

DDOS PROTECTION & MITIGATION SECURITY MARKET

GLOBAL FORECAST TO 2030

BY SOLUTION TYPE (NETWORK TRAFFIC ANALYZERS, THREAT MITIGATION SYSTEM,
BOTNET DETECTION & MANAGEMENT, SECURITY INFORMATION & EVENT MANAGEMENT,
ORCHESTRATION & AUTOMATION, OTHERS)

MarketsandMarkets™ is the world's largest revenue impact company, serving over 7,500 customers. 80% of the 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 USD 1 billion to USD 500 billion 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 © 2025 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.....	39
1.1	STUDY OBJECTIVES.....	39
1.2	MARKET DEFINITION.....	39
1.3	STUDY SCOPE	40
1.3.1	MARKET SEGMENTATION AND REGIONS COVERED	40
1.3.2	INCLUSIONS & EXCLUSIONS	41
1.4	YEARS CONSIDERED	41
1.5	CURRENCY CONSIDERED	42
1.6	STAKEHOLDERS	42
1.7	SUMMARY OF CHANGES.....	43
2	EXECUTIVE SUMMARY.....	44
2.1	KEY INSIGHTS AND MARKET HIGHLIGHTS.....	44
2.2	KEY MARKET PARTICIPANTS: MAPPING OF STRATEGIC DEVELOPMENTS	45
2.3	DISRUPTIONS SHAPING MARKET	46
2.4	HIGH GROWTH SEGMENTS.....	47
2.5	SNAPSHOT: GLOBAL MARKET SIZE, GROWTH RATE, AND FORECAST	47
3	PREMIUM INSIGHTS	49
3.1	ATTRACTIVE OPPORTUNITIES FOR PLAYERS IN DDOS PROTECTION & MITIGATION SECURITY MARKET	49
3.2	DDOS PROTECTION & MITIGATION SECURITY MARKET, BY OFFERING AND ORGANIZATION SIZE.....	50
3.3	DDOS PROTECTION & MITIGATION SECURITY MARKET, BY APPLICATION AREA	50
3.4	DDOS PROTECTION & MITIGATION SECURITY MARKET, BY VERTICAL.....	51
4	MARKET OVERVIEW.....	52
4.1	INTRODUCTION	52
4.2	MARKET DYNAMICS.....	52
4.2.1	DRIVERS.....	53
4.2.1.1	Rising frequency and complexity of DDoS attacks.....	53
4.2.1.2	Growing internet penetration and connectivity.....	54
4.2.2	RESTRAINTS.....	54
4.2.2.1	Limited integration across multi-vendor environments.....	54
4.2.2.2	Regulatory and data sovereignty constraints	54
4.2.3	OPPORTUNITIES.....	55
4.2.3.1	AI-driven predictive mitigation and automated threat correlation	55
4.2.3.2	Growing partnerships between ISPs, cloud providers, and security vendors.....	55
4.2.4	CHALLENGES	55

	4.2.4.1	Lack of skilled cybersecurity professionals	55
	4.2.4.2	Cost and complexity of solutions.....	56
4.3		UNMET NEEDS AND WHITE SPACES	56
4.4		INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES.....	56
4.5		STRATEGIC MOVES BY TIER-1/2/3 PLAYERS.....	57
5		INDUSTRY TRENDS	58
5.1		PORTER'S FIVE FORCES ANALYSIS	58
	5.1.1	THREAT OF NEW ENTRANTS	59
	5.1.2	THREAT OF SUBSTITUTES.....	59
	5.1.3	BARGAINING POWER OF SUPPLIERS	60
	5.1.4	BARGAINING POWER OF BUYERS	60
	5.1.5	INTENSITY OF COMPETITIVE RIVALRY	60
5.2		MACROECONOMICS INDICATORS.....	60
	5.2.1	INTRODUCTION	60
	5.2.2	GDP TRENDS AND FORECAST	61
	5.2.3	TRENDS IN GLOBAL DDOS PROTECTION & MITIGATION SECURITY INDUSTRY	61
5.3		SUPPLY CHAIN ANALYSIS	62
5.4		ECOSYSTEM ANALYSIS	63
5.5		PRICING ANALYSIS	64
	5.5.1	AVERAGE SELLING PRICE TREND OF KEY PLAYERS, BY OFFERING, 2024.....	64
	5.5.2	INDICATIVE PRICING ANALYSIS OF DDOS PROTECTION AND MITIGATION SECURITY, BY OFFERING, 2024	65
5.6		KEY CONFERENCES AND EVENTS	66
5.7		TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS	66
5.8		INVESTMENT AND FUNDING SCENARIO.....	67
5.9		CASE STUDY ANALYSIS.....	68
	5.9.1	XTEL COMMUNICATIONS CHOSE NETSCOUT TO IMPROVE VISIBILITY INTO NETWORK TRAFFIC	68
	5.9.2	PENTELEDATA SELECTED RADWARE'S AMS FOR TECHNICAL INTEGRATION WITH KENTIK TECHNOLOGIES	69
	5.9.3	CNI CHOSE CORERO TO PROTECT ITS CUSTOMERS FROM DDOS ATTACKS.....	69
5.10		DDOS PREVENTION TECHNIQUES.....	70
5.11		IMPACT OF 2025 US TARIFF – DDOS PROTECTION AND MITIGATION SECURITY MARKET.....	71
	5.11.1	INTRODUCTION	71
	5.11.2	KEY TARIFF RATES	71
	5.11.3	PRICE IMPACT ANALYSIS.....	72
	5.11.4	IMPACT ON COUNTRY/REGION.....	73
	5.11.4.1	North America	73
	5.11.4.2	Europe	74
	5.11.4.3	Asia Pacific	74
	5.11.5	IMPACT ON END-USE INDUSTRIES.....	75

6	TECHNOLOGICAL ADVANCEMENTS, AI-DRIVEN IMPACT, PATENTS, INNOVATIONS, AND FUTURE APPLICATIONS	77
6.1	KEY EMERGING TECHNOLOGIES	77
6.1.1	TRAFFIC FILTERING	77
6.1.2	RATE LIMITING	77
6.1.3	WEB APPLICATION FIREWALL (WAF)	77
6.2	COMPLEMENTARY TECHNOLOGIES	78
6.2.1	ARTIFICIAL INTELLIGENCE (AI)	78
6.2.2	MACHINE LEARNING (ML)	78
6.3	ADJACENT TECHNOLOGIES	78
6.3.1	LOAD BALANCERS	78
6.3.2	CONTENT DELIVERY NETWORKS (CDNS)	79
6.4	FUTURE LANDSCAPE OF DDOS PROTECTION AND MITIGATION SECURITY MARKET	79
6.4.1	DDOS PROTECTION AND MITIGATION SECURITY TECHNOLOGY ROADMAP TILL 2030	79
6.4.1.1	Short-term roadmap (2025–2026)	79
6.4.1.2	Mid-term roadmap (2027–2028)	79
6.4.1.3	Long-term roadmap (2029–2030)	79
6.5	PATENT ANALYSIS	80
6.5.1	METHODOLOGY	80
6.5.2	KEY PATENTS	81
6.6	IMPACT OF AI/GEN AI ON DDOS PROTECTION AND MITIGATION SECURITY MARKET	83
6.6.1	USE CASES OF GENERATIVE AI IN DDOS PROTECTION AND MITIGATION SECURITY	83
6.6.2	BEST PRACTICES	84
6.6.2.1	BFSI	84
6.6.2.2	Government	85
6.6.2.3	Healthcare	85
6.6.3	CASE STUDIES OF GENERATIVE AI IMPLEMENTATION	86
6.6.3.1	GenAI-enhanced traffic intelligence for large-scale cloud infrastructure	86
6.6.3.2	AI-automated incident analysis for multi-national financial group	86
6.6.3.3	GenAI-driven botnet attribution for government cyber defense agency	86
6.6.4	CLIENT READINESS AND IMPACT ASSESSMENT	86
6.6.4.1	Client A: Global digital commerce platform	86
6.6.4.2	Client B: Major public sector department	87
6.6.4.3	Client C: Large healthcare network	87
7	REGULATORY LANDSCAPE	88
7.1	REGULATORY LANDSCAPE	88
7.1.1	REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	88

7.1.1.1	National Credit Union Administration	92
7.1.1.2	Federal Financial Institutions Examination Council	92
7.1.1.3	General Data Protection Regulation (GDPR)	92
7.1.1.4	Payment Card Industry Data Security Standard (PCI-DSS)	93
7.1.1.5	Health Insurance Portability And Accountability Act (HIPAA)	93
7.1.1.6	Gramm-Leach-Bliley (GLB) Act	93
7.1.1.7	Sarbanes-Oxley (SOX) Act	93
7.1.1.8	SOC 2	94
7.1.1.9	SWIFT CSP	94
8	CUSTOMER LANDSCAPE AND BUYER BEHAVIOR	95
8.1	DECISION-MAKING PROCESS	95
8.2	BUYER STAKEHOLDERS AND BUYING EVALUATION CRITERIA	95
8.2.1	KEY STAKEHOLDERS IN BUYING PROCESS	95
8.2.2	BUYING CRITERIA	96
8.2.3	ADOPTION BARRIERS AND INTERNAL CHALLENGES	96
9	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING	97
9.1	INTRODUCTION	98
9.1.1	OFFERING: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS	98
9.2	HARDWARE SOLUTIONS	100
9.2.1	FIREWALLS	101
9.2.1.1	Hardware firewalls filter and block malicious traffic to enable efficient server access for legitimate requests	101
9.2.2	INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)	102
9.2.2.1	IDPS prevents DDoS attacks by continuously monitoring network traffic and actively blocking malicious requests	102
9.2.3	LOAD BALANCERS	103
9.2.3.1	Load balancers protect against DDoS attacks by distributing traffic across multiple servers	103
9.2.4	OTHER HARDWARE SOLUTIONS	104
9.3	SOFTWARE SOLUTIONS	105
9.3.1	GLOBAL RISE IN IOT DEVICES TO DRIVE MARKET	105
9.4	SERVICES	106
9.4.1	PROFESSIONAL SERVICES	108
9.4.2	DESIGN AND IMPLEMENTATION	110
9.4.2.1	Increase in need to improve network performance and reliability	110
9.4.3	CONSULTING AND ADVISORY	111
9.4.3.1	Growing concerns for cybersecurity and adoption of advanced technologies	111
9.4.4	TRAINING AND EDUCATION	112
9.4.4.1	Rising need for training and creating awareness of DDoS attacks	112
9.4.5	SUPPORT AND MAINTENANCE	113

9.4.5.1	Rising need for support for technical issues and guidance	113
9.4.6	MANAGED SERVICES	114
9.4.6.1	Need to increase business efficiency and operations	114
10	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE	116
10.1	INTRODUCTION	117
10.1.1	SOLUTION TYPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS	117
10.2	NETWORK TRAFFIC ANALYZERS	119
10.2.1	NETWORK LAYER ATTACKS TO INCREASE ADOPTION OF DDOS PROTECTION SOLUTIONS	119
10.3	THREAT MITIGATION SYSTEMS	120
10.3.1	RISE IN LAYER 7 ATTACKS TO INCREASE DEMAND FOR DDOS PROTECTION AND MITIGATION SECURITY SOLUTIONS	120
10.4	BOTNET DETECTION & MANAGEMENT	121
10.4.1	EVOLVING DISRUPTIVE TECHNOLOGIES AND EASY AVAILABILITY OF CLOUD-BASED APPLICATIONS TO DRIVE MARKET	121
10.5	OTHER SOLUTION TYPES	122
11	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA	124
11.1	INTRODUCTION	125
11.1.1	APPLICATION AREA: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS	125
11.2	NETWORK SECURITY	126
11.2.1	INCREASING NEED TO ENHANCE NETWORK PERFORMANCE AND ELIMINATE DISRUPTIONS	126
11.3	APPLICATION SECURITY	127
11.3.1	RIISING NEED TO MITIGATE DDOS ATTACKS AND MAINTAIN PROTECTION	127
11.4	CLOUD SECURITY	129
11.4.1	GREATER NEED FOR CLOUD-BASED APPLICATIONS SECURITY TO DRIVE MARKET	129
11.5	ENDPOINT SECURITY	130
11.5.1	INCREASING MOBILE DEVICES AND DIGITAL TRANSFORMATIONS TO DRIVE MARKET	130
12	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE	131
12.1	INTRODUCTION	132
12.1.1	DEPLOYMENT MODE: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS	132
12.2	ON-PREMISES	133
12.2.1	ON-PREMISES SERVICES PROVIDE FULL CONTROL OF DEPLOYED SOLUTIONS IT'S STAFF	133

12.3	CLOUD	134
12.3.1	CLOUD DEPLOYMENT HELPS MANAGE DNS, REROUTE TRAFFIC, AND SAFEGUARD WEBSITE TRAFFIC	134
13	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE	136
13.1	INTRODUCTION	137
13.1.1	ORGANIZATION SIZE: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS	137
13.2	LARGE ENTERPRISES.....	138
13.2.1	INCREASING SEVERITY OF DDOS DAMAGE CAUSED BY SINGLE ATTACK TO DRIVE MARKET.....	138
13.3	SMALL & MEDIUM-SIZED ENTERPRISES	139
13.3.1	GROWING NEED TO MITIGATE SECURITY ATTACKS TO ENHANCE MARKET GROWTH	139
14	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL	141
14.1	INTRODUCTION	142
14.1.1	VERTICAL: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS.....	142
14.2	GOVERNMENT AND DEFENSE	144
14.2.1	INCREASING NEED FOR DDOS PROTECTION AND MITIGATION SECURITY SOLUTIONS AND SERVICES TO HELP MARKET GROWTH.....	144
14.3	BANKING, FINANCIAL SERVICES, AND INSURANCE	145
14.3.1	FRAGILE DATA CENTER SECURITY AND RISK OF CLOUD STORAGE DATA LEAKS TO DRIVE MARKET	145
14.4	MANUFACTURING	146
14.4.1	EVOLVING VOLUMETRIC DDOS ATTACKS ON MANUFACTURING PROCESSES TO CONTRIBUTE TO MARKET GROWTH.....	146
14.5	ENERGY AND UTILITIES	147
14.5.1	INCREASING ADOPTION OF SMART SYSTEMS AND APPLICATIONS TO DRIVE MARKET.....	147
14.6	IT AND ITES	148
14.6.1	RISE OF ADVANCED TECHNOLOGIES TO FUEL MARKET	148
14.7	TELECOM	149
14.7.1	RISE IN NUMBER OF WEB AND MOBILE APPLICATIONS TO FUEL MARKET	149
14.8	HEALTHCARE.....	151
14.8.1	REGULATORY NORMS TO INCREASE DEPLOYMENT OF DDOS PROTECTION AND MITIGATION SECURITY SOLUTIONS.....	151
14.9	EDUCATION	152
14.9.1	NEED FOR CONFIDENTIALITY, INTEGRITY, AND EASY AVAILABILITY OF DATA AND RESOURCES TO AUGMENT MARKET GROWTH	152
14.10	RETAIL	153
14.10.1	GROWING CYBERATTACKS AND DATA THEFT TO INCREASE ADOPTION OF DDOS PROTECTION AND MITIGATION SECURITY SOLUTIONS	153
14.11	OTHER VERTICALS	154

15	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION.....	156
15.1	INTRODUCTION	157
15.2	NORTH AMERICA	159
15.2.1	NORTH AMERICA: MACROECONOMIC OUTLOOK	159
15.2.2	US	167
15.2.2.1	Presence of major vendors in US driving market growth	167
15.2.3	CANADA.....	173
15.2.3.1	Rapid technological advancements and increasing DDoS attacks on network infrastructure to drive market.....	173
15.3	EUROPE	179
15.3.1	EUROPE: MACROECONOMIC OUTLOOK.....	179
15.3.2	UK	186
15.3.2.1	Increasing demand for monitoring solutions among SMEs to drive market	186
15.3.3	GERMANY	192
15.3.3.1	Increasing investments in DDoS protection and mitigation solutions to drive market	192
15.3.4	REST OF EUROPE	197
15.4	ASIA PACIFIC.....	203
15.4.1	ASIA PACIFIC: MACROECONOMIC OUTLOOK	203
15.4.2	CHINA.....	211
15.4.2.1	Development of cybersecurity safeguard system to fuel market.....	211
15.4.3	JAPAN.....	217
15.4.3.1	Stringent laws and regulations for cybersecurity to drive market.....	217
15.4.4	INDIA.....	223
15.4.4.1	Increasing DDoS attacks leading to adoption of DDoS protection and mitigation security solutions	223
15.4.5	REST OF ASIA PACIFIC.....	229
15.5	MIDDLE EAST & AFRICA.....	234
15.5.1	MIDDLE EAST & AFRICA: MACROECONOMIC OUTLOOK	234
15.5.2	KSA	241
15.5.2.1	Increasing investments in mitigation security and growth in number of startups to drive market	241
15.5.3	UAE	247
15.5.3.1	Growing reliance on cloud-based applications to boost market.....	247
15.5.4	SOUTH AFRICA	247
15.5.4.1	Government initiatives and substantial foreign investments to drive market	247
15.5.5	REST OF MIDDLE EAST & AFRICA	247
15.6	LATIN AMERICA	247
15.6.1	LATIN AMERICA: MACROECONOMIC OUTLOOK	248
15.6.2	BRAZIL.....	254
15.6.2.1	Increasing focus on establishing effective cybersecurity strategies to drive market.....	254

15.6.3	MEXICO	260
15.6.3.1	Rising adoption of cloud-based services to drive market.....	260
15.6.4	REST OF LATIN AMERICA	266
16	COMPETITIVE LANDSCAPE	273
16.1	INTRODUCTION	273
16.2	KEY PLAYER STRATEGIES/RIGHT TO WIN, 2022–2025	273
16.3	REVENUE ANALYSIS, 2020–2024.....	275
16.4	MARKET SHARE ANALYSIS, 2024	275
16.4.1	MARKET RANKING ANALYSIS, 2024	278
16.5	COMPANY EVALUATION MATRIX: KEY PLAYERS, 2025.....	279
16.5.1	STARS.....	279
16.5.2	EMERGING LEADERS.....	279
16.5.3	PERVASIVE PLAYERS	279
16.5.4	PARTICIPANTS	279
16.5.5	COMPANY FOOTPRINT: KEY PLAYERS, 2025.....	281
16.5.5.1	Company footprint.....	281
16.5.5.2	Regional footprint	282
16.5.5.3	Offering footprint.....	283
16.5.5.4	Vertical footprint	284
16.6	COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2025.....	285
16.6.1	PROGRESSIVE COMPANIES.....	285
16.6.2	RESPONSIVE COMPANIES	285
16.6.3	DYNAMIC COMPANIES	285
16.6.4	STARTING BLOCKS	285
16.6.5	COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2025	287
16.6.5.1	Detailed list of key startups/SMEs	287
16.6.5.2	Competitive benchmarking of key startups/SMEs	288
16.7	COMPETITIVE SCENARIO	289
16.7.1	PRODUCT LAUNCHES & ENHANCEMENTS.....	289
16.7.2	DEALS.....	290
16.8	BRAND/PRODUCT COMPARISON	291
16.9	COMPANY VALUATION AND FINANCIAL METRICS, 2025	291
16.9.1	COMPANY VALUATION	291
16.9.2	FINANCIAL METRICS	292
17	COMPANY PROFILES.....	293
17.1	KEY PLAYERS.....	293
17.1.1	NETSCOUT	293
17.1.1.1	Business overview	293
17.1.1.2	Products/Solutions/Services offered.....	294
17.1.1.3	Recent developments	295

17.1.1.3.1	Product launches & enhancements	295
17.1.1.3.2	Deals	295
17.1.1.3.3	Expansions	296
17.1.1.4	MnM view	296
17.1.1.4.1	Right to win	296
17.1.1.4.2	Strategic choices	296
17.1.1.4.3	Weaknesses and competitive threats	296
17.1.2	AKAMAI TECHNOLOGIES	297
17.1.2.1	Business overview	297
17.1.2.2	Products/Solutions/Services offered	298
17.1.2.3	Recent developments	299
17.1.2.3.1	Product launches & enhancements	299
17.1.2.3.2	Deals	299
17.1.2.3.3	Expansions	300
17.1.2.4	MnM view	300
17.1.2.4.1	Right to win	300
17.1.2.4.2	Strategic choices	300
17.1.2.4.3	Weaknesses and competitive threats	301
17.1.3	RADWARE	302
17.1.3.1	Business overview	302
17.1.3.2	Products/Solutions/Services offered	303
17.1.3.3	Recent developments	304
17.1.3.3.1	Product launches & enhancements	304
17.1.3.3.2	Deals	305
17.1.3.4	MnM view	305
17.1.3.4.1	Right to win	305
17.1.3.4.2	Strategic choices	305
17.1.3.4.3	Weaknesses and competitive threats	305
17.1.4	CLOUDFLARE	306
17.1.4.1	Business overview	306
17.1.4.2	Products/Solutions/Services offered	307
17.1.4.3	MnM view	308
17.1.4.3.1	Key strengths	308
17.1.4.3.2	Strategic choices	308
17.1.4.3.3	Weaknesses and competitive threats	308
17.1.5	FORTINET	309
17.1.5.1	Business overview	309
17.1.5.2	Products/Solutions/Services offered	310
17.1.5.3	Recent developments	311
17.1.5.3.1	Deals	311
17.1.5.4	MnM view	311
17.1.5.4.1	Key strengths	311

	17.1.5.4.2	Strategic choices	311
	17.1.5.4.3	Weaknesses and competitive threats	311
17.1.6	HUAWEI		312
	17.1.6.1	Business overview	312
	17.1.6.2	Products/Solutions/Services offered	313
	17.1.6.3	Recent developments	314
	17.1.6.3.1	Deals	314
17.1.7	LINK11		315
	17.1.7.1	Business overview	315
	17.1.7.2	Products/Solutions/Services offered	315
	17.1.7.3	Recent developments	316
	17.1.7.3.1	Product launches & enhancements	316
	17.1.7.3.2	Deals	316
17.1.8	IMPERVA (A THALES COMPANY)		317
	17.1.8.1	Business overview	317
	17.1.8.2	Products/Solutions/Services offered	317
	17.1.8.3	Recent developments	318
	17.1.8.3.1	Deals	318
17.1.9	BT		319
	17.1.9.1	Business overview	319
	17.1.9.2	Products/Solutions/Services offered	320
	17.1.9.3	Recent developments	320
	17.1.9.3.1	Deals	320
17.1.10	A10 NETWORKS		321
	17.1.10.1	Business overview	321
	17.1.10.2	Products/Solutions/Services offered	322
17.1.11	NSFOCUS		323
	17.1.11.1	Business overview	323
	17.1.11.2	Products/Solutions/Services offered	323
17.1.12	NEXUSGUARD		325
	17.1.12.1	Business overview	325
	17.1.12.2	Products/Solutions/Services offered	326
	17.1.12.3	Recent developments	326
	17.1.12.3.1	Deals	326
17.2	OTHER PLAYERS		328
	17.2.1	FASTLY	328
	17.2.2	F5	329
	17.2.3	CORERO	330
	17.2.4	ALLOT	331
	17.2.5	STRATACORE	331
	17.2.6	SUCURI	332
	17.2.7	LUMEN TECHNOLOGIES	333

17.3	SMES/STARTUPS.....	334
17.3.1	SECEON.....	334
17.3.2	HALTDOS	334
17.3.3	DDOS-GUARD	335
17.3.4	INDUSFACE.....	335
17.3.5	ACTIVEREACH	336
17.3.6	MLYTICS	336
17.3.7	RIOREY	337
17.3.8	PHOENIXNAP	337
17.3.9	COMODO SECURITY SOLUTIONS.....	338
18	RESEARCH METHODOLOGY.....	339
18.1	RESEARCH DATA	339
18.1.1	SECONDARY DATA.....	340
18.1.2	PRIMARY DATA.....	340
18.1.2.1	Primary interviews with experts	341
18.1.2.2	Breakdown of primary profiles	341
18.1.2.3	Key insights from industry experts	342
18.2	MARKET SIZE ESTIMATION	342
18.2.1	TOP-DOWN APPROACH.....	343
18.2.2	BOTTOM-UP APPROACH	344
18.2.3	DDOS PROTECTION AND MITIGATION SECURITY MARKET ESTIMATION: DEMAND-SIDE ANALYSIS	345
18.3	DATA TRIANGULATION	347
18.4	RISK ASSESSMENT	348
18.5	RESEARCH ASSUMPTIONS	348
18.6	RESEARCH LIMITATIONS.....	349
19	ADJACENT AND RELATED MARKETS.....	350
19.1	INTRODUCTION	350
19.2	CYBERSECURITY MARKET	350
19.2.1	MARKET DEFINITION	350
19.3	SECURITY AS A SERVICE MARKET	355
19.3.1	MARKET DEFINITION	355
20	APPENDIX.....	361
20.1	DISCUSSION GUIDE	361
20.2	KNOWLEDGESTORE: MARKETSandMARKETS' SUBSCRIPTION PORTAL.....	365
20.3	CUSTOMIZATION OPTIONS.....	367
20.4	RELATED REPORTS	367
20.5	AUTHOR DETAILS.....	368

LIST OF TABLES

TABLE 1	INCLUSIONS & EXCLUSIONS	41
TABLE 2	USD EXCHANGE RATES, 2020–2024	42
TABLE 3	IMPACT OF PORTER'S FIVE FORCES ON DDOS PROTECTION AND MITIGATION SECURITY MARKET	58
TABLE 4	ROLE OF COMPANIES IN ECOSYSTEM	63
TABLE 5	AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2024	65
TABLE 6	INDICATIVE PRICING ANALYSIS OF DDOS PROTECTION AND MITIGATION SECURITY, BY OFFERING, 2024	65
TABLE 7	DDOS PROTECTION AND MITIGATION SECURITY MARKET: LIST OF KEY CONFERENCES AND EVENTS, 2025	66
TABLE 8	US-ADJUSTED RECIPROCAL TARIFF RATES	71
TABLE 9	EXPECTED CHANGE IN PRICES AND LIKELY IMPACT ON END-USE MARKET DUE TO TARIFF IMPACT	72
TABLE 10	LIST OF MAJOR PATENTS, 2015–2024	81
TABLE 11	NORTH AMERICA: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	88
TABLE 12	EUROPE: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	89
TABLE 13	ASIA PACIFIC: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	90
TABLE 14	REST OF THE WORLD: LIST OF REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	91
TABLE 15	INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS (%) 95	
TABLE 16	KEY BUYING CRITERIA FOR TOP THREE VERTICALS	96
TABLE 17	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	99
TABLE 18	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	99
TABLE 19	HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	100
TABLE 20	HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	100
TABLE 21	FIREWALLS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	101
TABLE 22	FIREWALLS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	101
TABLE 23	INTRUSION DETECTION AND PREVENTION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	102
TABLE 24	INTRUSION DETECTION AND PREVENTION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	102
TABLE 25	LOAD BALANCERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	103
TABLE 26	LOAD BALANCERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	103
TABLE 27	OTHER HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	104

TABLE 28	OTHER HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	104
TABLE 29	SOFTWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	105
TABLE 30	SOFTWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	105
TABLE 31	SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2019–2024 (USD MILLION)	107
TABLE 32	SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2025–2030 (USD MILLION)	107
TABLE 33	SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	107
TABLE 34	SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	108
TABLE 35	PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	109
TABLE 36	PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	109
TABLE 37	PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2019–2024 (USD MILLION)	109
TABLE 38	PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2025–2030 (USD MILLION)	110
TABLE 39	DESIGN AND IMPLEMENTATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	110
TABLE 40	DESIGN AND IMPLEMENTATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	111
TABLE 41	CONSULTING AND ADVISORY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	111
TABLE 42	CONSULTING AND ADVISORY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	112
TABLE 43	TRAINING AND EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	112
TABLE 44	TRAINING AND EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	113
TABLE 45	SUPPORT AND MAINTENANCE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	113
TABLE 46	SUPPORT AND MAINTENANCE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	114
TABLE 47	MANAGED SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	115
TABLE 48	MANAGED SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	115
TABLE 49	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	118
TABLE 50	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	118
TABLE 51	NETWORK TRAFFIC ANALYZERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	119
TABLE 52	NETWORK TRAFFIC ANALYZERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	120
TABLE 53	THREAT MITIGATION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	121

TABLE 54	THREAT MITIGATION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	121
TABLE 55	BOTNET DETECTION & MANAGEMENT: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	122
TABLE 56	BOTNET DETECTION & MANAGEMENT: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	122
TABLE 57	OTHER SOLUTION TYPES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	123
TABLE 58	OTHER SOLUTION TYPES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	123
TABLE 59	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	126
TABLE 60	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	126
TABLE 61	NETWORK SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	127
TABLE 62	NETWORK SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	127
TABLE 63	APPLICATION SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	128
TABLE 64	APPLICATION SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	128
TABLE 65	CLOUD SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	129
TABLE 66	CLOUD SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	129
TABLE 67	ENDPOINT SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	130
TABLE 68	ENDPOINT SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	130
TABLE 69	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	133
TABLE 70	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	133
TABLE 71	ON-PREMISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	134
TABLE 72	ON-PREMISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	134
TABLE 73	CLOUD: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	135
TABLE 74	CLOUD: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	135
TABLE 75	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	138
TABLE 76	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	138
TABLE 77	LARGE ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	139
TABLE 78	LARGE ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	139
TABLE 79	SMALL & MEDIUM-SIZED ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	140

TABLE 80	SMALL & MEDIUM-SIZED ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	140
TABLE 81	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	143
TABLE 82	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	144
TABLE 83	GOVERNMENT AND DEFENSE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	144
TABLE 84	GOVERNMENT AND DEFENSE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	145
TABLE 85	BFSI: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	145
TABLE 86	BFSI: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	146
TABLE 87	MANUFACTURING: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	147
TABLE 88	MANUFACTURING: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	147
TABLE 89	ENERGY AND UTILITIES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	148
TABLE 90	ENERGY AND UTILITIES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	148
TABLE 91	IT AND ITES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	149
TABLE 92	IT AND ITES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	149
TABLE 93	TELECOM: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	150
TABLE 94	TELECOM: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	150
TABLE 95	HEALTHCARE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	151
TABLE 96	HEALTHCARE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	152
TABLE 97	EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	152
TABLE 98	EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	153
TABLE 99	RETAIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	153
TABLE 100	RETAIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	154
TABLE 101	OTHER VERTICALS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	154
TABLE 102	OTHER VERTICALS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	155
TABLE 103	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	158
TABLE 104	DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	159
TABLE 105	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	160

TABLE 106	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	161
TABLE 107	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	161
TABLE 108	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	161
TABLE 109	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	162
TABLE 110	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	162
TABLE 111	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	162
TABLE 112	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	162
TABLE 113	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	163
TABLE 114	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	163
TABLE 115	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	163
TABLE 116	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	164
TABLE 117	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	164
TABLE 118	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	164
TABLE 119	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	164
TABLE 120	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	165
TABLE 121	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	165
TABLE 122	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	166
TABLE 123	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)	166
TABLE 124	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)	166
TABLE 125	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	167
TABLE 126	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	167
TABLE 127	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	168
TABLE 128	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	168
TABLE 129	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	168
TABLE 130	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	168
TABLE 131	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	169

TABLE 132	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	169
TABLE 133	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	169
TABLE 134	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	170
TABLE 135	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	170
TABLE 136	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	170
TABLE 137	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	171
TABLE 138	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	171
TABLE 139	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	171
TABLE 140	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	171
TABLE 141	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	172
TABLE 142	US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	172
TABLE 143	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	173
TABLE 144	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	173
TABLE 145	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	174
TABLE 146	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	174
TABLE 147	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	174
TABLE 148	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	174
TABLE 149	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	175
TABLE 150	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	175
TABLE 151	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	175
TABLE 152	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	176
TABLE 153	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	176
TABLE 154	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	176
TABLE 155	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	177
TABLE 156	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	177
TABLE 157	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	177

