services

17.1.13.3 Recent developments

17.1.13.3.1 Product launches & enhancements

TABLE 628 MICROSOFT: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
April 2025	Product enhancement	Microsoft (US)	Azure DDoS Protection – Add to Existing DDoS Protection Plan (Software/Platform)	Microsoft introduced the “Add to existing DDoS Protection Plan” capability, enabling individual Public IP resources configured with Azure DDoS IP Protection to be associated with an existing Azure DDoS Network Protection plan. The enhancement provided greater deployment and cost-management flexibility by allowing organizations to extend protection across individual IPs under an existing DDoS protection architecture.
April 2025	Partner ecosystem expansion	Microsoft (US)	Azure DDoS Protection Partner Integration (Software/Platform)	Microsoft published and enabled an expanded partner onboarding framework for Azure DDoS Protection, allowing technology partners to integrate Azure-native DDoS mitigation into services such as load balancers, firewalls, and web application firewalls. Partners can also integrate DDoS attack analytics and telemetry into customer-facing platforms and offer Azure DDoS Protection as part of their services

Source: Press Releases

17.1.14 F5

17.1.14.1 Business overview

F5 is an application delivery and cybersecurity company that helps organizations secure, optimize, and manage applications and APIs across on-premises, cloud, hybrid, multicloud, and edge environments. The company's portfolio is centered on the F5 Application Delivery and Security Platform (ADSP) and includes application delivery controllers, load balancing, web application and API security, network security, DDoS protection, bot defense, API security, fraud prevention, and distributed cloud services. Key offerings include F5 Distributed Cloud Services, BIG-IP, NGINX, F5 Distributed Cloud WAF, BIG-IP Advanced Firewall Manager (AFM), and F5 Distributed Cloud DDoS Mitigation.

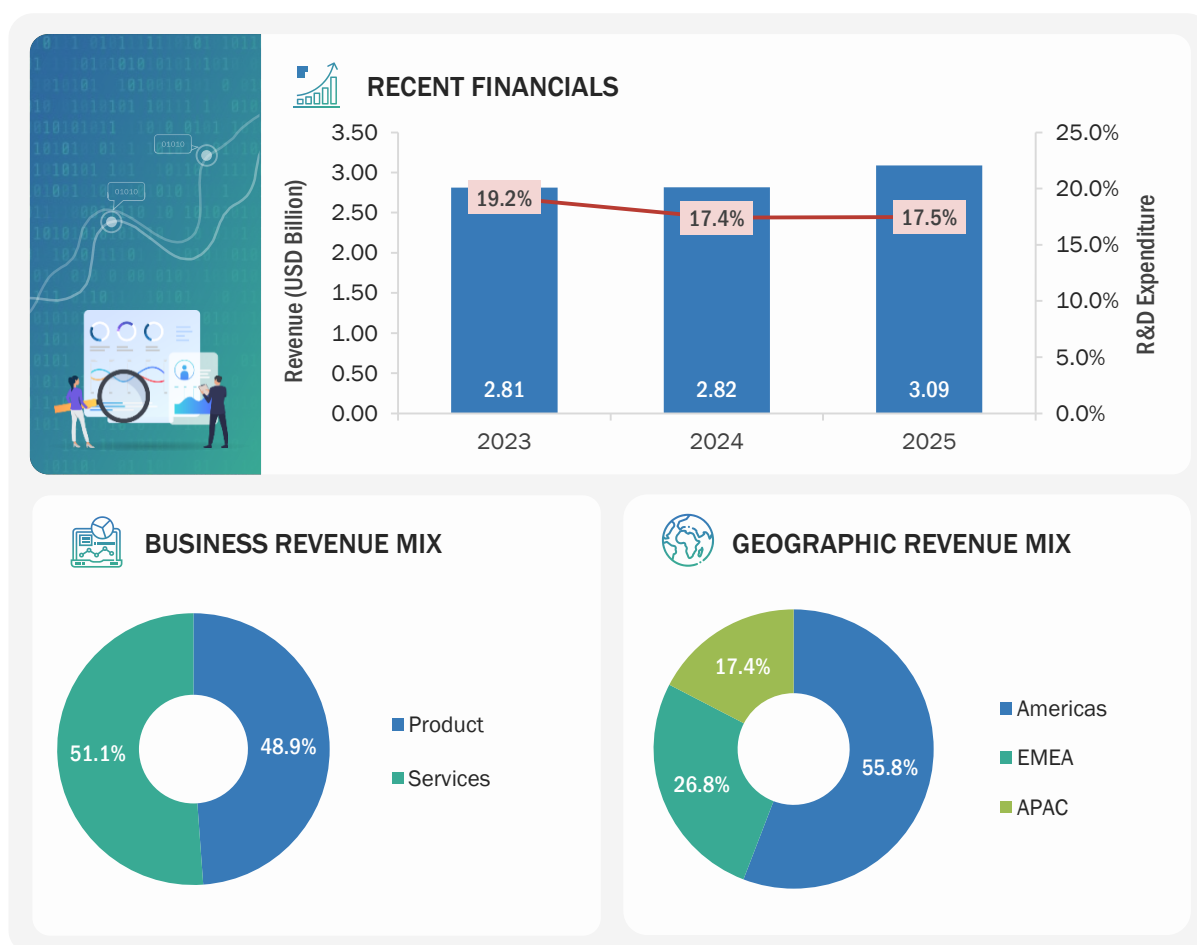
For the DDoS protection and mitigation market, F5 provides a multi-layered portfolio comprising F5 Distributed Cloud DDoS Mitigation, BIG-IP Advanced Firewall Manager (AFM), and NGINX App Protect DoS. F5 Distributed Cloud DDoS Mitigation is a cloud-delivered and managed service designed to detect and mitigate Layer 3–7 volumetric, protocol, DNS, SSL, and application-layer attacks before they reach customer infrastructure. BIG-IP AFM provides high-performance network-based DDoS protection alongside firewall, DNS security, and intrusion prevention capabilities, while NGINX App Protect DoS delivers behavioral application-layer DoS protection for modern cloud-native architectures. These offerings support cloud-based, on-premises, and hybrid DDoS defense models.

F5 serves organizations across industries including banking and financial services, government, healthcare, eCommerce, technology, telecommunications and service providers, manufacturing, and automotive. The company has a strong presence in North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America.

TABLE 629 F5: COMPANY OVERVIEW

F5	
Founded	1996
Country	US
City	Seattle, Washington
Ownership	Public (NASDAQ FFIV)

Source: Company Website

FIGURE 60 F5: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.14.2 Products/Solutions/Services offered**TABLE 630** F5: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
F5 Distributed Cloud DDoS Mitigation	F5 Distributed Cloud DDoS Mitigation is a cloud-delivered DDoS protection service that inspects, detects, and scrubs malicious traffic before it reaches network infrastructure and applications. It provides scalable protection across Layers 3–7 against volumetric, protocol, DNS, SSL, and application-layer attacks and supports cloud, on-premises, and hybrid environments.	Software/ platform	BFSI, telecommunications, government, technology, eCommerce, media & entertainment, healthcare
BIG-IP Advanced Firewall Manager (AFM)	BIG-IP Advanced Firewall Manager (AFM) is a high-performance network security solution combining network firewall, DDoS protection, DNS security, and intrusion prevention capabilities. It provides automatic and manual detection and mitigation for network, DNS, and SIP-based DoS/DDoS attacks using predefined, dynamic, and custom attack signatures, with protection applicable at device and individual protected-object levels.	Software/ platform	Telecommunications, service providers, data centers, BFSI, government, energy & utilities, large enterprises

BIG-IP DDoS Hybrid Defender	BIG-IP DDoS Hybrid Defender provides comprehensive DDoS protection across network and application layers with deployment flexibility for inline, out-of-band, and hybrid architectures. The solution supports coordinated protection against Layer 3–4 network attacks and Layer 7 application-layer attacks, enabling organizations to combine on-premises protection with scalable mitigation capabilities.	Software/ platform	Telecommunications, service providers, data centers, government, BFSI, critical infrastructure
F5 DoS for NGINX	F5 DoS for NGINX is an application-layer DoS and DDoS protection solution designed for applications and APIs running on NGINX Plus and NGINX Ingress Controller. It uses adaptive and multi-layered protection techniques to detect anomalous traffic behavior and mitigate attacks targeting application resources and service availability.	Software/ platform	Technology, eCommerce, financial services, media & entertainment, SaaS, digital services

Source: Company Website

17.1.14.3 Recent developments

17.1.14.3.1 Product launches & enhancements

TABLE 631 F5: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
November 2025	Product enhancement	F5 (US)	BIG-IP v21.0 (Software/Platform)	F5 launched BIG-IP v21.0 with major security and platform enhancements for hybrid and multicloud application environments. As BIG-IP incorporated Advanced Firewall Manager (AFM) capabilities, the release enhanced the broader BIG-IP security architecture supporting network and application protection.
June 2025	Product launch / General availability	F5 (US)	BIG-IP Next for Kubernetes on NVIDIA BlueField-3 DPUs (Software/Platform)	F5 announced general availability of BIG-IP Next for Kubernetes on NVIDIA BlueField-3 DPUs. The release added hardware-accelerated DDoS mitigation and edge firewall capabilities, extending DDoS protection to cloud-native and AI infrastructure environments.
May 2025	Product enhancement	F5 (US)	BIG-IP Next Cloud-Native Network Functions 2.0 (Software/Platform)	F5 introduced BIG-IP Next CNF 2.0 with enhanced scalable and secure cloud-native networking capabilities for telecommunications providers, ISPs, cloud service providers, and enterprises. The platform strengthened the infrastructure supporting high-bandwidth applications and security services.

Source: Press Releases

17.1.14.3.2 Deals

TABLE 632 F5: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
March 2025	Strategic partnership	F5 (US)	StarHub (Singapore)	F5 and StarHub signed a five-year strategic Memorandum of Understanding to integrate F5 Distributed Cloud Services into StarHub's Cloud Infinity program. The collaboration covers cloud-based application security and delivery services; however, DDoS protection is part of the broader F5 Distributed Cloud Services portfolio rather than explicitly named as a standalone deployment in the announcement.
November 2024	Technology partnership	F5 (US)	Console Connect (UK)	F5 introduced its collaboration with Console Connect, integrating Console Connect's network-as-a-service infrastructure with F5 across multiple points of presence. The partnership enabled customers to access F5 Distributed Cloud Services, including DDoS Protection, over Console Connect's global network for public-facing applications.

Source: Press Releases

17.1.15 ALIBABA CLOUD

17.1.15.1 Business overview

Alibaba Cloud is the cloud computing and technology services business of Alibaba Group, providing cloud infrastructure, computing, storage, databases, networking, security, AI, big data, and application development services. Established in 2009, Alibaba Cloud offers a broad portfolio comprising Elastic Compute Service (ECS), Object Storage Service (OSS), ApsaraDB databases, cloud networking, content delivery, edge security, AI platforms, data analytics, and cybersecurity solutions. Its security portfolio includes Anti-DDoS, Web Application Firewall, Cloud Firewall, Security Center, Managed Security Service, Cloud Security Posture Management, and identity and access management solutions. Alibaba Cloud operates a global cloud infrastructure supporting enterprises across Asia-Pacific and international markets.

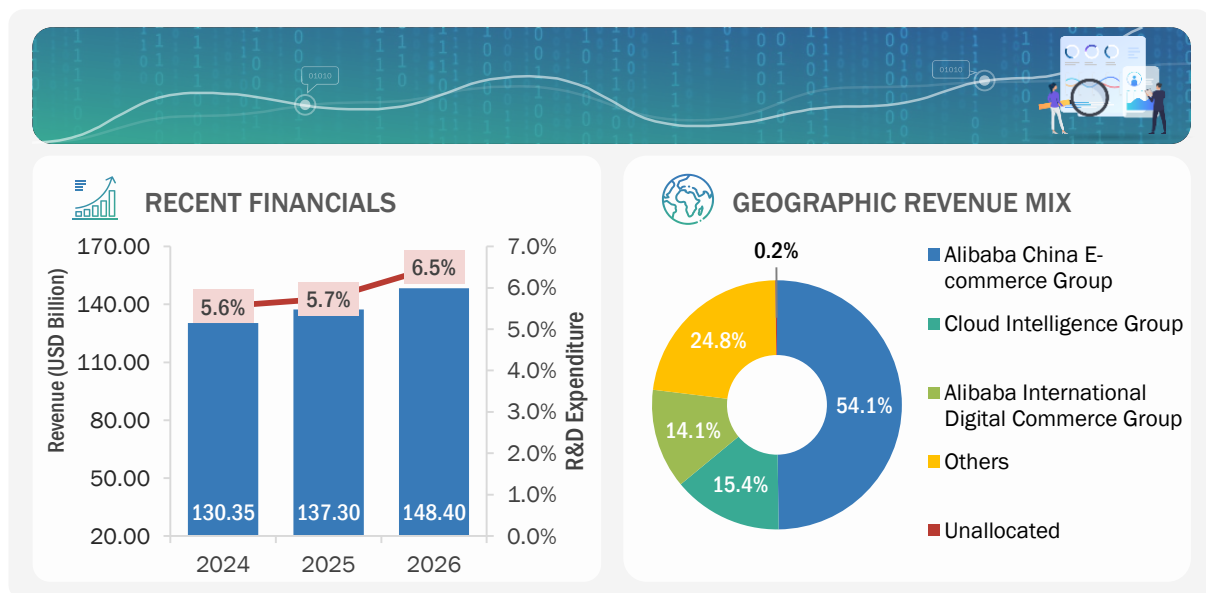
For the DDoS protection and mitigation market, Alibaba Cloud offers a tiered portfolio comprising Anti-DDoS Basic, Anti-DDoS Native, and Anti-DDoS Proxy. Anti-DDoS Basic provides automatically enabled baseline protection for eligible Alibaba Cloud resources with public IP addresses. Anti-DDoS Native provides native protection for Alibaba Cloud assets without requiring changes to business architecture and supports configurable traffic scrubbing and mitigation policies. Anti-DDoS Proxy provides enhanced protection by redirecting traffic through distributed scrubbing centers, filtering malicious traffic, and forwarding legitimate traffic to origin servers. The portfolio supports protection against Layer 3, Layer 4, and Layer 7 attacks, including volumetric attacks, SYN floods, UDP floods, HTTP floods, and other application-layer attacks.

Alibaba Cloud serves organizations across industries including financial services, retail and eCommerce, telecommunications, technology, gaming, media and entertainment, manufacturing, logistics, and public-sector organizations.