TABLE 158	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	177
TABLE 159	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	178
TABLE 160	CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	178
TABLE 161	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	180
TABLE 162	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	180
TABLE 163	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	180
TABLE 164	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	181
TABLE 165	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	181
TABLE 166	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	181
TABLE 167	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	181
TABLE 168	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	182
TABLE 169	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	182
TABLE 170	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	182
TABLE 171	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	183
TABLE 172	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	183
TABLE 173	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	183
TABLE 174	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	183
TABLE 175	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	184
TABLE 176	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	184
TABLE 177	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	184
TABLE 178	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	185
TABLE 179	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)	185
TABLE 180	EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)	185
TABLE 181	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	186
TABLE 182	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	186
TABLE 183	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	187

TABLE 184	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	187
TABLE 185	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	187
TABLE 186	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	187
TABLE 187	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	188
TABLE 188	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	188
TABLE 189	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	188
TABLE 190	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	189
TABLE 191	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	189
TABLE 192	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	189
TABLE 193	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	190
TABLE 194	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	190
TABLE 195	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	190
TABLE 196	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	190
TABLE 197	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	191
TABLE 198	UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	191
TABLE 199	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	192
TABLE 200	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	192
TABLE 201	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	192
TABLE 202	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	193
TABLE 203	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	193
TABLE 204	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	193
TABLE 205	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	193
TABLE 206	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	194
TABLE 207	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	194
TABLE 208	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	194
TABLE 209	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	195

TABLE 210	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	195
TABLE 211	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	195
TABLE 212	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	195
TABLE 213	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	196
TABLE 214	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	196
TABLE 215	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	196
TABLE 216	GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	197
TABLE 217	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	197
TABLE 218	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	198
TABLE 219	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	198
TABLE 220	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	198
TABLE 221	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	199
TABLE 222	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	199
TABLE 223	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	199
TABLE 224	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	199
TABLE 225	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	200
TABLE 226	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	200
TABLE 227	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	200
TABLE 228	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	201
TABLE 229	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	201
TABLE 230	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	201
TABLE 231	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	201
TABLE 232	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	202
TABLE 233	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	202
TABLE 234	REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	203
TABLE 235	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	204

TABLE 236	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	205
TABLE 237	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	205
TABLE 238	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	205
TABLE 239	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	206
TABLE 240	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	206
TABLE 241	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	206
TABLE 242	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	206
TABLE 243	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	207
TABLE 244	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	207
TABLE 245	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	207
TABLE 246	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	208
TABLE 247	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	208
TABLE 248	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	208
TABLE 249	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	208
TABLE 250	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	209
TABLE 251	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	209
TABLE 252	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	210
TABLE 253	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)	210
TABLE 254	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)	210
TABLE 255	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	211
TABLE 256	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	211
TABLE 257	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	212
TABLE 258	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	212
TABLE 259	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	212
TABLE 260	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	212
TABLE 261	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	213

TABLE 262	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	213
TABLE 263	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	213
TABLE 264	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	214
TABLE 265	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	214
TABLE 266	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	214
TABLE 267	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	215
TABLE 268	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	215
TABLE 269	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	215
TABLE 270	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	215
TABLE 271	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	216
TABLE 272	CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	216
TABLE 273	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	217
TABLE 274	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	217
TABLE 275	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	218
TABLE 276	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	218
TABLE 277	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	218
TABLE 278	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	218
TABLE 279	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	219
TABLE 280	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	219
TABLE 281	JAPAN DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	219
TABLE 282	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	220
TABLE 283	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	220
TABLE 284	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	220
TABLE 285	JAPAN DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	221
TABLE 286	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	221
TABLE 287	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	221

TABLE 288	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	221
TABLE 289	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	222
TABLE 290	JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	222
TABLE 291	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	223
TABLE 292	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	223
TABLE 293	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	224
TABLE 294	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	224
TABLE 295	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	224
TABLE 296	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	224
TABLE 297	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	225
TABLE 298	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	225
TABLE 299	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	225
TABLE 300	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	226
TABLE 301	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	226
TABLE 302	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	226
TABLE 303	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	226
TABLE 304	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	227
TABLE 305	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	227
TABLE 306	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	227
TABLE 307	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	228
TABLE 308	INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	228
TABLE 309	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	229
TABLE 310	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	229
TABLE 311	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	229
TABLE 312	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	230
TABLE 313	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	230

TABLE 314	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	230
TABLE 315	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	230
TABLE 316	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	231
TABLE 317	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	231
TABLE 318	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	231
TABLE 319	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	232
TABLE 320	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	232
TABLE 321	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	232
TABLE 322	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	232
TABLE 323	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	233
TABLE 324	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	233
TABLE 325	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	233
TABLE 326	REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	234
TABLE 327	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	235
TABLE 328	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	235
TABLE 329	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	235
TABLE 330	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	236
TABLE 331	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	236
TABLE 332	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	236
TABLE 333	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	236
TABLE 334	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	237
TABLE 335	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	237
TABLE 336	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	237
TABLE 337	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	238
TABLE 338	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	238
TABLE 339	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	238

TABLE 340	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	238
TABLE 341	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	239
TABLE 342	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	239
TABLE 343	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	239
TABLE 344	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	240
TABLE 345	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)	240
TABLE 346	MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)	240
TABLE 347	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	241
TABLE 348	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	241
TABLE 349	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	242
TABLE 350	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	242
TABLE 351	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	242
TABLE 352	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	242
TABLE 353	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	243
TABLE 354	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	243
TABLE 355	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	243
TABLE 356	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	244
TABLE 357	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	244
TABLE 358	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	244
TABLE 359	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	245
TABLE 360	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	245
TABLE 361	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	245
TABLE 362	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	245
TABLE 363	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	246
TABLE 364	KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	246
TABLE 365	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	248

TABLE 366	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	248
TABLE 367	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	249
TABLE 368	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	249
TABLE 369	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	249
TABLE 370	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	249
TABLE 371	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	250
TABLE 372	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	250
TABLE 373	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	250
TABLE 374	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	251
TABLE 375	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	251
TABLE 376	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	251
TABLE 377	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	252
TABLE 378	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	252
TABLE 379	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	252
TABLE 380	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	252
TABLE 381	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	253
TABLE 382	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	253
TABLE 383	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)	254
TABLE 384	LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)	254
TABLE 385	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	255
TABLE 386	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	255
TABLE 387	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	255
TABLE 388	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	256
TABLE 389	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	256
TABLE 390	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	256
TABLE 391	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	256

TABLE 392	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	257
TABLE 393	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	257
TABLE 394	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	257
TABLE 395	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	258
TABLE 396	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	258
TABLE 397	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	258
TABLE 398	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	258
TABLE 399	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	259
TABLE 400	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	259
TABLE 401	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	259
TABLE 402	BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	260
TABLE 403	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	260
TABLE 404	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	261
TABLE 405	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	261
TABLE 406	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	261
TABLE 407	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	262
TABLE 408	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	262
TABLE 409	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	262
TABLE 410	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	262
TABLE 411	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	263
TABLE 412	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	263
TABLE 413	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	263
TABLE 414	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	264
TABLE 415	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	264
TABLE 416	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	264
TABLE 417	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	264

TABLE 418	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	265
TABLE 419	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	265
TABLE 420	MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	266
TABLE 421	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	266
TABLE 422	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	267
TABLE 423	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)	267
TABLE 424	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)	267
TABLE 425	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)	268
TABLE 426	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)	268
TABLE 427	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)	268
TABLE 428	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)	268
TABLE 429	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	269
TABLE 430	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	269
TABLE 431	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)	269
TABLE 432	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)	270
TABLE 433	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	270
TABLE 434	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	270
TABLE 435	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	270
TABLE 436	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	271
TABLE 437	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	271
TABLE 438	REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	272
TABLE 439	DDOS PROTECTION AND MITIGATION SECURITY MARKET: OVERVIEW OF STRATEGIES DEPLOYED BY KEY PLAYERS	273
TABLE 440	DDOS PROTECTION AND MITIGATION SECURITY MARKET: DEGREE OF COMPETITION, 2024	276
TABLE 441	DDOS PROTECTION AND MITIGATION SECURITY MARKET: REGIONAL FOOTPRINT, 2025 282	
TABLE 442	DDOS PROTECTION AND MITIGATION SECURITY MARKET: OFFERING FOOTPRINT, 2025 283	
TABLE 443	DDOS PROTECTION AND MITIGATION SECURITY MARKET: VERTICAL FOOTPRINT, 2025 284	

TABLE 444	DDOS PROTECTION AND MITIGATION SECURITY MARKET: KEY STARTUPS/SMES, 2025	287
TABLE 445	DDOS PROTECTION AND MITIGATION SECURITY MARKET: COMPETITIVE BENCHMARKING OF KEY STARTUPS/SMES, 2025	288
TABLE 446	DDOS PROTECTION AND MITIGATION SECURITY MARKET: PRODUCT LAUNCHES AND ENHANCEMENTS, APRIL 2023–AUGUST 2025	289
TABLE 447	DDOS PROTECTION AND MITIGATION SECURITY MARKET: DEALS, FEBRUARY 2022–MAY 2024	290
TABLE 448	NETSCOUT: COMPANY OVERVIEW	293
TABLE 449	NETSCOUT: PRODUCTS/SOLUTIONS/SERVICES OFFERED	294
TABLE 450	NETSCOUT: PRODUCT LAUNCHES & ENHANCEMENTS	295
TABLE 451	NETSCOUT: DEALS	295
TABLE 452	NETSCOUT: EXPANSIONS	296
TABLE 453	AKAMAI TECHNOLOGIES: COMPANY OVERVIEW	297
TABLE 454	AKAMAI TECHNOLOGIES: PRODUCTS/SOLUTIONS/SERVICES OFFERED	298
TABLE 455	AKAMAI TECHNOLOGIES: PRODUCT LAUNCHES & ENHANCEMENTS	299
TABLE 456	AKAMAI TECHNOLOGIES: DEALS	299
TABLE 457	AKAMAI TECHNOLOGIES: EXPANSIONS	300
TABLE 458	RADWARE: COMPANY OVERVIEW	302
TABLE 459	RADWARE: PRODUCTS/SOLUTIONS/SERVICES OFFERED	303
TABLE 460	RADWARE: PRODUCT LAUNCHES & ENHANCEMENTS	304
TABLE 461	RADWARE: DEALS	305
TABLE 462	CLOUDFLARE: COMPANY OVERVIEW	306
TABLE 463	CLOUDFLARE: PRODUCTS/SOLUTIONS/SERVICES OFFERED	307
TABLE 464	FORTINET: COMPANY OVERVIEW	309
TABLE 465	FORTINET: PRODUCTS/SOLUTIONS/SERVICES OFFERED	310
TABLE 466	FORTINET: DEALS	311
TABLE 467	HUAWEI: COMPANY OVERVIEW	312
TABLE 468	HUAWEI: PRODUCTS/SOLUTIONS/SERVICES OFFERED	313
TABLE 469	HUAWEI: DEALS	314
TABLE 470	LINK11: COMPANY OVERVIEW	315
TABLE 471	LINK11: PRODUCTS/SOLUTIONS/SERVICES OFFERED	315
TABLE 472	LINK11: PRODUCT LAUNCHES & ENHANCEMENTS	316
TABLE 473	LINK11: DEALS	316
TABLE 474	IMPERVA: COMPANY OVERVIEW	317
TABLE 475	IMPERVA: PRODUCTS/SOLUTIONS/SERVICES OFFERED	317
TABLE 476	IMPERVA: DEALS	318
TABLE 477	BT: COMPANY OVERVIEW	319
TABLE 478	BT: PRODUCTS/SOLUTIONS/SERVICES OFFERED	320
TABLE 479	BT: DEALS	320
TABLE 480	A10 NETWORKS: COMPANY OVERVIEW	321
TABLE 481	A10 NETWORKS: PRODUCTS/SOLUTIONS/SERVICES OFFERED	322
TABLE 482	NSFOCUS: COMPANY OVERVIEW	323
TABLE 483	NSFOCUS: PRODUCTS/SOLUTIONS/SERVICES OFFERED	323
TABLE 484	NEXUSGUARD: COMPANY OVERVIEW	325

TABLE 485	NEXUSGUARD: PRODUCTS/SOLUTIONS/SERVICES OFFERED	326
TABLE 486	NEXUSGUARD: DEALS	326
TABLE 487	PRIMARY INTERVIEWS WITH EXPERTS	341
TABLE 488	RISK ASSESSMENT	348
TABLE 489	CYBERSECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)	351
TABLE 490	CYBERSECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)	351
TABLE 491	CYBERSECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)	351
TABLE 492	CYBERSECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)	352
TABLE 493	CYBERSECURITY MARKET, BY SECURITY TYPE, 2019–2024 (USD MILLION)	352
TABLE 494	CYBERSECURITY MARKET, BY SECURITY TYPE, 2025–2030 (USD MILLION)	352
TABLE 495	CYBERSECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)	353
TABLE 496	CYBERSECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)	353
TABLE 497	CYBERSECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)	353
TABLE 498	CYBERSECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)	353
TABLE 499	CYBERSECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)	354
TABLE 500	CYBERSECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)	354
TABLE 501	CYBERSECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)	355
TABLE 502	CYBERSECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)	355
TABLE 503	SECURITY AS A SERVICE MARKET SIZE, BY COMPONENT, 2016–2020 (USD MILLION)	356
TABLE 504	SECURITY AS A SERVICE MARKET SIZE, BY COMPONENT, 2021–2026 (USD MILLION)	356
TABLE 505	SECURITY AS A SERVICE MARKET SIZE, BY SOLUTION, 2016–2020 (USD MILLION)	356
TABLE 506	SECURITY AS A SERVICE MARKET SIZE, BY SOLUTION, 2021–2026 (USD MILLION)	357
TABLE 507	SECURITY AS A SERVICE MARKET SIZE, BY SERVICE, 2016–2020 (USD MILLION)	357
TABLE 508	SECURITY AS A SERVICE MARKET SIZE, BY SERVICE, 2021–2026 (USD MILLION)	357
TABLE 509	SECURITY AS A SERVICE MARKET SIZE, BY APPLICATION, 2016–2020 (USD MILLION)	358
TABLE 510	SECURITY AS A SERVICE MARKET SIZE, BY APPLICATION, 2021–2026 (USD MILLION)	358
TABLE 511	SECURITY AS A SERVICE MARKET SIZE, BY ORGANIZATION SIZE, 2016–2020 (USD MILLION)	358
TABLE 512	SECURITY AS A SERVICE MARKET SIZE, BY ORGANIZATION SIZE, 2021–2026 (USD MILLION)	359
TABLE 513	SECURITY AS A SERVICE MARKET SIZE, BY VERTICAL, 2016–2020 (USD MILLION)	359
TABLE 514	SECURITY AS A SERVICE MARKET SIZE, BY VERTICAL, 2021–2026 (USD MILLION)	360
TABLE 515	SECURITY AS A SERVICE MARKET SIZE, BY REGION, 2016–2020 (USD MILLION)	360
TABLE 516	SECURITY AS A SERVICE MARKET SIZE, BY REGION, 2021–2026 (USD MILLION)	360

LIST OF FIGURES

FIGURE 1	MARKET SEGMENTATION AND REGIONS COVERED	40
FIGURE 2	STUDY YEARS CONSIDERED	41
FIGURE 3	MARKET SCENARIO	44
FIGURE 4	GLOBAL DDOS PROTECTION & MITIGATION SECURITY MARKET, 2025–2030 (USD MILLION)	45
FIGURE 5	MAJOR STRATEGIES ADOPTED BY KEY PLAYERS IN DDOS PROTECTION & MITIGATION SECURITY MARKET, 2025	45
FIGURE 6	DISRUPTIVE TRENDS INFLUENCING GROWTH OF DDOS PROTECTION & MITIGATION SECURITY MARKET	46
FIGURE 7	HIGH-GROWTH SEGMENTS IN DDOS PROTECTION & MITIGATION SECURITY MARKET, 2025	47
FIGURE 8	ASIA PACIFIC TO REGISTER HIGHEST GROWTH DURING FORECAST PERIOD	47
FIGURE 9	RISING ADOPTION OF AI-DRIVEN CLOUD SECURITY SOLUTIONS ACTS AS OPPORTUNITY IN DDOS PROTECTION & MITIGATION SECURITY MARKET	49
FIGURE 10	HARDWARE AND LARGE ENTERPRISES ACCOUNTED FOR LARGEST MARKET SHARE IN 2025	50
FIGURE 11	APPLICATION SECURITY SEGMENT SET TO DOMINATE DDOS PROTECTION & MITIGATION SECURITY MARKET IN 2025	50
FIGURE 12	BFSI VERTICAL TO ACCOUNT FOR LARGEST MARKET SHARE IN 2025	51
FIGURE 13	DDOS PROTECTION AND MITIGATION SECURITY MARKET: DRIVERS, RESTRAINTS, OPPORTUNITIES, AND CHALLENGES	53
FIGURE 14	DDOS PROTECTION AND MITIGATION SECURITY MARKET: PORTER'S FIVE FORCES ANALYSIS	59
FIGURE 15	SUPPLY CHAIN ANALYSIS	62
FIGURE 16	DDOS PROTECTION AND MITIGATION SECURITY MARKET: ECOSYSTEM ANALYSIS	63
FIGURE 17	AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2024 (USD)	65
FIGURE 18	TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS	67
FIGURE 19	INVESTMENT AND FUNDING SCENARIO, 2019–2024	68
FIGURE 20	LIST OF PATENTS APPLIED AND GRANTED, 2015–2024	80
FIGURE 21	USE CASES OF GENERATIVE AI IN DDOS PROTECTION & MITIGATION SECURITY	84
FIGURE 22	GENERATIVE AI BEST PRACTICES ACROSS MAJOR INDUSTRIES	85
FIGURE 23	INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS	95
FIGURE 24	KEY BUYING CRITERIA FOR TOP THREE VERTICALS	96
FIGURE 25	SERVICES SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD	99
FIGURE 26	MANAGED SERVICES SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD	106
FIGURE 27	CONSULTING & ADVISORY SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD	108
FIGURE 28	BOTNET DETECTION & MITIGATION SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD	118
FIGURE 29	APPLICATION SECURITY SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD	125
FIGURE 30	CLOUD SEGMENT TO RECORD FASTER GROWTH DURING FORECAST PERIOD	132
FIGURE 31	SMES SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD	137

FIGURE 32	BFSI SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD	143
FIGURE 33	NORTH AMERICA TO LEAD MARKET FROM 2025 TO 2030	157
FIGURE 34	ASIA PACIFIC TO REGISTER HIGHEST CAGR DURING FORECAST PERIOD	158
FIGURE 35	NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET SNAPSHOT	160
FIGURE 36	ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET SNAPSHOT	204
FIGURE 37	DDOS PROTECTION AND MITIGATION SECURITY MARKET: REVENUE ANALYSIS OF FIVE KEY PLAYERS, 2020–2024	275
FIGURE 38	SHARE ANALYSIS OF LEADING COMPANIES IN DDOS PROTECTION AND MITIGATION SECURITY MARKET, 2024	276
FIGURE 39	MARKET RANKING ANALYSIS OF TOP FIVE PLAYERS	278
FIGURE 40	DDOS PROTECTION AND MITIGATION SECURITY MARKET: COMPANY EVALUATION MATRIX (KEY PLAYERS), 2025	280
FIGURE 41	DDOS PROTECTION AND MITIGATION SECURITY MARKET: COMPANY FOOTPRINT, 2025	281
FIGURE 42	DDOS PROTECTION AND MITIGATION SECURITY MARKET: COMPANY EVALUATION MATRIX (STARTUPS/SMES), 2025	286
FIGURE 43	BRAND/PRODUCT COMPARISON	291
FIGURE 44	COMPANY VALUATION, 2025 (USD BILLION)	291
FIGURE 45	FINANCIAL METRICS, 2025	292
FIGURE 46	NETSCOUT: COMPANY SNAPSHOT	294
FIGURE 47	AKAMAI TECHNOLOGIES: COMPANY SNAPSHOT	298
FIGURE 48	RADWARE: COMPANY SNAPSHOT	302
FIGURE 49	CLOUDFLARE: COMPANY SNAPSHOT	307
FIGURE 50	FORTINET: COMPANY SNAPSHOT	310
FIGURE 51	HUAWEI: COMPANY SNAPSHOT	313
FIGURE 52	BT: COMPANY SNAPSHOT	320
FIGURE 53	A10 NETWORKS: COMPANY SNAPSHOT	322
FIGURE 54	DDOS PROTECTION AND MITIGATION SECURITY MARKET: RESEARCH DESIGN	339
FIGURE 55	BREAKDOWN OF PRIMARY INTERVIEWS, BY COMPANY TYPE, DESIGNATION, AND REGION	341
FIGURE 56	KEY INSIGHTS FROM INDUSTRY EXPERTS	342
FIGURE 57	DDOS PROTECTION AND MITIGATION SECURITY MARKET: TOP-DOWN AND BOTTOM-UP APPROACHES	343
FIGURE 58	APPROACH 1 (SUPPLY SIDE): REVENUE OF VENDORS IN DDOS PROTECTION AND MITIGATION SECURITY MARKET	344
FIGURE 59	APPROACH 2 (DEMAND SIDE): DDOS PROTECTION AND MITIGATION SECURITY MARKET	345
FIGURE 60	MARKET SIZE ESTIMATION METHODOLOGY: DEMAND-SIDE ANALYSIS	345
FIGURE 61	TECHNOLOGY/PRODUCT ROADMAP	346
FIGURE 62	DDOS PROTECTION AND MITIGATION SECURITY MARKET: DATA TRIANGULATION	347

LIST OF ABBREVIATIONS

ABBREVIATION	FULL FORM
APPI	Act on the Protection of Personal Information
AWS	Amazon Web Services
AICPA	American Institute of CPAs
APIs	Application Programming Interfaces
AED	Arbor Edge Defense
AI	Artificial Intelligence
AR	Augmented Reality
BoJ	Bank of Japan
BFSI	Banking, financial services, and insurance
BI	Business Intelligence
BUs	Business Units
CCPA	California Consumer Privacy Act
CEOs	Chief Executive Officers
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CTO	Chief Technology Officer
CBRS	Citizens Broadband Radio Service
CSA	Cloud Security Alliance
CERL	Computer Education Research Laboratory
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CDN	Content Delivery Network
CSP	Customer Security Program
DSL	Data Security Law
DIA	Dedicated Internet Access
DoS	Denial of Service
DVDs	Digital Video Discs
DDoS	Distributed Denial of Service

DNS	Domain Name System
OECD	Economic Cooperation and Development
ECC-Net	European Consumer Centers Network
ENISA	European Union Agency for Network and Information Security
XMLRPC	eXtensible Markup Language Remote Procedure Call
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security and Management Act
FTC	Federal Trade Commission
FY	Financial year
FAQs	Frequently Asked Questions
GDPR	General Data Protection Regulation
GCA	Global Cybersecurity Agenda
GLB	GRAMM-LEACH-BLILEY
GWP	Gross World Product
HIPAA	Health Insurance Portability and Accountability ACT
HLEG	High Level Experts Group
HBAD	Host Behavior Anomaly Detection (
HTTP	Hypertext Transfer Protocol
HIVs	Independent Hardware Vendors
ISVs	Independent Software Vendors
ICT	Information and Communication Technology
IMS	Information Management System
IT	Information Technology
IRS	Internal Revenue Service
IMF	International Monetary Fund
ITU	International Telecommunications Union
ICMP	Internet Control Message Protocol
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
ISPs	Internet Service Providers
IEC	Israel Electric Corporation

KSA	Kingdom of Saudi Arabia
LEO	Low Earth Orbit
ML	Machine Learning
MSSPs	Managed Security Service Providers
MSS	Managed Security Services
MD	Managing Director
MTCS	Multi-tier Cloud Security
NCCIC	National Cybersecurity and Communications Integration Center
NBAD	Network Behavior Anomaly Detection
NFV	Network Functions Virtualization
NTP	Network Time Protocol
ATA	of Arbor Threat Analytics
OSI	Open Systems Interconnection
OTM	Open Threat Management
OEM	Original Equipment Manufacturer
PCI-DSS	Payment Card Industry - Data Security Standard
PIPL	Personal Information Protection Law
PoS	Point of Sale
PHI	Protected health information
PPP	Purchasing Power Parity
RDDoS	Ransom Distributed Denial of Service
R&D	research and development
SOX	SARBANES-OXLEY
SSL	Secure Sockets Layer
SEC	Securities and Exchange Commission
SEIM	Security Information and Event Management
SOC	Security Operations Center
SECaaS	Security-as-a-Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
SME	Small and Medium-sized Enterprise

SaaS	Software-as-a-Service
SDN	Software-defined Networking
SQL	Structured Query Language
TCS	Tata Consultancy Services
TMS	Threat Mitigation System
TCP	Transmission Control Protocol
UAE	United Arab Emirates
USD	United States Dollar
USB	Universal Serial Bus
UDP	User Datagram Protocol
VAR	Value-added Reseller
VP	Vice President
VR	Virtual Reality
VoIP	Voices over Internet Protocol
WAF	Web Application Firewall
WEO	World Economic Outlook
WISR	Worldwide Infrastructure Security Report

1 INTRODUCTION

1.1 STUDY OBJECTIVES

- To define, describe, and forecast the Distributed Denial of Service (DDoS) protection and mitigation security market by offering (hardware solutions, software solutions, and services), software solutions, 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 and mitigation security market
- To study the complete value chain and related industry segments, and perform a value chain analysis of the DDoS protection and mitigation security market landscape
- To strategically analyze the macro and micromarkets with respect to individual growth trends, prospects, and contributions to the total DDoS protection and mitigation security market
- To analyze the industry trends, pricing data, patents, and innovations related to the DDoS protection and mitigation security market
- To analyze the opportunities for stakeholders by identifying the high-growth segments of the DDoS protection and mitigation security 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 and development (R&D) activities

1.2 MARKET DEFINITION

DDoS (Distributed Denial of Service) protection and mitigation security 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

1.3.1 MARKET SEGMENTATION AND REGIONS COVERED

The following figure gives an overview of the segments and subsegments covered in the DDoS protection and mitigation security market report.

FIGURE 1 MARKET SEGMENTATION AND REGIONS COVERED



Note: Other solutions include predictive maintenance, digital twin, and fleet management

Other verticals include agriculture, life sciences, and telecom.

Rest of Europe includes Belgium and the remaining countries.

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

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

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

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

1.3.2 INCLUSIONS & EXCLUSIONS

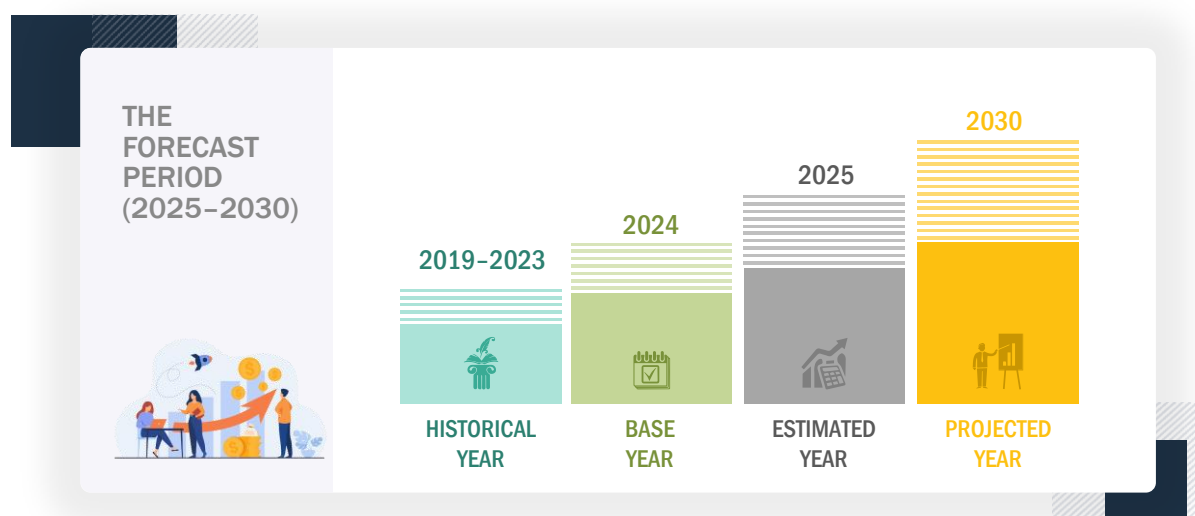
TABLE 1 INCLUSIONS & EXCLUSIONS

CATEGORY	INCLUSION	EXCLUSION
Offering	Hardware solutions, software solutions, and services are included in the scope.	The managed services considered in the report are only the pre-deployment services. Post-deployment managed services are excluded.
Software Solutions	Network traffic analyzers, threat mitigation systems, botnet detection & management, and other software solutions (security information and event management (SIEM), anomaly detection, orchestration & automation) are included.	Open source or third-party software is not considered in the scope.
Application Area	Network security, application security, endpoint security, and cloud security are included.	NA
Deployment Mode	On-premises and cloud deployment modes are included.	NA
Organization Size	The large enterprises and small & medium enterprises are included.	NA
Verticals	BFSI, government & defense, IT & ITeS, telecom, manufacturing, energy & utilities, healthcare, retail, education, and other verticals (media & entertainment, transportation & logistics, travel & hospitality, oil & gas) are included	NA

Source: Secondary Research and MarketsandMarkets Analysis

1.4 YEARS CONSIDERED

FIGURE 2 STUDY YEARS CONSIDERED



Note: The forecast period is from 2025 to 2030.

1.5 CURRENCY CONSIDERED

- USD was used in this report to indicate the market size (in terms of value) and company revenues.
- ISO 4217 codes were used to depict currency names; the market size, in terms of value, was represented using “USD.”
- The market was mainly studied in terms of USD million, with certain values provided in USD billion. The denomination is based on the size of values, enabling uniform accommodation of these values within tables, figures, or any form of study of a particular segment.
- Single digit was considered post the decimal point to differentiate between the market sizes of the segments.
- The figures were sourced from their annual reports for companies reporting their revenues in USD.
- For companies reporting their revenue in other currencies, the average yearly currency conversion rates of the respective years from the US IRS were used for the particular year to convert the value to USD equivalent.

TABLE 2 USD EXCHANGE RATES, 2020-2024

Currency	2020	2021	2022	2023	2024
EUR	0.877	0.846	0.951	0.924	0.924
JPY	106.725	109.817	131.454	140.511	151.353
CNY	6.900	6.452	6.730	7.075	7.189
SEK	9.025	8.584	10.122	10.613	10.577

Source: The US Internal Revenue Service (IRS)

1.6 STAKEHOLDERS

- DDoS protection and mitigation hardware vendors
- DDoS protection and mitigation software vendors
- DDoS protection and 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)

1.7 SUMMARY OF CHANGES

- The updated study is segmented based on offering, solution type, deployment type, vertical, application area, organization type, and region.
- The current study includes quantitative data for the historical years, 2019 to 2023; base year, 2024; and forecast years, 2025 to 2030.
- It includes updated market developments undertaken by vendors from 2022 to 2025.
- It also focuses on the market size for major countries in all regions.
- It includes an updated enterprise and startup evaluation matrix.
- It provides updated financial information on key vendors from 2019 to 2024.
- It includes company profiles for 29 vendors in the market.

2 EXECUTIVE SUMMARY

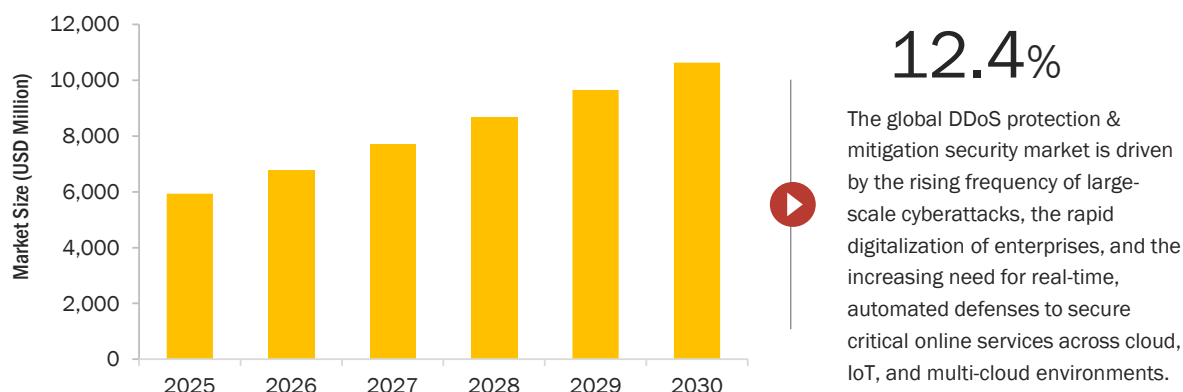
2.1 KEY INSIGHTS AND MARKET HIGHLIGHTS

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, e-commerce, 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, 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 & MITIGATION SECURITY MARKET, 2025–2030 (USD MILLION)



The global DDoS protection & mitigation security market is projected to grow steadily from USD 5,932 million in 2025 to USD 10,627 million by 2030, supported by a strong 12.4% 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 & MITIGATION SECURITY MARKET, 2025

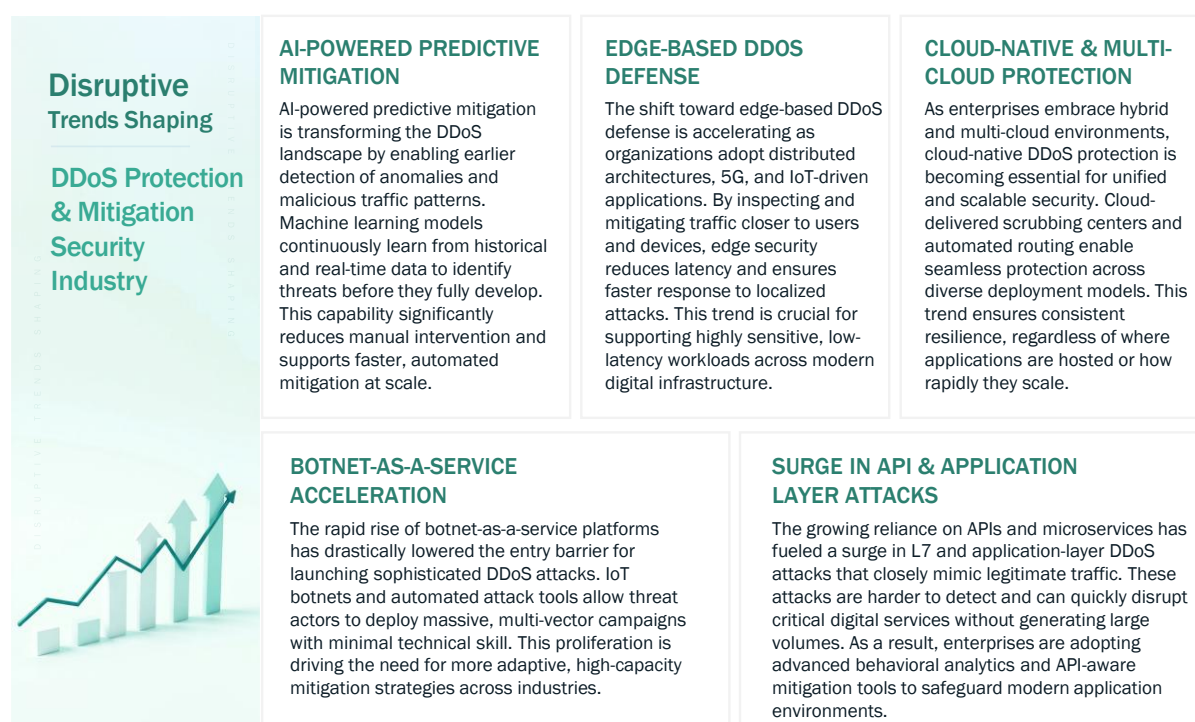
COMPANY	NETSCOUT	Akamai	radware	FORTINET	CLOUDFLARE
Product Launches	●	●	●	●	●
Mergers & Acquisitions	●	●	●	●	●
Partnerships, Agreements, Collaborations, and Joint Ventures	●	●	●	●	●
Expansions	●	●	●	●	●
IMPACT	● EXCELLENT	● GOOD	● FAIR	● POOR	

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

The DDoS protection & mitigation security market is consolidated, with the top five players holding a combined market share of 50–55%. 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 & mitigation security industry.

2.3 DISRUPTIONS SHAPING MARKET

FIGURE 6 DISRUPTIVE TRENDS INFLUENCING GROWTH OF DDOS PROTECTION & MITIGATION SECURITY MARKET

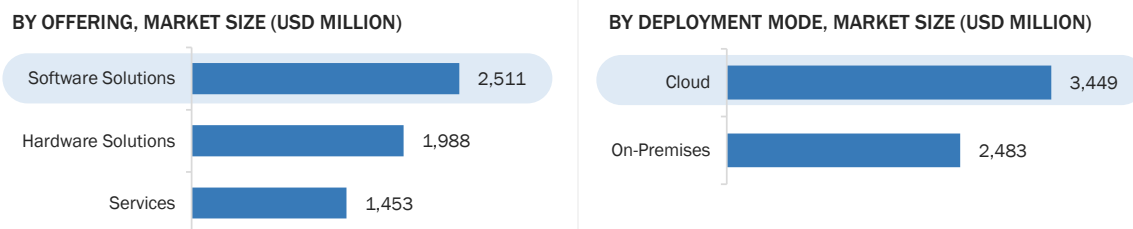


Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

Various industries such as BFSI, e-commerce, IT & telecom, gaming, government, and healthcare are increasingly relying on advanced DDoS protection as disruptive trends to 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, e-commerce, 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 e-commerce, 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 & MITIGATION SECURITY MARKET, 2025

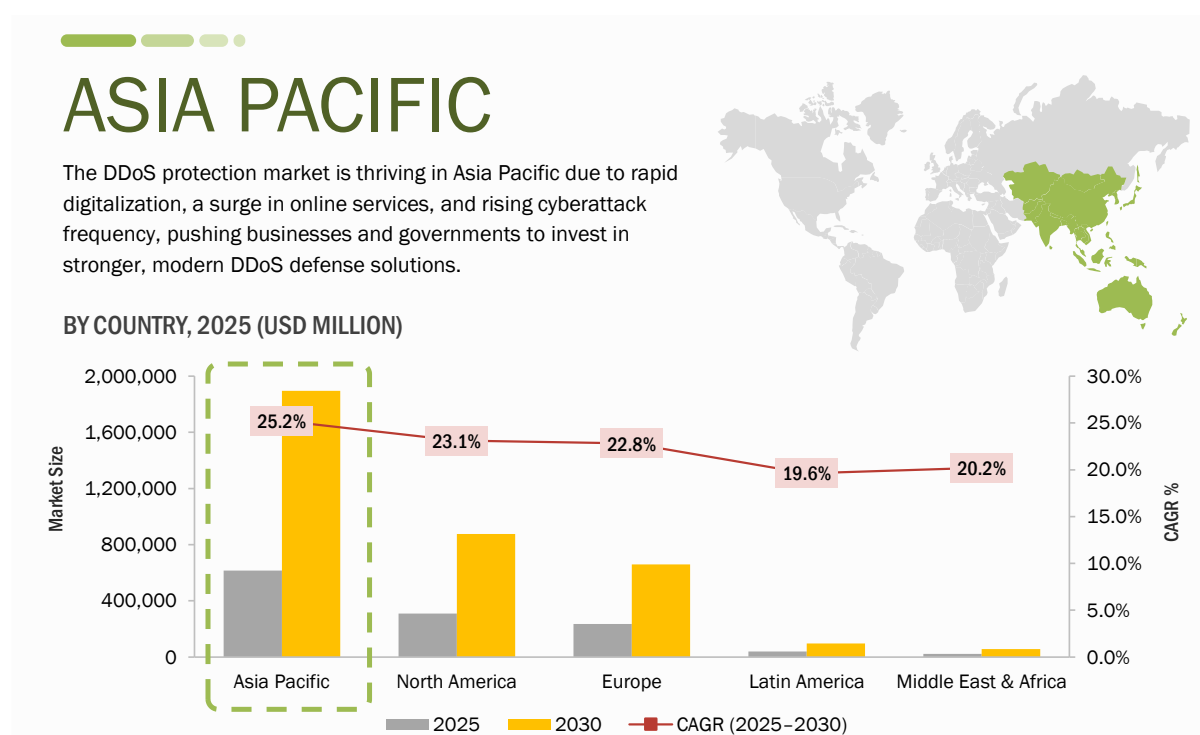


Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

The infographic highlights the fastest-growing segments within the DDoS protection & mitigation security market across offerings and deployment modes. 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



Note: CAGRs and market shares are provided in terms of value.

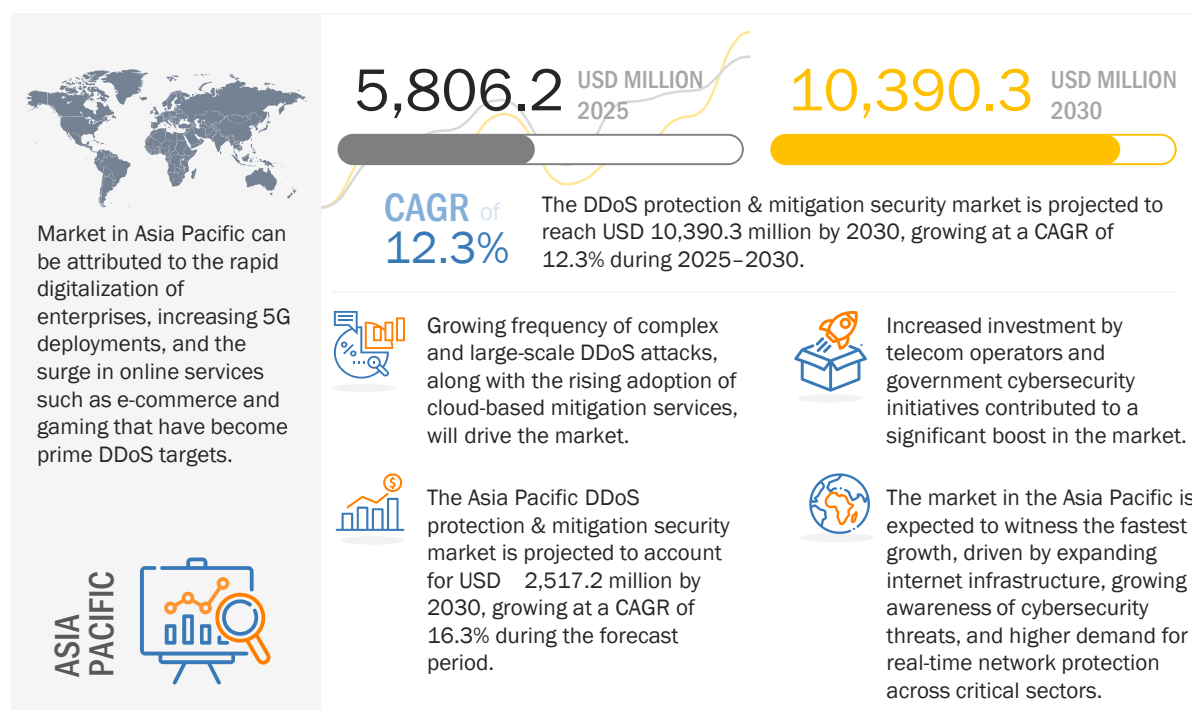
Source: Interviews with Experts, Secondary Research, and MarketsandMarkets Analysis

The DDoS protection and mitigation market in Asia Pacific is expanding rapidly, driven by accelerated digital transformation, mass adoption of e-commerce, 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, telecom, IT, healthcare, and e-commerce. As a result, APAC 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 SECURITY MARKET

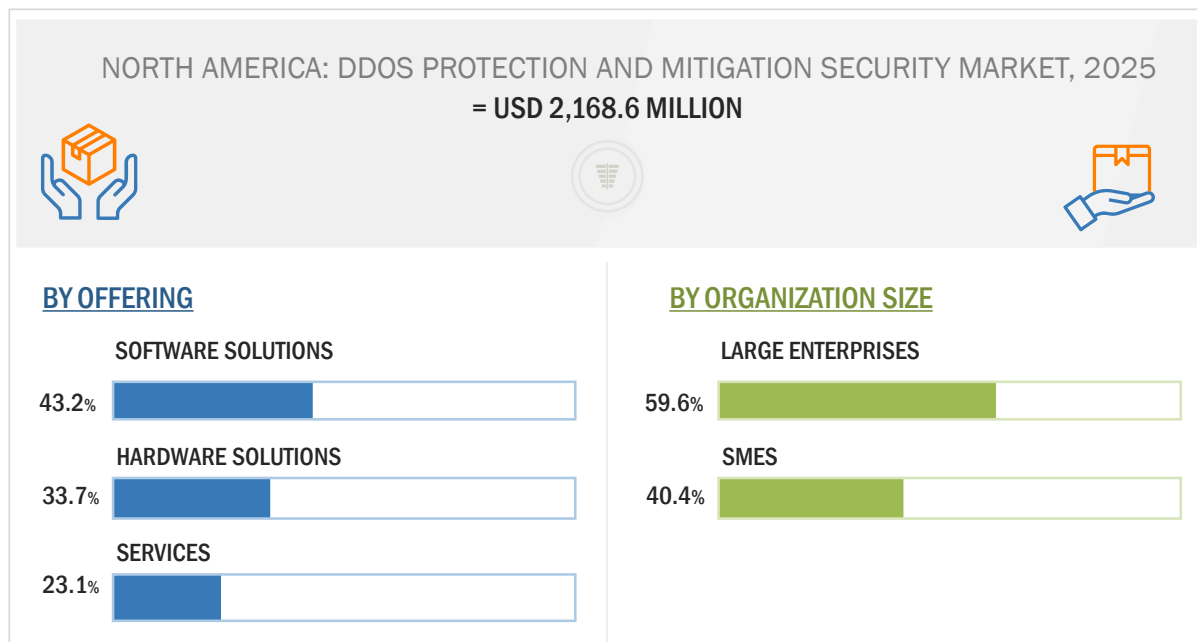
FIGURE 9 RISING ADOPTION OF AI-DRIVEN CLOUD SECURITY SOLUTIONS ACTS AS OPPORTUNITY IN DDOS PROTECTION & MITIGATION SECURITY MARKET



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

3.2 DDOS PROTECTION & MITIGATION SECURITY MARKET, BY OFFERING AND ORGANIZATION SIZE

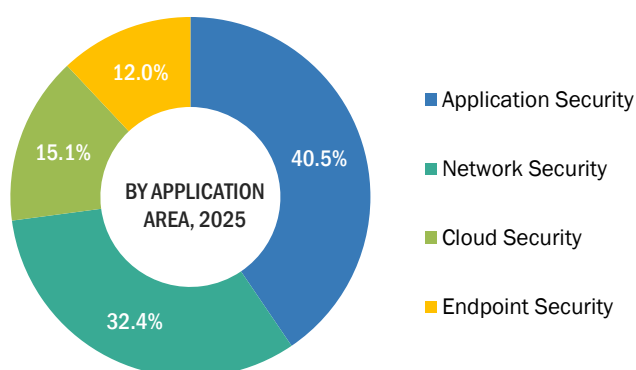
FIGURE 10 HARDWARE AND LARGE ENTERPRISES ACCOUNTED FOR LARGEST MARKET SHARE IN 2025



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

3.3 DDOS PROTECTION & MITIGATION SECURITY MARKET, BY APPLICATION AREA

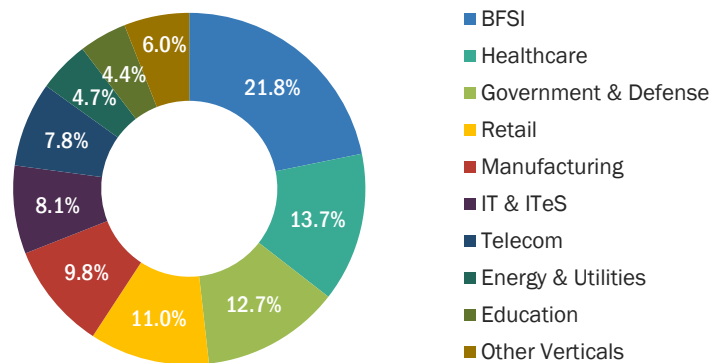
FIGURE 11 APPLICATION SECURITY SEGMENT SET TO DOMINATE DDOS PROTECTION & MITIGATION SECURITY MARKET IN 2025



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

3.4 DDOS PROTECTION & MITIGATION SECURITY MARKET, BY VERTICAL

FIGURE 12 BFSI VERTICAL TO ACCOUNT FOR LARGEST MARKET SHARE IN 2025



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 and mitigation security 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 security 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 security 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 and mitigation security market.

4.2 MARKET DYNAMICS

This research study indicates that the DDoS protection and mitigation security 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 security 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 and mitigation security market are listed below.

FIGURE 13 DDOS PROTECTION AND MITIGATION SECURITY MARKET: DRIVERS, RESTRAINTS, OPPORTUNITIES, AND CHALLENGES

 DRIVERS	▪ Rising frequency and complexity of DDoS attacks ▪ Growing internet penetration and connectivity
 RESTRAINTS	▪ Limited integration across multi-vendor environments ▪ Regulatory and data sovereignty constraints
 OPPORTUNITIES	▪ AI-driven predictive mitigation and automated threat correlation ▪ Growing partnerships between ISPs, cloud providers, and security vendors
 CHALLENGES	▪ Lack of skilled cybersecurity professionals ▪ Cost and complexity of solutions

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's. 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 Growing internet penetration and connectivity

Rapid broadband expansion, 5G rollouts, cloud migration, and surging API usage have materially enlarged both traffic volumes and exposed attack surfaces, driving demand for scalable DDoS defenses. In the Asia Pacific, specifically, reports documented a near doubling of DDoS activity in 2024, tied to increased internet adoption and politically timed campaigns around elections, prompting service providers and CSPs to embed mitigation into edge networks for low-latency protection. Cloudflare's Q4/2024 telemetry (millions of events mitigated quarter-over-quarter) and vendor threat reports from Akamai, showing more complex and simultaneous vectors, indicate that enterprises are reacting to actual, measured increases in attack opportunities rather than hypothetical risks. For regulated digital services, including banks, e-commerce platforms, and healthcare portals, higher user concurrency and cross-border traffic flows mean that even short service degradations have outsized revenue and compliance impacts. Therefore, organizations are converting point solutions into platform subscriptions (CDN+DDoS+WAF) to ensure integrated performance and resilience. This shift expands the addressable market size and raises the requirements for global scrubbing capacity, as well as edge-based detection co-located with carrier infrastructure.

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. 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 AI-driven predictive mitigation and automated threat correlation

Applying machine learning and behavioral analytics to global telemetry enables earlier detection, automated playbooks, and correlated threat context across networks, reducing mean time to mitigate and lowering dependence on scarce human analysts. Vendors have recently embedded ML models into mitigation pipelines, Cloudflare's quarterly threat reports highlight automated blocking at scale, and Akamai's 2024/25 commentary emphasizes AI-enhanced detection, while managed service partnerships (LevelBlue + Akamai) now advertise AI-driven auto-prioritization and automated policy management. These capabilities convert raw attack volumes into actionable signals, enabling systems to auto-tune filters and escalate to carrier scrubbing only when necessary, thereby reducing false positives and preserving legitimate traffic. For customers, predictive engines integrated with SIEM/SOAR and orchestration tools reduce SOC load and enable playbook-driven remediation. For vendors, AI products unlock higher-value managed services, recurring revenue for analytics, and differentiation in bids for large enterprise and telco contracts. Challenges remain around model drift, adversarial ML, and the need for diverse training telemetry, but current deployments demonstrate measurable reductions in response time and operational overhead.

4.2.3.2 Growing partnerships between ISPs, cloud providers, and security vendors

Closer collaboration among telcos, hyperscalers, and security vendors places mitigation nearer to attack ingress, improving capacity, lowering latency, and simplifying procurement through bundled services. Recent examples include cloud providers offering native protections (AWS Shield, Azure DDoS Protection, Google Cloud Armor) combined with third-party integrations, as well as the LevelBlue and Akamai-managed WAAP launch, which packages DDoS, WAF, and API protection with managed operations. Telecom operators are also extending carrier-grade scrubbing as a managed service, enabling enterprises in regions lacking global PoPs to access local scrubbing capacity through their ISP. These alliances accelerate time-to-protect for customers by reducing complex routing changes and providing unified support channels during incidents. For vendors, channel plays broaden reach into regulated or infrastructure-constrained markets, while carriers gain revenue from value-added security services. Commercially, the trend encourages consumption-based pricing, joint SLAs, and integrated telemetry portals, but successful deployments require clear responsibilities for routing, logging, and incident escalation between partners.

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, 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 24x7 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. In 2024, several mid-market organizations in sectors such as fintech and e-commerce 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

End-users across various sectors continue to face significant unmet needs in DDoS mitigation, driven by the rising sophistication of attacks and the expanding digital footprints of their targets. Organizations are increasingly requiring real-time, automated, and scalable DDoS defenses that extend beyond traditional traffic scrubbing. BFSI and e-commerce players seek near-zero latency protection for mission-critical transactions, while government agencies demand high-assurance, compliance-aligned mitigation for citizen-facing platforms. Healthcare organizations require IoMT-specific DDoS protection with guaranteed uptime and device-level anomaly detection.

Enterprises across various industries emphasize the need for enhanced visibility into multi-vector attacks, seamless interoperability with firewalls/SIEMs, and AI-driven predictive capabilities to anticipate and neutralize threats before they impact service. Emerging white spaces include protection for edge environments, low-latency mitigation for 5G networks, defense for hybrid multi-cloud architectures, and DDoS resilience tailored for SMEs, which remain underserved. These gaps create opportunities for next-generation, adaptive DDoS solutions that deliver proactive defense, transparent pricing, and frictionless integration.

4.4 INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES

- **Integration with Adjacent Security Markets:** DDoS protection is increasingly embedded into broader cybersecurity ecosystems, aligning with API security, zero-trust frameworks, WAF, and bot management solutions. This creates bundled adoption opportunities as enterprises shift toward unified detection and response platforms.
- **Expansion Through Cloud and Multi-cloud Partnerships:** Cloud hyperscalers such as AWS (Shield Advanced), Google Cloud (Cloud Armor), and Microsoft Azure (Front Door + DDoS Protection) integrate mitigation directly into application delivery workflows, enabling cross-deployment adoption across multi-cloud and distributed architectures.
- **Growing Collaboration with Telecom Operators & ISPs:** Major carriers, including Verizon, Lumen, Tata Communications, and NTT, are packaging DDoS scrubbing with backbone-level traffic filtering, opening pathways for vendors to reach enterprise and government customers through carrier-driven managed security offerings.

- **Opportunities in Edge Computing & CDN Ecosystems:** The rise of CDNs and edge platforms, supported by providers like Cloudflare, Akamai, Fastly, and telecom edge networks, creates demand for low-latency, edge-native DDoS mitigation integrated directly into traffic delivery layers.
- **Cross-sector Demand from Digitized Industry Verticals:** Industries such as digital payments, online gaming, media streaming, healthcare, and Industry 4.0 operations require continuous uptime and latency stability, driving demand for resilient DDoS protection embedded within application and platform infrastructures.
- **Enablement of Platform-wide Security Bundles:** Convergence across security, networking, and observability tools encourages vendors to offer consolidated bundles that integrate global threat intelligence, routing optimization, and automated mitigation, opening opportunities for solution expansion into enterprise-wide digital infrastructure.

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

Tier-1 Players: Scaling Infrastructure, Integrating Platforms, and Global Expansion

Tier-1 vendors, including Akamai, Cloudflare, AWS, Google, and Microsoft, are advancing their market positions through massive capacity upgrades, multi-terabit scrubbing expansion, and integration of DDoS mitigation with core cloud and application delivery platforms. These players are investing heavily in automated, machine-learning-driven detection pipelines and expanding into high-growth regions such as APAC and LATAM through new data centers and edge nodes. Tier-1 firms are also forming deep technical alliances with telecom operators, IXPs, and hyperscale cloud providers to deliver end-to-end mitigation embedded directly into network backbones and multi-cloud architectures.

Tier-2 Players: Product Specialization, Industry Partnerships, and Vertical Focus

Tier-2 players such as Corero Network Security, Radware, NETSCOUT, Fortinet, and Imperva are strengthening their presence through specialized hardware-software combinations, hybrid deployment capabilities, and targeted offerings for sectors like BFSI, government, and telecom. These companies are prioritizing behavioral analytics, encrypted traffic inspection, and real-time threat intelligence integrations while forming OEM and MSP partnerships to broaden reach. Many are enhancing managed services portfolios and co-developing solutions with regional carriers and data center operators to compete more effectively against Tier-1 scale.

Tier-3 Players: Niche Innovation, Regional Penetration, and Flexible Deployment Models

Tier-3 vendors, including Link11 regional SOC providers, are focusing on agility, cost efficiency, and rapid deployment models to win customers in mid-market and emerging economies. Their strategies include delivering API-focused mitigation, automated L7 protection, and single-purpose cloud scrubbing optimized for latency-sensitive workloads. These players are expanding through reseller ecosystems, cybersecurity distributors, and localized managed service agreements, offering customizable SLAs and consumption-based pricing that appeal to organizations with limited security budgets and lean IT teams.

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 analyses the DDoS protection and mitigation security 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 and mitigation security market in terms of profitability.

TABLE 3 IMPACT OF PORTER'S FIVE FORCES ON DDoS PROTECTION AND MITIGATION SECURITY 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 14 DDOS PROTECTION AND MITIGATION SECURITY 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 and mitigation security 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 and mitigation security market; hence, suppliers face the constant pressure of losing customers to their competitors. The suppliers for organizations in the DDoS protection and mitigation security 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 and mitigation security market have major price sensitivity issues due to the availability of cost-competitive DDoS protection and mitigation security solutions from small-scale solution providers. The DDoS protection and mitigation security 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 and mitigation security 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 and mitigation security 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, e-commerce, 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

- Global GDP growth is driving higher digital adoption, expanding online services, and increasing exposure to large-scale DDoS attacks.
- Enterprise IT investments rise in line with GDP expansion, leading to higher spending on security infrastructure and managed DDoS mitigation services.
- Emerging economies in Asia Pacific, Latin America, and the Middle East show stronger GDP momentum, accelerating cloud usage, 5G deployments, and data center growth, boosting demand for DDoS protection.
- During slow GDP periods, enterprises lean toward cost-efficient managed services instead of high-capex on-premises appliances.
- Government-led digitalization and smart infrastructure initiatives, which scale with economic output, increase adoption of robust DDoS defense frameworks.
- High-income regions maintain advanced cybersecurity maturity, enabling faster uptake of AI-driven and hybrid mitigation models.

5.2.3 TRENDS IN GLOBAL DDOS PROTECTION & MITIGATION SECURITY 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, e-commerce, 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 SUPPLY CHAIN ANALYSIS

The supply chain analysis helps analyze the source of competitive advantage among market players, from the basic material suppliers to the end users. The model works by segregating firms into their strategically relevant activities to understand the behavior of costs and identify any sources of differentiation. For firms to achieve a competitive advantage, they must reduce costs in these strategically important activities.

The supply chain for the DDoS protection and mitigation security market comprises hardware providers, software providers, service providers, and end users. The following figure illustrates the complete supply chain, spanning from hardware providers to end users in the market.

FIGURE 15 SUPPLY CHAIN ANALYSIS

DDOS PROTECTION & MITIGATION SECURITY MARKET				
HARDWARE AND INFRASTRUCTURE PROVIDERS		SOFTWARE PROVIDERS	SERVICE PROVIDERS	END USERS/ APPLICATIONS
▪ RioRey RE and RS Hardware Series ▪ On-premises DDoS Mitigation Hardware ▪ AntiDDoS8000 DDoS Protection System		▪ Network Layer ▪ Null Routing ▪ Sinkholing ▪ Scrubbing ▪ Application Layer ▪ DNS Routing ▪ BGP Routing	▪ Managed Service Providers ▪ Professional Service Providers	▪ BFSI ▪ IT & ITeS ▪ Telecom ▪ Government & Defense ▪ Manufacturing ▪ Energy & Utilities ▪ Healthcare ▪ Retail ▪ Others
▪ Huawei Technologies ▪ Fortinet ▪ RioRey	▪ NETSCOUT ▪ Akamai ▪ Radware ▪ Fortinet ▪ Link11 ▪ Imperva ▪ Cloudflare ▪ BT ▪ A10 Networks ▪ Seceon ▪ Nexusguard	▪ Haltdos ▪ Corero ▪ RioRey ▪ PhoenixNAP ▪ DDoS-Guard ▪ Allot ▪ StrataCore ▪ F5 ▪ Indusface ▪ Mlytics	▪ NETSCOUT ▪ Radware ▪ Link11 ▪ Cloudflare ▪ A10 Networks ▪ Fastly ▪ Nexusguard ▪ Haltdos ▪ Corero ▪ DDoS-Guard ▪ Allot	▪ BFSI ▪ IT & ITeS ▪ Telecom ▪ Government & Defense ▪ Manufacturing ▪ Energy & Utilities ▪ Healthcare ▪ Retail ▪ Others

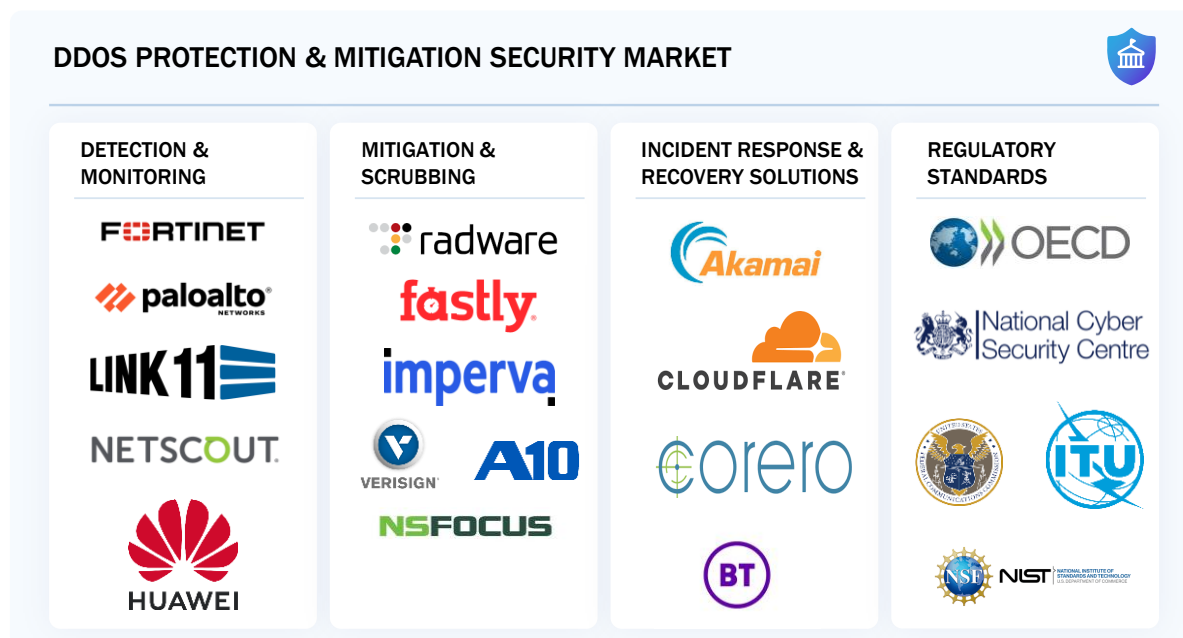
Note: The list of vendors and end users is not exhaustive.