TABLE 633 ALIBABA CLOUD: COMPANY OVERVIEW

ALIBABA CLOUD	
Founded	2009
Country	China
City	Hangzhou
Ownership	Business unit of Alibaba Group Holding Limited (HKG: 9988)

Source: Company Website

FIGURE 61 ALIBABA CLOUD: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.15.2 Products/Solutions/Services offered**TABLE 634 ALIBABA CLOUD: PRODUCTS/SOLUTIONS/SERVICES OFFERED**

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Anti-DDoS Basic	Anti-DDoS Basic is a free DDoS protection service automatically enabled for supported Alibaba Cloud resources with public IP addresses. It provides baseline network- and transport-layer protection through traffic analysis, configurable thresholds, blackhole filtering, and traffic scrubbing capabilities to protect cloud assets against common DDoS attacks.	Software/ platform	Technology, SMEs, eCommerce, gaming, digital services, cloud-native enterprises
Anti-DDoS Native	Anti-DDoS Native provides native DDoS protection for Alibaba Cloud public IP assets without requiring changes to the underlying business architecture. The solution supports multiple protected assets and ports, configurable mitigation policies, traffic scrubbing thresholds, automated protection workflows, monitoring, alerting, and always-on protection capabilities for supported Enhanced EIPs.	Software/ platform	BFSI, eCommerce, gaming, technology, telecommunications, manufacturing, large enterprises
Anti-DDoS Proxy	Anti-DDoS Proxy provides enhanced cloud-based DDoS protection by redirecting traffic to distributed scrubbing centers, where malicious traffic is detected and filtered before legitimate traffic is forwarded to the origin server. The solution supports multilayer protection against Layer 3/4 volumetric and protocol attacks and Layer 7 attacks, including HTTP floods. It also includes configurable mitigation policies, TLS fingerprint-based protection, HTTP/2 attack protection, packet capture, traffic analysis, and protection for website and non-HTTP services.	Software/ platform	BFSI, eCommerce, gaming, telecommunications, media & entertainment, technology, government, large enterprises

Source: Company Website

17.1.15.3 Recent developments

17.1.15.3.1 Product launches & enhancements

TABLE 635 ALIBABA CLOUD: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
May 2025	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Proxy (Software/Platform)	Alibaba Cloud enhanced Anti-DDoS Proxy with mutual authentication capabilities for website configurations, strengthening service security for Internet of Vehicles scenarios across Chinese Mainland and Outside Chinese Mainland deployments.
November 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Native 2.0 (Software/Platform)	Alibaba Cloud introduced 95th-percentile burstable clean bandwidth billing for subscription-based Anti-DDoS Native 2.0, providing large enterprises with greater flexibility in handling unpredictable traffic requirements during events such as major promotional campaigns.
November 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Proxy (Software/Platform)	Alibaba Cloud expanded Anti-DDoS Proxy to protect non-HTTP application-layer services delivered over Layer 4 TCP ports, extending its mitigation coverage beyond conventional website and HTTP-based services.
October 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Native (Software/Platform)	Alibaba Cloud enabled always-on DDoS protection for supported Advanced EIPs, enhancing continuous mitigation capabilities for protected cloud assets.
August 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Proxy (Software/Platform)	Alibaba Cloud added protection against DDoS attacks exploiting HTTP/2 protocol vulnerabilities, strengthening application-layer mitigation capabilities for protected services.
May 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Proxy (Software/Platform)	Alibaba Cloud enhanced CC/HTTP flood protection through additional origin-server status code analysis, HTTP field-based rule configuration, targeted signature analysis, and a new Monitor action for improved attack detection and mitigation policy management.
April 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Proxy (Software/Platform)	Alibaba Cloud added protection against abnormal packet attacks originating from botnets, including scenarios where botnets such as Mirai generate large volumes of abnormal packets after TCP connection establishment.

February 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Native (Software/Platform)	Alibaba Cloud introduced automated protected-object onboarding based on attack status, enabling assets experiencing blackhole filtering or traffic scrubbing events to be automatically added for Anti-DDoS protection and reducing manual operational overhead.
January 2024	Product enhancement	Alibaba Cloud (China)	Anti-DDoS Proxy (Software/Platform)	Alibaba Cloud introduced client TLS fingerprint detection and protection, enabling Anti-DDoS Proxy to identify and mitigate attacks based on TLS fingerprint characteristics and strengthen encrypted traffic protection

Source: Press Releases

17.1.16 CORERO

17.1.16.1 Business Overview

Corero Network Security (Corero) is a cybersecurity company specializing in denial-of-service (DoS) and distributed denial-of-service (DDoS) protection and service availability/resiliency solutions. The company's portfolio is centered on protecting network infrastructure and digital services through automated detection, mitigation, traffic visibility, analytics, and reporting capabilities. Corero's primary platform offerings include SmartWall ONE, CORE, and associated SecureWatch managed services. The company provides flexible deployment models spanning hardware, software, virtual, SaaS, and cloud-native environments. Corero protects thousands of organizations globally and have around 400 live customer deployments, supported by around 50 channel partners.

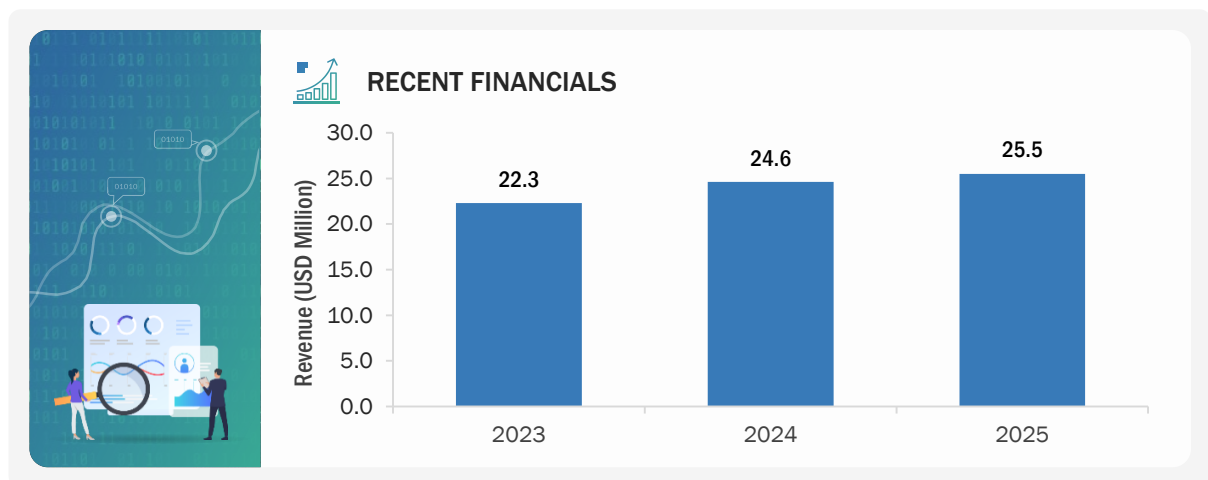
In the DDoS protection and mitigation market, Corero's primary offering is SmartWall ONE, an adaptive DDoS protection platform designed for real-time detection and automated mitigation of attacks across Layers 3-7, including HTTPS/TLS encrypted attack protection. The platform supports on-premises and hybrid-cloud deployments and combines DDoS mitigation with traffic visibility, analytics, and application-layer protection capabilities. Corero also offers CORE, a cloud-native observability and resiliency platform that extends the company's capabilities into traffic analysis, application security, Zero Trust admission control, and other related availability functions. In addition, Corero's SecureWatch provides managed services and DDoS intelligence capabilities to support customers' ongoing operations.

Corero primarily serves internet service providers, hosting providers, cloud providers, self-hosting SaaS providers, and enterprises across various sectors such as finance, healthcare, retail, gaming, education, and government. The company has strategic alliances with technology and infrastructure providers, including Akamai and HPE Juniper, for embedding their DDoS protection technologies within broader network infrastructure and cloud environments. Corero has a strong global presence in over 50 countries including its offices in North America and Europe. The company is listed on the London Stock Exchange's AIM (ticker: CNS) and the US OTC Market (OTCQX: DDoSF).

TABLE 636 CORERO NETWORK SECURITY: COMPANY OVERVIEW

founded	2011
Headquarter 1	Marlborough, MA, US
Headquarter 2	London, UK
Ownership	Public (LON: CNS)

Source: Company Website

FIGURE 62 CORERO: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.16.2 Products/Solutions/Services offered

TABLE 637 CORERO: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS

PRODUCT TYPE	PRODUCT/SOLUTION/SERVICE	DESCRIPTION	VERTICAL
Software/ Platform & Hardware	SmartWall ONE	Corero's modular DDoS protection solution providing real-time detection and automated mitigation of DoS and DDoS attacks. It supports protection across Layers 3–7 with unencrypted and encrypted traffic inspection, attack detection, mitigation, visibility, analytics, and reporting. SmartWall ONE supports flexible on-premises and hybrid-cloud deployment architectures and can be deployed through hardware, software, or virtualized configurations.	- ISPs - Hosting - Finance - Healthcare - Retail, Gaming - Education - Government
Software/ Platform	CORE Platform	Cloud-native, AI-augmented, observability and resiliency platform extending Corero's protection capabilities beyond conventional DDoS mitigation. The platform combines traffic visibility with AI-powered analysis, threat intelligence feeds, support for Zero Trust admission control, and defenses against availability-impacting application and API threats. It is designed to complement SmartWall ONE within Corero's broader service availability and resiliency protection architecture.	- ISPs - Hosting - Finance - Healthcare - Retail, Gaming - Education - Government
Services	SecureWatch	Portfolio of managed and intelligence-led services designed to support the operation of Corero's DDoS protection environment. Services include managed DDoS protection and threat intelligence capabilities, supported by Corero specialists and threat research to help customers monitor attack activity, optimize protection policies, and strengthen their DDoS defense posture.	- ISPs - Hosting - Finance - Healthcare - Retail, Gaming - Education - Government

Source: Company Website

17.1.16.3 Recent developments

17.1.16.3.1 Product launches & enhancements

TABLE 638 CORERO: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
August 2026	Product launch	Corero Network Security	AI-Augmented Cloud-Assist for SmartWall ONE (Software/Platform)	Corero launched AI-Augmented Cloud-Assist for SmartWall ONE, extending its DDoS protection capabilities with cloud-delivered AI-assisted analysis, threat intelligence, and policy optimization. The capability creates a feedback loop between cloud intelligence and deployed protection environments to support faster identification of emerging threats and mitigation policy development.
July 2026	Software release/Product enhancement	Corero Network Security	SmartWall ONE 15.x (Software/Platform)	Corero made SmartWall ONE version 15.x generally available. The release represents the latest major version of Corero's DDoS detection and mitigation platform, with intelligent TLS inspection and mitigation orchestration, plus outbound traffic monitoring, and enhanced edge router visibility and control.
June 2025	Software release/Product enhancement	Corero Network Security	SmartWall ONE 14.x (Software/Platform)	Corero made SmartWall ONE version 14.x generally available. The release represents the latest major version of Corero's DDoS detection and mitigation platform, adding bare metal software protectors, multi-site solution resiliency, and enhanced edge router mitigation.
October 2024	Product launch	Corero Network Security	Corero Observability & Resiliency Ecosystem (CORE) (Software/Platform)	Corero launched CORE, a cloud-based availability protection platform designed to extend visibility and defensive capabilities across existing security infrastructure. The platform uses data collection and AI/ML-assisted insights to support service availability and resilience.
October 2024	Product launch	Corero Network Security	Network Threat Detector (NTD) 3400 (Hardware)	Corero launched the NTD 3400, an 800Gbps throughput hardware appliance and enhancement to its SmartWall ONE DDoS protection portfolio. The appliance was introduced to provide 400GE and higher-capacity connectivity with scalable DDoS detection and mitigation.
August 2024	Software release/Product enhancement	Corero Network Security	SmartWall ONE Service Portal 3.x (Software/Platform)	Corero made version 3.x of the SmartWall ONE Service Portal generally available, supporting the delivery and management of DDoS Protection-as-a-Service offerings.
June 2024	Product enhancement	Corero Network Security	SmartWall ONE Service Portal (Software/Platform)	Corero introduced enhanced SmartWall ONE Service Portal capabilities, including features designed to support service and hosting providers in managing DDoS protection services, improving customer visibility, and supporting service monetization.

March 2024	Service launch	Corero Network Security	Corero DDoS Intelligence Service (CDIS) (Service)	Corero introduced its DDoS Intelligence Service, an automated, AI-assisted subscription service for SmartWall ONE customers. The service uses Corero's threat research and intelligence to support predictive and pre-emptive DDoS mitigation.
March 2024	Major software release/ Product enhancement	Corero Network Security	SmartWall ONE 12.x (Software/ Platform)	Corero made SmartWall ONE version 12.x generally available as a major software release for its automated DDoS detection and mitigation platform.
February 2024	Product enhancement	Corero Network Security	SmartWall ONE 400G Extension (Software/ Platform)	Corero extended SmartWall ONE capabilities to support 400G-connected DDoS detection, mitigation, and protection from the network edge to the core, addressing demand for higher-capacity protection architectures.

Source: Press Releases

17.1.16.3.2 Deals

TABLE 639 CORERO: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
July 2026	Strategic partnership	Corero Network Security	Commercis (UK)	Corero entered into a strategic partnership with Commercis to expand the availability of its real-time DDoS protection platform across the Middle East. The partnership targets telecommunications, internet services, banking, government, energy, critical infrastructure, and enterprise organizations.
June 2026	Strategic partnership	Corero Network Security	ITcare (Poland)	Corero partnered with ITcare to expand access to SmartWall ONE and deliver real-time DDoS protection and cyber resilience capabilities to enterprises, service providers, and critical infrastructure organizations.
February 2026	Strategic partnership	Corero Network Security	EdgeUno (US)	Corero partnered with EdgeUno to expand automated DDoS protection as a managed service across Latin America, combining Corero's automated defense capabilities with EdgeUno's regional connectivity infrastructure.
January 2026	Strategic partnership	Corero Network Security	Auben Networks (Argentina)	Corero partnered with Auben Networks to expand its Latin American presence. Under the agreement, Auben Networks can offer Corero's portfolio, including the SmartWall ONE DDoS protection platform, to customers in the region.
September 2025	Partnership expansion	Corero Network Security	ONESECURE Asia (Singapore)	Corero entered a strategic partnership with ONESECURE Asia, marking its entry into the Singapore market and expanding its Southeast Asian presence. The partnership combines Corero's DDoS protection technology with ONESECURE's local capabilities for telecom operators, enterprises, and service providers.