Source: Secondary Research and MarketsandMarkets Analysis

5.4 ECOSYSTEM ANALYSIS

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

FIGURE 16 DDoS PROTECTION AND MITIGATION SECURITY MARKET: ECOSYSTEM ANALYSIS



Source: MarketsandMarkets Analysis

TABLE 4 ROLE OF COMPANIES IN ECOSYSTEM

ROLE IN ECOSYSTEM	COMPANY
Application Security	▪ Link11
	▪ Fastly
	▪ Sucuri
	▪ Indusface
Network Security	▪ BT
	▪ A10 Networks
	▪ RioRey
	▪ PhoenixNAP
Network Security, Application Security	▪ Huawei
	▪ Imperva
	▪ Cloudflare
	▪ Nexusguard
	▪ Haltdos
	▪ Corero
	▪ DDoS-Guard

Network Security, Application Security, Database Security	▪ StrataCore ▪ F5 ▪ activereach ▪ Mlytics ▪ Comodo Security Solutions
	▪ Radware ▪ NETSCOUT ▪ Akamai ▪ NSFocus ▪ Fortinet ▪ Lumen Technologies ▪ Seceon ▪ Allot

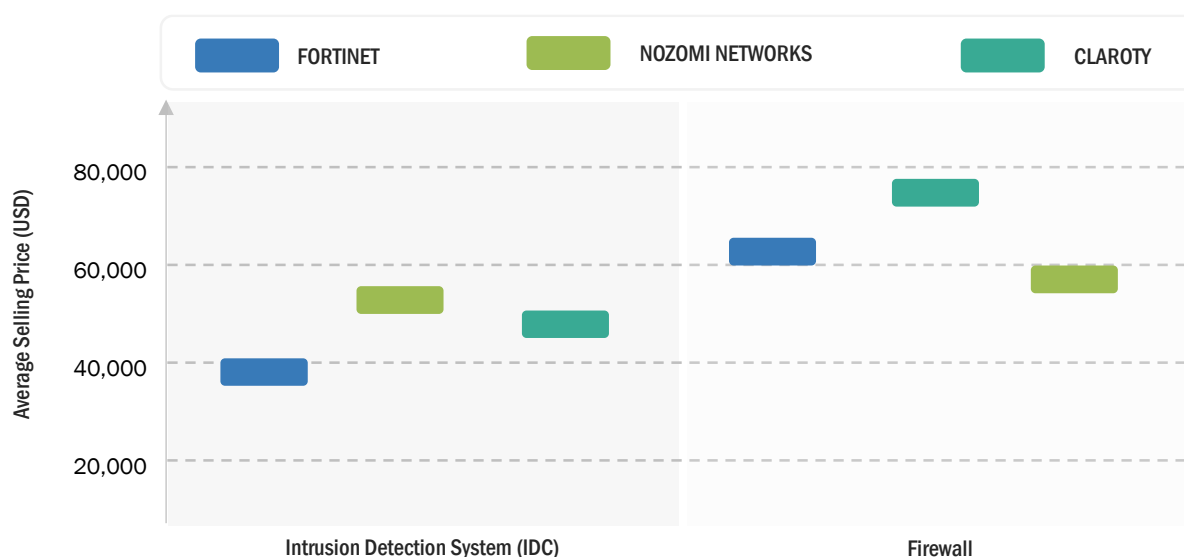
Source: MarketsandMarkets Analysis

5.5 PRICING ANALYSIS

The pricing of DDoS protection and mitigation security 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 security 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, 2024

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 17 AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2024 (USD)

Source: Company Websites and MarketsandMarkets Analysis

TABLE 5 AVERAGE SELLING PRICE OF KEY PLAYERS, BY OFFERING, 2024

Offering/Company	Fortinet	Nozomi Networks	Claroty
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 SECURITY, BY OFFERING, 2024

DDoS protection and mitigation security 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 6 INDICATIVE PRICING ANALYSIS OF DDOS PROTECTION AND MITIGATION SECURITY, BY OFFERING, 2024

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	<u>Free</u> - for personal or hobby projects that are not business-critical
		On-premises	<u>Pro</u> - for business websites that are not business-critical - USD 20/month
		Hybrid	<u>Business</u> - for small businesses operating online - USD 200/month
			Enterprise- for mission-critical applications that are core to businesses

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

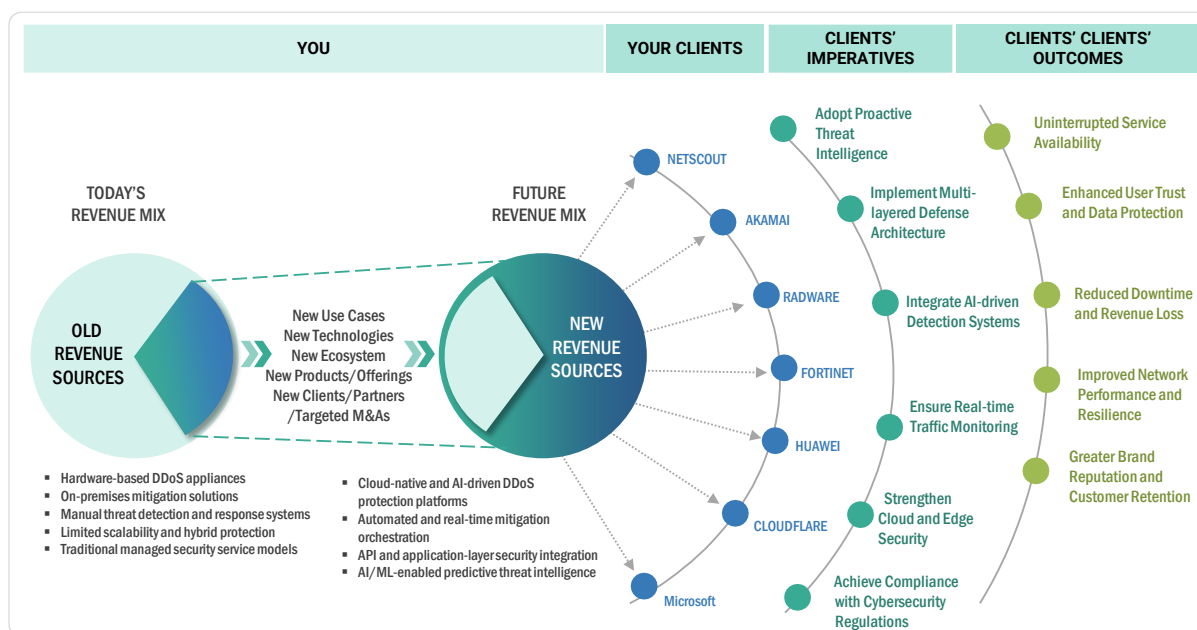
TABLE 7 DDOS PROTECTION AND MITIGATION SECURITY MARKET: LIST OF KEY CONFERENCES AND EVENTS, 2025

YEAR/QUARTER	NORTH AMERICA	EUROPE	ASIA PACIFIC	REST OF THE WORLD
Q1 '25	[February] NDSS Symposium 2025		[March] International Conference on Information and Network Technologies (ICINT 2025)	[January] Intersec 2025
Q3 '25	[July] The International Conference on Cyber Security (ICCS)		[July] International Conference on Information Security and Network Security (ISNS 2025)	

Note: Secondary Research and MarketsandMarkets Analysis

5.7 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS

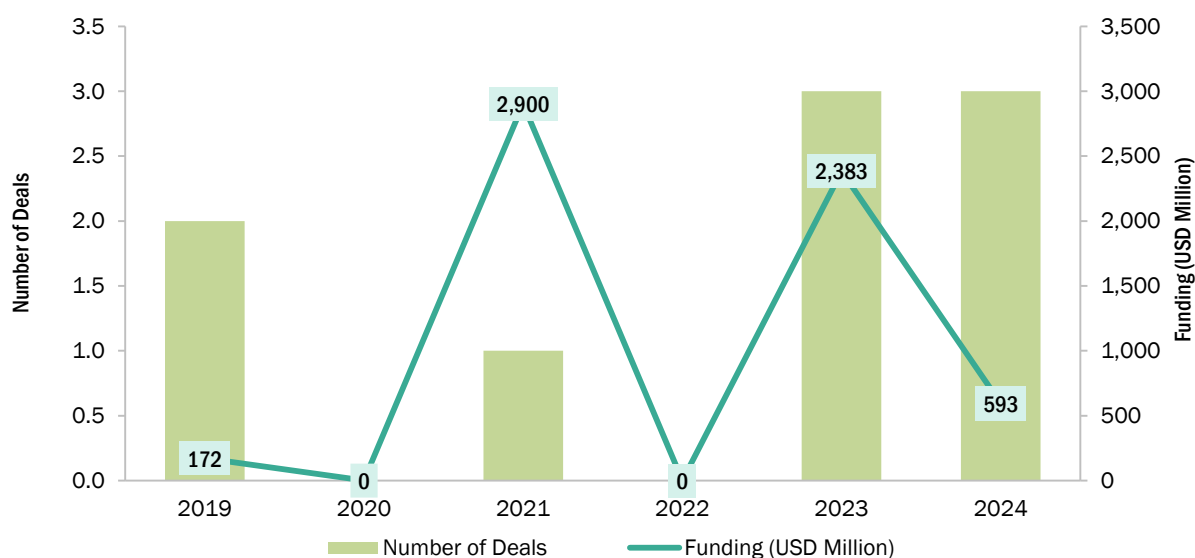
The market is steadily transitioning from legacy, hardware-heavy DDoS protection models toward cloud-delivered, automated, and AI-enhanced security architectures that offer greater scalability, faster response, and broader threat visibility. Enterprises increasingly expect proactive threat intelligence, continuous monitoring, and multi-layered defenses that integrate seamlessly across hybrid environments, prompting leading vendors such as NETSCOUT, Akamai, 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 18 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 and mitigation security 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. Additionally, some firms have pursued public offerings to raise capital, such as Cloudflare's IPO in 2019, underscoring the growing importance of DDoS protection within the broader cybersecurity landscape.

FIGURE 19 INVESTMENT AND FUNDING SCENARIO, 2019–2024

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 security companies are increasingly gearing up to address the challenges of their clients with innovative solutions.

5.9.1 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 provide protection 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

5.9.2 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 seeks 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

5.9.3 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 SECURITY MARKET

5.11.1 INTRODUCTION

In April 2025, the US implemented a broad "reciprocal tariff" framework, levying a standard 10% duty on all imports and significantly higher tariffs, reaching up to 50% or more, on 57 other countries. The most severe impact was felt by China, where US tariffs escalated to a staggering 245% on Chinese goods. In retaliation, China imposed a 125% tariff on US imports. These extraordinary measures have considerably disrupted global supply chains and triggered a wave of counter-tariffs in critical markets.

In a dramatic turn of events, implementation has been temporarily paused for most countries under a 90-day window, though tariffs on China took immediate effect, signaling both intent and urgency. This extensive tariff regime has rendered many product flows vulnerable to increased costs. Imports into the US from Europe will be subject to new duties ranging from 10% to 20%, with duties reaching 20% for goods from EU member states, while China-origin inputs will become prohibitively expensive due to the 125% US tariff. Conversely, US exports to Europe could face retaliatory tariffs averaging 25%, and shipments to China will be taxed at 125%, posing significant challenges to price competitiveness in both markets.

- Enhancement of Section 301 tariffs on Chinese imports, raising the applicable rates from 25% to 35% for existing categories while expanding the scope to include additional product classifications.
- Introduction of tariff measures on European imports, with rates varying between 10% and 25% across different sectors.
- Establishment of a universal base tariff set at 10% on all imports that do not fall under specific higher tariff thresholds.
- Implementation of a limited exemption framework for critical materials that lack domestic availability.
- Reinforcement of customs enforcement mechanisms, along with updated anti-circumvention regulations to tighten compliance.

5.11.2 KEY TARIFF RATES

TABLE 8 US-ADJUSTED RECIPROCAL TARIFF RATES

Rank	Country	US Imports, 2024 (USD Bn)	US Imports, 2024, Share	Tariffs Charged to US (%)	Adjusted Reciprocal Tariffs (%) *
1	Mexico	510.0	15.2	NA	NA
2	China	462.6	13.8	67	125
3	Canada	421.2	12.5	NA	NA
4	Germany	163.4	4.9	39	20
5	Japan	152.1	4.5	46	24
6	Vietnam	142.5	4.2	90	46
7	Korea	135.5	4.0	50	25
8	Taiwan	118.7	3.5	64	32
9	Ireland	103.8	3.1	39	20
10	India	91.2	2.7	52	26
11	Italy	78.4	2.3	39	20

12	UK	68.8	2.1	10	10
15	France	61.1	1.8	39	20
17	Brazil	44.2	1.3	40	20
18	Singapore	43.6	1.3	10	10

*Tariff rates are as of April 13, 2025. Elevated tariffs above the 10% baseline are subject to a 90-day implementation pause starting April 9, 2025, except for China, where increased rates took immediate effect.

Source: WITS, World Bank, White House Press Releases, 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 9 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 & E-commerce	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.
- Strain on cybersecurity budgets in public hospitals, affecting the rollout of robust mitigation layers.

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

6.1 KEY EMERGING TECHNOLOGIES

6.1.1 TRAFFIC FILTERING

Traffic filtering technology is a crucial component of DDoS protection and mitigation security. 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 blacklisting, 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.

6.1.2 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.

6.1.3 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.

6.2 COMPLEMENTARY TECHNOLOGIES

6.2.1 ARTIFICIAL INTELLIGENCE (AI)

AI technology is increasingly being integrated into DDoS protection and mitigation security, 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.

6.2.2 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.

6.3 ADJACENT TECHNOLOGIES

6.3.1 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.

6.3.2 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 whitelisting, and blacklisting 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.

6.4 FUTURE LANDSCAPE OF DDOS PROTECTION AND MITIGATION SECURITY MARKET

6.4.1 DDOS PROTECTION AND MITIGATION SECURITY TECHNOLOGY ROADMAP TILL 2030

The following technologies will be an essential part of the roadmap of the DDoS protection and mitigation security market.

6.4.1.1 Short-term roadmap (2025–2026)

The DDoS protection and mitigation security market is set for significant progress between 2025 and 2026, with significant advancements in technologies. AI and ML will play a crucial role in intelligent threat detection, predictive analytics, and automated mitigation. Cloud-based solutions will continue to gain popularity due to their scalability and flexibility. IoT security will be a major focus, with specialized solutions emerging to protect vulnerable devices. Integration with network automation will enable automated response and mitigation, while hybrid solutions will provide flexibility and scalability. As the threat of DDoS attacks continues to evolve, organizations will need to stay informed about the latest advancements and adopt solutions that can effectively protect their critical infrastructure.

6.4.1.2 Mid-term roadmap (2027–2028)

The DDoS protection and mitigation security market is expected to make significant strides between 2027 and 2028. The future of DDoS protection and mitigation security will be characterized by increased automation, intelligence, and integration with other security technologies. AI-powered solutions will enable real-time anomaly detection, predictive analytics, and automated mitigation. Cloud-based DDoS protection will continue to offer scalability and flexibility, while blockchain technology can establish a decentralized network for distributed trust and transparency. IoT security will require specialized mitigation techniques to address unique threats. Regulatory compliance and industry standards will also play a crucial role in shaping the future landscape of DDoS protection.

6.4.1.3 Long-term roadmap (2029–2030)

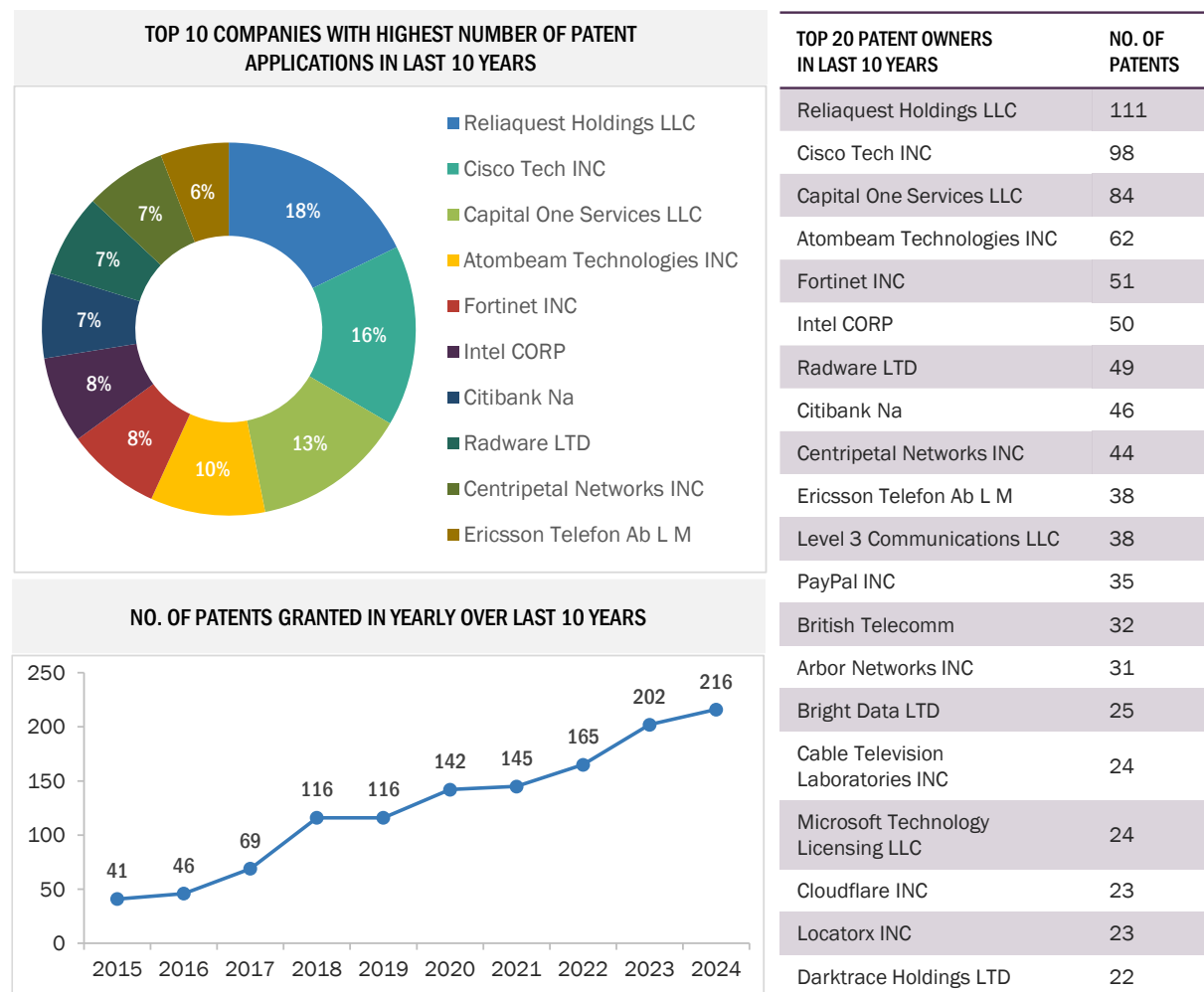
By 2029–2030, the DDoS protection and mitigation security market will be characterized by a convergence of advanced technologies, such as AI, quantum computing, and blockchain. AI-powered systems will enable real-time threat detection and automated response, while quantum computing can enhance security and threat detection. Edge-based security will reduce latency and improve response times for IoT devices. Blockchain can provide immutable records and distributed trust, while increased focus on supply chain security and regulatory compliance will be essential. Organizations that invest in these areas will be better positioned to protect their critical infrastructure and data in the face of evolving cyber threats.

6.5 PATENT ANALYSIS

6.5.1 METHODOLOGY

The patent analysis offers crucial insights into patent filing, business interests, and patenting activities yearly and country-wise. It is a technique used to understand the information contained in patents. This study defines patents claiming inventions linked to the DDoS protection and mitigation security market. For this study, a well-planned strategy is devised. Patents are categorized and analyzed using DDoS protection and mitigation security. This keyword is used for titles or abstracts to understand patent filing profiles. This section aims to provide an overview of patenting activities. Sources used for this analysis are The Lens-Patent, Scholarly Search, and Patent Scope.

FIGURE 20 LIST OF PATENTS APPLIED AND GRANTED, 2015–2024



Source: Lens.org

6.5.2 KEY PATENTS

TABLE 10 LIST OF MAJOR PATENTS, 2015–2024

YEAR	TITLE	PUBLICATION NUMBER	INVENTOR	DESCRIPTION
March 2024	Fraud or Distributed Denial of Service (DDoS) Protection For Session Initiation Protocol (SIP) - Based Communication	US 2023/0029971 A1	Uzelac Adam, Bailey Ronnie, Richter Craig	Novel tools and techniques are provided for implementing fraud or distributed denial of service (“DDoS”) protection for session initiation protocol (“SIP”)-based communication. In various embodiments, a computing system may receive, from a first router, first SIP data indicating a request to initiate a SIP-based media communication session between a calling party at a source address and a called party at a destination address. The computing system may analyze the received first SIP data to determine whether the received first SIP data comprises any abnormalities indicative of potential fraudulent or malicious actions. If so, the computing system may reroute the first SIP data to a security deep packet inspection (“DPI”) engine, which may perform a deep scan of the received first SIP data to identify any known fraudulent or malicious attack vectors contained within the received first SIP data. If so, the security DPI engine may initiate mitigation actions.
March 2023	Techniques for reducing the time to mitigate of DDoS attacks	US 11606387 B2	Doron Ehud, Ben Ezra Yotam, Aviv David	A system and method for reducing a time to mitigate distributed denial of service (DDoS) attacks are provided. The method includes receiving a plurality of attack feeds on at least one protected object in a secured environment; analyzing the plurality of attack feeds to determine characteristics of a DDoS attack against the secure environment; determining a set of optimal mitigation resources assigned to the secured environment; selecting, based on the set of optimal mitigation resources and the attack characteristics, at least one optimal workflow scheme; and initiating a proactive mitigation action by setting each mitigation resource in the set of optimal mitigation resources according to the selected optimal workflow scheme.

November 2022	Mitigation of DDos Attacks on Mobile Networks	US 2020/0314655 A1	Jain Hemant Kumar	Systems and methods for inspection of traffic between UE and the core network to mitigate DDoS attacks on mobile networks are provided. According to one embodiment, the method involves parsing SCTP packets and monitoring header anomalies to block anomalous packet floods. According to another embodiment, a memory table maintains requesting S1AP-IDs which have sent certain monitored commands and then blocking those which are sending these messages at abnormally high rates. According to yet another embodiment, a packet classifier parses the GTP-U protocol, unwraps the encapsulated IP packet and then monitors layer 3, 4 and 7 rate-based attacks such as UDP, ICMP, SYN, HTTP GET floods and drops them to protect the targeted Internet server as well as mobile infrastructure (e.g., the MME, the SGW, the PGW, and the PDN) downstream from the DDoS mitigation system.
August 2022	Distributed denial of service (DDoS) defense techniques for applications hosted in cloud computing platforms	US 11405417 B2	Doron Ehud, Ilani Nir, Aviv David, Ben Ezra Yotam, Bismut Amit	A defense platform for protecting a cloud-hosted application against distributed denial-of-services (DDoS) attacks, wherein the defense platform is deployed out-of-path of incoming traffic of the cloud-hosted application hosted in a plurality of cloud computing platforms, comprising: a detector; a mitigator; and a controller communicatively connected to the detector and the mitigator; wherein the detector is configured to: receive telemetries related to behavior of the cloud-hosted application from sources deployed in the plurality of cloud computing platforms; and detect, based on the telemetries, a potential DDoS attack; wherein, the controller, upon detection of a potential DDoS attack, is configured to: divert traffic directed to the cloud-hosted application to the mitigator; cause the mitigator to perform at least one mitigation action to remove malicious traffic from the diverted traffic; and cause injection of clean traffic to at least one of the plurality of cloud computing platforms hosting the cloud-hosted application.

Source: Lens.org

6.6 IMPACT OF AI/GEN AI ON DDOS PROTECTION AND MITIGATION SECURITY 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, 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 response, 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.

6.6.1 USE CASES OF GENERATIVE AI IN DDOS PROTECTION AND MITIGATION SECURITY

GenAI is emerging across the DDoS protection landscape through a set of practical, company-led implementations that enhance detection, analysis, and incident response. Cloudflare has begun integrating large-scale AI models into its anomaly-detection pipeline, where GenAI helps summarize attack telemetry for customers, draft incident reports, and automatically recommend mitigation policies based on historical Layer 3/4 traffic patterns. Akamai is exploring GenAI-driven log-analysis assistants within its Security Operations Command Center to convert massive DDoS traffic dumps into human-readable threat narratives, accelerating triage during multi-vector attacks. AWS is incorporating GenAI into Shield Advanced workflows, particularly for automated post-incident summaries and real-time recommendations that guide customers on rate-limiting, WAF rule tuning, and attack signature refinement. Microsoft's Copilot for Security, used by several enterprises integrating Azure DDoS Protection, applies GenAI to produce rapid attack reconstructions, natural-language threat explanations, and auto-generated remediation scripts. Palo Alto Networks has deployed GenAI in its Cortex platform to enrich network-level DDoS telemetry with contextual threat intelligence, enabling analysts to identify botnet origins faster. These implementations collectively demonstrate how GenAI is moving beyond prediction and into auto-documentation, automated tuning, human-readable attack intelligence, and rapid-response augmentation, making DDoS defense faster, more adaptive, and significantly less analyst-dependent.

Below are key use cases demonstrating how generative AI enhances DDoS Protection & Mitigation Security market:

FIGURE 21 USE CASES OF GENERATIVE AI IN DDOS PROTECTION & MITIGATION SECURITY

Source: Secondary Research and MarketsandMarkets Analysis

6.6.2 BEST PRACTICES

Different industries are adopting GenAI in the DDoS protection and mitigation security market in unique ways. Here are some best practices:

6.6.2.1 BFSI

- Implement GenAI-driven behavioral analytics to detect anomalies in real-time high-volume transactional traffic.
- Use AI-generated mitigation runbooks to reduce response times during multi-vector attacks on digital banking platforms.
- Deploy GenAI assistants for 24/7 SOC support to quickly analyze logs across ATM networks, payment gateways, and trading systems.
- Utilize GenAI to simulate large-scale DDoS attack scenarios for stress-testing critical financial infrastructure.

- Leverage AI-optimized routing and rate-limiting strategies for real-time protection of APIs and online banking portals.

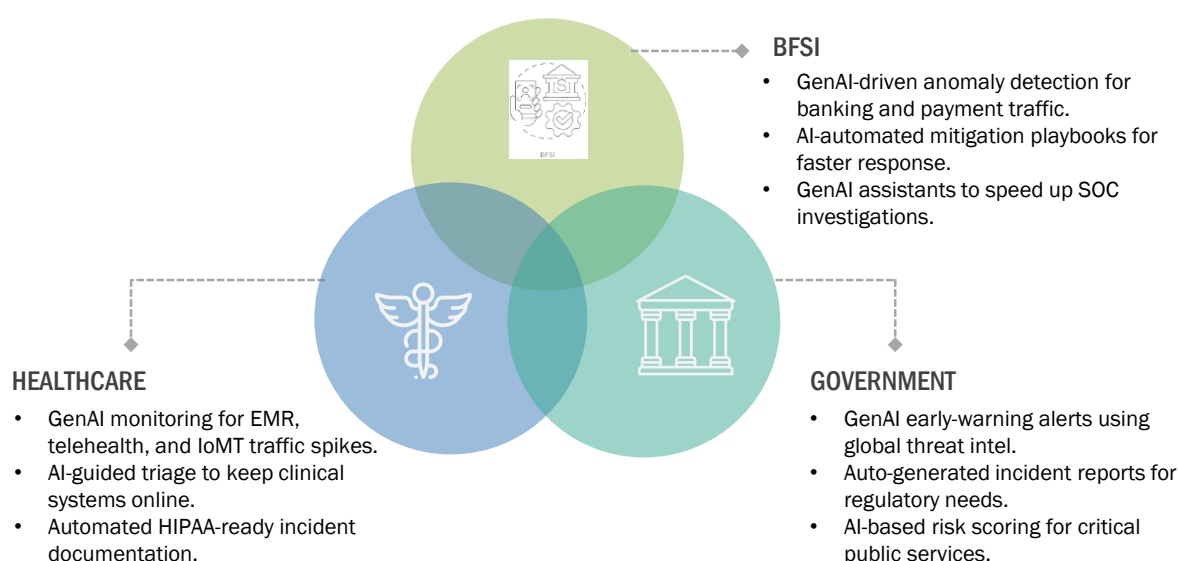
6.6.2.2 Government

- Deploy GenAI-based early-warning systems that correlate global threat intelligence with national cyber grids.
- Use GenAI to automatically generate compliance-ready attack reports for CERT, regulatory bodies, and security audits.
- Implement AI-driven risk scoring to prioritize mitigation for critical public services (tax portals, citizen ID systems, emergency services)
- Utilize GenAI to identify coordinated botnet campaigns targeting election platforms or public-sector networks.
- Enable AI-guided incident response workflows to help understaffed government SOC teams act faster during high-volume attacks.

6.6.2.3 Healthcare

- Apply GenAI to monitor irregular traffic surges targeting hospital EMR systems, telehealth platforms, and connected medical devices.
- Use AI-driven triage recommendations to maintain uptime for patient care systems during active attacks.
- Generate automated post-incident compliance documentation for HIPAA and healthcare cybersecurity audits.
- Enhance protection of IoMT (Internet of Medical Things) by detecting botnet-driven anomalies in device-to-cloud communications.
- Deploy GenAI models to simulate DDoS attack paths on healthcare networks to improve disaster recovery preparedness.

FIGURE 22 GENERATIVE AI BEST PRACTICES ACROSS MAJOR INDUSTRIES



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

6.6.3 CASE STUDIES OF GENERATIVE AI IMPLEMENTATION

6.6.3.1 GenAI-enhanced traffic intelligence for large-scale cloud infrastructure

A major global cloud provider integrated GenAI models into its DDoS detection pipeline to analyze billions of daily traffic logs and identify micro-anomalies missed by legacy systems. The deployment enabled the SOC to correlate multi-region traffic bursts, classify attack vectors in real time, and automatically generate mitigation rules for edge locations. This reduced incident triage time from hours to minutes and improved detection of zero-day botnet behaviors targeting customer workloads across gaming, fintech, and streaming platforms.

6.6.3.2 AI-automated incident analysis for multi-national financial group

A leading financial enterprise adopted a GenAI-powered investigation assistant that summarizes attack events, highlights malicious traffic patterns, and produces compliance-ready reports for regulators. The system integrates with payment networks and API gateways, allowing analysts to query logs conversationally and receive actionable insights instantly. As a result, the organization cut manual report preparation time by 70% and improved response coordination during high-volume DDoS attempts on its online banking services.