September 2025	Partnership expansion	Corero Network Security	Netceed (UK)	Corero expanded its strategic partnership with Netceed into the UK, enabling UK service providers to access Corero's DDoS protection, traffic analysis, and Zero Trust Admission Control capabilities.
June 2025	Agreement	Corero Network Security	Rocket Fibre (UK)	Rocket Fibre signed a multi-year agreement and selected Corero's SmartWall ONE solution to provide scalable, real-time DDoS protection across its network and support the delivery of DDoS protection services to customers.
April 2025	Partnership expansion	Corero Network Security	Juniper Networks (US)	Corero and Juniper expanded their partnership, enabling Juniper to sell Corero's full DDoS protection portfolio, including SmartWall ONE and the CORE platform, to customers across multi-vendor network environments.
August 2024	Strategic partnership	Corero Network Security	stc Bahrain (Bahrain)	Corero entered a partnership with stc Bahrain to support the delivery of DDoS-protected services and enhance protection against external and internally generated DDoS threats for stc Bahrain's customers.
August 2024	Strategic partnerships	Corero Network Security	NovaRed (Chile), VGL (New Zealand) & GreyMatter (Chile)	Corero signed three strategic partner agreements with NovaRed, VGL, and GreyMatter to expand the availability of its DDoS protection solutions and strengthen its channel presence in Chile and Latin America.

Source: Press Releases

17.1.17 AWS

17.1.17.1 Business Overview

Amazon Web Services (AWS) is a cloud computing business of Amazon that provides cloud infrastructure and technology services across computing, storage, databases, networking, analytics, artificial intelligence, security, and application development. Launched in 2006, AWS offers a broad portfolio of cloud services, including Amazon EC2, Amazon S3, Amazon RDS, Amazon VPC, Amazon CloudFront, Amazon Route 53, AWS Lambda, Amazon Bedrock, and AWS security services. Its cybersecurity portfolio includes AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), Amazon GuardDuty, AWS Security Hub, AWS WAF, AWS Firewall Manager, and AWS Shield. For the DDoS protection and mitigation market, its key offerings include AWS Shield Standard, AWS Shield Advanced, and the AWS WAF Anti-DDoS Managed Rule Group.

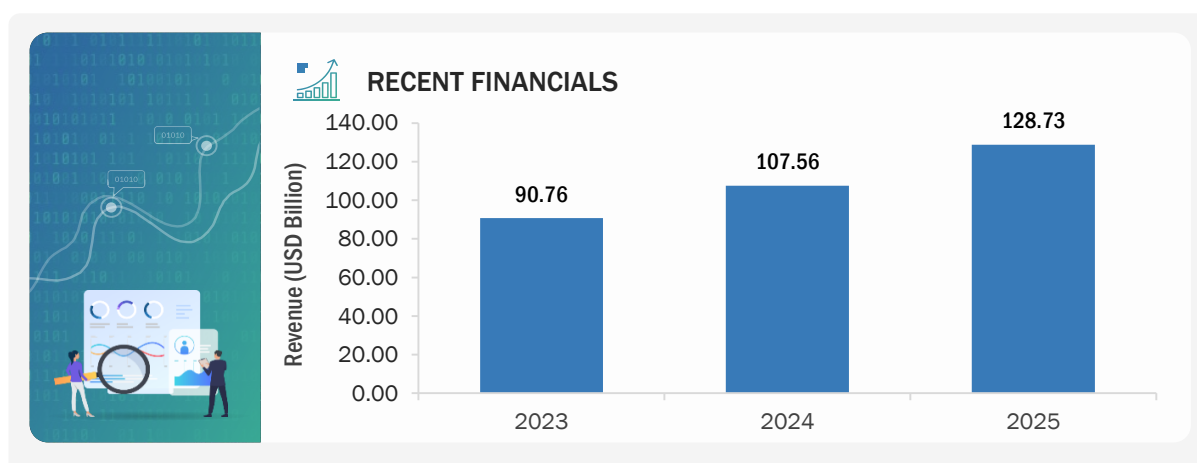
For the DDoS protection and mitigation market, AWS provides a layered, cloud-native protection portfolio through AWS Shield and AWS WAF. AWS Shield Standard provides automatically enabled protection against common network- and transport-layer DDoS attacks, while AWS Shield Advanced delivers enhanced detection and mitigation capabilities for larger and more sophisticated attacks, along with attack visibility, access to the AWS Shield Response Team, and DDoS-related cost protection. AWS also introduced the AWS WAF Anti-DDoS Managed Rule Group in June 2025 to provide automated application-layer protection against HTTP request floods. The rule group can be used independently with AWS WAF or as part of AWS Shield Advanced, extending AWS's protection capabilities across Layers 3, 4, and 7.

AWS serves organizations ranging from startups and enterprises to governments and non-profit organizations across industries such as financial services, healthcare and life sciences, retail and consumer goods, telecommunications, media and entertainment, gaming, manufacturing, automotive, energy and utilities, education, and the public sector. The company has a global presence in North America, Europe, Asia Pacific, the Middle East and Africa, and Latin America.

TABLE 640 **AWS: COMPANY OVERVIEW**

founded	2006
Country	US
City	Seattle, Washington
Ownership	Business segment of Amazon.com Inc. (NASDAQ: AMZN)

Source: Company Website

FIGURE 63 AWS: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.17.2 Products/Solutions/Services offered**TABLE 641** AWS: PRODUCTS/SOLUTIONS/SERVICES OFFERINGS

PRODUCT TYPE	PRODUCT/SOLUTION/SERVICE	DESCRIPTION	VERTICAL
Software/ platform	AWS Shield Standard	Automatically provides baseline DDoS protection for AWS customers against common network- and transport-layer attacks. It uses always-on network flow monitoring, traffic signatures, anomaly detection, and automatic inline mitigation techniques to protect supported AWS services and applications from common volumetric and state-exhaustion attacks.	- BFSI - Government - Healthcare, Retail & eCommerce - Technology - Telecommunications - Media & Entertainment - Gaming - Manufacturing - Education
Software/ platform	AWS Shield Advanced	Managed DDoS protection service provides enhanced detection and automated mitigation against large and sophisticated attacks targeting protected AWS resources. The service supports protection across network, transport, and application layers and includes attack visibility, AWS WAF integration, access to the AWS Shield Response Team (SRT), proactive engagement capabilities, and DDoS-related cost protection.	- BFSI - Government - Healthcare - Retail & eCommerce - Technology - Telecommunications - Media & Entertainment - Gaming, Manufacturing - Energy & Utilities
Software/ platform	AWS WAF Anti-DDoS Managed Rule Group	The AWS-managed rule group is designed specifically to automatically detect and mitigate application-layer DDoS attacks involving HTTP request floods. It analyzes traffic behavior to identify anomalous attack patterns and can rapidly apply mitigations without requiring customers to create and continuously manage custom DDoS rules. The offering can be deployed as part of AWS WAF or used with AWS Shield Advanced.	- BFSI - Retail & eCommerce - Technology, Media & Entertainment - Gaming - Healthcare - Government - SaaS

17.1.17.3 Recent developments

17.1.17.3.1 Product launches & enhancements

TABLE 642 AWS: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
July 2026	Product enhancement	AWS (US)	AWS Shield Advanced/AWS WAF Anti-DDoS Managed Rule Group (Software/Platform)	AWS Shield Advanced began adopting the AWS WAF Anti-DDoS Managed Rule Group as its default application-layer DDoS protection capability, initiating a phased migration for eligible web ACLs.
May 2026	Product enhancement	AWS (US)	AWS Shield Advanced DDoS Attack Flow Logs (Software/Platform)	AWS introduced DDoS attack flow logs for Shield Advanced, providing packet-level visibility into traffic during DDoS attacks. The logs capture details such as IP addresses, ports, protocols, packet and byte counts, and source-country information, and can be delivered to Amazon S3, Amazon CloudWatch Logs, or Amazon Data Firehose.
June 2025	Product launch	AWS (US)	AWS WAF Anti-DDoS Managed Rule Group (Software/Platform)	AWS launched the Anti-DDoS Managed Rule Group, a capability specifically designed to automatically detect and mitigate Layer 7 DDoS attacks involving HTTP request floods. The offering profiles application traffic and responds to anomalous attack patterns through automated AWS WAF protections.

Source: Press Releases

17.2 OTHER KEY PLAYERS

17.2.1 FASTLY

Founded	2002
Country	US
City	San Mateo, California
Ownership	Public (NYSE: FSLY)
Business Overview	Fastly is a global edge cloud platform provider that helps companies deliver digital content, applications, and services faster and more securely. The company operates a content delivery network (CDN) designed to improve internet performance by caching content closer to users, reducing latency, and enhancing speed. Fastly's platform offers real-time visibility and control, enabling customers to update content quickly and manage traffic spikes more effectively. The company's security solutions, including DDoS protection, Web Application Firewalls (WAF), and API protection, are strengthened by its acquisition of Signal Sciences in 2020. Fastly serves various industries, including eCommerce, media, and SaaS, with notable clients like Shopify and The New York Times. Its business model is consumption-based, meaning clients pay based on bandwidth usage and network requests. The company serves to verticals such as streaming media, retail and eCommerce, travel and hospitality, financial services, technology, education and gaming.
Products/Solutions Offered	▪ DDOS Protection and Mitigation Solution ▪ Next-Gen WAF ▪ Professional Services
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

17.2.2 ALLOT

Founded	1996
Country	Israel
City	Hod-Hasharon
Ownership Type	Public (NASDAQ: ALLT, TASE: ALLT)
Business Overview	Allot is one of the leading providers of innovative network intelligence and security solutions worldwide for service providers and enterprises. Its multi-service platform is utilized by more than 500 mobile, fixed, and cloud service providers, as well as over 1,000 enterprises. In Europe alone, more than 18 million subscribers are currently using Allot's network-based security-as-a-service solution, achieving over 50% penetration with certain service providers. The company's DDoS protection solution protects enterprise networks. Allot's advanced Network Behavior Anomaly Detection (NBAD) technology can identify volumetric attacks. Allot's solution uses advanced technologies like machine learning and artificial intelligence to learn normal traffic behavior, enabling rapid, accurate detection and mitigation of the attack.
Products/Solutions Offered	▪ Allot DDOS Secure ▪ 5G Secure ▪ Network Secure ▪ DNS Secure ▪ Endpoint Secure
Geographic Presence	North America, Europe, the Middle East & Africa, and Latin America

Source: Company Website

17.2.3 STRATACORE

Founded	2003
Country	US
City	Seattle, Washington
Ownership Type	Private
Business Overview	StrataCore works with other IT teams as a strategic partner, technology matchmaker, and loyal customer champion to help them achieve peak enterprise outcomes. It acts as a single-source technology lifecycle advocate. For DDoS protection, StrataCore provides managed DDoS protection, which allows networks to gain visibility into potential DDoS attacks, complete mitigation, volume, and stealth-based attack and threat detection. The company's area of expertise is colocation, contact center, connectivity, cloud computing, cyber security, DDoS protection, and managed security. StrataCore has strategic relationships with over 400 global service providers. It has a strong presence in the market, with more than 200 clients and over 2,500 contracts negotiated worldwide.
Products/Solutions Offered	▪ Managed DDoS Protection ▪ Managed Intrusion Detection Prevention System (IDPS) ▪ Security Consul
Geographic Presence	North America

Source: Company Website

17.2.4 SUCURI (GODADDY)

Founded	2010
Country	US
City	Menifee, California (Subsidiary of GoDaddy)
Ownership Type	Private
Business Overview	Sucuri is a website security company specializing in website protection, monitoring, malware detection and removal, and web application security. Established in 2010, the company offers a portfolio comprising the Sucuri Website Security Platform, Website Firewall, website monitoring, malware removal, virtual patching, and CDN services. Sucuri became part of GoDaddy in 2017 and operates within GoDaddy's security business. Sucuri's Website Firewall is a cloud-based security platform that provides DDoS protection and mitigation for websites and web applications. The solution combines a Web Application Firewall (WAF), intrusion detection capabilities, and a globally distributed Anycast network to inspect and filter incoming traffic before it reaches the protected website. Its DDoS protection covers Layer 3, Layer 4, and Layer 7 attacks, including network-based volumetric attacks and application-based request floods. Sucuri also provides DNS management, traffic filtering, virtual patching, malicious bot blocking, and website acceleration through its CDN. For enterprise customers, the company offers advanced DDoS mitigation, custom SLAs, dedicated support, and SIEM/SOC integration. Sucuri serves businesses, agencies, bloggers, SMBs, eCommerce companies, software companies, managed WordPress hosts, and enterprises. The company states that customers in more than 130 countries use its website security solutions. Its customer ecosystem includes organizations such as WPBeginner, Yoast, iThemes, Kinsta, and other web-focused businesses
Products/Solutions Offered	▪ Sucuri Website Security Platform ▪ Sucuri Website Firewall ▪ DDoS Protection & Mitigation Solution ▪ Website Monitoring ▪ Malware Detection & Removal ▪ Virtual Patching & Hardening ▪ CDN & Website Performance Optimization
Geographic Presence	North America, Europe, and Asia Pacific

Source: Company Website

17.2.5 LUMEN TECHNOLOGIES

Founded	2020
Country	US
City	Monroe, Louisiana
Ownership Type	Public (NYSE: LUMN)
Business Overview	Lumen Technologies is a US-based telecommunications and technology company providing network, connectivity, edge, cloud, and security solutions to businesses and organizations. Its portfolio includes connectivity services, network solutions, edge and cloud services, cybersecurity solutions, and DDoS protection and mitigation services. Within the DDoS protection and mitigation market, Lumen offers Lumen DDoS Mitigation Service, Lumen DDoS Hyper, and Lumen DDoS Essentials. Lumen's DDoS Mitigation Service provides network- and application-layer protection against multi-vector and mixed application-layer attacks. Its capabilities include automated detection and response through Rapid Threat Defense, Black Lotus Labs threat intelligence, intelligent traffic routing, flow-based monitoring, and global scrubbing infrastructure. Lumen reports 170 Tbps of network-based mitigation capacity across 500+ global scrubbing locations, with Always-On and On-Demand deployment options and a reported 1-second time-to-mitigate after most attack traffic reaches its scrubbing centers. Lumen also offers DDoS Hyper, which provides automated, self-service activation of DDoS protection, and DDoS Essentials, an on-demand solution designed for volumetric attacks. Lumen integrates DDoS protection with its global network infrastructure and Black Lotus Labs threat intelligence capabilities. Its DDoS solutions support Lumen and third-party connections and can protect IPv4 and IPv6 environments. The company serves business and public-sector customers and provides DDoS mitigation through global scrubbing locations and security operations centers.
Products/Solutions Offered	▪ Lumen DDoS Mitigation Service ▪ Lumen DDoS Hyper ▪ Lumen DDoS Essentials ▪ Rapid Threat Defense ▪ Web Application Firewall (WAF) / Application Protection ▪ Black Lotus Labs Threat Intelligence
Geographic Presence	North America and Asia Pacific

Source: Company Website

17.2.6 SECEON

Founded	2015
Country	US
City	Westford, Massachusetts
Ownership Type	Private
Business Overview	Seceon is a cybersecurity company that provides AI/ML-driven security solutions for enterprises and managed security service providers (MSSPs). Founded in 2015, the company offers a unified security platform designed to consolidate security information and event management (SIEM), extended detection and response (XDR), security orchestration, automation and response (SOAR), user and entity behavior analytics (UEBA), threat intelligence, and network detection and response (NDR) capabilities. Seceon's Open Threat Management (OTM) Platform incorporates DDoS detection and automated response capabilities as part of its broader threat detection and response functionality. The platform analyzes network traffic and security telemetry, applies AI/ML, behavioral analytics, and anomaly detection to identify malicious activity, and enables automated containment and remediation. Seceon states in an official customer case study that OTM detects DDoS attacks, along with other threats, and can initiate automated remediation. Its platform can also execute response actions such as blocking malicious IP addresses and enforcing security policies through automated playbooks. Seceon primarily serves enterprises, MSSPs, and MSPs, with its platform supporting multi-tenant deployments. The company states that its platform protects 9,000+ organizations worldwide and is supported by 700+ partners in its 2025 company profile. Its stated global reach includes offices, distributors, and data centers across North America, South America, Europe, Africa, Asia, and Australia.
Products/Solutions Offered	▪ Seceon Open Threat Management (OTM) Platform ▪ aiSIEM ▪ aiXDR ▪ SOAR ▪ I-JEBA/Behavioral Analytics ▪ Threat Intelligence ▪ NDR ▪ aiSecOT360 - OT/IoT/ICS Security
Geographic Presence	North America, Europe, Asia Pacific, and the Middle East & Africa

Source: Company Website

17.2.7 HALTDOS

Founded	2015
Country	India
City	Noida
Ownership Type	Private
Business Overview	Haltdos is an AI-powered cybersecurity OEM specializing in network and application security. Founded in 2015, the company provides a unified Edge Security & Delivery Platform designed to protect and optimize critical digital infrastructure across on-premises, cloud, and hybrid environments. Its overall portfolio includes Anti-DDoS, Web Application Firewall (WAF), WAAP, Anti-Bot, DNS Firewall, Application Delivery Controller (ADC), load balancing, API Gateway, SSL VPN, and CDN solutions. Haltdos states that its patented platform is designed to autonomously detect and mitigate threats ranging from volumetric DDoS attacks to sophisticated zero-day exploit. Haltdos' Anti-DDoS Solution provides multi-layered protection against DDoS attacks from Layer 2 to Layer 7 using AI/ML-based detection, behavioral analysis, traffic filtering, and automated mitigation. The enterprise solution supports always-on protection, multi-vector defense, amplification and reflection attack protection, mass-scale IP blocking, traffic shaping, and multi-protocol support. Haltdos also offers DDoS Shield through Haltdos Cloud, providing over 25 Tbps of scrubbing capacity, while its broader multi-cloud infrastructure leverages more than 30 Tbps of total capacity across infrastructure partners. Its cloud service uses Anycast routing and multiple cloud service providers for distributed traffic scrubbing. Haltdos serves enterprises, government organizations, BFSI institutions, ISPs, data centers, and critical infrastructure. The company protects organizations across India and 120+ countries, reflecting its expanding global presence in cybersecurity and DDoS protection.
Products/Solutions Offered	▪ Anti-DDoS Enterprise ▪ DDoS Shield ▪ Web Application Firewall (WAF) ▪ Enterprise WAAP ▪ Anti-Bot ▪ DNS Firewall ▪ Application Delivery Controller (ADC) ▪ Link Load Balancer ▪ Global Server Load Balancer (GSLB) ▪ API Gateway ▪ Content Delivery Network (CDN) ▪ Remote Access Gateway
Geographic Presence	North America and Asia Pacific

Source: Company Website

17.2.8 DDOS-GUARD

Founded	2011
Country	Russia
City	Rostov-on-Don
Ownership Type	Private
Business Overview	DDoS-Guard is a Russia-based cybersecurity and Internet infrastructure company specializing in DDoS protection and mitigation, website security, content delivery, and protected hosting services. Established in 2011, the company provides solutions designed to protect websites, networks, servers, and online infrastructure against DDoS attacks while maintaining service availability. Its portfolio includes DDoS protection, website protection, CDN, protected hosting, IP transit, and network security services. DDoS-Guard operates a geographically distributed infrastructure with scrubbing nodes across Europe, the US, South America, and Asia. Offering DDoS-Guard's DDoS Protection service uses traffic analysis and distributed scrubbing infrastructure to identify and filter malicious traffic while allowing legitimate traffic to reach protected resources. The service provides protection against volumetric, protocol, and application-layer DDoS attacks and can be applied to websites, servers, networks, and other Internet-facing infrastructure. DDoS-Guard states that its geo-distributed network can scrub more than 3.2 Tbps of attack traffic and provides a 99.95% SLA availability. The company's protection architecture includes traffic monitoring, malicious-packet filtering, distributed traffic scrubbing, and mitigation capabilities designed to maintain availability during large-scale and complex botnet attacks. DDoS-Guard provides DDoS mitigation and related infrastructure services to customers requiring protection for websites, online services, networks, and servers. Its distributed scrubbing infrastructure spans Europe, North America, South America, and Asia, supporting its global service delivery model. The company also provides protected hosting, CDN, IP transit, and website protection services as part of its broader Internet infrastructure portfolio.
Products/Solutions Offered	▪ DDoS Protection ▪ Website Protection ▪ Network Protection ▪ Protected Hosting ▪ CDN/ Website Acceleration ▪ IP Transit ▪ Protected Servers
Geographic Presence	North America, Europe, and Asia Pacific

Source: Company Website

17.2.9 INDUSFACE

Founded	2012
Country	India
City	Vadodara
Ownership Type	Private
Business Overview	Indusface is an application security company specializing in protecting web, API, and AI applications against cyber threats. Its portfolio includes web application firewall (WAF), API security, bot management, DDoS mitigation, application security testing, vulnerability management, and AI application security. The company's primary platform is AppTrana, an AI-powered, fully managed application and API security platform that integrates multiple application security capabilities. Indusface's AppTrana DDoS Protection provides fully managed, AI-powered DDoS protection for websites and APIs. The solution uses behavioral and machine-learning-based detection to establish traffic baselines and identify anomalous activity, with protection against Layer 3, Layer 4, and Layer 7 attacks. Its capabilities include always-on and unmetered DDoS mitigation, granular rate limiting based on URI, IP, host, session, and geography, automated attack blocking, and 24×7 SOC monitoring. AppTrana also provides URI-based DDoS protection, enabling organizations to apply granular controls to high-value resources such as login, checkout, and signup pages. Indusface states that AppTrana can block DDoS attacks of up to 2.3 Tbps and 700,000 requests per second, supported by AWS infrastructure. The company also provides a 100% uptime SLA covering its protection layer. Indusface serves organizations across multiple industries and states that its customer base spans 95+ countries. Its customer references include organizations such as Tata Consultancy Services, Tata Power, HDFC ERGO, Bandhan Life, Tata Capital, and ITC Hotels. The company also has a technology ecosystem that includes AWS and maintains global offices across the US and India
Products/Solutions Offered	▪ AppTrana WAAP ▪ AppTrana DDoS Protection ▪ AppTrana API Protection ▪ Web Application Firewall (WAF) ▪ Bot Management ▪ API Security ▪ Web Application Scanning ▪ API Scanning ▪ DAST/Application Security Testing ▪ AI Application & LLM Security
Geographic Presence	North America and Asia Pacific

Source: Company Website

17.2.10 MLYTICS

Founded	2017
Country	Singapore
City	Singapore
Ownership Type	Private
Business Overview	Mlytics is a digital infrastructure and cloud technology company specializing in multi-CDN management, website performance, resilience, and security. Founded in 2017, the company provides a SaaS-based platform designed to help organizations optimize and secure websites and web applications. Its portfolio includes Multi CDN, Smart Load Balancer, Origin Shield, Cloud WAF, DDoS Protection, Bot Management, API Protection, DNS, and real-user monitoring capabilities. Mlytics' platform combines multiple CDN networks to improve website availability, performance, and resilience. Mlytics provides DDoS Protection through its Origin Shield security suite and Multi CDN platform. Its DDoS protection architecture combines traffic distribution across multiple CDN networks with dedicated security controls positioned in front of the origin server. For Layer 3 and Layer 4 attacks, Mlytics uses CDN-based port restrictions and distributed traffic absorption at the edge, while its Layer 7 protection applies capabilities such as challenge and response, browser integrity checks, scanner and crawler blocking, rate limiting, and traffic analysis. Origin Shield further integrates Cloud WAF, bot management, L7 DDoS protection, and API protection across multiple CDNs. Mlytics states that its Multi CDN architecture provides access to 2,300+ PoPs and 2,600 Tbps of combined CDN capacity, enabling distributed traffic absorption and resilience. Mlytics' ecosystem is centered on integrating multiple third-party CDN networks through its Multi CDN platform, allowing customers to manage and orchestrate different CDN providers through a unified interface. The company serves businesses operating websites and web applications and has demonstrated DDoS protection deployments for eCommerce customers, including S3 Beauty in Taiwan. Mlytics has a global presence, with locations in Singapore, Taiwan, and Hong Kong.
Products/Solutions Offered	▪ Multi CDN ▪ Smart Load Balancer ▪ Origin Shield ▪ Cloud WAF ▪ DDoS Protection ▪ Bot Management ▪ API Protection ▪ DNS & DNS Routing ▪ Real User Monitoring ▪ CDN Marketplace
Geographic Presence	Europe and Asia Pacific

Source: Company Website

17.2.11 RIOREY

Founded	2006
Country	US
City	Bethesda, Maryland
Ownership Type	Private
Business Overview	RioRey protects against layer 3, 4, and 7 DDoS attacks with its algorithm-based solutions. This algorithmic-centric technology is recognized as a next-generation solution in DDoS detection and mitigation. The combination of powerful on-premises protection with an on-demand cloud-based scrubbing service provides defense against a full spectrum of DDoS attacks, including stealthy layer 7 application attacks and large-scale volumetric attacks. RioRey's product portfolio caters to Fortune 1000 companies, small and medium businesses, government agencies, telcos, and hosting companies worldwide. To defend modern networks, RioRey provides a powerful browser-based management and reporting system, rWeb. rWeb forms an all-in-one platform for managing DDoS defense by combining network visibility and its powerful tools.
Products/Solutions Offered	rWeb
Geographic Presence	North America, Europe, the Middle East & Africa, and Asia Pacific

Source: Company Website

17.2.12 PHOENIXNAP

Founded	2009
Country	US
City	Phoenix, Arizona
Ownership Type	Private
Business Overview	phoenixNAP is a global Infrastructure-as-a-Service (IaaS) provider, founded in 2009. Its extensive portfolio of infrastructure services is designed to address sophisticated IT challenges. phoenixNAP operates a geographically distributed network of data centers and network nodes across five continents worldwide. These servers are located in various places throughout the US, including Virginia, Arizona, and Georgia, as well as in Amsterdam, Serbia, and Singapore. As a Next Wave Intel CSP, phoenixNAP continually works with Intel on driving the IaaS market forward. phoenixNAP uses Kentik's advanced monitoring tools to improve network stability. It makes sure that business operations keep running with its automated traffic filtering tools and lightning-fast DDoS mitigation infrastructure during any cyber-attack. DDoS traffic is prevented from taking down servers with automatic screening and rigorous traffic filtering through globally distributed scrubbing centers. In 2021, a new 500,000 sq. ft. data center campus in Phoenix, Arizona, was acquired by phoenixNAP.
Products/Solutions Offered	phoenixNAP DDoS Protect
Geographic Presence	North America, Europe, and Asia Pacific

Source: Company Website

17.2.13 XCITIUM

Founded	1998 (Comodo Security Solutions), 2022 (Rebranded as Xcitium)
Country	US
City	Bloomfield, New Jersey
Ownership Type	Private
Business Overview	Xcitium is a cybersecurity company specializing in zero-trust security, endpoint protection, threat detection and response, and managed security services. The company provides a broad cybersecurity portfolio spanning endpoint protection, EDR/XDR, managed detection and response, cloud workload protection, threat intelligence, and unified threat management. Its portfolio includes the Xcitium Unified Threat Management Platform, Xcitium Client Security, Xcitium Advanced, Xcitium Complete, Xcitium MDR, Xcitium Managed SOC, and Xcitium CNAPP. Xcitium was previously known as Comodo Security Solutions and officially rebranded to Xcitium in July 2022 as part of the company's transition toward its zero-threat security positioning. Xcitium addresses DDoS protection as part of its Unified Threat Management Platform, which consolidates security technologies and provides centralized visibility and threat management across the organization's environment. Xcitium's official UTM platform page specifically identifies DDoS among the advanced threats that organizations can prevent and stop through the platform. The platform provides a single-pane approach for security teams to monitor the broader threat ecosystem, block malicious activity, and manage potential threats and vulnerabilities. Xcitium operates through an ecosystem that includes managed service providers (MSPs), managed security service providers (MSSPs), technology partners, and channel partners. Its platform portfolio supports enterprises and organizations requiring endpoint, network, cloud, and managed security protection.
Products/Solutions Offered	Xcitium Unified Threat Management Platform
Geographic Presence	North America

Source: Company Website

17.2.14 MAZEBOLT

Founded	2013
Country	Israel
City	Ramat Gan
Ownership Type	Private
Business Overview	MazeBolt is a cybersecurity company specializing in DDoS vulnerability management, testing, validation, and remediation. Founded in 2013 as a cyber services company, the company initially focused on extensive red-team testing before developing its patented RADAR platform to provide continuous, nondisruptive DDoS security. Its portfolio is centered on MazeBolt RADAR, supported by DDoS testing, vulnerability management, remediation, validation, and professional services. The company works with enterprises and DDoS mitigation providers to identify vulnerabilities in existing DDoS protection deployments. MazeBolt's RADAR™ is a continuous, nondisruptive DDoS testing and vulnerability management platform designed to identify and help remediate vulnerabilities and misconfigurations in deployed DDoS protection. Rather than functioning as a conventional DDoS scrubbing provider, RADAR continuously simulates DDoS attacks against live production environments without disrupting online services. The platform tests Layers 3, 4, and 7 and evaluates protection against known DDoS attack vectors across IPs, FQDNs, and services. It provides visibility into the DDoS attack surface, identifies vulnerabilities, prioritizes remediation, and revalidates protection after remediation. Mazebolt has partnerships with vendors including F5, while noting that MazeBolt is vendor-neutral and works with DDoS mitigation providers. The company serves customers across financial services, insurance, government, gaming, eCommerce, and other enterprise sectors.
Products/Solutions Offered	▪ MazeBolt RADAR ▪ Continuous DDoS Testing ▪ DDoS Vulnerability Management ▪ DDoS Validation & Remediation ▪ DDoS Attack Simulation ▪ DDoS Professional Services
Geographic Presence	North America, Middle East