6.6.3.3 GenAI-driven botnet attribution for government cyber defense agency

A national cyber defense team deployed GenAI tools to enrich threat intelligence by correlating global DNS activity, malware signatures, and darknet chatter. The model identified emerging botnet clusters, traced command-and-control infrastructure, and predicted likely targets within critical infrastructure networks. This implementation enabled the agency to uncover coordinated attack campaigns weeks earlier than traditional monitoring systems and strengthened its ability to issue proactive national-level security advisories.

6.6.4 CLIENT READINESS AND IMPACT ASSESSMENT

Top clients are adapting to GenAI in several ways:

- Strong push to use GenAI for faster SOC analysis and reduced manual workload.
- High interest in GenAI-driven anomaly detection for multi-vector attacks.
- Adoption of AI-generated mitigation playbooks for quicker incident response.
- Growing use of natural-language log analysis to simplify investigations.
- Demand for AI-based risk scoring to prioritize critical assets.
- Increasing reliance on GenAI for automated regulatory and audit reporting.
- More clients testing GenAI attack simulation models for preparedness.

6.6.4.1 Client A: Global digital commerce platform

- **Implementation:** This client deployed a GenAI-enhanced detection engine within its edge security stack, integrating real-time traffic telemetry from global storefronts and payment endpoints. The system used AI-driven correlation models to flag micro-anomalies across multiple geographies and auto-generate mitigation rules tailored to live attack behavior. GenAI was also embedded into the SOC workflow to automatically summarize attack events, classify vectors, and provide analyst-ready insights during peak sales seasons.

- **Impact:** The platform achieved significantly faster detection of botnet-driven surges targeting its checkout systems, reducing response time by nearly 60%. The GenAI-generated remediation rules helped prevent revenue-impacting downtime during high-traffic events. Compliance reporting for financial regulators also became more efficient, with automated summaries replacing manual documentation, enabling the security team to focus on higher-level threat hunting.

6.6.4.2 Client B: Major public sector department

- **Implementation:** A government cybersecurity unit implemented GenAI-based intelligence enrichment to cross-analyze DNS logs, ISP-level telemetry, and external threat feeds. The model continuously scanned for early signals of coordinated attack campaigns and produced predictive patterns that were shared across national CERT teams. The agency also used GenAI to auto-generate incident reports and actionable advisories for downstream departments.
- **Impact:** The deployment improved early warning capabilities, helping the agency detect coordinated botnet build-ups weeks before traditional monitoring methods. Proactive advisories sent to regional centers enhanced protection across multiple public services, including citizen portals and emergency communication systems. Internal reporting cycles were reduced from days to hours, improving national-level readiness and inter-agency response coordination.

6.6.4.3 Client C: Large healthcare network

- **Implementation:** This healthcare group integrated GenAI into its DDoS defense stack to monitor EMR, telehealth, and IoMT traffic for abnormal surges. GenAI-assisted log analysis enabled clinical IT teams to quickly identify malicious traffic patterns and differentiate between legitimate medical device activity and botnet-generated noise. The organization also adopted AI-driven triage recommendations during active incidents.
- **Impact:** The healthcare system experienced improved service availability during attacks, ensuring uninterrupted access to critical clinical applications. Response time dropped significantly due to automated, AI-guided recommendations, allowing smaller IT teams to manage large-scale incidents with higher confidence. Compliance processes related to healthcare cybersecurity standards were streamlined, with GenAI producing structured reports aligned with audit frameworks.

7 REGULATORY LANDSCAPE

7.1 REGULATORY LANDSCAPE

Regulatory bodies play a key role in the DDoS protection and mitigation security 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 11 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 DHS, leads the national effort to protect critical infrastructure against cybersecurity threats. It can be involved in shaping regulations and guidelines for securing networks, including the use of NGFW solutions.
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 12 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 13 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 Directorate (ASD)	Government Agency	The Australian Signals Directorate (ASD) is an intelligence agency that provides cybersecurity, intelligence, and offensive 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 14 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 infrastructures, 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

7.1.1.1 National Credit Union Administration

The National Credit Union Administration (NCUA) is focused on warning financial institutions and credit unions to prevent them from being disrupted by DDoS attacks. The NCUA releases risk alerts and advises financial organizations to conduct risk assessments for DDoS attack detection, establish incident response protocols in case of attacks, and prioritize due diligence to identify and manage risks related to traffic.

7.1.1.2 Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council (FFIEC) is a regulatory body focused on safeguarding financial organizations against advanced DDoS attacks. This council expects the financial organizations to create and maintain security programs, monitor internet traffic, implement security and incident response plans, and hire good security staff. It also emphasizes identifying attacks and performing a risk assessment. With the mandates levied by the FFIEC, financial institutions can safeguard themselves against advanced DDoS attacks, which may be volumetric, network-layer, or application-layer.

7.1.1.3 General Data Protection Regulation (GDPR)

GDPR is a privacy regulation in the EU that came into force in all EU countries on May 25, 2018. It primarily aims to give individuals control over their personal data and simplify the regulatory environment for international business by unifying the regulations in the EU. GDPR defines seven principles for the lawful processing of personal data. Processing includes the collection, organization, structuring, storage, alteration, consultation, use, communication, combination, restriction, erasure, or destruction of personal data. It covers personal information and activities in the EU even when the party processing the personal information is not in the EU. Organizations failing to comply with GDPR are imposed hefty penalties. GDPR

would ensure that European enterprises are well-equipped with cybersecurity solutions for networks, applications, data, endpoints, and cloud security. Hence, the sales of DDoS protection and mitigation solutions and services are expected to increase.

7.1.1.4 Payment Card Industry Data Security Standard (PCI-DSS)

The PCI-DSS compliance was developed by payment brands, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa International. It defines a set of 12 requirements for enhancing the payment account data security to include the policies, tools, and controls needed to protect cardholder data. The standard requires merchants and member service providers that store, process, or transmit cardholder data to establish and maintain a secure IT network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, and regularly monitor and test their networks. One of the primary objectives of PCI-DSS is to prevent data breaches, which requires businesses to install security software to protect themselves from threats, control physical access to information, and test the network's security to minimize the risks for card companies and their customers.

7.1.1.5 Health Insurance Portability And Accountability Act (HIPAA)

HIPAA compliance provides federal protection for personal health information and affords patients the right to access and control their protected health information (PHI). This ensures data privacy and security provisions for safeguarding medical information. The healthcare vertical is moving toward electronic healthcare records accessible via web and mobile-based applications, which are the main targets for hackers to gain access to sensitive healthcare customer/patient data. According to compliance regulations, if web and mobile-based applications send, store, or share data related to doctors, patients, or other health-related information, they must comply with the HIPAA guidelines. Most violations of the HIPAA standards result from businesses not following policies and procedures for safeguarding healthcare records. Organizations handling PHI must ensure that all necessary physical, process, and network security measures are in place and followed.

7.1.1.6 Gramm-Leach-Bliley (GLB) Act

The GLB Act, also known as the Financial Services Modernization Act of 1999, is a federal law enacted by the US to regulate how financial institutions handle individuals' private information. This includes provisions to protect consumers' personal financial information held by banks, securities companies, and insurance companies. Under the jurisdiction of the Federal Trade Commission (FTC), these financial institutions are required to design, implement, and maintain an information security program to protect the privacy and integrity of customer data.

7.1.1.7 Sarbanes-Oxley (SOX) Act

The Sarbanes-Oxley (SOX) Act of 2002 was passed by the US Congress to protect shareholders and the public from accounting errors and fraudulent practices within enterprises, as well as to enhance the accuracy of corporate disclosures. The main objective of designing SOX compliance is to increase transparency in corporate governance and financial reporting and formalize a system of internal checks and balances. Penalties for non-compliance with SOX include fines and removal from listing on public stock exchanges. Security vendors offer solutions and services to ensure SOX compliance, adhering to industry best practices for risk assessment, intrusion detection, analytics, and security monitoring. Today, most attacks are directed at applications that include financial transactions, and any security gap in these applications puts data integrity at risk. Organizations must ensure that such web and mobile-based applications are tested for vulnerabilities.

7.1.1.8 SOC 2

Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality, and privacy. SOC 2 is an auditing procedure that ensures third-party service providers securely manage enterprise data to protect the interests of the organization and the privacy of its clients. For security-conscious businesses, SOC 2 compliance is a minimal requirement when considering a SaaS provider. SOC 2 reports are of two types. In line with specific business practices, each designs its controls to comply with one or more trust principles. These internal reports provide enterprises with important information about how the service provider manages data.

7.1.1.9 SWIFT CSP

The SWIFT Customer Security Program (CSP) is a framework designed to help improve the security of the SWIFT interbank communications system, as well as the financial institutions that rely on it to send and receive information about financial transactions. The SWIFT CSP contains a range of mandatory and advisory controls designed to help organizations secure their environment, track and limit access, and detect and respond to threats. Principle 2 of the CSP requires organizations to reduce their attack surface and manage vulnerabilities.

8 CUSTOMER LANDSCAPE AND BUYER BEHAVIOR

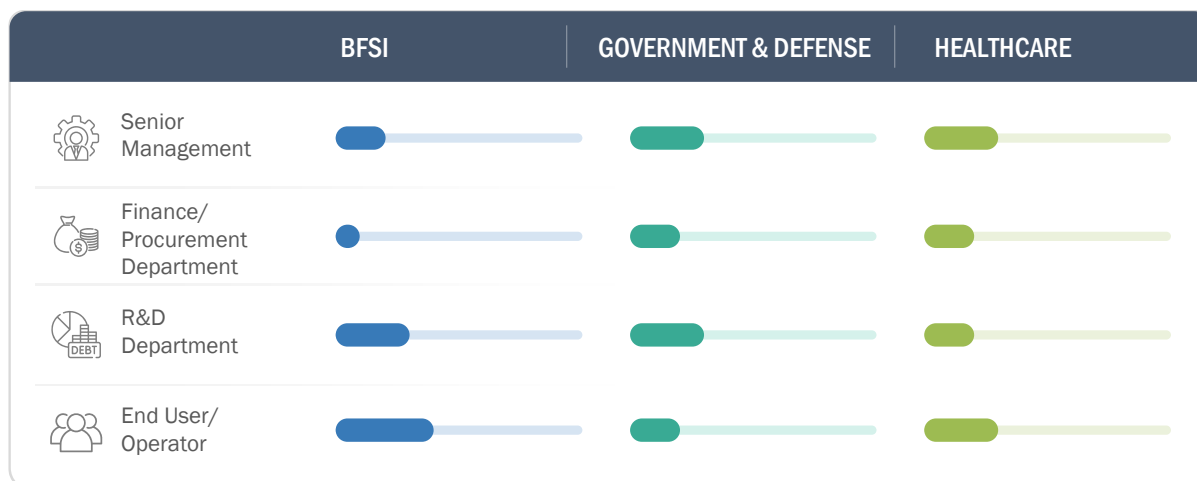
8.1 DECISION-MAKING PROCESS

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.

8.2 BUYER STAKEHOLDERS AND BUYING EVALUATION CRITERIA

8.2.1 KEY STAKEHOLDERS IN BUYING PROCESS

FIGURE 23 INFLUENCE OF STAKEHOLDERS ON BUYING PROCESS FOR TOP THREE VERTICALS



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

TABLE 15 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 24 KEY BUYING CRITERIA FOR TOP THREE VERTICALS



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

TABLE 16 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.

9 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING

KEY FINDINGS

- By offering, the services segment is projected to register the highest CAGR of 13.4% during the forecast period, reaching USD 2,667.9 million by 2030.
- The software solutions segment is expected to dominate the DDoS protection and mitigation security market, with USD 2,458.2 million in 2025, and is projected to register a CAGR of 12.4% 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 security 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

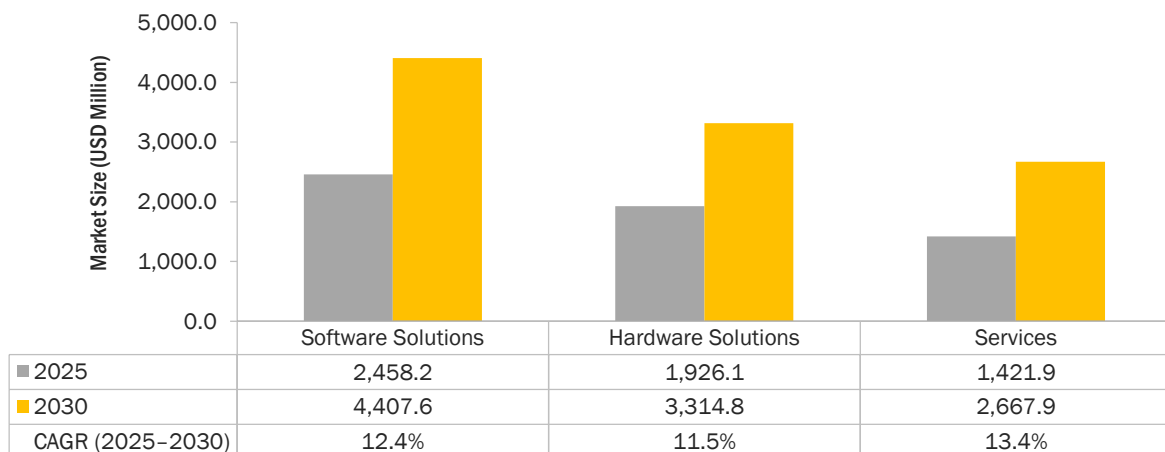
The DDoS protection and mitigation security market, by offering, has been segmented into hardware solutions, software solutions, and services. DDoS solutions and services play a crucial role in safeguarding data, servers, endpoints, cloud infrastructure, and organizational networks from attackers.

A DDoS attack, or Distributed Denial of Service attack, is a malicious attempt to disrupt an organization's functioning. These attacks pose a significant threat to businesses, and organizations must implement measures to protect their applications, network solutions, and services against the increasingly sophisticated nature of DDoS attacks. DDoS attacks target various resources, including networks, websites, servers, and endpoints, by overwhelming them with traffic. In contrast, DoS attacks (Denial of Service attacks) focus on making a specific target machine unavailable to legitimate users by flooding it with false requests.

DDoS attacks affect the application layer, protocol layer, and network bandwidth. Organizations utilize DDoS protection and mitigation security solutions and services to provide adaptive defense against DDoS attacks. DDoS attacks compromise the confidentiality, integrity, and availability of resources, potentially resulting in millions of dollars in losses for organizations. The target system becomes slow and unresponsive, as it lacks the capacity to handle legitimate traffic due to being flooded with falsified network traffic. The attacker tries to infiltrate an organization's device through malware or a backdoor entry. The device under the attacker's control functions as a command-and-control server, commonly referred to as a botnet. With a series of botnets under the control of an attacker, he/she disrupts the target resources by flooding traffic from the botnets. Therefore, organizations across various verticals, including retail, BFSI, government and defense, healthcare, energy and utilities, and manufacturing, ultimately adopt DDoS protection and mitigation security solutions and associated services. One of the major reasons for the increase in demand for these solutions and services can be attributed to the growing awareness among organizations about the evolving threat landscape and the need to have a disaster recovery plan in place before a DDoS attack significantly impacts the business.

9.1.1 OFFERING: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS

- The increasing demand for ensuring operational efficiency is fueling the demand for hardware solutions.
- Seamless, flexible, and easy-to-deploy options to fuel the demand for DDoS protection and mitigation security software solutions.
- The services segment is expected to grow due to the increasing demand for DDoS protection and mitigation security 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 security market.

FIGURE 25 SERVICES SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD

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

TABLE 17 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	847.6	957.4	1,115.1	1,290.9	1,483.0	1,693.8	14.9%
Software Solutions	1,031.2	1,174.3	1,378.6	1,608.5	1,862.6	2,144.5	15.8%
Services	563.3	647.6	767.7	904.4	1,057.4	1,228.9	16.9%
Total	2,442.0	2,779.3	3,261.4	3,803.8	4,403.0	5,067.3	15.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 18 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	1,926.1	2,181.8	2,457.4	2,744.3	3,033.2	3,314.8	11.5%
Software Solutions	2,458.2	2,807.3	3,187.6	3,589.1	3,999.8	4,407.6	12.4%
Services	1,421.9	1,638.9	1,878.0	2,133.8	2,399.4	2,667.9	13.4%
Total	5,806.2	6,628.0	7,523.0	8,467.1	9,432.3	10,390.3	12.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.2 HARDWARE SOLUTIONS

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 19 HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	361.9	408.4	465.4	526.5	590.8	658.7	12.7%
Europe	209.2	242.2	283.5	329.7	380.2	435.5	15.8%
Asia Pacific	156.8	166.7	200.5	239.9	285.0	337.0	16.5%
Middle East & Africa	84.1	98.5	116.5	137.0	159.7	184.9	17.1%
Latin America	35.6	41.6	49.2	57.8	67.2	77.8	16.9%
Total	847.6	957.4	1,115.1	1,290.9	1,483.0	1,693.8	14.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 20 HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	730.8	807.1	885.3	961.5	1,031.8	1,092.9	8.4%
Europe	496.2	563.0	634.9	709.7	784.9	857.3	11.6%
Asia Pacific	396.6	465.0	542.1	626.8	717.5	811.8	15.4%
Middle East & Africa	213.0	244.3	278.4	314.6	351.7	390.0	12.9%
Latin America	89.5	102.5	116.7	131.7	147.2	162.9	12.7%
Total	1,926.1	2,181.8	2,457.4	2,744.3	3,033.2	3,314.8	11.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.2.1 FIREWALLS

9.2.1.1 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 security, 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.

TABLE 21 FIREWALLS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	141.1	159.6	182.1	206.4	232.1	259.2	12.9%
Europe	81.8	94.9	111.2	129.6	149.7	171.8	16.0%
Asia Pacific	59.9	63.8	76.9	92.2	109.7	129.9	16.8%
Middle East & Africa	32.6	38.3	45.4	53.5	62.4	72.4	17.3%
Latin America	13.7	16.0	19.0	22.3	26.0	30.1	17.1%
Total	329.1	372.5	434.6	503.9	579.9	663.4	15.1%

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

TABLE 22 FIREWALLS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	288.1	318.7	350.2	381.0	409.6	434.6	8.6%
Europe	196.1	222.9	251.8	282.0	312.4	341.8	11.8%
Asia Pacific	153.2	179.9	210.1	243.4	279.1	316.4	15.6%
Middle East & Africa	83.5	96.0	109.6	124.0	138.9	154.3	13.1%
Latin America	34.7	39.9	45.5	51.4	57.5	63.8	12.9%
Total	755.6	857.4	967.2	1,081.8	1,197.6	1,310.9	11.6%

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

9.2.2 INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

9.2.2.1 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, blacklisting, 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.

TABLE 23 INTRUSION DETECTION AND PREVENTION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	94.5	105.7	119.5	134.1	149.2	165.0	11.8%
Europe	54.4	62.5	72.5	83.6	95.7	108.6	14.8%
Asia Pacific	41.4	43.7	52.1	61.8	72.8	85.4	15.6%
Middle East & Africa	22.2	25.8	30.3	35.3	40.8	46.9	16.1%
Latin America	9.7	11.2	13.2	15.3	17.7	20.3	16.0%
Total	222.1	248.9	287.6	330.2	376.3	426.3	13.9%

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

TABLE 24 INTRUSION DETECTION AND PREVENTION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	181.5	198.8	216.2	232.8	247.6	260.0	7.4%
Europe	122.8	138.1	154.4	171.1	187.6	203.1	10.6%
Asia Pacific	99.7	115.9	134.0	153.6	174.4	195.6	14.4%
Middle East & Africa	53.5	60.9	68.8	77.1	85.5	94.0	11.9%
Latin America	23.2	26.4	29.8	33.3	36.9	40.5	11.8%
Total	480.8	540.1	603.2	668.0	732.0	793.1	10.5%

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

9.2.3 LOAD BALANCERS

9.2.3.1 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.

TABLE 25 LOAD BALANCERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	69.1	78.8	90.7	103.6	117.3	132.1	13.8%
Europe	40.4	47.2	55.8	65.5	76.3	88.2	16.9%
Asia Pacific	30.6	32.8	39.9	48.2	57.7	68.9	17.7%
Middle East & Africa	16.3	19.3	23.1	27.4	32.2	37.6	18.2%
Latin America	6.9	8.2	9.8	11.6	13.6	15.9	18.0%
Total	163.3	186.3	219.1	256.2	297.2	342.7	16.0%

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

TABLE 26 LOAD BALANCERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	147.9	164.9	182.5	200.1	216.7	231.6	9.4%
Europe	101.4	116.1	132.2	149.1	166.4	183.4	12.6%
Asia Pacific	81.9	96.9	113.9	132.9	153.6	175.3	16.4%
Middle East & Africa	43.7	50.6	58.2	66.4	74.9	83.8	13.9%
Latin America	18.5	21.4	24.5	27.9	31.5	35.2	13.8%
Total	393.4	449.9	511.4	576.5	643.0	709.2	12.5%

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

9.2.4 OTHER HARDWARE SOLUTIONS

Scrubbing devices, rate limiters, and anti-DDoS gateways are vital offerings in the DDoS protection and mitigation security 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.

TABLE 27 OTHER HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	57.2	64.3	73.1	82.4	92.2	102.4	12.4%
Europe	32.6	37.7	43.9	50.9	58.5	66.8	15.4%
Asia Pacific	24.9	26.4	31.7	37.8	44.7	52.7	16.2%
Middle East & Africa	13.0	15.1	17.8	20.9	24.3	28.0	16.7%
Latin America	5.3	6.2	7.3	8.5	9.9	11.4	16.5%
Total	133.0	149.7	173.8	200.5	229.6	261.4	14.5%

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

TABLE 28 OTHER HARDWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	113.3	124.7	136.3	147.6	157.9	166.7	8.0%
Europe	75.9	85.9	96.5	107.5	118.5	129.0	11.2%
Asia Pacific	61.9	72.3	84.0	96.8	110.5	124.6	15.0%
Middle East & Africa	32.2	36.8	41.8	47.0	52.4	57.9	12.5%
Latin America	13.1	14.9	16.9	19.0	21.2	23.4	12.3%
Total	296.3	334.5	375.5	418.0	460.5	501.6	11.1%

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

9.3 SOFTWARE SOLUTIONS

9.3.1 GLOBAL RISE IN IOT DEVICES TO DRIVE MARKET

DDoS protection and mitigation security solutions are crucial for safeguarding organizations against advanced DDoS attacks. Nowadays, adversaries use readily available software tools to launch sophisticated DDoS attacks. These attacks primarily fall into four categories: volumetric, asymmetric, computational, and vulnerability-based. The volumetric and application-specific attacks are the most damaging ones. Some of the most critical DDoS attacks include the NTP amplification attack, DNS attack, R.U.D.Y. attack, SYN flood, and HTTP POST attacks. DDoS protection and mitigation security solutions safeguard websites, infrastructure, and DNS from DDoS attacks. DDoS protection and mitigation solutions can be integrated into cloud, on-premises, and hybrid environments.

Organizations are seeking solutions that are seamless, flexible, and easy to deploy. These solutions should also enable quicker responses for DDoS defense. As a result, organizations prefer options that leverage advanced ML, big data analytics, and AI. These technologies offer superior threat detection capabilities that traditional signature-based models cannot provide. Next-generation DDoS protection and mitigation solutions, equipped with behavioral analytics engines, offer both signature-based and signature-less detection of DDoS attacks, along with low false-positive rates. Additionally, these solutions do not impact the operational efficiency of an organization's network and resources. The rapid growth in the number of IoT devices worldwide is cited as one of the key drivers for the adoption of DDoS protection and mitigation security solutions.

TABLE 29 SOFTWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	442.1	502.8	577.5	658.6	744.9	837.2	13.6%
Europe	258.5	301.7	355.9	417.3	485.3	560.4	16.7%
Asia Pacific	187.2	200.6	243.3	293.4	351.4	418.9	17.5%
Middle East & Africa	101.6	119.9	143.1	169.6	199.4	232.8	18.0%
Latin America	41.8	49.3	58.8	69.6	81.7	95.2	17.9%
Total	1,031.2	1,174.3	1,378.6	1,608.5	1,862.6	2,144.5	15.8%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 30 SOFTWARE SOLUTIONS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	936.4	1,042.6	1,153.0	1,262.6	1,366.3	1,459.3	9.3%
Europe	644.0	736.8	838.0	944.8	1,054.0	1,161.2	12.5%
Asia Pacific	497.0	587.5	690.5	805.2	929.5	1,060.5	16.4%
Middle East & Africa	270.4	312.7	359.4	409.6	461.9	516.7	13.8%
Latin America	110.5	127.6	146.6	166.9	188.0	209.9	13.7%
Total	2,458.2	2,807.3	3,187.6	3,589.1	3,999.8	4,407.6	12.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

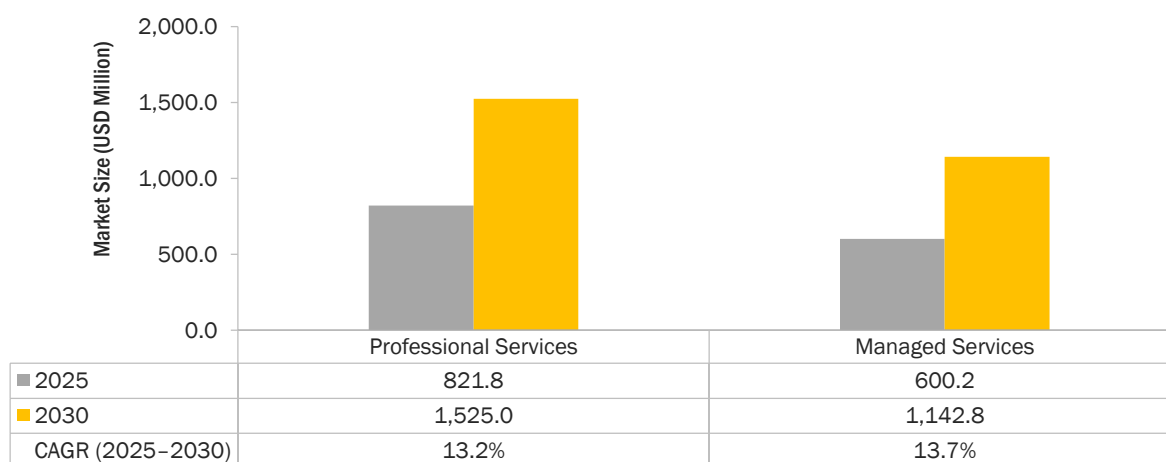
9.4 SERVICES

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 security 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 security 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 26 MANAGED SERVICES SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD



Note: According to the primary respondent's viewpoint, managed services are expected to grow at a higher CAGR due to the increasing complexity of IT infrastructure.

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

TABLE 31 SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2019–2024 (USD MILLION)

Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	330.4	378.6	447.7	526.2	613.8	711.8	16.6%
Managed Services	232.9	269.0	320.0	378.2	443.5	517.1	17.3%
Total	563.3	647.6	767.7	904.4	1,057.4	1,228.9	16.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 32 SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2025–2030 (USD MILLION)

Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	821.8	945.0	1,080.5	1,225.0	1,374.5	1,525.0	13.2%
Managed Services	600.2	693.8	797.5	908.8	1,024.9	1,142.8	13.7%
Total	1,421.9	1,638.9	1,878.0	2,133.8	2,399.4	2,667.9	13.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 33 SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	224.1	257.3	298.3	343.3	391.8	444.3	14.7%
Europe	147.7	173.8	206.8	244.5	286.6	333.7	17.7%
Asia Pacific	103.9	112.3	137.4	167.1	201.9	242.6	18.5%
Middle East & Africa	60.9	72.5	87.2	104.2	123.4	145.2	19.0%
Latin America	26.6	31.6	38.0	45.3	53.6	63.0	18.8%
Total	563.3	647.6	767.7	904.4	1,057.4	1,228.9	16.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 34 SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

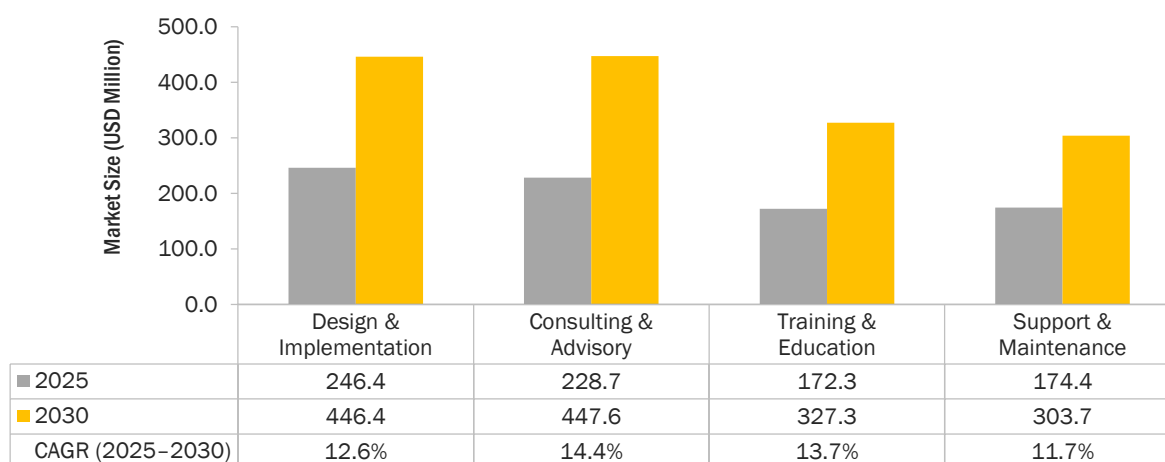
Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	501.4	563.2	628.2	693.9	757.3	815.7	10.2%
Europe	386.6	445.8	511.1	580.7	652.8	724.8	13.4%
Asia Pacific	290.3	346.0	410.0	481.9	560.8	644.9	17.3%
Middle East & Africa	170.0	198.1	229.5	263.5	299.4	337.4	14.7%
Latin America	73.7	85.7	99.2	113.7	129.0	145.1	14.5%
Total	1,421.9	1,638.9	1,878.0	2,133.8	2,399.4	2,667.9	13.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.4.1 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 security 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 27 CONSULTING & ADVISORY SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD


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

TABLE 35 PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	132.2	151.4	175.1	201.0	228.8	258.8	14.4%
Europe	81.2	95.4	113.1	133.4	155.9	181.1	17.4%
Asia Pacific	64.4	69.5	84.8	102.9	123.9	148.6	18.2%
Middle East & Africa	35.2	41.8	50.1	59.8	70.6	82.9	18.7%
Latin America	17.3	20.5	24.6	29.3	34.5	40.5	18.5%
Total	330.4	378.6	447.7	526.2	613.8	711.8	16.6%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 36 PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	291.3	326.4	363.1	400.0	435.5	467.8	9.9%
Europe	209.1	240.5	275.0	311.6	349.3	386.7	13.1%
Asia Pacific	177.4	210.9	249.3	292.3	339.3	389.2	17.0%
Middle East & Africa	96.7	112.4	129.9	148.8	168.6	189.4	14.4%
Latin America	47.2	54.8	63.3	72.4	81.9	91.9	14.3%
Total	821.8	945.0	1,080.5	1,225.0	1,374.5	1,525.0	13.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 37 PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2019–2024 (USD MILLION)

Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	101.9	116.2	136.8	160.0	185.8	214.4	16.0%
Consulting and Advisory	86.0	99.6	119.2	141.7	167.1	196.0	17.9%
Training and Education	67.3	77.5	92.1	108.7	127.5	148.5	17.2%
Support and Maintenance	75.2	85.2	99.7	115.8	133.4	152.9	15.3%
Total	330.4	378.6	447.7	526.2	613.8	711.8	16.6%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 38 PROFESSIONAL SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY TYPE, 2025–2030 (USD MILLION)

Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	246.4	282.0	320.9	362.1	404.3	446.4	12.6%
Consulting and Advisory	228.7	265.9	307.3	352.1	399.2	447.6	14.4%
Training and Education	172.3	199.1	228.7	260.5	293.7	327.3	13.7%
Support and Maintenance	174.4	198.1	223.7	250.4	277.3	303.7	11.7%
Total	821.8	945.0	1,080.5	1,225.0	1,374.5	1,525.0	13.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.4.2 DESIGN AND IMPLEMENTATION

9.4.2.1 Increase in need to improve network performance and reliability

Design and implementation services help organizations configure, validate, and implement DDoS protection and mitigation security 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 39 DESIGN AND IMPLEMENTATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	40.2	45.8	52.7	60.2	68.2	76.7	13.8%
Europe	25.6	29.9	35.3	41.4	48.2	55.7	16.8%
Asia Pacific	20.3	21.8	26.4	31.9	38.3	45.7	17.6%
Middle East & Africa	10.5	12.4	14.8	17.6	20.7	24.2	18.1%
Latin America	5.3	6.3	7.5	8.9	10.4	12.2	17.9%
Total	101.9	116.2	136.8	160.0	185.8	214.4	16.0%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 40 DESIGN AND IMPLEMENTATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	85.9	95.8	106.0	116.2	125.8	134.5	9.4%
Europe	64.0	73.2	83.3	93.9	104.8	115.4	12.5%
Asia Pacific	54.3	64.2	75.5	88.1	101.8	116.2	16.4%
Middle East & Africa	28.1	32.4	37.3	42.5	47.9	53.5	13.8%
Latin America	14.1	16.3	18.7	21.3	24.0	26.8	13.7%
Total	246.4	282.0	320.9	362.1	404.3	446.4	12.6%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.4.3 CONSULTING AND ADVISORY

9.4.3.1 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 41 CONSULTING AND ADVISORY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	34.5	40.0	46.7	54.3	62.5	71.4	15.7%
Europe	20.6	24.5	29.4	35.1	41.5	48.7	18.7%
Asia Pacific	17.0	18.6	22.9	28.1	34.2	41.5	19.5%
Middle East & Africa	9.3	11.2	13.5	16.3	19.5	23.1	20.0%
Latin America	4.6	5.5	6.6	8.0	9.5	11.3	19.8%
Total	86.0	99.6	119.2	141.7	167.1	196.0	17.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 42 CONSULTING AND ADVISORY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	81.3	92.0	103.5	115.2	126.7	137.5	11.1%
Europe	56.9	66.1	76.4	87.5	99.2	111.0	14.3%
Asia Pacific	50.0	60.1	71.8	85.1	99.7	115.6	18.2%
Middle East & Africa	27.3	32.0	37.4	43.3	49.6	56.3	15.6%
Latin America	13.3	15.6	18.2	21.0	24.0	27.2	15.5%
Total	228.7	265.9	307.3	352.1	399.2	447.6	14.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.4.4 TRAINING AND EDUCATION

9.4.4.1 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 43 TRAINING AND EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	26.8	30.9	35.9	41.4	47.4	53.8	14.9%
Europe	16.7	19.7	23.5	27.9	32.7	38.2	18.0%
Asia Pacific	13.1	14.2	17.4	21.2	25.7	30.9	18.8%
Middle East & Africa	7.1	8.5	10.2	12.2	14.5	17.2	19.2%
Latin America	3.5	4.2	5.0	6.0	7.2	8.4	19.1%
Total	67.3	77.5	92.1	108.7	127.5	148.5	17.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 44 TRAINING AND EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	60.9	68.5	76.6	84.8	92.8	100.1	10.5%
Europe	44.3	51.2	58.8	67.0	75.4	83.9	13.6%
Asia Pacific	37.1	44.3	52.6	62.0	72.3	83.3	17.6%
Middle East & Africa	20.1	23.5	27.3	31.4	35.7	40.4	14.9%
Latin America	9.9	11.5	13.4	15.3	17.5	19.7	14.8%
Total	172.3	199.1	228.7	260.5	293.7	327.3	13.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.4.5 SUPPORT AND MAINTENANCE

9.4.5.1 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 security products.