Source: Company Website

17.2.15 QRATOR LABS

Founded	2010
Country	Czech Republic
City	Prague
Ownership Type	Private
Business Overview	Qrator Labs is a cybersecurity and network security company specializing in DDoS protection, web application security, DNS security, bot protection, and network monitoring. The company evolved from a DDoS research initiative and launched its own distributed filtering network in 2010. Its portfolio includes Qrator.AntiDDoS, Qrator.WAF, Qrator.AntiBot, Qrator.SecondaryDNS, and Qrator.Radar, supported by its proprietary geo-distributed network security infrastructure. Qrator Labs provides cloud-based security solutions designed to maintain the availability and resilience of websites, applications, and network infrastructure. Qrator Labs' Qrator.AntiDDoS is a cloud-based DDoS mitigation service that protects applications and network infrastructure against attacks across Layers 3–7. The service operates through Qrator Labs' proprietary geo-distributed filtering network using a unified BGP Anycast architecture. The company currently reports more than 6 Tbps of filtering capacity and 15 global scrubbing centers on its DDoS service page. It supports Always-On, automated protection and provides both DNS-based and BGP-based connectivity, as well as targeted infrastructure protection. Qrator Labs serves organizations across industries including banking, eCommerce, media, education, gaming, online trading, and technology. The company states that its solutions are trusted by 1,000+ enterprises globally. Its filtering infrastructure connects to transcontinental Tier 1 and regional backbone providers and covers North America, Latin America, Europe, Asia Pacific, and the Middle East and North Africa.
Products/Solutions Offered	▪ Qrator.AntiDDoS ▪ Qrator.WAF ▪ Qrator.AntiBot ▪ Qrator.SecondaryDNS ▪ Qrator.Radar
Geographic Presence	North America, Europe, Asia Pacific, Middle East & Africa, Latin America

Source: Company Website

17.2.16 GCORE

Founded	2014
Country	Luxembourg
City	Contern
Ownership Type	Private
Business Overview	Gcore is a global edge, cloud, network, and security solutions provider specializing in infrastructure for applications, digital services, and AI workloads. Founded in 2014, the company offers a broad portfolio comprising Edge Cloud, Edge Network, CDN, hosting, bare metal, streaming, AI infrastructure, DDoS Protection, and Web Application and API Protection (WAAP). Gcore operates its own globally distributed infrastructure, comprising 210+ edge locations, 50+ cloud locations, 14,000+ peering partners, and 200+ Tbps of total network capacity. Gcore's DDoS Protection provides multi-layered protection across Layers 3, 4, and 7, using globally distributed scrubbing centers to analyze incoming traffic, filter malicious packets, and deliver clean traffic to protected infrastructure. The company offers protection for websites, applications, servers, networks, cloud infrastructure, and gaming environments. Its current DDoS protection network provides 200+ Tbps of filtering capacity, with a 99.99% uptime SLA and 24/7 expert support. Deployment options include Always-On and on-demand protection, GRE-based traffic diversion, proxy-based protection, and direct connectivity to Gcore scrubbing centers. Gcore also provides automated DDoS mitigation through integrations such as FastNetMon, which can detect attacks and trigger BGP-based traffic redirection to Gcore's scrubbing centers in under 1 second. In October 2025, Gcore reported successfully mitigating a 6 Tbps DDoS attack, demonstrating the capacity of its infrastructure to handle large-scale attacks. Gcore's ecosystem includes 14,000+ peering partners and 120+ Internet Exchange Points (IXPs), together with direct connectivity to Tier 1 ISPs. The company provides DDoS protection for industries including gaming, financial services, eCommerce, SaaS, hosting, and digital services. Its infrastructure spans 210+ edge locations across 6 continents and 50+ cloud locations, enabling global traffic distribution and geographically distributed DDoS mitigation.
Products/Solutions Offered	▪ DDoS Protection ▪ WAAP/Web Application Protection ▪ CDN ▪ Edge Cloud ▪ Edge Network ▪ Bare Metal ▪ Cloud Hosting ▪ AI Infrastructure ▪ Streaming Platform ▪ Load Balancing
Geographic Presence	North America, Europe, Asia Pacific, Middle East & Africa, Latin America

Source: Company Website

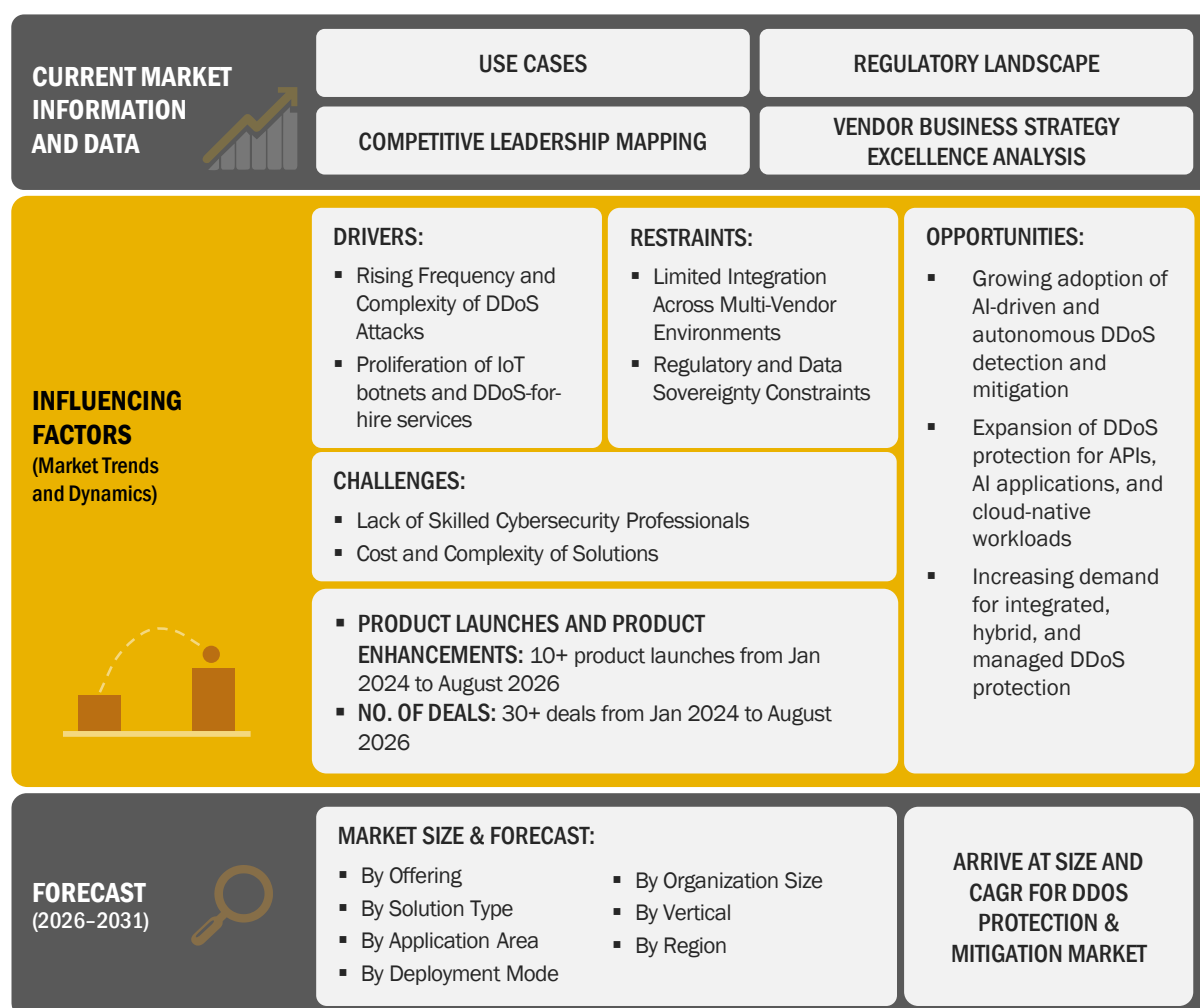
18 RESEARCH METHODOLOGY

18.1 RESEARCH DATA

This technical, market-oriented, and commercial study of the DDoS protection & mitigation market involved using extensive secondary sources, directories, and databases, such as D&B Hoovers and Bloomberg Businessweek, to identify and collect relevant information. The primary sources included industry experts from core and related industries, suppliers, manufacturers, distributors, service providers, technology developers, alliances, and organizations across all segments of this industry's value chain. In-depth interviews were conducted with various primary respondents, including key opinion leaders, subject-matter experts, C-level executives from companies offering DDoS protection & mitigation solutions, tools, and services, and industry consultants, to obtain and verify critical qualitative and quantitative information and to assess the market's prospects and industry trends. The following figure highlights the market research methodology applied in this report on the DDoS protection & mitigation market.

The figure below outlines the market research methodology used in preparing this report.

FIGURE 64 DDOS PROTECTION & MITIGATION MARKET: RESEARCH DESIGN



Source: Secondary Research, Industry Experts, and MarketsandMarkets Analysis

18.1.1 SECONDARY DATA

In the secondary research process, various sources were consulted to identify and collect information for the study. Secondary sources included annual reports, press releases, and investor presentations of DDoS protection & mitigation vendors, forums, certified publications, and whitepapers. The secondary research was used to obtain critical information on the industry's value chain, the total pool of key players, market classification, and segmentation from the market and technology-oriented perspectives.

FACTORS CONSIDERED FOR ESTIMATING THE REGIONAL-LEVEL MARKET SIZE ARE AS FOLLOWS:

- Gross domestic product (GDP) growth
- Information and communications technology (ICT) security spending
- Recent market developments
- Technology adoption
- Adoption of adjacent markets, such as the Anti-money Laundering (AML) and eGRC market

18.1.2 PRIMARY DATA

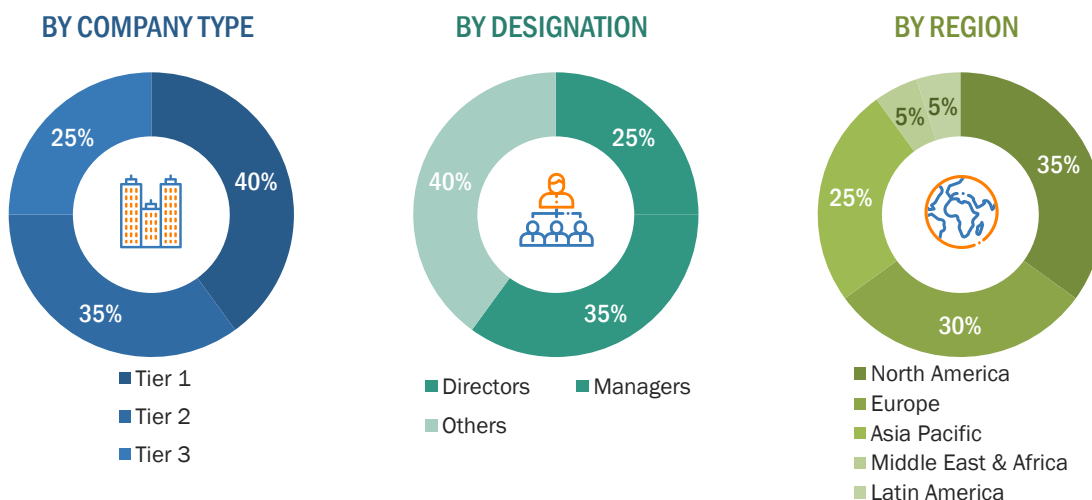
In the primary research process, various primary sources from both the supply and demand sides of the DDoS protection & mitigation market ecosystem were interviewed to obtain qualitative and quantitative information. The primary sources on the supply side included industry experts, such as Chief Executive Officers (CEOs), Vice Presidents (VPs), marketing directors, technology and innovation directors, and other key executives from various vendors providing DDoS protection & mitigation solutions, associated service providers, and system integrators operating in the targeted regions. All possible parameters that affect the market covered in this research study were accounted for, viewed in extensive detail, verified through primary research, and analyzed to obtain the final quantitative and qualitative data.

After the complete market engineering process (including calculations for market statistics, market breakups, market size estimations, market forecasting, and data triangulation), extensive primary research was conducted to gather information and verify and validate the critical numbers arrived at. The primary research helped identify and validate segmentation types, industry trends, key players, the competitive landscape of DDoS protection & mitigation solutions offered by several market vendors, and key market dynamics, including drivers, restraints, opportunities, and challenges.

In the complete market engineering process, bottom-up and top-down approaches, along with several data triangulation methods, were extensively used to perform the market estimation and market forecasting for the overall market segments and subsegments listed in this report. Extensive qualitative and quantitative analysis was performed across the complete market engineering process to present key information/insights throughout the report.

18.1.2.1 Breakup of primary profiles

FIGURE 65 BREAKUP OF PRIMARY PROFILES, BY COMPANY TYPE, DESIGNATION, AND REGION



Note 1: The companies have been categorized based on their total annual revenue; tier 1 companies = revenue greater than USD 10 billion; tier 2 companies = revenue between USD 1 billion and USD 10 billion; tier 3 companies = revenue between USD 500 million and USD 1 billion.

Note 2: Others include sales managers, marketing managers, and product managers

Source: MarketsandMarkets Analysis

18.1.2.2 Key industry insights

FIGURE 66 KEY INSIGHTS FROM INDUSTRY EXPERTS



The rapid growth of hyper-volumetric and multi-vector DDoS attacks is making automated, always-on mitigation a business imperative. Organizations are moving beyond reactive, manual defenses toward AI-driven systems that can detect abnormal traffic and respond within seconds, minimizing service disruption and protecting critical digital infrastructure.

- Chief Product Officer (CPO)
Leading DDoS Protection & Mitigation Solution Provider

Application and API infrastructure is becoming a critical DDoS protection priority. As organizations accelerate AI adoption and expand API-driven services, attackers are increasingly combining API abuse, web application attacks, and Layer 7 DDoS activity. Organizations require application-aware protection that can distinguish legitimate traffic from sophisticated attacks without affecting customer experience.

- CTO
Global Application & DDoS Protection Provider





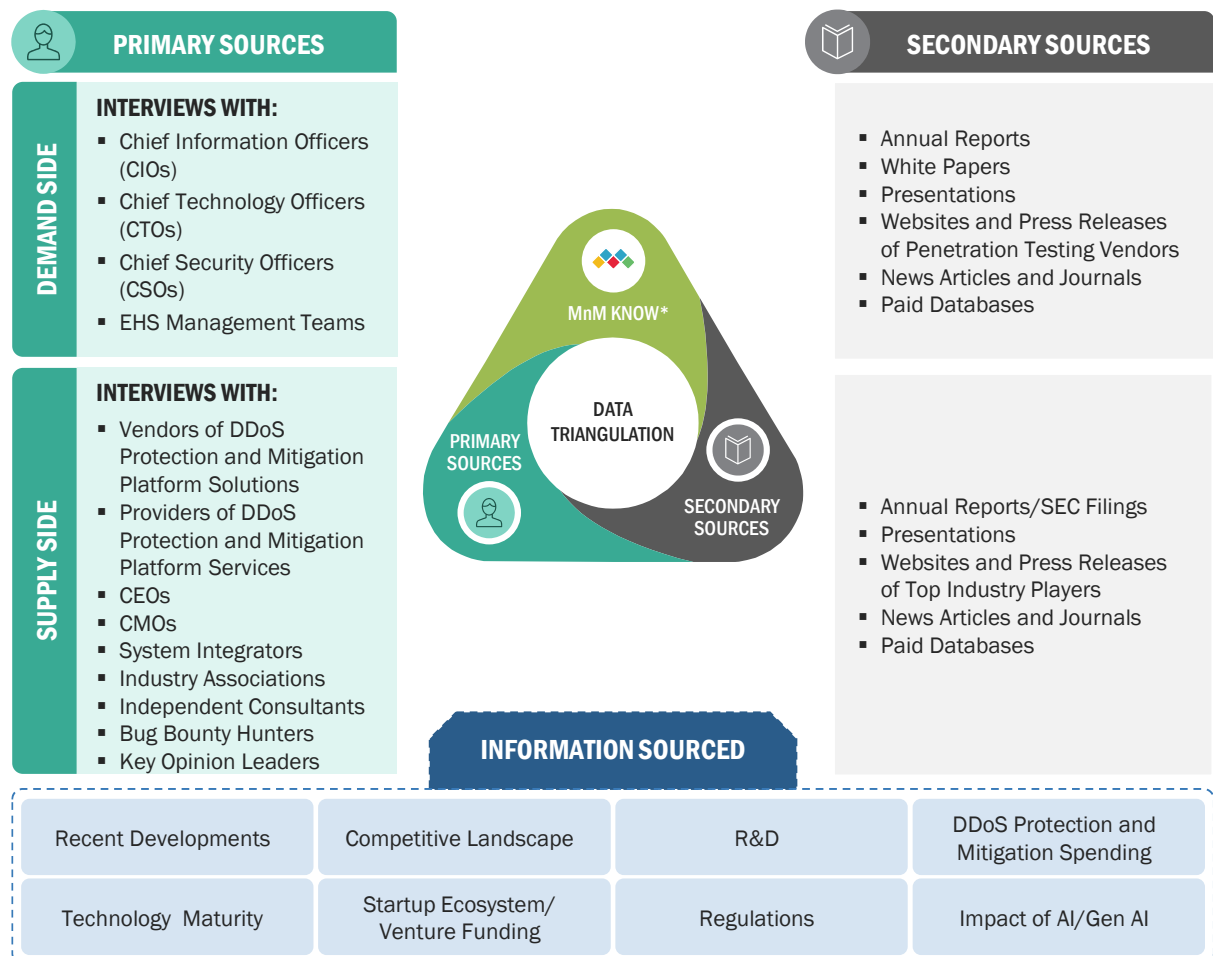
The convergence of DDoS protection with cloud, network, and application security is transforming how enterprises manage digital resilience. Unified platforms combining traffic analysis, automated mitigation, WAF, API security, and threat intelligence are improving visibility and accelerating response while helping organizations protect increasingly distributed infrastructure.

- VP, Financial Crime Solutions
Leading Network & DDoS Security Provider

Source: Industry Experts

18.2 DATA TRIANGULATION

FIGURE 67 DATA TRIANGULATION



*MnM KNOW stands for MarketsandMarkets' "Knowledge Asset Management" framework. In this context, it stands for the existing market research knowledge repository of over 5,000 granular markets, our flagship competitive intelligence and market research platform, "Knowledge Store", subject matter experts, and independent consultants. MnM KNOW acts as an independent source that helps us validate the information gathered from primary and secondary sources. MarketsandMarkets reports, such as the cybersecurity market report, have been referred to in making this report.

Source: MarketsandMarkets Analysis

18.3 MARKET SIZE ESTIMATION

Top-down and bottom-up approaches were used to estimate and validate the size of the global DDoS protection & mitigation market and its dependent subsegments. The research methodology used to estimate the market size included the following details:

- Key players in the market were identified through secondary research, and their revenue contributions in the respective regions were determined through primary and secondary research.
- This procedure included studying top market players' annual and financial reports and extensive interviews for key insights from industry leaders, such as CEOs, VPs, directors, and marketing executives.
- All percentage splits and breakdowns were determined using secondary sources and verified through primary sources.

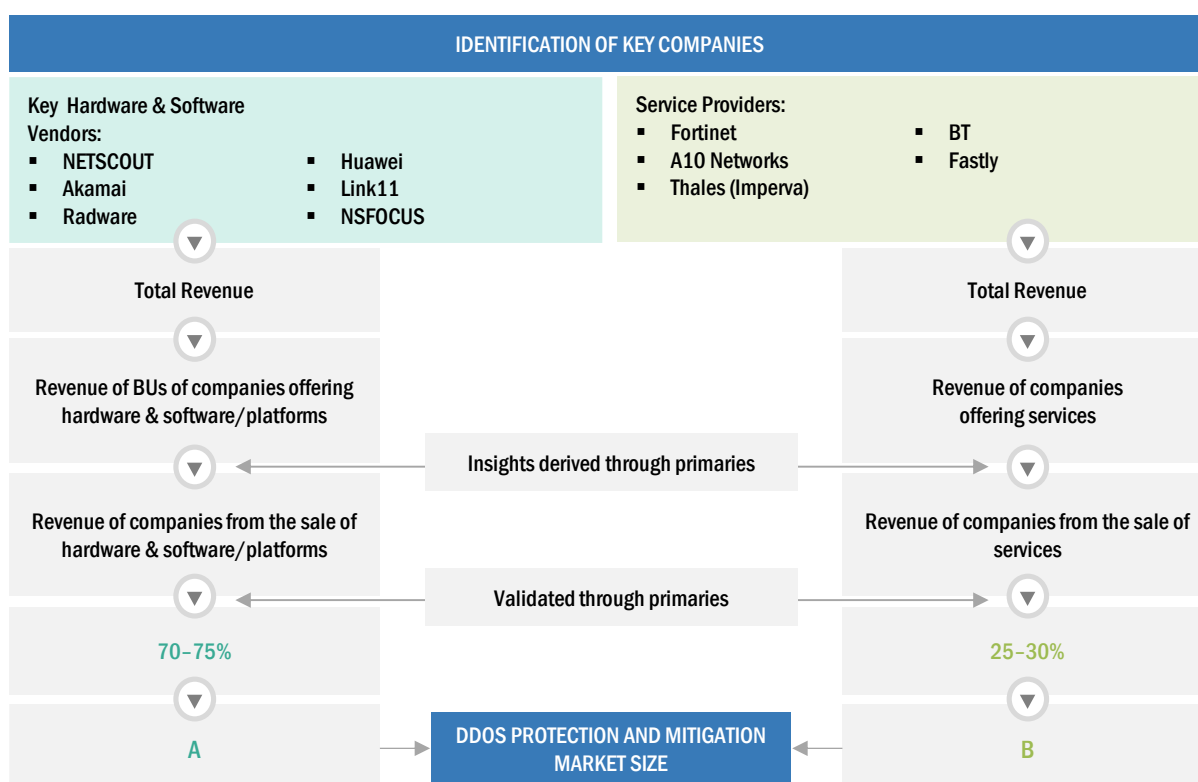
- All the possible parameters that impact the market covered in this research study have been accounted for, examined in detail, verified through primary research, and analyzed to yield the final quantitative and qualitative data. This data is consolidated and supplemented with detailed inputs and analysis from MarketsandMarkets.

18.3.1 TOP-DOWN APPROACH

In the top-down approach, an exhaustive list of all the vendors offering DDoS protection & mitigation solutions and services in the market is provided. The revenue contribution for all the vendors in the market was estimated through annual reports, press releases, funding, investor presentations, paid databases, and primary interviews. Each vendor was evaluated based on their products/solutions by technology, product type, service, and application. The aggregate of all company revenues was extrapolated to reach the overall market size.

Each subsegment was studied and analyzed for its global market size and regional penetration. The markets were triangulated through primary and secondary research. The primary procedure included extensive interviews with industry leaders, including Chief Executive Officers (CEOs), Vice Presidents (VPs), directors, and marketing executives, to obtain key insights. These market numbers were further triangulated with the existing MarketsandMarkets repository for validation.

FIGURE 68 **APPROACH 1 (SUPPLY SIDE): REVENUE OF VENDORS IN DDOS PROTECTION & MITIGATION MARKET**



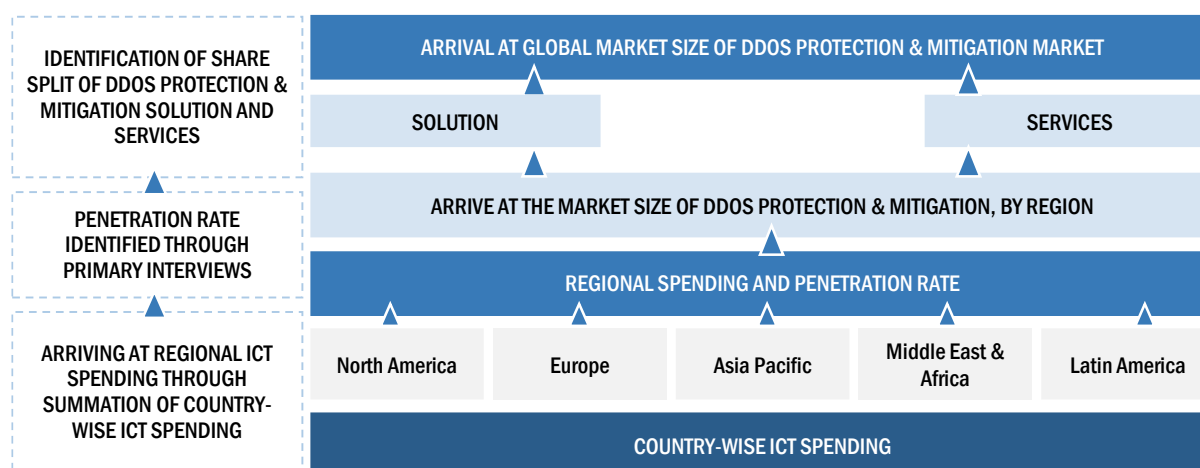
Source: Secondary Research and MarketsandMarkets Analysis

18.3.2 BOTTOM-UP APPROACH

The bottom-up approach identified the adoption rates of DDoS protection & mitigation solutions and services across different verticals in key countries, focusing on the region that contributes the most to market share. Further, for cross-validation, the adoption rate of DDoS protection & mitigation solutions and services in various industries and use cases was identified and extrapolated. In addition, weights were given to the use cases identified in different regions for calculation.

Based on these numbers, the regional split was determined by primary and secondary sources. The procedure included an analysis of regional penetration in the market. Provincial spending on Information and Communications Technology (ICT), socioeconomic analysis of each country, strategic vendor analysis of major DDoS protection & mitigation providers, and organic and inorganic business development activities of regional and global players were estimated based on secondary research. With the data triangulation procedure and data validation through primary data, this study determined and confirmed the exact values of the overall DDoS protection & mitigation market size and its segments' market size.

FIGURE 69 **APPROACH 2 (DEMAND SIDE): DDOS PROTECTION & MITIGATION MARKET**

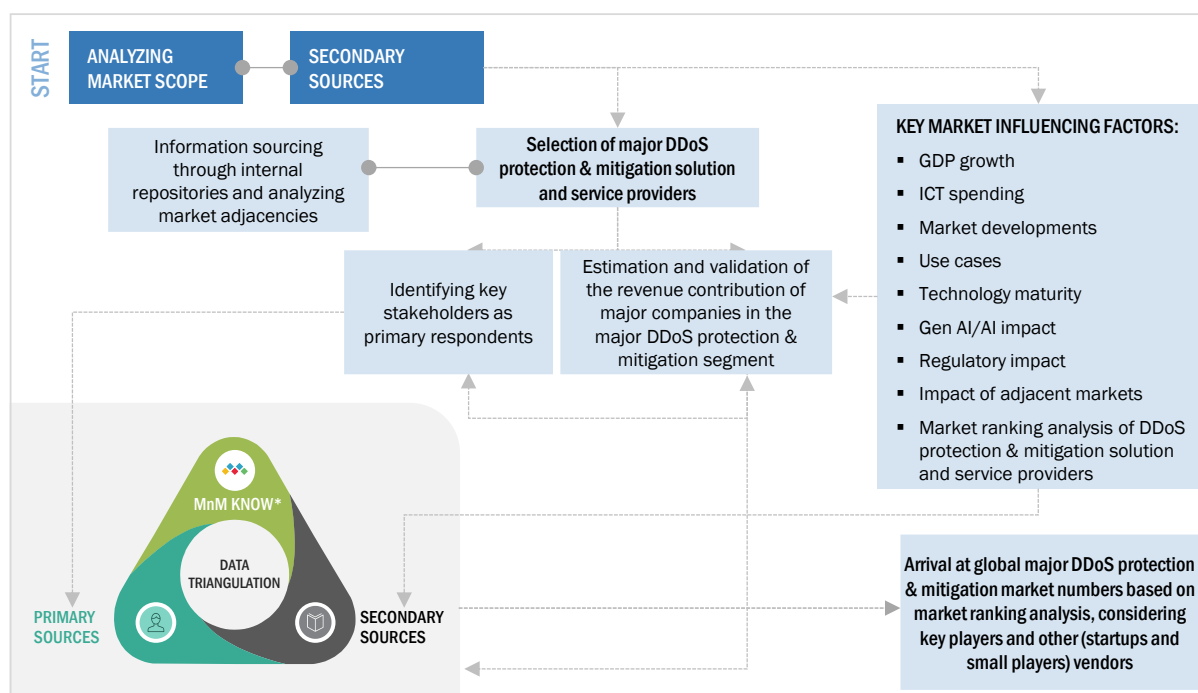


Source: Secondary Research and MarketsandMarkets

FIGURE 70 **TECHNOLOGY/PRODUCT ROADMAP**

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Identification of 18–20 major DDoS protection and mitigation companies, such as NETSCOUT, Akamai, Radware, NSFOCUS, Huawei, Fortinet, Link11, Thales (Imperva), Cloudflare, BT, A10 Networks, Fastly, Nexusguard, Corero, RioRey, PhoenixNAP, Allot, StrataCore, Sucuri, StackPath, Seceon, HaltDos, DDoS-Guard, Indusface, Mlytics, F5	Estimation of top players' potential revenue from their respective BUs that offer DDoS protection and mitigation hardware solutions & software solutions, and services	Identification of the revenue contribution of DDoS protection and mitigation hardware solutions & software solutions, and services to the relevant BU/BUS	Calculation of the total market size of DDoS protection and mitigation platforms, solutions, and services using the combined share of top companies and their revenues	Revalidation of the total market size and market share estimations with primary respondents
KEY SOURCES OF INFORMATION:				
Secondary sources such as company financials, press releases, paid databases (Factiva), and primary research	Secondary sources such as company financials, press releases, paid databases (Factiva), and primary research	Primary research (CEOs, VPs, marketing directors, and technology and innovation directors, among other stakeholders)	MarketsandMarkets calculations, company websites, and annual reports	Primary research (directors - product development, VPs - operations, DDoS protection and mitigation managers, COOs, and CSOs)