TABLE 45 SUPPORT AND MAINTENANCE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	30.7	34.8	39.7	45.1	50.8	56.8	13.1%
Europe	18.3	21.2	24.9	29.0	33.5	38.5	16.1%
Asia Pacific	14.0	15.0	18.1	21.7	25.8	30.5	16.8%
Middle East & Africa	8.3	9.7	11.5	13.6	15.9	18.4	17.4%
Latin America	3.9	4.6	5.4	6.4	7.5	8.6	17.2%
Total	75.2	85.2	99.7	115.8	133.4	152.9	15.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 46 SUPPORT AND MAINTENANCE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	63.2	70.0	77.0	83.8	90.1	95.7	8.6%
Europe	43.9	49.9	56.4	63.1	69.9	76.4	11.7%
Asia Pacific	36.0	42.3	49.4	57.1	65.5	74.1	15.5%
Middle East & Africa	21.3	24.5	27.9	31.6	35.4	39.3	13.1%
Latin America	10.0	11.4	13.0	14.7	16.5	18.3	12.9%
Total	174.4	198.1	223.7	250.4	277.3	303.7	11.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

9.4.6 MANAGED SERVICES

9.4.6.1 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 as well as 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 47 **MANAGED SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)**

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	91.9	105.9	123.2	142.3	163.0	185.5	15.1%
Europe	66.5	78.5	93.7	111.1	130.7	152.7	18.1%
Asia Pacific	39.5	42.9	52.6	64.3	77.9	94.0	19.0%
Middle East & Africa	25.7	30.7	37.1	44.4	52.8	62.4	19.4%
Latin America	9.3	11.1	13.4	16.1	19.1	22.5	19.3%
Total	232.9	269.0	320.0	378.2	443.5	517.1	17.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 48 **MANAGED SERVICES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)**

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	210.1	236.8	265.1	293.9	321.9	347.9	10.6%
Europe	177.4	205.3	236.1	269.2	303.6	338.1	13.8%
Asia Pacific	112.9	135.1	160.7	189.6	221.5	255.7	17.8%
Middle East & Africa	73.3	85.7	99.6	114.8	130.8	147.9	15.1%
Latin America	26.4	30.9	35.9	41.3	47.1	53.2	15.0%
Total	600.2	693.8	797.5	908.8	1,024.9	1,142.8	13.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

10 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE

KEY FINDINGS

- By solution type, the network traffic analyzers segment is estimated to account for the largest market size of USD 846.1 million in 2025. This segment is projected to reach USD 1,530 million by 2030, at a CAGR of 12.6% during the forecast period.
- The botnet detection & mitigation segment is projected to register the highest CAGR of 13.2% during the forecast period, reaching USD 1,023.8 million by 2030.
- The demand for DDoS protection and mitigation security 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.

10.1 INTRODUCTION

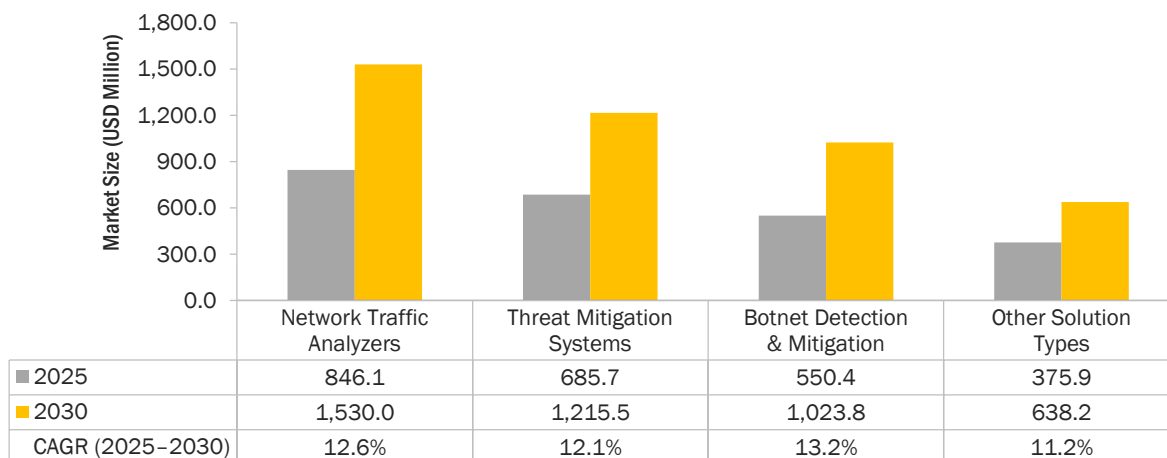
The cybersecurity landscape faces significant threats from increasingly sophisticated DDoS attacks. Cybercriminals utilize advanced hacking tools to infiltrate organizations' network infrastructures, obstructing legitimate traffic and disrupting vital services, often resulting in financial losses that 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 security 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 SECURITY 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.
- Increased awareness among businesses about the potential financial and reputational damage from DDoS attacks is driving investment in comprehensive protection solutions.

FIGURE 28 BOTNET DETECTION & MITIGATION SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD



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

TABLE 49 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	351.1	400.7	471.2	550.8	638.9	736.9	16.0%
Threat Mitigation Systems	291.5	331.3	388.0	451.8	522.0	599.6	15.5%
Botnet Detection & Management	220.5	253.1	299.4	352.0	410.8	476.5	16.7%
Other Solution Types	168.1	189.3	219.9	253.9	291.0	331.5	14.5%
Total	1,031.2	1,174.3	1,378.6	1,608.5	1,862.6	2,144.5	15.8%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 50 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	846.1	967.9	1,101.0	1,241.7	1,386.1	1,530.0	12.6%
Threat Mitigation System	685.7	781.3	885.2	994.4	1,105.6	1,215.5	12.1%
Botnet Detection & Management	550.4	633.3	724.4	821.7	922.4	1,023.8	13.2%
Other Solution Types	375.9	424.7	477.1	531.3	585.6	638.2	11.2%
Total	2,458.2	2,807.3	3,187.6	3,589.1	3,999.8	4,407.6	12.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 security 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 51 NETWORK TRAFFIC ANALYZERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	152.1	173.3	199.5	227.9	258.3	290.9	13.9%
Europe	90.2	105.5	124.7	146.5	170.7	197.6	17.0%
Asia Pacific	62.5	67.2	81.6	98.6	118.4	141.4	17.7%
Middle East & Africa	32.9	38.9	46.6	55.3	65.2	76.2	18.3%
Latin America	13.4	15.8	18.9	22.4	26.4	30.8	18.1%
Total	351.1	400.7	471.2	550.8	638.9	736.9	16.0%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 52 NETWORK TRAFFIC ANALYZERS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	326.1	363.8	403.1	442.3	479.6	513.2	9.5%
Europe	227.5	260.8	297.2	335.7	375.2	414.2	12.7%
Asia Pacific	168.1	199.1	234.5	274.0	317.0	362.4	16.6%
Middle East & Africa	88.7	102.8	118.5	135.3	152.9	171.4	14.1%
Latin America	35.8	41.5	47.7	54.5	61.5	68.8	13.9%
Total	846.1	967.9	1,101.0	1,241.7	1,386.1	1,530.0	12.6%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 SECURITY SOLUTIONS

Threat mitigation systems are essential software solutions in the DDoS protection and mitigation security 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.

Additionally, 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 53 THREAT MITIGATION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	122.0	138.4	158.6	180.4	203.5	228.1	13.3%
Europe	75.5	87.9	103.4	121.0	140.3	161.7	16.5%
Asia Pacific	52.4	56.0	67.8	81.5	97.4	115.8	17.2%
Middle East & Africa	29.9	35.2	41.9	49.5	58.1	67.6	17.7%
Latin America	11.7	13.8	16.4	19.3	22.6	26.3	17.6%
Total	291.5	331.3	388.0	451.8	522.0	599.6	15.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 54 THREAT MITIGATION SYSTEMS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	254.5	282.7	311.8	340.5	367.5	391.5	9.0%
Europe	185.3	211.5	240.0	269.9	300.4	330.1	12.2%
Asia Pacific	137.1	161.6	189.5	220.4	253.8	288.8	16.1%
Middle East & Africa	78.4	90.4	103.7	117.8	132.6	147.9	13.6%
Latin America	30.5	35.1	40.2	45.7	51.3	57.2	13.4%
Total	685.7	781.3	885.2	994.4	1,105.6	1,215.5	12.1%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 security 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 55 BOTNET DETECTION & MANAGEMENT: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	95.0	109.0	126.1	144.9	165.2	187.1	14.5%
Europe	55.1	64.8	77.0	91.0	106.7	124.1	17.7%
Asia Pacific	39.9	43.1	52.6	64.0	77.2	92.8	18.4%
Middle East & Africa	21.5	25.6	30.8	36.8	43.6	51.3	19.0%
Latin America	8.9	10.6	12.8	15.2	18.0	21.2	18.8%
Total	220.5	253.1	299.4	352.0	410.8	476.5	16.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 56 BOTNET DETECTION & MANAGEMENT: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	210.9	236.6	263.6	290.8	317.0	341.0	10.1%
Europe	143.7	165.7	189.9	215.7	242.4	269.1	13.4%
Asia Pacific	110.9	132.1	156.5	183.8	213.8	245.7	17.2%
Middle East & Africa	60.1	70.0	81.1	93.1	105.8	119.2	14.7%
Latin America	24.8	28.8	33.4	38.3	43.4	48.9	14.5%
Total	550.4	633.3	724.4	821.7	922.4	1,023.8	13.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

10.5 OTHER SOLUTION TYPES

In DDoS protection and mitigation security, solution types such as Security Information and Event Management (SIEM), anomaly detection, orchestration, and automation are vital for enhancing cybersecurity measures. SIEM systems are increasingly employed to identify early indicators of DDoS attacks by collecting and analyzing security events in real-time. They offer comprehensive visibility into network activities, enabling organizations to detect anomalies that might signal an impending attack. By integrating with other security tools, SIEMs can automate responses to mitigate threats before they escalate, thereby ensuring service continuity.

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 57 OTHER SOLUTION TYPES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	72.9	82.1	93.3	105.3	117.8	131.0	12.4%
Europe	37.7	43.5	50.8	58.8	67.5	77.1	15.3%
Asia Pacific	32.4	34.4	41.3	49.3	58.4	68.9	16.3%
Middle East & Africa	17.3	20.2	23.8	28.0	32.5	37.6	16.8%
Latin America	7.8	9.1	10.7	12.6	14.6	16.9	16.8%
Total	168.1	189.3	219.9	253.9	291.0	331.5	14.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 58 OTHER SOLUTION TYPES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	145.0	159.6	174.6	189.0	202.2	213.5	8.1%
Europe	87.5	98.8	111.0	123.5	136.0	147.8	11.1%
Asia Pacific	80.9	94.6	110.1	127.0	145.0	163.6	15.1%
Middle East & Africa	43.2	49.4	56.2	63.4	70.7	78.2	12.6%
Latin America	19.4	22.2	25.3	28.5	31.8	35.1	12.6%
Total	375.9	424.7	477.1	531.3	585.6	638.2	11.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

11 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA

KEY FINDINGS

- By application area, the application security segment is estimated to account for the largest market size of USD 2,350.6 million in 2025. This segment is projected to reach USD 4,364.5 million by 2030, registering the highest CAGR of 13.2% during the forecast period.
- The cloud security segment is projected to register the second-highest CAGR of 12.6% during the forecast period and reach USD 1,587.3 million by 2030.
- The demand for DDoS protection and mitigation security services 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.

11.1 INTRODUCTION

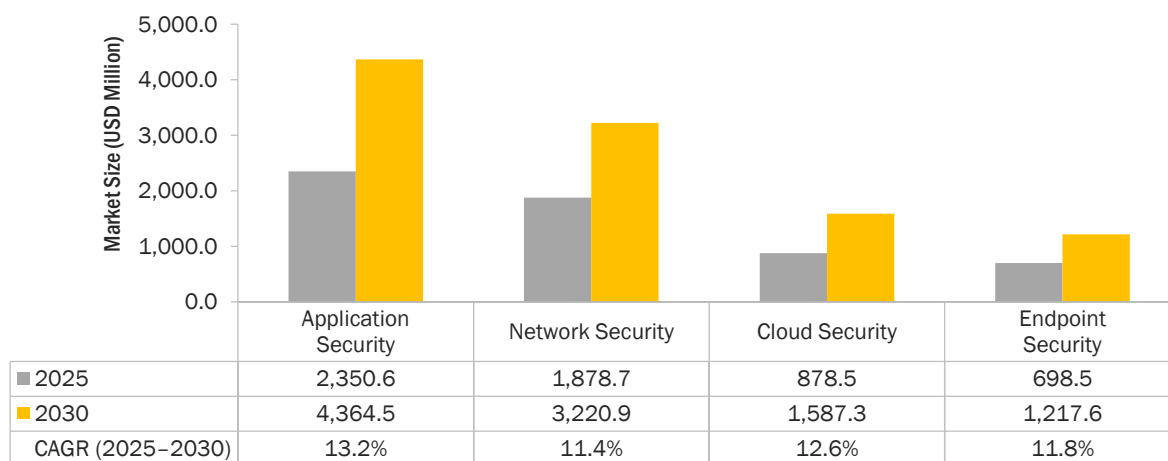
Cybercriminals use innovative hacking tools to attack organizations' network infrastructure and block all legitimate traffic. DDoS attacks disrupt the functioning of organizations and can cause losses amounting to millions of dollars. Some of the motives behind DDoS attacks include criminals demonstrating their DDoS attack capabilities, extortion attempts, vandalism, social network-related crimes, political disputes, data exfiltration, and competitive rivalry between business organizations, as well as interpersonal rivalries and financial market manipulation.

The extensive adoption of DDoS protection solutions and services among organizations across various verticals, such as retail, BFSI, government and defense, healthcare, and manufacturing, can be attributed to increasing awareness about mitigating devastating volumetric attacks. To ensure that each node of an organization's infrastructure is protected, the DDoS protection and mitigation security market has been classified into application areas, including network security, application security, database security, and endpoint security. Advanced DDoS protection and mitigation security services are necessary to safeguard various application areas within organizations.

11.1.1 APPLICATION AREA: DDoS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS

- Disruptions in network performance and internet services are expected to fuel the adoption of DDoS protection and mitigation solutions.
- The increasing sophistication of botnet armies in carrying out DDoS attacks has led to the growth of the market.
- Illegitimate traffic and target vulnerabilities to endpoints will fuel the adoption of DDoS protection and mitigation solutions.
- Increasing trends of BYOD and CYOD are expected to trigger DDoS attacks, resulting in increased demand for DDoS protection and mitigation solutions and services.
- Organizations moving toward cloud-based solutions for achieving cost savings, agility, and flexibility are making their critical data more vulnerable to cyberattacks. The application security segment is witnessing the highest demand among all DDoS protection and mitigation security market.

FIGURE 29 APPLICATION SECURITY SEGMENT TO WITNESS HIGHEST CAGR DURING FORECAST PERIOD



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

TABLE 59 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	830.3	937.1	1,090.7	1,261.8	1,448.6	1,653.4	14.8%
Application Security	944.0	1,082.8	1,280.6	1,505.2	1,755.7	2,036.0	16.6%
Database Security	302.8	343.0	400.4	464.7	535.2	612.7	15.1%
Endpoint Security	364.8	416.4	489.6	572.1	663.6	765.2	16.0%
Total	2,442.0	2,779.3	3,261.4	3,803.8	4,403.0	5,067.3	15.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 60 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	1,878.7	2,126.5	2,393.3	2,670.6	2,949.5	3,220.9	11.4%
Application Security	2,350.6	2,703.4	3,091.4	3,505.1	3,933.4	4,364.5	13.2%
Database Security	698.5	793.2	895.6	1,002.8	1,111.2	1,217.6	11.8%
Endpoint Security	878.5	1,004.8	1,142.7	1,288.6	1,438.2	1,587.3	12.6%
Total	5,806.2	6,628.0	7,523.0	8,467.1	9,432.3	10,390.3	12.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

11.2 NETWORK SECURITY

11.2.1 INCREASING NEED TO ENHANCE NETWORK PERFORMANCE AND ELIMINATE DISRUPTIONS

DDoS attacks originating from multiple sources deny users access to a network service. Network attacks are primarily focused on layers 3 and 4 of the Open Systems Interconnection (OSI) model. Layer 3 and Layer 4 DDoS attacks are volumetric attacks that eventually degrade a legitimate user's access. DDoS attacks disturb the normal functioning of the network by flooding it and causing congestion.

The botnets flood the network with numerous illegitimate requests. Botnets can utilize packets from TCP, UDP, and the Internet Control Message Protocol (ICMP). Some of the major attacks on the network layer include SYN floods, UDP floods, Smurf attacks, BGP hijacking, ICMP floods, and DNS amplification attacks. These DDoS attacks slow down the network performance and disrupt internet services. Smurf attacks broadcast packets to all computers in the network, thereby consuming more network bandwidth. UDP floods are larger in bandwidth and are usually sent in the form of error messages. ICMP floods overload the target networks by sending error messages. When the target network receives a SYN flood, the user is unable to connect to the server. DNS amplification attacks cause congestion on the target system by utilizing DNS response traffic, thereby disrupting the target system. BGP (Border Gateway Protocol) hijacking refers to hacking a group of IP addresses by corrupting the internet services using BGP. Advanced solutions and services protect organizations from volumetric attacks, resulting in no bandwidth

consumption that arises due to illegitimate traffic. According to A10 Networks' mobile operator survey report, 63% of the respondents believe that an advanced DDoS protection and mitigation solution is required to protect 5G networks.

TABLE 61 NETWORK SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	345.4	389.3	443.1	500.7	561.1	624.7	12.6%
Europe	210.5	243.5	284.7	330.8	381.1	436.1	15.7%
Asia Pacific	155.0	164.6	197.8	236.5	280.7	331.5	16.4%
Middle East & Africa	83.4	97.5	115.3	135.4	157.7	182.4	17.0%
Latin America	36.1	42.2	49.8	58.5	68.0	78.6	16.8%
Total	830.3	937.1	1,090.7	1,261.8	1,448.6	1,653.4	14.8%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 62 NETWORK SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	692.2	763.5	836.2	906.9	971.9	1,027.9	8.2%
Europe	496.5	562.8	634.1	708.1	782.4	853.7	11.4%
Asia Pacific	389.7	456.4	531.5	614.0	702.1	793.4	15.3%
Middle East & Africa	209.9	240.4	273.7	309.0	345.0	382.2	12.7%
Latin America	90.4	103.4	117.7	132.7	148.1	163.8	12.6%
Total	1,878.7	2,126.5	2,393.3	2,670.6	2,949.5	3,220.9	11.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

11.3 APPLICATION SECURITY

11.3.1 RISING NEED TO MITIGATE DDOS ATTACKS AND MAINTAIN PROTECTION

DDoS attacks are becoming increasingly sophisticated and complex on a daily basis. Application layer (layer 7) attacks are launched by hackers or cyberterrorists using highly automated tools. Such DDoS attacks require proactive monitoring and advanced alerting to mitigate risks at an early phase. Advanced DDoS protection solutions can distinguish human traffic from bot traffic. DDoS solution providers are continuously adopting newer technologies to combat the ever-changing attacks, signatures, and patterns. The application layer deals with protocols, such as Simple Mail Transfer Protocol (SMTP), HTTP, and HTTPS, which are responsible for managing web browsers and emails, as well as handling requests for various applications.

Adversaries target Layer 7 of applications with DDoS attacks, attempting to flood them with illegitimate requests and disrupt the application. An HTTP flood attack on the application layer can exploit the same page request repeatedly, affecting a large pool of IP addresses and disrupting the network's functioning and resources. WordPress eXtensible Markup Language Remote Procedure Call (XMLRPC) floods utilize WordPress pingbacks to generate flood requests and disturbances. The growing adoption of application-layer DDoS protection solutions is attributed to the rise in Layer 7 attacks, according to the Global DDoS Attacks and Cyber Security Insights Report.

TABLE 63 APPLICATION SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	393.8	451.0	521.7	599.1	682.4	772.2	14.4%
Europe	240.6	282.8	336.0	396.6	464.3	539.8	17.5%
Asia Pacific	173.3	187.1	228.4	277.4	334.5	401.4	18.3%
Middle East & Africa	95.6	113.7	136.6	163.0	192.9	226.8	18.8%
Latin America	40.7	48.3	57.9	69.1	81.6	95.8	18.7%
Total	944.0	1,082.8	1,280.6	1,505.2	1,755.7	2,036.0	16.6%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 64 APPLICATION SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	869.6	974.8	1,085.3	1,196.4	1,303.2	1,401.0	10.0%
Europe	624.4	719.2	823.3	934.3	1,049.0	1,163.1	13.2%
Asia Pacific	479.5	570.5	675.1	792.3	920.7	1,057.2	17.1%
Middle East & Africa	265.1	308.7	357.2	409.7	465.0	523.5	14.6%
Latin America	111.9	130.1	150.4	172.4	195.4	219.6	14.4%
Total	2,350.6	2,703.4	3,091.4	3,505.1	3,933.4	4,364.5	13.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

11.4 CLOUD SECURITY

11.4.1 GREATER NEED FOR CLOUD-BASED APPLICATIONS SECURITY TO DRIVE MARKET

Cloud security has become a critical application area due to the rapid adoption of cloud services and the increased frequency of large-scale, complex DDoS attacks. As organizations migrate workloads to the cloud, they face heightened exposure to DDoS threats, which can severely disrupt cloud-based applications, services, and infrastructure. Attackers are using more sophisticated, multi-vector DDoS attacks that require flexible, scalable cloud security solutions capable of defending against both volumetric and application-layer attacks.

This demand for cloud security in DDoS protection is expected to continue growing, driven by the expansion of cloud adoption and the evolution of cyber threats.

TABLE 65 CLOUD SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	160.4	182.8	210.3	240.3	272.3	306.5	13.8%
Europe	87.4	102.2	120.8	142.0	165.4	191.5	17.0%
Asia Pacific	64.5	69.3	84.2	101.7	122.1	145.8	17.7%
Middle East & Africa	37.0	43.7	52.3	62.1	73.2	85.6	18.3%
Latin America	15.6	18.4	22.0	26.1	30.7	35.8	18.1%
Total	364.8	416.4	489.6	572.1	663.6	765.2	16.0%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 66 CLOUD SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	343.5	383.2	424.5	465.7	504.9	540.2	9.5%
Europe	220.5	252.8	288.1	325.4	363.8	401.6	12.7%
Asia Pacific	173.3	205.3	241.8	282.5	326.8	373.5	16.6%
Middle East & Africa	99.6	115.4	132.9	151.7	171.4	192.1	14.0%
Latin America	41.6	48.2	55.5	63.3	71.4	79.9	13.9%
Total	878.5	1,004.8	1,142.7	1,288.6	1,438.2	1,587.3	12.6%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

11.5 ENDPOINT SECURITY

11.5.1 INCREASING MOBILE DEVICES AND DIGITAL TRANSFORMATIONS TO DRIVE MARKET

Endpoint DDoS protection is provided for network devices, such as servers, desktops, laptops, smartphones, tablets, barcode readers, and Point of Sale (PoS) machines, which are connected to a client-server. Network devices are often connected remotely, creating an entry point for potential cyber threats. DDoS attacks on endpoints aim to exhaust CPUs' resources and memory, causing system breakdown. DDoS attacks can also flood the endpoint resources with illegitimate traffic and target vulnerabilities in the application stack, which can block legitimate traffic from completing its cycle.

The rapid growth in the number of mobile devices, IoT, and digital transformations across the globe is one of the driving factors for the growth of this market. Due to the increasing number of mobile devices, networks are becoming more vulnerable to cyberattacks, and hence, it has become essential to assess organizations' security posture and incorporate security systems to mitigate risk. Advanced DDoS protection and mitigation solutions and services, combined with threat detection and behavioral analytics, are required to safeguard endpoints from advanced threats.

TABLE 67 ENDPOINT SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	128.5	145.4	166.0	188.3	211.8	236.7	13.0%
Europe	76.9	89.3	104.8	122.2	141.2	162.2	16.1%
Asia Pacific	55.1	58.7	70.8	84.9	101.1	119.8	16.8%
Middle East & Africa	30.6	36.0	42.7	50.3	58.8	68.2	17.4%
Latin America	11.7	13.7	16.2	19.1	22.2	25.8	17.2%
Total	302.8	343.0	400.4	464.7	535.2	612.7	15.1%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 68 ENDPOINT SECURITY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	263.3	291.5	320.5	349.0	375.5	398.8	8.7%
Europe	185.3	210.9	238.5	267.3	296.5	324.8	11.9%
Asia Pacific	141.4	166.1	194.2	225.1	258.3	293.0	15.7%
Middle East & Africa	78.8	90.6	103.6	117.3	131.6	146.3	13.2%
Latin America	29.7	34.1	38.9	44.0	49.3	54.7	13.0%
Total	698.5	793.2	895.6	1,002.8	1,111.2	1,217.6	11.8%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

12 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE

KEY FINDINGS

- By deployment mode, the cloud segment is projected to register a CAGR of 12.7% during the forecast period. This segment is projected to reach USD 3,375.4 million by 2030.
- Cloud DDoS protection and mitigation security 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 2,430.9 million in 2025 to USD 4,241.8 million by 2030, at a CAGR of 11.8% 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.