Source: Secondary Research and MarketsandMarkets Analysis

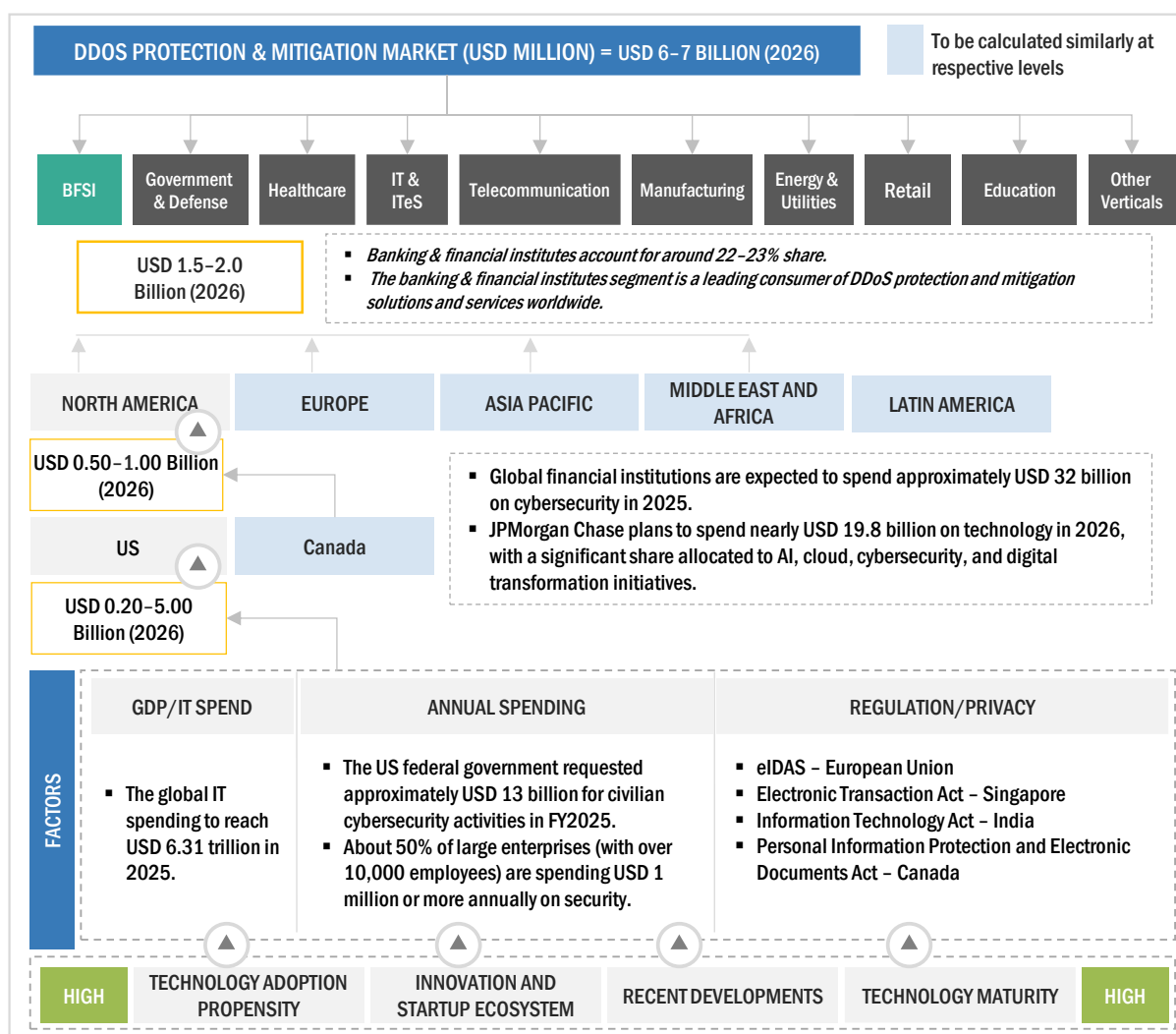
FIGURE 71 DDOS PROTECTION & MITIGATION MARKET ESTIMATION: RESEARCH FLOW

Source: MarketsandMarkets Analysis

In this approach for market estimation, the key companies offering DDoS protection & mitigation globally were identified. This crucial factor contributes to nearly half of the DDoS protection & mitigation market. After finalizing these companies, the data was validated by industry experts through primary interviews with the market's leading vendors. Furthermore, their total revenue was estimated through annual reports, the US Securities and Exchange Commission (SEC) filings, and paid databases.

The revenue of the Business Units (BUs) that offer DDoS protection & mitigation would be identified through similar sources. Furthermore, revenue data generated by the global DDoS protection & mitigation industry was collected through primary sources.

The collective revenue of key companies offering DDoS protection & mitigation accounted for more than 25% of the market, as confirmed through primary interviews with industry experts. With the assumption that the rest of the market is contributed by local or smaller players (part of the unorganized market), the market size of organized players (55–60%) and unorganized players (40–45%) was collectively assumed to be the market size of the global DDoS protection & mitigation market for the Financial Year (FY) 2025–2026.

FIGURE 72 **APPROACH 2: BOTTOM-UP (DEMAND SIDE) - PLATFORMS/SOLUTIONS/SERVICES**


Source: MarketsandMarkets Analysis

18.4 MARKET FORECAST

Factors that directly or indirectly impact the market were analyzed to estimate the market's overall trend during the forecast period. Each element was analyzed on a scale of 1–3 (1 = low, 3 = high). After analyzing each factor and its impact on the market, different forecasting techniques were used to determine the market size.

TABLE 643 **FACTOR ANALYSIS**

FACTOR	INFERENCE	IMPACT
DDoS Threat Landscape	The increasing frequency, scale, and sophistication of DDoS attacks are driving demand for advanced detection and mitigation capabilities. Cloudflare reported 23.2 million network-layer DDoS attacks in H1 2026, while NETSCOUT recorded more than 8 million attacks globally in 2H 2025, with attacks reaching up to 30 Tbps.	High
Cloud & Digital Infrastructure Adoption	Rapid adoption of cloud computing, distributed infrastructure, data centers, and Internet-facing digital services is expanding the attack surface and increasing the need for scalable DDoS protection. Organizations increasingly require cloud-based and hybrid mitigation to protect distributed workloads and maintain service availability.	High

Web Applications & API Adoption	The proliferation of web applications, APIs, digital platforms, and application-driven services is increasing exposure to application-layer DDoS attacks. Organizations are consequently investing in application-aware mitigation, WAF integration, API protection, bot management, and behavioral traffic analysis.	High
AI & Automation Adoption	AI, machine learning, behavioral analytics, and automated response are increasingly being incorporated into DDoS detection and mitigation to identify anomalous traffic and accelerate response. Cloudflare reported that hyper-volumetric attacks exceeding 1 Tbps surged significantly in Q2 2026, reinforcing the need for automated protection capable of responding faster than manual intervention.	High
Network & Internet Infrastructure Expansion	Expansion of broadband networks, 5G, data centers, edge infrastructure, and connected digital services is increasing the volume of Internet traffic and the number of assets requiring protection. Telecommunications providers, cloud providers, and enterprises are therefore increasing investments in network-level traffic analysis and high-capacity mitigation.	High
Application & DNS Attack Evolution	DDoS attacks are increasingly targeting DNS and application layers alongside traditional volumetric attacks. Cloudflare reported that DNS-based attacks represented 34.3% of network-layer activity in H1 2026, while DNS Floods increased substantially between Q1 and Q2. This is driving demand for specialized DNS, application, and multi-layer protection.	High
Cybersecurity Spending	Increasing enterprise cybersecurity spending is supporting investment in DDoS protection as organizations prioritize business continuity, network resilience, and protection of critical digital services. DDoS protection is increasingly being integrated with broader network, application, cloud, and security operations infrastructure rather than being treated as an isolated security control.	High
Cloud-Based DDoS Protection Adoption	Cloud-based mitigation enables organizations to absorb large-scale attacks using distributed scrubbing infrastructure without deploying equivalent capacity on premises. The ability to rapidly scale protection and support hybrid and multi-cloud environments is increasing adoption among enterprises and service providers.	High
Botnet & IoT Proliferation	The growing number of connected devices, routers, and IoT endpoints is increasing the resources available to attackers for launching distributed DDoS campaigns. NETSCOUT identified large-scale IoT botnets capable of generating attacks exceeding 1 Tbps, increasing demand for botnet detection, traffic intelligence, and automated mitigation.	High
Managed DDoS Services Adoption	Organizations with limited cybersecurity resources are increasingly relying on managed DDoS protection for continuous monitoring, detection, mitigation, and incident response. Managed services reduce the requirement for specialized internal expertise and provide access to distributed mitigation infrastructure, supporting adoption among enterprises and SMEs.	Medium
Regulatory & Business Continuity Requirements	Increasing emphasis on operational resilience, cybersecurity risk management, and continuity of critical digital services is encouraging organizations to strengthen availability protection. Financial institutions, government organizations, telecommunications providers, and critical infrastructure operators have particularly strong requirements for maintaining uninterrupted services.	Medium
Recent Developments	Recent developments include programmable DDoS mitigation, AI-assisted attack operations, expanded cloud mitigation capacity, DNS-focused attacks, and integration of DDoS protection with broader security platforms. Cloudflare has also introduced programmable flow protection that allows customers to deploy customized DDoS mitigation logic across its global network.	Medium

Source: MarketsandMarkets Analysis

18.5 RESEARCH ASSUMPTIONS

The following assumptions were taken into consideration to complete the overall market engineering for the DDoS protection & mitigation market:

PARAMETER	ASSUMPTION
Global DDoS Protection & Mitigation Market Size	Market size estimates are based on a conservative adoption outlook considering the increasing frequency and complexity of DDoS attacks, growing cloud and digital infrastructure, adoption of AI-driven detection and automated mitigation, and increasing protection requirements across network infrastructure, web applications, APIs, and DNS environments.
Exchange Rate	It is assumed that fluctuations in major currencies against the US dollar remain within historical ranges and do not materially affect the overall market estimates.
Quantitative Assumption	The market size may not add up exactly due to rounding. Market estimation considers adjacent technology markets such as network security, application security, cloud security, bot management, traffic analysis, and cybersecurity services; only the DDoS-specific portion of these offerings is considered. Open-source, freeware, and internally developed DDoS protection tools and solutions are excluded.
Global Economic Condition	The global economy is assumed to remain moderately stable despite inflationary pressures, geopolitical uncertainties, and varying enterprise technology spending. Continued investments in cloud computing, data centers, 5G, digital services, and cybersecurity are expected to sustain demand for DDoS protection & mitigation solutions. The increasing scale of attacks further supports cybersecurity spending focused on business continuity and infrastructure resilience.
Geographic Analysis	The study covers North America, Europe, Asia Pacific, Middle East & Africa, and Latin America. Regional market estimates are based on cloud adoption, Internet infrastructure, digital transformation, cybersecurity spending, DDoS attack activity, and deployment of DDoS protection across enterprises, telecommunications providers, cloud service providers, and government organizations.
Vendor/Product Mapping	Vendor revenues are estimated based on the proportion attributable to DDoS protection & mitigation offerings. For diversified vendors, only the relevant DDoS-related revenue contribution is considered rather than total company revenue. Integrated products containing DDoS capabilities are considered only to the extent that DDoS protection forms part of the addressable offering.
Market Segmentation	The market is estimated across Offering (Hardware, Software/Platforms, Services), Solution Type, Application Area, Deployment Mode, Organization Size, and Vertical. Segments are structured to minimize overlap, and the total market size is reconciled across the primary offering segmentation.
Attack and Threat Environment	The market outlook assumes continued growth in volumetric, protocol, application-layer, DNS, and multi-vector DDoS attacks. Recent Cloudflare data indicates that it mitigated 23.2 million network-layer DDoS attacks and 29.64 trillion HTTP DDoS requests in H1 2026, supporting the assumption of sustained demand for automated and scalable protection.
Technology Adoption	Increasing adoption of AI/ML-based traffic analysis, autonomous mitigation, cloud-based scrubbing, application/API protection, and hybrid deployment is assumed to support continued market expansion. The market increasingly favors always-on automated mitigation because many attacks are too short-lived for manual intervention.

Source: MarketsandMarkets Analysis

18.6 RESEARCH LIMITATIONS

The following limitations were taken into consideration to complete the overall market engineering process of the DDoS protection & mitigation market:

 METHODOLOGY – RELATED LIMITATIONS	 SCOPE – RELATED LIMITATIONS
▪ The report focuses on DDoS protection and mitigation solutions offered by major vendors for the study. The analysis is limited to core DDoS protection and mitigation solutions and services provided, and the potential capabilities of cybersecurity solutions and services. ▪ The quantitative and qualitative information on market estimates and trends is aggregated and triangulated with the initial overall revenue estimates of DDoS protection and mitigation vendors. The triangulation of data points is continued through a cycle of concurrent validation with multiple stakeholders to limit the possibility of double-counting for any solution to a minimum.	▪ The report covers five major regions and country-wise segmentation: North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America. ▪ There are a total of 196 countries in the world. Analyzing each country for the market would not be feasible. Hence, the market study does not include all the country-level analyses. ▪ For a few countries (China), information and data available from secondary sources have been considered due to the unavailability of authentic sources and primary sources due to language and political barriers. ▪ Market share/value analysis may have a $\pm 10\%$ deviation.