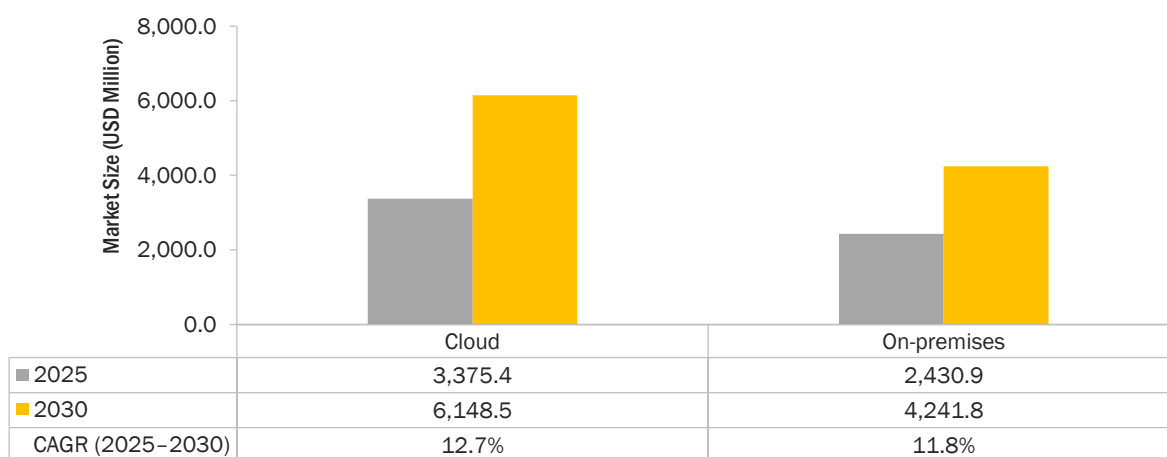
12.1 INTRODUCTION

DDoS protection and mitigation security 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 SECURITY 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 30 CLOUD SEGMENT TO RECORD FASTER GROWTH DURING FORECAST PERIOD



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

TABLE 69 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	1,052.4	1,192.4	1,392.4	1,616.2	1,861.7	2,132.0	15.2%
Cloud	1,389.6	1,586.9	1,868.9	2,187.6	2,541.3	2,935.3	16.1%
Total	2,442.0	2,779.3	3,261.4	3,803.8	4,403.0	5,067.3	15.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 70 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	2,430.9	2,761.2	3,118.4	3,492.1	3,870.5	4,241.8	11.8%
Cloud	3,375.4	3,866.8	4,404.6	4,975.0	5,561.8	6,148.5	12.7%
Total	5,806.2	6,628.0	7,523.0	8,467.1	9,432.3	10,390.3	12.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

12.2 ON-PREMISES

12.2.1 ON-PREMISES SERVICES PROVIDE FULL CONTROL OF DEPLOYED SOLUTIONS IT'S STAFF

On-premises deployment is the traditional approach to implementing DDoS protection solutions and services across organizations. On-premises 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-premises 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 71 ON-PREMISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	444.1	502.5	574.0	651.1	732.5	818.7	13.0%
Europe	272.0	315.8	370.7	432.3	500.0	574.4	16.1%
Asia Pacific	190.3	202.9	244.7	293.5	349.6	414.4	16.8%
Middle East & Africa	101.6	119.3	141.5	166.8	195.0	226.3	17.4%
Latin America	44.3	52.0	61.6	72.5	84.7	98.2	17.2%
Total	1,052.4	1,192.4	1,392.4	1,616.2	1,861.7	2,132.0	15.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 72 ON-PREMISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	910.8	1,008.6	1,109.3	1,208.0	1,300.1	1,380.8	8.7%
Europe	656.5	747.1	845.2	947.7	1,051.5	1,152.2	11.9%
Asia Pacific	489.0	574.7	671.8	778.9	894.2	1,014.4	15.7%
Middle East & Africa	261.3	300.5	343.5	389.2	436.3	485.2	13.2%
Latin America	113.3	130.1	148.6	168.2	188.5	209.3	13.1%
Total	2,430.9	2,761.2	3,118.4	3,492.1	3,870.5	4,241.8	11.8%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 security market, especially among SMEs, as it is cost-effective. Cloud deployment helps SMEs avoid costs related to hardware, software, storage, and technical staff.

SMEs, in particular, 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 security 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 the 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 73 CLOUD: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	584.0	666.0	767.1	877.3	995.0	1,121.4	13.9%
Europe	343.4	401.9	475.6	559.2	652.1	755.2	17.1%
Asia Pacific	257.5	276.8	336.5	407.0	488.7	584.1	17.8%
Middle East & Africa	145.0	171.6	205.3	244.0	287.6	336.6	18.3%
Latin America	59.7	70.6	84.4	100.1	117.9	137.8	18.2%
Total	1,389.6	1,586.9	1,868.9	2,187.6	2,541.3	2,935.3	16.1%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 74 CLOUD: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	1,257.8	1,404.3	1,557.3	1,709.9	1,855.4	1,987.0	9.6%
Europe	870.2	998.5	1,138.8	1,287.5	1,440.3	1,591.1	12.8%
Asia Pacific	695.0	823.7	970.8	1,134.9	1,313.7	1,502.8	16.7%
Middle East & Africa	392.0	454.6	523.9	598.6	676.7	758.9	14.1%
Latin America	160.3	185.7	213.9	244.1	275.7	308.7	14.0%
Total	3,375.4	3,866.8	4,404.6	4,975.0	5,561.8	6,148.5	12.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

13 DDOS PROTECTION AND MITIGATION SECURITY 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 2025 to USD 4,161.7 million by 2030.
- With the increasing adoption of BYOD and cloud-based applications for business operations, SMEs are adopting DDoS protection and mitigation security solutions to protect their critical data from theft.
- The large enterprises segment is projected to grow from USD 3,586.3 million in 2025 to USD 6,228.6 million by 2030, 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 security solutions for data security.

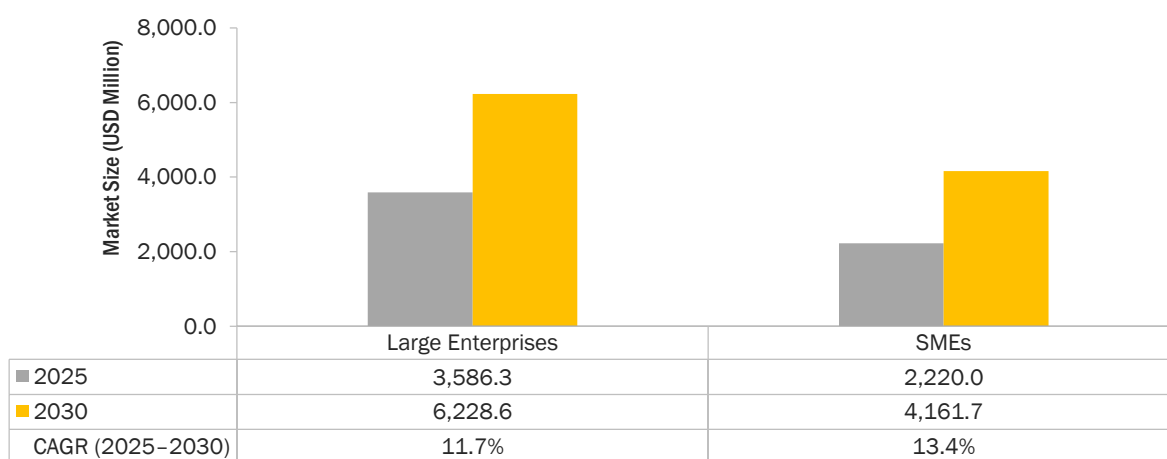
13.1 INTRODUCTION

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 security 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 security solutions among SMEs and large enterprises is expected to drive the growth of the DDoS protection and mitigation security market.

13.1.1 ORGANIZATION SIZE: DDOS PROTECTION AND MITIGATION SECURITY MARKET DRIVERS

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

FIGURE 31 SMEs SEGMENT TO RECORD HIGHER CAGR DURING FORECAST PERIOD



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

TABLE 75 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	879.3	1,011.8	1,199.3	1,412.6	1,651.3	1,918.9	16.9%
Large Enterprises	1,562.7	1,767.5	2,062.1	2,391.2	2,751.7	3,148.4	15.0%
Total	2,442.0	2,779.3	3,261.4	3,803.8	4,403.0	5,067.3	15.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 76 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	2,220.0	2,558.4	2,931.3	3,330.0	3,743.9	4,161.7	13.4%
Large Enterprises	3,586.3	4,069.6	4,591.7	5,137.1	5,688.4	6,228.6	11.7%
Total	5,806.2	6,628.0	7,523.0	8,467.1	9,432.3	10,390.3	12.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 77 LARGE ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	637.4	719.8	820.8	929.2	1,043.4	1,164.1	12.8%
Europe	400.0	463.7	543.3	632.6	730.4	837.7	15.9%
Asia Pacific	293.8	312.7	376.6	451.1	536.5	635.1	16.7%
Middle East & Africa	162.0	189.9	225.1	265.0	309.3	358.6	17.2%
Latin America	69.5	81.4	96.3	113.3	132.1	152.9	17.1%
Total	1,562.7	1,767.5	2,062.1	2,391.2	2,751.7	3,148.4	15.0%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 78 LARGE ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	1,292.5	1,428.5	1,567.9	1,704.1	1,830.2	1,939.9	8.5%
Europe	955.7	1,085.8	1,226.1	1,372.4	1,520.0	1,662.4	11.7%
Asia Pacific	748.2	878.2	1,025.0	1,186.6	1,360.0	1,540.5	15.5%
Middle East & Africa	413.6	474.9	542.1	613.4	686.8	762.6	13.0%
Latin America	176.2	202.2	230.5	260.6	291.5	323.2	12.9%
Total	3,586.3	4,069.6	4,591.7	5,137.1	5,688.4	6,228.6	11.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 hacktivists. 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.

Nowadays, 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 79 SMALL & MEDIUM-SIZED ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	390.7	448.7	520.3	599.1	684.1	776.1	14.7%
Europe	215.4	254.1	303.0	358.9	421.7	492.0	18.0%
Asia Pacific	154.1	166.9	204.6	249.4	301.8	363.5	18.7%
Middle East & Africa	84.6	100.9	121.7	145.9	173.2	204.3	19.3%
Latin America	34.5	41.2	49.6	59.4	70.5	83.1	19.2%
Total	879.3	1,011.8	1,199.3	1,412.6	1,651.3	1,918.9	16.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 80 SMALL & MEDIUM-SIZED ENTERPRISES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	876.1	984.5	1,098.6	1,213.9	1,325.3	1,428.0	10.3%
Europe	571.0	659.9	757.9	862.8	971.8	1,080.8	13.6%
Asia Pacific	435.7	520.2	617.6	727.3	847.8	976.7	17.5%
Middle East & Africa	239.8	280.1	325.3	374.4	426.3	481.4	15.0%
Latin America	97.4	113.7	131.9	151.7	172.7	194.8	14.9%
Total	2,220.0	2,558.4	2,931.3	3,330.0	3,743.9	4,161.7	13.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

14 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL

KEY FINDINGS

- By vertical, the BFSI segment is projected to register the highest CAGR of 14.3% during the forecast period, reaching a market size of USD 2,477.5 million by 2030.
- The telecom segment is projected to register the second-highest CAGR of 13.8% during the forecast period. This segment is projected to grow from USD 450.7 million in 2025 to USD 859.6 million by 2030.
- 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. Hence, the healthcare segment is expected to hold the second-largest market share in the DDoS protection and mitigation security market by 2025.
- The healthcare segment is projected to register a CAGR of 13.1% during the forecast period.
- 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 security 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.

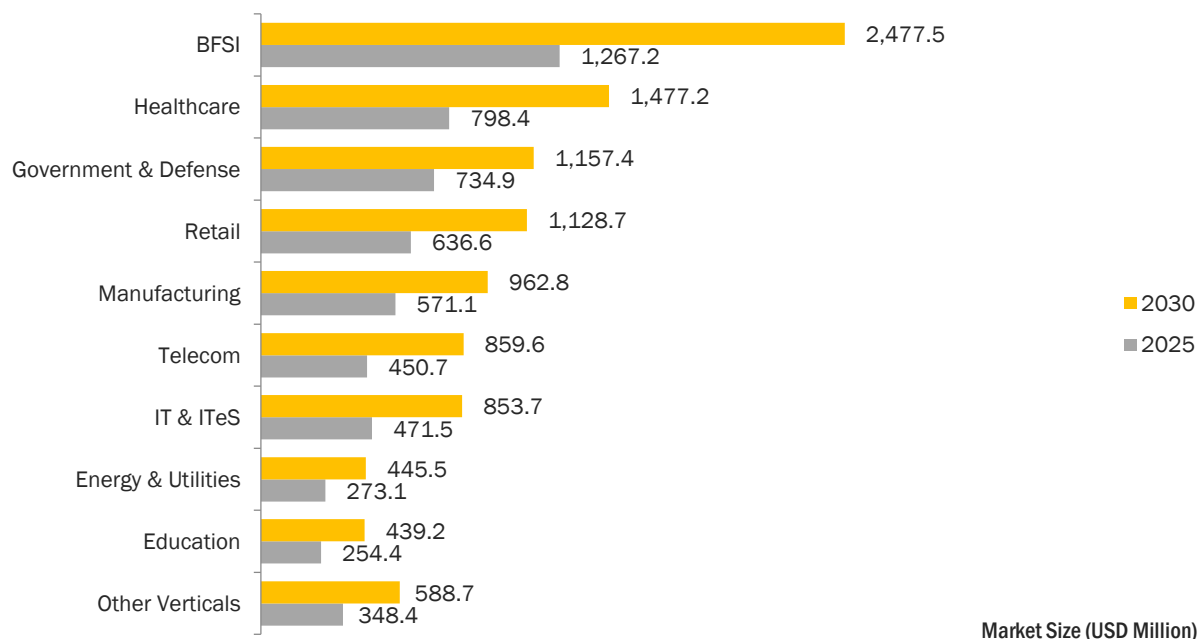
Moreover, the shift toward cloud technology and the widespread use of mobile devices in enterprises have made organizational data more vulnerable to cyberattacks. As cyberattacks continue to rise, enterprises are increasingly adopting next-generation DDoS protection and mitigation solutions. These services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

According to Cloudflare's DDoS Attack Trends for Q4 2021 report, the manufacturing, business services, and gaming/gambling industries were the most targeted by application-layer DDoS attacks, with attacks on manufacturing companies increasing by 641% quarter-on-quarter during Q4.

14.1.1 VERTICAL: DDOS PROTECTION AND MITIGATION SECURITY 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 32 BFSI SEGMENT TO RECORD HIGHEST GROWTH RATE DURING FORECAST PERIOD



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

TABLE 81 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	473.2	550.3	659.0	784.0	925.3	1,085.4	18.1%
Government & Defense	353.3	393.9	452.3	516.0	584.0	656.7	13.2%
IT & ITeS	195.6	223.1	262.4	306.7	355.9	410.5	16.0%
Telecom	174.6	201.5	239.8	283.6	332.7	388.1	17.3%
Manufacturing	257.2	289.3	335.7	387.2	443.2	504.2	14.4%
Energy & Utilities	127.4	142.4	164.3	188.5	214.4	242.6	13.7%
Healthcare	322.0	369.1	436.2	512.3	597.2	692.0	16.5%
Retail	271.3	307.8	360.4	419.5	484.6	556.7	15.5%
Education	111.2	125.9	146.8	170.1	195.6	223.6	15.0%
Other Verticals	156.2	176.0	204.4	235.9	270.1	307.5	14.5%
Total	2,442.0	2,779.3	3,261.4	3,803.8	4,403.0	5,067.3	15.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 82 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	1,267.2	1,473.4	1,702.8	1,950.7	2,211.1	2,477.5	14.3%
Government & Defense	734.9	818.8	906.5	994.6	1,079.3	1,157.4	9.5%
IT & ITeS	471.5	539.5	613.8	692.5	773.2	853.7	12.6%
Telecom	450.7	521.2	599.3	683.2	770.7	859.6	13.8%
Manufacturing	571.1	644.4	722.8	803.9	884.8	962.8	11.0%
Energy & Utilities	273.1	306.2	341.3	377.0	412.2	445.5	10.3%
Healthcare	798.4	917.6	1,048.5	1,188.0	1,332.2	1,477.2	13.1%
Retail	636.6	725.3	821.7	923.2	1,026.5	1,128.7	12.1%
Education	254.4	288.4	325.0	363.2	401.6	439.2	11.5%
Other Verticals	348.4	393.2	441.3	490.9	540.6	588.7	11.1%
Total	5,806.2	6,628.0	7,523.0	8,467.1	9,432.3	10,390.3	12.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

14.2 GOVERNMENT AND DEFENSE

14.2.1 INCREASING NEED FOR DDOS PROTECTION AND MITIGATION SECURITY 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 83 GOVERNMENT AND DEFENSE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	150.1	167.1	187.8	209.4	231.5	254.2	11.1%
Europe	89.2	101.9	117.6	134.8	153.2	172.9	14.1%
Asia Pacific	63.6	66.7	79.0	93.2	109.0	126.8	14.8%
Middle East & Africa	36.0	41.6	48.6	56.3	64.7	73.7	15.4%
Latin America	14.4	16.6	19.3	22.4	25.6	29.1	15.1%
Total	353.3	393.9	452.3	516.0	584.0	656.7	13.2%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 84 GOVERNMENT AND DEFENSE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	277.6	301.6	325.3	347.2	366.0	380.6	6.5%
Europe	193.9	216.5	240.1	263.8	286.6	307.2	9.6%
Asia Pacific	146.8	169.2	193.8	220.1	247.3	274.4	13.3%
Middle East & Africa	83.6	94.4	105.8	117.5	129.1	140.6	10.9%
Latin America	33.0	37.1	41.5	46.0	50.4	54.6	10.6%
Total	734.9	818.8	906.5	994.6	1,079.3	1,157.4	9.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

14.3 BANKING, FINANCIAL SERVICES, AND INSURANCE

14.3.1 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 85 BFSI: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	207.7	240.9	282.2	328.0	378.0	432.7	15.8%
Europe	116.9	139.4	167.9	200.9	238.3	280.6	19.1%
Asia Pacific	82.9	90.7	112.4	138.4	169.2	205.7	19.9%
Middle East & Africa	46.1	55.6	67.8	82.0	98.3	117.1	20.5%
Latin America	19.6	23.6	28.7	34.7	41.6	49.4	20.3%
Total	473.2	550.3	659.0	784.0	925.3	1,085.4	18.1%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 86 BFSI: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	492.7	558.4	628.2	699.7	769.9	835.9	11.2%
Europe	328.6	383.0	443.6	509.2	578.1	648.0	14.5%
Asia Pacific	248.9	299.8	359.1	426.4	501.2	582.0	18.5%
Middle East & Africa	138.6	163.4	191.3	222.0	254.9	290.1	15.9%
Latin America	58.5	68.8	80.5	93.3	107.0	121.6	15.8%
Total	1,267.2	1,473.4	1,702.8	1,950.7	2,211.1	2,477.5	14.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 87 MANUFACTURING: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	104.9	117.8	133.6	150.4	167.9	186.3	12.2%
Europe	67.7	78.1	91.1	105.5	121.2	138.3	15.4%
Asia Pacific	49.3	52.2	62.5	74.5	88.2	103.8	16.1%
Middle East & Africa	24.4	28.4	33.5	39.2	45.5	52.4	16.5%
Latin America	11.0	12.8	15.0	17.6	20.4	23.5	16.4%
Total	257.2	289.3	335.7	387.2	443.2	504.2	14.4%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 88 MANUFACTURING: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	205.6	225.9	246.4	266.1	284.0	299.1	7.8%
Europe	157.0	177.4	199.2	221.7	244.2	265.5	11.1%
Asia Pacific	121.7	142.1	164.9	189.9	216.4	243.7	14.9%
Middle East & Africa	60.0	68.4	77.5	87.1	96.8	106.7	12.2%
Latin America	26.9	30.7	34.8	39.1	43.4	47.8	12.2%
Total	571.1	644.4	722.8	803.9	884.8	962.8	11.0%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

14.5 ENERGY AND 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 89 ENERGY AND UTILITIES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	51.4	57.4	64.6	72.3	80.2	88.3	11.4%
Europe	30.2	34.5	39.9	45.9	52.3	59.2	14.4%
Asia Pacific	25.5	26.9	32.1	38.0	44.8	52.4	15.5%
Middle East & Africa	14.8	17.2	20.2	23.5	27.2	31.2	16.1%
Latin America	5.5	6.4	7.5	8.7	10.0	11.4	15.7%
Total	127.4	142.4	164.3	188.5	214.4	242.6	13.7%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 90 ENERGY AND UTILITIES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	96.7	105.4	114.1	122.3	129.4	135.0	6.9%
Europe	66.6	74.5	82.9	91.4	99.7	107.3	10.0%
Asia Pacific	61.1	70.9	81.8	93.6	106.0	118.6	14.2%
Middle East & Africa	35.7	40.5	45.8	51.3	56.8	62.3	11.8%
Latin America	13.0	14.8	16.6	18.5	20.4	22.3	11.4%
Total	273.1	306.2	341.3	377.0	412.2	445.5	10.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 security 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 91 IT AND ITES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	83.3	94.9	109.2	124.7	141.3	159.1	13.8%
Europe	49.2	57.6	68.0	79.9	93.1	107.7	16.9%
Asia Pacific	36.3	38.9	47.3	57.2	68.6	81.9	17.7%
Middle East & Africa	18.7	22.2	26.5	31.5	37.1	43.3	18.3%
Latin America	8.1	9.5	11.4	13.5	15.9	18.5	18.1%
Total	195.6	223.1	262.4	306.7	355.9	410.5	16.0%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 92 IT AND ITES: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	178.3	198.8	220.3	241.6	261.9	280.2	9.5%
Europe	124.0	142.1	161.9	182.8	204.3	225.5	12.7%
Asia Pacific	97.3	115.2	135.7	158.5	183.3	209.4	16.6%
Middle East & Africa	50.4	58.4	67.3	76.8	86.8	97.3	14.0%
Latin America	21.5	24.9	28.7	32.7	36.9	41.3	13.9%
Total	471.5	539.5	613.8	692.5	773.2	853.7	12.6%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

14.7 TELECOM

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

The DDoS protection and mitigation security market within the 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 93 TELECOM: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	72.0	83.0	96.6	111.6	127.8	145.5	15.1%
Europe	45.5	53.8	64.3	76.3	89.9	105.0	18.2%
Asia Pacific	32.7	35.5	43.6	53.2	64.5	77.9	19.0%
Middle East & Africa	17.3	20.7	25.0	30.0	35.7	42.2	19.6%
Latin America	7.2	8.6	10.4	12.4	14.8	17.5	19.5%
Total	174.6	201.5	239.8	283.6	332.7	388.1	17.3%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 94 TELECOM: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	164.8	185.8	208.0	230.5	252.4	272.8	10.6%
Europe	122.1	141.4	162.7	185.5	209.3	233.2	13.8%
Asia Pacific	93.5	111.9	133.1	156.9	183.3	211.4	17.7%
Middle East & Africa	49.7	58.1	67.7	78.0	89.0	100.8	15.2%
Latin America	20.5	24.0	27.9	32.2	36.7	41.4	15.1%
Total	450.7	521.2	599.3	683.2	770.7	859.6	13.8%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 SECURITY 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 security 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 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 95 HEALTHCARE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	139.8	160.1	185.1	212.4	241.9	273.6	14.4%
Europe	79.4	93.3	110.9	130.9	153.2	178.2	17.5%
Asia Pacific	58.2	62.8	76.7	93.2	112.3	134.8	18.3%
Middle East & Africa	31.3	37.2	44.7	53.4	63.2	74.3	18.9%
Latin America	13.2	15.7	18.8	22.4	26.5	31.2	18.7%
Total	322.0	369.1	436.2	512.3	597.2	692.0	16.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 96 HEALTHCARE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	307.9	345.1	384.0	423.1	460.7	495.1	10.0%
Europe	206.1	237.4	271.8	308.5	346.4	384.1	13.3%
Asia Pacific	161.0	191.6	226.7	266.0	309.1	354.9	17.1%
Middle East & Africa	86.9	101.2	117.1	134.3	152.5	171.7	14.6%
Latin America	36.4	42.3	48.9	56.1	63.6	71.5	14.5%
Total	798.4	917.6	1,048.5	1,188.0	1,332.2	1,477.2	13.1%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 97 EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	44.2	49.9	56.9	64.3	72.2	80.5	12.7%
Europe	33.8	39.3	46.0	53.6	62.0	71.1	16.0%
Asia Pacific	18.8	20.0	24.1	28.8	34.2	40.4	16.5%
Middle East & Africa	9.9	11.5	13.7	16.1	18.7	21.7	17.0%
Latin America	4.5	5.2	6.2	7.3	8.5	9.8	17.0%
Total	111.2	125.9	146.8	170.1	195.6	223.6	15.0%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 98 EDUCATION: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	89.3	98.7	108.3	117.6	126.2	133.7	8.4%
Europe	81.2	92.3	104.4	116.9	129.6	141.8	11.8%
Asia Pacific	47.6	55.8	65.0	75.2	86.1	97.4	15.4%
Middle East & Africa	25.0	28.6	32.6	36.8	41.2	45.7	12.8%
Latin America	11.3	12.9	14.7	16.6	18.6	20.6	12.8%
Total	254.4	288.4	325.0	363.2	401.6	439.2	11.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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 SECURITY 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 security 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 99 RETAIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	118.2	134.1	153.7	174.8	197.3	221.2	13.3%
Europe	64.0	74.5	87.7	102.5	118.9	137.0	16.4%
Asia Pacific	52.8	56.5	68.3	82.2	98.2	116.8	17.2%
Middle East & Africa	24.7	29.0	34.5	40.8	47.9	55.7	17.7%
Latin America	11.5	13.6	16.1	19.1	22.3	26.0	17.6%
Total	271.3	307.8	360.4	419.5	484.6	556.7	15.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 100 RETAIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	246.8	274.1	302.4	330.3	356.6	379.9	9.0%
Europe	157.0	179.1	203.2	228.4	254.2	279.3	12.2%
Asia Pacific	138.3	163.1	191.2	222.4	256.1	291.5	16.1%
Middle East & Africa	64.6	74.5	85.4	97.0	109.1	121.7	13.5%
Latin America	30.0	34.6	39.7	45.0	50.6	56.4	13.4%
Total	636.6	725.3	821.7	923.2	1,026.5	1,128.7	12.1%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

14.11 OTHER VERTICALS

The DDoS protection and mitigation security 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 101 OTHER VERTICALS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	56.5	63.3	71.6	80.4	89.5	98.9	11.8%
Europe	39.4	45.4	52.8	61.1	70.0	79.8	15.2%
Asia Pacific	27.8	29.4	35.1	41.7	49.3	57.9	15.8%
Middle East & Africa	23.4	27.4	32.4	38.0	44.3	51.2	16.9%
Latin America	9.1	10.6	12.5	14.6	17.0	19.6	16.7%
Total	156.2	176.0	204.4	235.9	270.1	307.5	14.5%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

TABLE 102 OTHER VERTICALS: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	108.9	119.2	129.6	139.5	148.3	155.6	7.4%
Europe	90.4	101.9	114.3	127.0	139.5	151.4	10.9%
Asia Pacific	67.7	78.9	91.3	104.9	119.2	133.9	14.6%
Middle East & Africa	58.9	67.5	76.9	86.7	96.8	107.2	12.7%
Latin America	22.5	25.7	29.2	32.9	36.7	40.5	12.5%
Total	348.4	393.2	441.3	490.9	540.6	588.7	11.1%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors.

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

15 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION

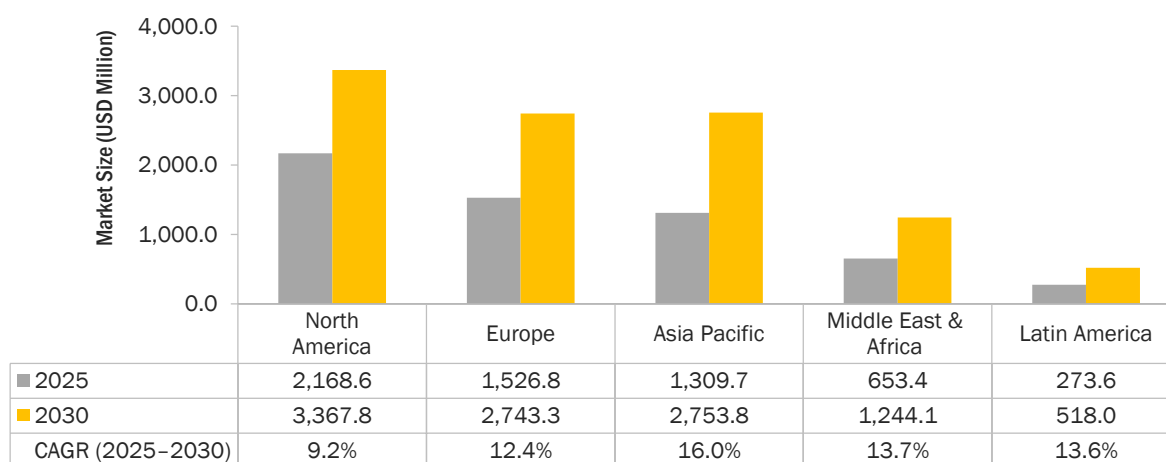
KEY FINDINGS

- North America is estimated to account for the largest share (37.3%) of the DDoS protection and mitigation security market in 2025. The market in this region is projected to register a CAGR of 9.2% from 2025 to 2030.
- 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 16.0%.
- After Asia Pacific, the Middle East & Africa is projected to register the second-highest CAGR of 13.7% during the forecast period.
- 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.