Source: MarketsandMarkets Analysis

19 APPENDIX

19.1 DISCUSSION GUIDE

A discussion guide is a set of questions and pain points for which an analyst wants to gain insights from industry and subject matter experts.

We are conducting a global DDoS protection & mitigation market study focusing on current trends and opportunities. The report provides comprehensive details and forecast analysis of the overall market and its submarkets. It also features a detailed analysis of the opportunities, market drivers, restraints, roadmaps, competitive landscape, and profiles of key industry players.

Name

Designation

Company Name

Phone No

Email ID

Q. 1. Could you provide a brief on your offerings related to the DDoS protection & mitigation market?

Primary's Viewpoint: _____

Q. 2. How do you see the growth of the DDoS protection & mitigation market globally, now, and in the next five years? What would be the projected market size and growth rate of the market by 2031 and between 2026 and 2031, respectively?

Primary's Viewpoint: _____

Q. 3. What are the DDoS protection & mitigation market's top three drivers, restraints, opportunities, and challenges?

SR. NO.	DRIVERS	RESTRAINTS	OPPORTUNITIES	CHALLENGES
1				
2				
3				

- Q. 4.** We have segmented the DDoS protection & mitigation market based on offering, as given below. According to you, which offering is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–2, with 2 being the most lucrative.

SR. NO.	OFFERING	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Solutions		
2	Services		

Comments: _____

- Q. 5.** We have segmented the DDoS protection & mitigation market based on solution type, as given below. According to you, which solution type is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–4, with 4 being the most lucrative.

SR. NO.	SOLUTION TYPE	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Network Traffic Analyzers		
2	Threat Mitigation Systems		
3	Botnet Detection & Management Systems		
4	Other Solution Types (Orchestration & Management and Threat Intelligence)		

Comments: _____

- Q. 6.** We have segmented the DDoS protection & mitigation market based on application area, as given below. According to you, which service is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–3, with 3 being the most lucrative.

SR. NO.	APPLICATION AREA	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Network & IP Infrastructure		
2	Web Applications & APIs		
3	DNS Infrastructure		

Comments: _____

- Q. 7.** We have segmented the DDoS protection & mitigation market based on deployment mode size, as given below. According to you, which deployment mode is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–3, with 3 being the most lucrative.

SR. NO.	DEPLOYMENT MODE	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	On-Premises		
2	Cloud		
3	Hybrid		

Comments: _____

- Q. 8.** We have segmented the DDoS protection & mitigation market based on organization size, as given below. According to you, which organization size is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–2, with 2 being the most lucrative.

SR. NO.	ORGANIZATION SIZE	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	Large Enterprises		
2	SMEs		

Comments: _____

- Q. 9.** We have segmented the DDoS protection & mitigation market based on vertical. Which vertical, in your opinion, is the most attractive in terms of market opportunities now and in the future? Please rate on a scale of 1–11, with 11 being the most lucrative.

SR. NO.	VERTICAL	ATTRACTIVENESS OF OPPORTUNITY, 2026	ATTRACTIVENESS OF OPPORTUNITY, 2031
1	BFSI		
2	Government & Defense		
3	Healthcare		
4	IT & ITeS		
5	Telecommunications		
6	Manufacturing		
7	Energy & Utilities		
8	Retail		
9	Education		
10	Other Verticals		

Comments: _____

Q. 10. In your opinion, which region contributes the highest (1) and lowest (5) revenue now (2026) and in the future (2031) to the DDoS protection & mitigation market? Please rank on a scale of 1-5, with 1 being the highest.

SR. NO.	REGION	REVENUE SHARE, 2026	REVENUE SHARE, 2031
1	North America		
2	Europe		
3	Latin America		
4	Asia Pacific		
5	Middle East & Africa		

Comments: _____

Q. 11. What are the various regulations and standards impacting the DDoS protection & mitigation market?

Response: _____

Q. 12. What innovations are you expecting in the DDoS protection & mitigation market that would have a high impact on the market?

Response: _____

Q. 13. Please name and rank your three main competitors.

Primary's Viewpoint: _____

Q. 14. What would you like to see covered additionally in the report besides the market segmentation mentioned?

Primary's Viewpoint: _____

19.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL

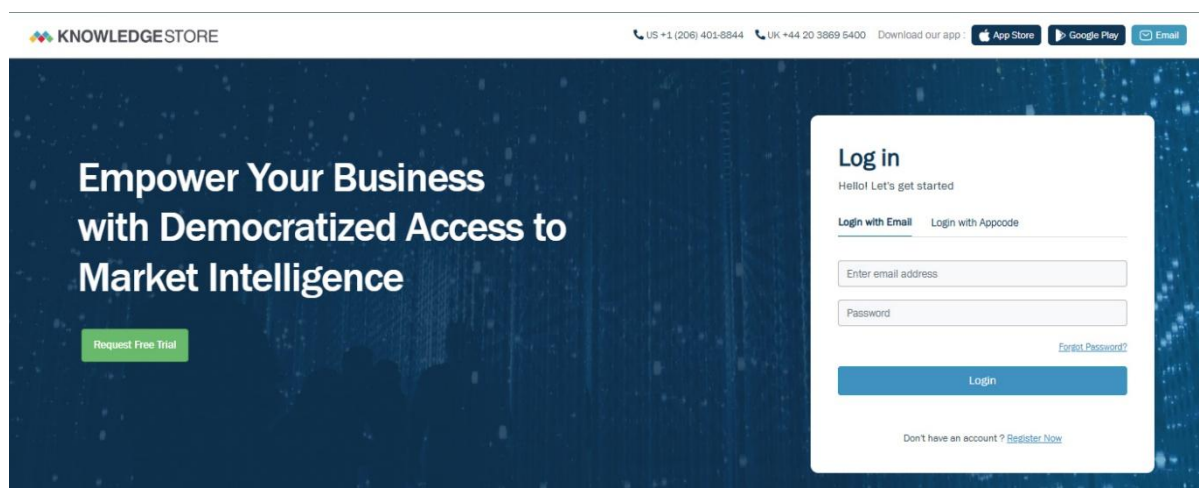
KnowledgeStore contains unique market insights of MarketsandMarkets. As a subscriber, you have access to all of the published titles and any new ones added over the course of the subscription period. You can subscribe to a specific number of reports or domains of your interest.

KNOWLEDGESTORE ENABLES YOU TO:

- View & download all subscribed reports from a single, online platform
- Contact our analysts to answer any questions related to our reports or request a custom research
- Share comments on specific reports with the other users of your organization
- Suggest titles/topics to our research teams that you would like us to cover in our future reports
- Identify reports published on the high-growth markets within your industry

Get started now by requesting a demo and learning more about KnowledgeStore [at www.mnmks.com](http://www.mnmks.com).

MARKETSANDMARKETS KNOWLEDGESTORE SNAPSHOT



The image shows a screenshot of the KnowledgeStore website. The header includes the KnowledgeStore logo, contact numbers for the US (+1 206 401-8844) and UK (+44 20 3869 5400), and links to download the app from the App Store and Google Play, along with an email link. The main content area has a dark blue background with a grid pattern. On the left, the text 'Empower Your Business with Democratized Access to Market Intelligence' is displayed, with a green 'Request Free Trial' button below it. On the right, there is a white login box titled 'Log in' with the subtitle 'Hello! Let's get started'. It offers 'Login with Email' and 'Login with Appcode' options. The email login section includes input fields for 'Enter email address' and 'Password', a 'Forgot Password?' link, and a blue 'Login' button. At the bottom of the login box, it says 'Don't have an account? Register Now'.

MARKETSANDMARKETS KNOWLEDGESTORE: INFORMATION & COMMUNICATION TECHNOLOGY SNAPSHOT

KNOWLEDGESTORE Home Insights Trends Companies News Tools Admin

Search Advanced Search

INDUSTRY TRENDS

Information & Communications Technology Reports: 1200+

- Aerospace & Defence
- Agriculture
- Automotive & Transportation
- Banking, Financial Services & Insurance
- Chemicals & Material
- Energy & Power
- Food & Beverage
- Healthcare
- Information & Communications Technology**
- Packaging, Construction, Mining & Gases
- Retail & eCommerce
- Semiconductor & Electronics

Analytics (100+), Application Security (50+), Cloud Computing (100+), Cyber Security (100+), Data Centre & Networking (80+), Digitalization & IoT (100+), Endpoint Security (30+), Mobility & Telecom (100+), Network Security (50+), Public Safety (30+), Software & Services (300+), Software Defined Anything(SDx) (10+)

Ask Analyst, Request Workshop, Suggest Title

KNOWLEDGESTORE Home Insights Trends Companies News Tools Admin

Search Advanced Search

HIGH GROWTH MARKETS

You Selected: Information & Communications Technology (1071)

Industries

- ☐ Aerospace & Defence (350)
- ☐ Agriculture (222)
- ☐ Automotive & Transportation (354)
- ☐ Chemicals & Material (1296)
- ☐ Energy & Power (396)
- ☐ Food & Beverage (349)
- ☐ Healthcare (585)
- ☒ Information & Communications Technology (1071)
 - ☒ Analytics (167)
 - ☒ Cloud Computing (97)
 - ☒ Data Centre & Networking (80)
 - ☒ Digitalization & IoT (93)
 - ☒ Information Security (185)
 - ☒ Mobility & Telecom (124)
 - ☒ Software & Services (325)

Search Reports

Export Excel

All market sizes are in USD Bn

REPORT TITLE	DOMAIN	MARKET SIZE-2022	CAGR %	PUBLISHED
Blockchain in Retail Market by Provider, Application (Compliance Management, Identity Management, Loyalty & Rewards Management, Payment, Smart Contracts, and Supply Chain Management), Organization Size, and Region - Global Forecast to 2027	Information & Communications Technology	1.19	96.4	Jun 2018

22.74%, 22.72%, 21.28%, 19.00%, 18.60%, 16.02%, 13.60%

19.3 CUSTOMIZATION OPTIONS

With the given market data, MarketsandMarkets offers customizations per company-specific needs. The following customization options are available for the report:

COMPANY INFORMATION

- Detailed analysis and profiling of additional market players (up to five)

GEOGRAPHIC ANALYSIS

- Further breakdown of the geographies into respective countries

19.4 RELATED REPORTS

SR. NO	REPORT TITLE	PUBLISHED DATE
1	ATTACK SURFACE MANAGEMENT MARKET - GLOBAL FORECAST TO 2029 By Offering (Solutions, Services), Deployment Mode (Cloud, On-premises), Organization Size (Large Enterprises, SMEs), Vertical (BFSI, Healthcare, Retail & E-Commerce) and Region https://www.marketsandmarkets.com/Market-Reports/attack-surface-management-market-175286676.html	April 2024
2	AUTOMATED BREACH AND ATTACK SIMULATION MARKET - GLOBAL FORECAST TO 2029 By Application (Configuration Management, Patch Management, Threat Intelligence), Vertical (BFSI, Healthcare, IT & ITeS, Education, Manufacturing) https://www.marketsandmarkets.com/Market-Reports/automated-breach-attack-simulation-market-43164821.html	October 2024

19.5 AUTHOR DETAILS

Harminder Singh Bhatia

*Assistant Vice President,
Information and
Communications Technology*

Strategic Market Intelligence Leader with 17+ years of expertise in Research, Sales Enablement, Client Engagement, and Business Advisory. Demonstrated success in establishing and scaling research functions, delivering actionable market insights, optimizing sales processes, and shaping business strategies for clients across North America and Europe. Career experience spans leadership roles with PwC, Innova Solutions, Cognizant, Copal Amba (Moody's), and GlobalData.

Proficient in account and client management, competitive intelligence, emerging technology trends, vendor evaluations, and strategic consulting engagements. Recognized for driving market entry and expansion strategies, growth advisory initiatives, stakeholder analysis, and large-scale project execution. Experienced in leading technology integration and consulting programs within the ICT domain, covering multiple industry verticals.

Holds a Master of Business Administration (Finance & Marketing) and a Bachelor of Commerce, complemented by a professional certification from the National University of Singapore.

Vivek Ravichandran

*Senior Research Manager,
Information and
Communications Technology*

17 years of experience in Business Advisory, Strategy & Growth Consulting, and Best Practices Benchmarking.

In his current role, Vivek focuses on revenue impact for clients through new revenue opportunities driven by the everchanging revenue mix, uses cases driving the change, and how clients can tap new revenue streams while leveraging the current revenue streams (cash cows).

Before MarketsandMarkets, he worked with Ramco Systems, Zinnov (deputed), Infiniti Research (TechNavio), and Cognizant, where he played the role of a strategic partner for Mobility and CIS teams to penetrate key accounts from core pillars and strengthen revenue streams.

Vivek holds a Master's in Business Administration with a dual specialization in Finance & Marketing from NMIMS and a Bachelor of Engineering in Electronics and Communication from Anna University.

Contributors

Sayali Saste
Manager

Vidhu Rawat
Assistant Manager

Shivam Jethwa
Team Lead

Aditi Deshmukh
Sr. Research Associate

Disclaimer: MarketsandMarkets™ provides strategic analysis services to a select group of customers in response to orders. Our customers acknowledge when ordering that these strategic analysis services are solely for internal use and not for general publication or disclosure to any third party. MarketsandMarkets™ does not endorse any vendor, product, or service profiled in its publications. MarketsandMarkets™ strategic analysis constitutes estimations and projections based on secondary and primary research and are therefore subject to variations. MarketsandMarkets™ disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness, for any particular purpose. MarketsandMarkets™ takes no responsibility for incorrect information supplied to it by manufacturers or users.

Trademarks, copyrights, and other forms of intellectual property belong to MarketsandMarkets™ or their respective owners and are protected by law. Under no circumstance may any of these be reproduced, copied, or circulated in any form, without the prior written approval of MarketsandMarkets™ or its owner—as the case may be. No part of this strategic analysis service may be given, lent, resold, or disclosed to any third party, without express permission from MarketsandMarkets™.

Reproduction and/or transmission in any form and by any means, including photocopying, mechanical, electronic, recording, or otherwise, without the permission of MarketsandMarkets™, is prohibited.

For information regarding permission, contact:
Tel: +1-888-600-6441