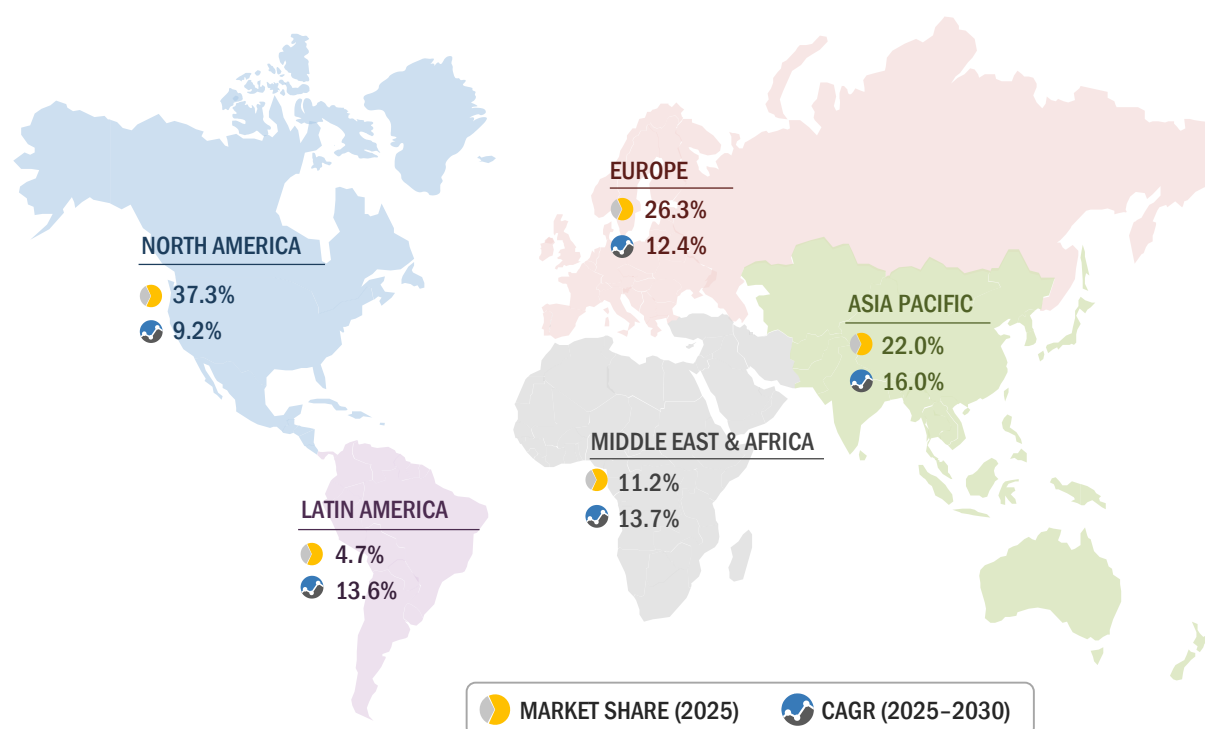
15.1 INTRODUCTION

The DDoS protection and mitigation security 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 encryption solutions include the presence of dynamic business environments, rising commercial espionage and cyberattacks, and the growing need to adhere to regulatory standards for implementing encryption solutions. North America and Asia Pacific are the largest revenue contributors to the DDoS protection and mitigation security 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 33 NORTH AMERICA TO LEAD MARKET FROM 2025 TO 2030



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

FIGURE 34 ASIA PACIFIC TO REGISTER HIGHEST CAGR DURING FORECAST PERIOD

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

TABLE 103 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2019-2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019-2024)
North America	1,028.1	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	13.5%
Europe	615.4	717.7	846.3	991.5	1,152.1	1,329.6	16.7%
Asia Pacific	447.9	535.4	647.7	779.3	930.9	1,106.8	19.8%
Middle East & Africa	246.6	290.9	346.9	410.9	482.6	562.9	17.9%
Latin America	104.0	122.5	145.9	172.7	202.6	236.0	17.8%
Total	2,442.0	2,835.0	3,327.8	3,882.6	4,495.6	5,175.5	16.2%

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

TABLE 104 DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	2,168.6	2,413.0	2,666.6	2,917.9	3,155.5	3,367.8	9.2%
Europe	1,526.8	1,745.7	1,984.0	2,235.2	2,491.8	2,743.3	12.4%
Asia Pacific	1,309.7	1,543.8	1,809.5	2,103.6	2,421.2	2,753.8	16.0%
Middle East & Africa	653.4	755.1	867.4	987.8	1,113.1	1,244.1	13.7%
Latin America	273.6	315.9	362.5	412.4	464.2	518.0	13.6%
Total	5,932.0	6,773.3	7,689.9	8,656.9	9,645.7	10,627.0	12.4%

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

15.2 NORTH AMERICA

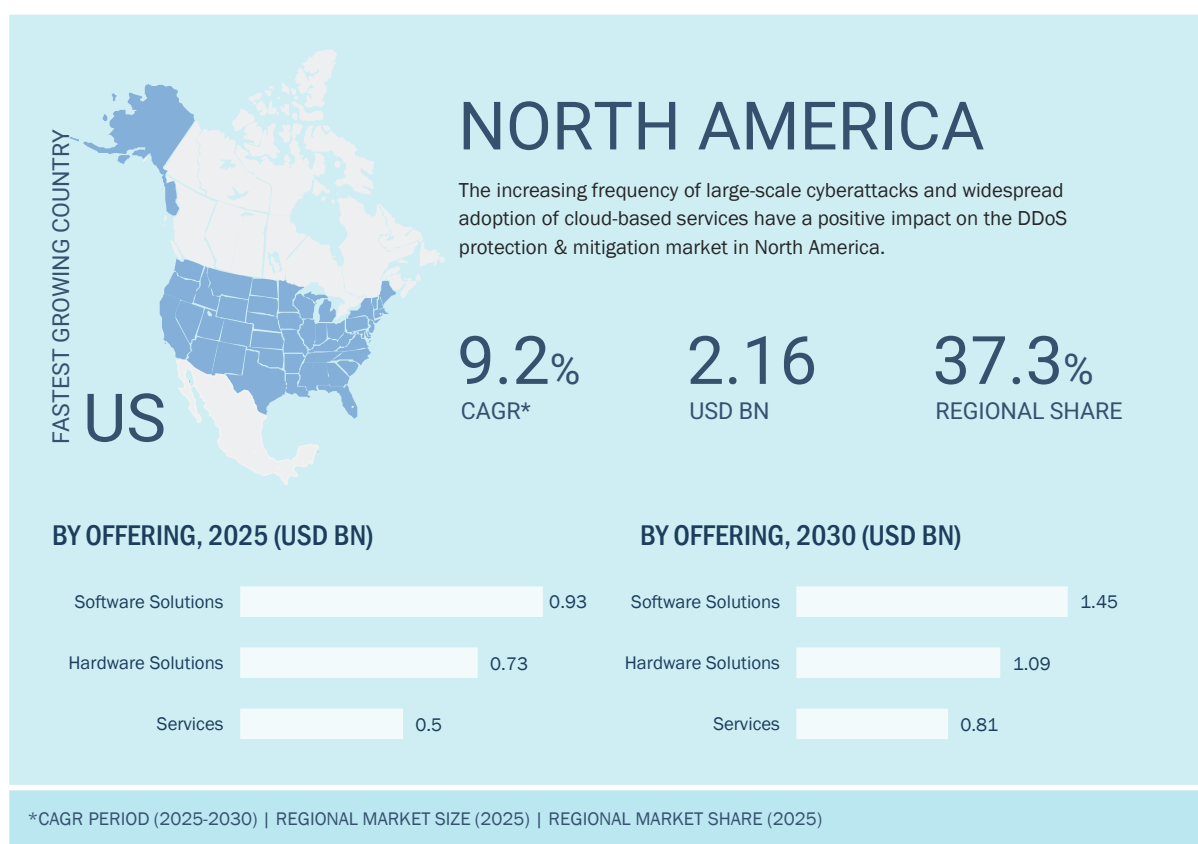
North America is estimated to lead the DDoS protection and mitigation security market during the forecast period. Organizations in this region, especially in the US, have leveraged the benefits of AI, ML, and deep learning technologies to stay ahead in the market. North American countries have well-established economies, which enable DDoS protection and mitigation security 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 security 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.

15.2.1 NORTH AMERICA: MACROECONOMIC OUTLOOK

- The US economy has been incredibly resilient amid high inflation and elevated interest rates over the last two years. Real gross domestic product (GDP) expanded by 2.9% in the first nine months of 2024, compared to the same period a year ago. It also surpassed the 10-year, pre-pandemic average economic performance of 2.4%, which marked the beginning of interest rate and inflation increases.
- Changes in US trade policy are profoundly impacting the global economy and financial markets. The US administration's on-off tariff policy has led to a confidence crisis, with businesses favoring a wait-and-see approach in the face of historically elevated policy uncertainty.
- The US average tariff rate has risen by about 22 percentage points (ppt) to 24% as of April 20, 2025. It can be assumed that exemptions, along with a reduction of tariffs on China, will bring the average tariff rate closer to 17% through most of Q2 and Q3.

FIGURE 35 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET SNAPSHOT



Source: Interviews with Experts and MarketsandMarkets Analysis

TABLE 105 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019-2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019-2024)
Hardware Solutions	361.9	408.4	465.4	526.5	590.8	658.7	12.7%
Software Solutions	442.1	502.8	577.5	658.6	744.9	837.2	13.6%
Services	224.1	257.3	298.3	343.3	391.8	444.3	14.7%
Total	1,028.1	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	13.5%

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

TABLE 106 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	730.8	807.1	885.3	961.5	1,031.8	1,092.9	8.4%
Software Solutions	936.4	1,042.6	1,153.0	1,262.6	1,366.3	1,459.3	9.3%
Services	501.4	563.2	628.2	693.9	757.3	815.7	10.2%
Total	2,168.6	2,413.0	2,666.6	2,917.9	3,155.5	3,367.8	9.2%

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

TABLE 107 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	141.1	159.6	182.1	206.4	232.1	259.2	12.9%
Intrusion Detection & Prevention Systems	94.5	105.7	119.5	134.1	149.2	165.0	11.8%
Load Balancers	69.1	78.8	90.7	103.6	117.3	132.1	13.8%
Other Hardware Solutions	57.2	64.3	73.1	82.4	92.2	102.4	12.4%
Total	361.9	408.4	465.4	526.5	590.8	658.7	12.7%

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

TABLE 108 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	288.1	318.7	350.2	381.0	409.6	434.6	8.6%
Intrusion Detection & Prevention Systems	181.5	198.8	216.2	232.8	247.6	260.0	7.4%
Load Balancers	147.9	164.9	182.5	200.1	216.7	231.6	9.4%
Other Hardware Solutions	113.3	124.7	136.3	147.6	157.9	166.7	8.0%
Total	730.8	807.1	885.3	961.5	1,031.8	1,092.9	8.4%

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

TABLE 109 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	132.2	151.4	175.1	201.0	228.8	258.8	14.4%
Managed Services	91.9	105.9	123.2	142.3	163.0	185.5	15.1%
Total	224.1	257.3	298.3	343.3	391.8	444.3	14.7%

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

TABLE 110 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	291.3	326.4	363.1	400.0	435.5	467.8	9.9%
Managed Services	210.1	236.8	265.1	293.9	321.9	347.9	10.6%
Total	501.4	563.2	628.2	693.9	757.3	815.7	10.2%

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

TABLE 111 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	40.2	45.8	52.7	60.2	68.2	76.7	13.8%
Consulting and Advisory	34.5	40.0	46.7	54.3	62.5	71.4	15.7%
Training and Education	26.8	30.9	35.9	41.4	47.4	53.8	14.9%
Support and Maintenance	30.7	34.8	39.7	45.1	50.8	56.8	13.1%
Total	132.2	151.4	175.1	201.0	228.8	258.8	14.4%

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

TABLE 112 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	85.9	95.8	106.0	116.2	125.8	134.5	9.4%
Consulting and Advisory	81.3	92.0	103.5	115.2	126.7	137.5	11.1%
Training and Education	60.9	68.5	76.6	84.8	92.8	100.1	10.5%
Support and Maintenance	63.2	70.0	77.0	83.8	90.1	95.7	8.6%
Total	291.3	326.4	363.1	400.0	435.5	467.8	9.9%

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

TABLE 113 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	152.1	173.3	199.5	227.9	258.3	290.9	13.9%
Threat Mitigation Systems	122.0	138.4	158.6	180.4	203.5	228.1	13.3%
Botnet Detection & Management	95.0	109.0	126.1	144.9	165.2	187.1	14.5%
Other Solution Types	72.9	82.1	93.3	105.3	117.8	131.0	12.4%
Total	442.1	502.8	577.5	658.6	744.9	837.2	13.6%

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

TABLE 114 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	326.1	363.8	403.1	442.3	479.6	513.2	9.5%
Threat Mitigation Systems	254.5	282.7	311.8	340.5	367.5	391.5	9.0%
Botnet Detection & Management	210.9	236.6	263.6	290.8	317.0	341.0	10.1%
Other Solution Types	145.0	159.6	174.6	189.0	202.2	213.5	8.1%
Total	936.4	1,042.6	1,153.0	1,262.6	1,366.3	1,459.3	9.3%

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

TABLE 115 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	345.4	389.3	443.1	500.7	561.1	624.7	12.6%
Application Security	393.8	451.0	521.7	599.1	682.4	772.2	14.4%
Endpoint Security	128.5	145.4	166.0	188.3	211.8	236.7	13.0%
Cloud Security	160.4	182.8	210.3	240.3	272.3	306.5	13.8%
Total	1,028.1	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	13.5%

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

TABLE 116 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	692.2	763.5	836.2	906.9	971.9	1,027.9	8.2%
Application Security	869.6	974.8	1,085.3	1,196.4	1,303.2	1,401.0	10.0%
Endpoint Security	263.3	291.5	320.5	349.0	375.5	398.8	8.7%
Cloud Security	343.5	383.2	424.5	465.7	504.9	540.2	9.5%
Total	2,168.6	2,413.0	2,666.6	2,917.9	3,155.5	3,367.8	9.2%

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

TABLE 117 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	444.1	502.5	574.0	651.1	732.5	818.7	13.0%
Cloud	584.0	666.0	767.1	877.3	995.0	1,121.4	13.9%
Total	1,028.1	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	13.5%

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

TABLE 118 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	910.8	1,008.6	1,109.3	1,208.0	1,300.1	1,380.8	8.7%
Cloud	1,257.8	1,404.3	1,557.3	1,709.9	1,855.4	1,987.0	9.6%
Total	2,168.6	2,413.0	2,666.6	2,917.9	3,155.5	3,367.8	9.2%

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

TABLE 119 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	390.7	448.7	520.3	599.1	684.1	776.1	14.7%
Large Enterprises	637.4	719.8	820.8	929.2	1,043.4	1,164.1	12.8%
Total	1,028.1	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	13.5%

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

TABLE 120 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	876.1	984.5	1,098.6	1,213.9	1,325.3	1,428.0	10.3%
Large Enterprises	1,292.5	1,428.5	1,567.9	1,704.1	1,830.2	1,939.9	8.5%
Total	2,168.6	2,413.0	2,666.6	2,917.9	3,155.5	3,367.8	9.2%

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

TABLE 121 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	207.7	240.9	282.2	328.0	378.0	432.7	15.8%
Government & Defense	150.1	167.1	187.8	209.4	231.5	254.2	11.1%
IT & ITeS	83.3	94.9	109.2	124.7	141.3	159.1	13.8%
Telecom	72.0	83.0	96.6	111.6	127.8	145.5	15.1%
Manufacturing	104.9	117.8	133.6	150.4	167.9	186.3	12.2%
Energy and Utilities	51.4	57.4	64.6	72.3	80.2	88.3	11.4%
Healthcare	139.8	160.1	185.1	212.4	241.9	273.6	14.4%
Retail	118.2	134.1	153.7	174.8	197.3	221.2	13.3%
Education	44.2	49.9	56.9	64.3	72.2	80.5	12.7%
Other Verticals	56.5	63.3	71.6	80.4	89.5	98.9	11.8%
Total	1,028.1	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	13.5%

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

TABLE 122 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	492.7	558.4	628.2	699.7	769.9	835.9	11.2%
Government & Defense	277.6	301.6	325.3	347.2	366.0	380.6	6.5%
IT & ITeS	178.3	198.8	220.3	241.6	261.9	280.2	9.5%
Telecom	164.8	185.8	208.0	230.5	252.4	272.8	10.6%
Manufacturing	205.6	225.9	246.4	266.1	284.0	299.1	7.8%
Energy and Utilities	96.7	105.4	114.1	122.3	129.4	135.0	6.9%
Healthcare	307.9	345.1	384.0	423.1	460.7	495.1	10.0%
Retail	246.8	274.1	302.4	330.3	356.6	379.9	9.0%
Education	89.3	98.7	108.3	117.6	126.2	133.7	8.4%
Other Verticals	108.9	119.2	129.6	139.5	148.3	155.6	7.4%
Total	2,168.6	2,413.0	2,666.6	2,917.9	3,155.5	3,367.8	9.2%

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

TABLE 123 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)

Country	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
US	865.7	980.0	1,121.2	1,273.6	1,434.1	1,603.3	13.1%
Canada	162.3	188.5	219.9	254.7	293.4	336.8	15.7%
Total	1,028.1	1,168.5	1,341.1	1,528.3	1,727.5	1,940.2	13.5%

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

TABLE 124 NORTH AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)

Country	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
US	1,782.9	1,973.7	2,171.0	2,366.4	2,551.0	2,716.8	8.8%
Canada	385.7	439.3	495.5	551.5	604.4	651.0	11.0%
Total	2,168.6	2,413.0	2,666.6	2,917.9	3,155.5	3,367.8	9.2%

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

15.2.2 US

15.2.2.1 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 security 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 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 125 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	296.3	333.0	378.2	426.4	476.6	528.8	12.3%
Software Solutions	367.9	416.8	477.2	542.4	611.2	683.8	13.2%
Services	201.5	230.2	265.8	304.8	346.3	390.7	14.2%
Total	865.7	980.0	1,121.2	1,273.6	1,434.1	1,603.3	13.1%

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

TABLE 126 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	583.5	641.0	699.7	756.8	809.4	855.3	7.9%
Software Solutions	760.9	843.0	927.9	1,012.1	1,091.8	1,163.6	8.9%
Services	438.4	489.7	543.4	597.5	649.7	698.0	9.7%
Total	1,782.9	1,973.7	2,171.0	2,366.4	2,551.0	2,716.8	8.8%

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

TABLE 127 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	115.3	129.8	147.6	166.8	186.7	207.5	12.5%
Intrusion Detection & Prevention Systems	77.9	86.9	97.9	109.5	121.3	133.5	11.4%
Load Balancers	57.8	65.6	75.2	85.6	96.5	108.1	13.4%
Other Hardware Solutions	45.3	50.8	57.5	64.6	72.0	79.6	11.9%
Total	296.3	333.0	378.2	426.4	476.6	528.8	12.3%

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

TABLE 128 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	229.4	252.5	276.1	299.2	320.5	339.3	8.1%
Intrusion Detection & Prevention Systems	146.1	159.2	172.3	184.7	195.9	205.2	7.0%
Load Balancers	120.4	133.5	147.1	160.5	173.2	184.7	8.9%
Other Hardware Solutions	87.5	95.8	104.3	112.4	119.8	126.2	7.6%
Total	583.5	641.0	699.7	756.8	809.4	855.3	7.9%

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

TABLE 129 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	116.8	133.2	153.4	175.4	198.8	223.7	13.9%
Managed Services	84.6	97.0	112.4	129.4	147.5	167.0	14.6%
Total	201.5	230.2	265.8	304.8	346.3	390.7	14.2%

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

TABLE 130 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	250.3	278.9	308.7	338.5	367.1	393.3	9.5%
Managed Services	188.1	210.8	234.8	259.0	282.6	304.7	10.1%
Total	438.4	489.7	543.4	597.5	649.7	698.0	9.7%

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

TABLE 131 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	35.2	39.9	45.7	52.0	58.6	65.7	13.3%
Consulting and Advisory	30.6	35.3	41.1	47.5	54.5	62.0	15.1%
Training and Education	24.1	27.6	31.9	36.7	41.7	47.2	14.4%
Support and Maintenance	27.0	30.4	34.7	39.2	43.9	48.9	12.6%
Total	116.8	133.2	153.4	175.4	198.8	223.7	13.9%

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

TABLE 132 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	73.1	81.0	89.2	97.3	105.0	111.9	8.9%
Consulting and Advisory	70.1	78.9	88.3	97.8	107.2	116.0	10.6%
Training and Education	53.1	59.4	66.1	72.8	79.3	85.3	10.0%
Support and Maintenance	54.1	59.5	65.1	70.6	75.6	80.0	8.2%
Total	250.3	278.9	308.7	338.5	367.1	393.3	9.5%

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

TABLE 133 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	125.8	142.8	163.9	186.7	210.7	236.3	13.4%
Threat Mitigation Systems	102.7	116.0	132.5	150.2	168.8	188.4	12.9%
Botnet Detection & Management	78.4	89.5	103.3	118.3	134.3	151.5	14.1%
Other Solution Types	61.1	68.5	77.6	87.3	97.3	107.7	12.0%
Total	367.9	416.8	477.2	542.4	611.2	683.8	13.2%

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

TABLE 134 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	263.4	292.4	322.5	352.5	381.0	406.9	9.1%
Threat Mitigation Systems	209.1	231.1	253.7	276.0	297.0	315.7	8.6%
Botnet Detection & Management	169.8	189.6	210.3	231.1	251.1	269.6	9.7%
Other Solution Types	118.6	129.9	141.4	152.5	162.7	171.4	7.7%
Total	760.9	843.0	927.9	1,012.1	1,091.8	1,163.6	8.9%

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

TABLE 135 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	289.2	324.6	368.2	414.7	462.9	513.1	12.2%
Application Security	331.6	378.3	436.1	499.3	566.5	638.1	14.0%
Endpoint Security	109.9	123.9	141.0	159.5	178.7	198.8	12.6%
Cloud Security	135.1	153.3	175.8	200.2	226.0	253.3	13.4%
Total	865.7	980.0	1,121.2	1,273.6	1,434.1	1,603.3	13.1%

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

TABLE 136 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	565.5	620.5	676.5	730.8	780.6	823.7	7.8%
Application Security	714.9	797.4	883.6	970.2	1,053.6	1,130.2	9.6%
Endpoint Security	220.0	242.4	265.3	287.8	308.7	327.1	8.3%
Cloud Security	282.4	313.4	345.6	377.7	408.2	435.8	9.1%
Total	1,782.9	1,973.7	2,171.0	2,366.4	2,551.0	2,716.8	8.8%

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

TABLE 137 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	367.9	414.6	472.0	533.6	598.0	665.4	12.6%
Cloud	497.8	565.5	649.1	740.0	836.1	937.9	13.5%
Total	865.7	980.0	1,121.2	1,273.6	1,434.1	1,603.3	13.1%

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

TABLE 138 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	736.3	811.2	888.0	963.1	1,033.2	1,094.9	8.3%
Cloud	1,046.6	1,162.5	1,283.1	1,403.3	1,517.9	1,621.9	9.2%
Total	1,782.9	1,973.7	2,171.0	2,366.4	2,551.0	2,716.8	8.8%

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

TABLE 139 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	320.3	366.5	423.8	486.5	553.6	625.3	14.3%
Large Enterprises	545.4	613.5	697.4	787.1	880.5	978.0	12.4%
Total	865.7	980.0	1,121.2	1,273.6	1,434.1	1,603.3	13.1%

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

TABLE 140 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	702.5	785.5	872.8	960.8	1,045.9	1,124.8	9.9%
Large Enterprises	1,080.4	1,188.2	1,298.3	1,405.7	1,505.1	1,592.1	8.1%
Total	1,782.9	1,973.7	2,171.0	2,366.4	2,551.0	2,716.8	8.8%

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

TABLE 141 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	174.0	201.1	234.8	272.0	312.3	355.9	15.4%
Government & Defense	124.7	138.2	154.7	171.9	189.3	206.8	10.7%
IT & ITeS	71.0	80.6	92.4	105.2	118.7	133.1	13.4%
Telecom	61.5	70.6	81.8	94.2	107.6	121.9	14.7%
Manufacturing	87.4	97.8	110.5	124.1	138.0	152.3	11.7%
Energy and Utilities	44.2	49.1	55.2	61.5	68.0	74.6	11.0%
Healthcare	116.9	133.3	153.6	175.8	199.3	224.5	13.9%
Retail	97.0	109.6	125.1	141.9	159.5	178.0	12.9%
Education	37.2	41.8	47.5	53.6	59.9	66.5	12.3%
Other Verticals	51.9	58.0	65.5	73.4	81.5	89.8	11.6%
Total	865.7	980.0	1,121.2	1,273.6	1,434.1	1,603.3	13.1%

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

TABLE 142 US: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	403.3	454.7	509.3	565.1	619.9	671.6	10.7%
Government & Defense	224.6	242.8	260.5	276.9	290.8	301.6	6.1%
IT & ITeS	148.3	164.6	181.5	198.3	214.3	228.8	9.0%
Telecom	137.3	153.9	171.5	189.3	206.6	222.8	10.2%
Manufacturing	167.2	182.8	198.4	213.5	227.0	238.5	7.4%
Energy and Utilities	81.3	88.2	95.1	101.5	107.1	111.7	6.6%
Healthcare	251.4	280.3	310.5	340.8	369.9	396.7	9.6%
Retail	197.5	218.3	239.7	260.8	280.6	298.3	8.6%
Education	73.5	80.7	88.1	95.4	102.0	107.9	8.0%
Other Verticals	98.4	107.4	116.4	124.9	132.7	139.1	7.2%
Total	1,782.9	1,973.7	2,171.0	2,366.4	2,551.0	2,716.8	8.8%

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

15.2.3 CANADA

15.2.3.1 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 143 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	56.3	64.9	75.2	86.5	98.9	112.7	14.9%
Software Solutions	68.2	79.2	92.5	107.2	123.6	142.0	15.8%
Services	37.8	44.3	52.2	61.0	70.9	82.2	16.8%
Total	162.3	188.5	219.9	254.7	293.4	336.8	15.7%

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

TABLE 144 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	128.0	144.7	162.0	179.0	194.6	208.0	10.2%
Software Solutions	162.7	185.4	209.3	233.1	255.7	275.6	11.1%
Services	95.0	109.1	124.2	139.4	154.1	167.4	12.0%
Total	385.7	439.3	495.5	551.5	604.4	651.0	11.0%

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

TABLE 145 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	21.6	25.0	29.0	33.4	38.2	43.7	15.1%
Intrusion Detection & Prevention Systems	15.0	17.2	19.8	22.5	25.6	28.9	14.0%
Load Balancers	10.8	12.6	14.7	17.1	19.7	22.7	16.0%
Other Hardware Solutions	8.8	10.2	11.7	13.4	15.3	17.4	14.5%
Total	56.3	64.9	75.2	86.5	98.9	112.7	14.9%

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

TABLE 146 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	49.7	56.3	63.1	69.8	76.1	81.5	10.4%
Intrusion Detection & Prevention Systems	32.6	36.5	40.5	44.4	47.9	50.7	9.3%
Load Balancers	26.0	29.7	33.6	37.4	41.1	44.3	11.2%
Other Hardware Solutions	19.7	22.2	24.8	27.3	29.6	31.5	9.8%
Total	128.0	144.7	162.0	179.0	194.6	208.0	10.2%

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

TABLE 147 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	22.7	26.5	31.2	36.3	42.1	48.7	16.5%
Managed Services	15.1	17.8	21.0	24.7	28.8	33.5	17.2%
Total	37.8	44.3	52.2	61.0	70.9	82.2	16.8%

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

TABLE 148 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	56.1	64.3	73.0	81.8	90.2	97.7	11.7%
Managed Services	38.8	44.8	51.2	57.7	64.0	69.7	12.4%
Total	95.0	109.1	124.2	139.4	154.1	167.4	12.0%

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

TABLE 149 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	7.1	8.2	9.6	11.2	12.9	14.8	15.9%
Consulting and Advisory	6.1	7.2	8.6	10.1	11.8	13.8	17.8%
Training and Education	4.7	5.5	6.5	7.6	8.8	10.3	17.1%
Support and Maintenance	4.8	5.6	6.5	7.5	8.6	9.8	15.1%
Total	22.7	26.5	31.2	36.3	42.1	48.7	16.5%

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

TABLE 150 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	17.0	19.4	21.9	24.4	26.8	28.9	11.2%
Consulting and Advisory	16.1	18.7	21.4	24.2	27.0	29.5	12.9%
Training and Education	11.9	13.7	15.6	17.6	19.5	21.2	12.2%
Support and Maintenance	11.1	12.6	14.1	15.6	17.0	18.1	10.3%
Total	56.1	64.3	73.0	81.8	90.2	97.7	11.7%

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

TABLE 151 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	22.1	25.7	30.1	35.0	40.4	46.5	16.0%
Threat Mitigation Systems	19.2	22.2	25.9	29.9	34.4	39.4	15.5%
Botnet Detection & Management	14.3	16.8	19.7	23.1	26.8	31.0	16.7%
Other Solution Types	12.6	14.5	16.8	19.3	22.0	25.1	14.7%
Total	68.2	79.2	92.5	107.2	123.6	142.0	15.8%

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

TABLE 152 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	53.4	61.0	69.0	77.0	84.6	91.4	11.4%
Threat Mitigation Systems	45.0	51.2	57.6	64.0	70.1	75.3	10.8%
Botnet Detection & Management	35.8	41.1	46.8	52.5	58.0	63.0	12.0%
Other Solution Types	28.4	32.1	35.9	39.6	43.0	45.8	10.0%
Total	162.7	185.4	209.3	233.1	255.7	275.6	11.1%

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

TABLE 153 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	55.5	63.9	74.0	85.0	97.1	110.5	14.8%
Application Security	63.5	74.3	87.3	101.9	118.2	136.8	16.6%
Endpoint Security	20.1	23.3	27.0	31.1	35.7	40.8	15.2%
Cloud Security	23.2	27.0	31.6	36.7	42.4	48.8	16.0%
Total	162.3	188.5	219.9	254.7	293.4	336.8	15.7%

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

TABLE 154 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	125.4	141.6	158.4	174.7	189.8	202.6	10.1%
Application Security	157.7	181.0	205.6	230.5	254.5	276.0	11.8%
Endpoint Security	46.4	52.6	59.1	65.4	71.3	76.4	10.5%
Cloud Security	56.1	64.0	72.4	80.9	88.9	96.0	11.3%
Total	385.7	439.3	495.5	551.5	604.4	651.0	11.0%

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

TABLE 155 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	66.9	77.3	89.7	103.4	118.5	135.4	15.2%
Cloud	95.5	111.2	130.2	151.3	174.9	201.4	16.1%
Total	162.3	188.5	219.9	254.7	293.4	336.8	15.7%

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

TABLE 156 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	154.3	174.8	196.2	217.3	236.9	253.9	10.5%
Cloud	231.4	264.4	299.3	334.2	367.5	397.1	11.4%
Total	385.7	439.3	495.5	551.5	604.4	651.0	11.0%

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

TABLE 157 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	56.8	66.7	78.7	92.2	107.4	124.6	17.0%
Large Enterprises	105.5	121.8	141.2	162.5	186.0	212.2	15.0%
Total	162.3	188.5	219.9	254.7	293.4	336.8	15.7%

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

TABLE 158 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	144.2	166.0	189.3	212.9	235.7	256.5	12.2%
Large Enterprises	241.4	273.2	306.2	338.6	368.7	394.5	10.3%
Total	385.7	439.3	495.5	551.5	604.4	651.0	11.0%

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

TABLE 159 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	31.5	37.4	44.5	52.6	61.9	72.4	18.1%
Government & Defense	21.6	24.5	27.9	31.6	35.5	39.7	13.0%
IT & ITeS	18.2	21.1	24.7	28.7	33.1	38.1	15.9%
Telecom	12.8	15.1	17.8	20.9	24.4	28.3	17.1%
Manufacturing	16.9	19.4	22.3	25.6	29.1	33.0	14.4%
Energy and Utilities	5.5	6.3	7.2	8.1	9.2	10.3	13.2%
Healthcare	23.5	27.5	32.3	37.7	43.7	50.5	16.5%
Retail	10.6	12.2	14.2	16.4	18.8	21.6	15.4%
Education	14.0	16.1	18.7	21.4	24.5	28.0	14.9%
Other Verticals	7.8	8.9	10.2	11.7	13.3	15.0	14.0%
Total	162.3	188.5	219.9	254.7	293.4	336.8	15.7%

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

TABLE 160 CANADA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	84.5	98.1	112.8	127.8	142.7	156.4	13.1%
Government & Defense	44.4	49.2	54.0	58.5	62.3	65.1	8.0%
IT & ITeS	43.7	49.8	56.3	62.8	68.9	74.3	11.2%
Telecom	32.8	37.8	43.1	48.5	53.8	58.6	12.3%
Manufacturing	37.3	42.0	46.8	51.4	55.6	59.1	9.6%
Energy and Utilities	11.5	12.8	14.1	15.3	16.3	17.1	8.3%
Healthcare	58.2	66.8	75.8	84.9	93.7	101.6	11.8%
Retail	24.6	27.9	31.4	34.9	38.1	40.9	10.7%
Education	31.8	35.9	40.2	44.5	48.4	51.7	10.2%
Other Verticals	16.9	18.9	21.0	23.0	24.8	26.2	9.2%
Total	385.7	439.3	495.5	551.5	604.4	651.0	11.0%

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 security 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 cyber-attacks targeting cloud data. These concerns have led to the substantial adoption of encryption 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.

15.3.1 EUROPE: MACROECONOMIC OUTLOOK

- The euro area annual inflation rate was 2.2% in March 2025, down from 2.3% in February. A year earlier, the rate was 2.4%. The European Union's annual inflation was 2.5% in March 2025, down from 2.7% in February. The lowest annual rates were registered in France (0.9%), Denmark (1.4%), and Luxembourg (1.5%). The highest annual rates were recorded in Romania (5.1%), Hungary (4.8%), and Poland (4.4%). Compared to February 2025, annual inflation decreased in 16 member states, remained stable in one, and increased in 10.
- High-tech goods output growth in Europe is expected to slow to 0.3% this year, following a 4.4% increase in 2023. ICT consumption and investment continue to face headwinds from high interest rates and lower investment.
- The European Central Bank (ECB) and the national central banks of the Eurozone countries manage monetary policy for the Eurozone. The ECB's primary objective is to maintain price stability, which means keeping inflation stable and predictable. The Governing Council has decided to reduce the three key ECB interest rates by 25 basis points. This adjustment follows a review that shows inflation has decreased significantly, and the inflation outlook has improved.
- Although underlying inflation and expectations have eased, domestic price pressures remain strong, partly due to elevated wage growth. Inflation is expected to remain above target next year, with revised projections indicating that headline inflation will average 2.5% in 2024, 2.2% in 2025, and 1.9% in 2026. For inflation, excluding energy and food, staff projects an average of 2.8% in 2024, 2.2% in 2025, and 2.0% in 2026. Economic growth is expected to rise to 0.9% in 2024, 1.4% in 2025, and 1.6% in 2026.
- The UK experienced minimal growth of just 0.1% in 2023, largely due to a weak fourth quarter and downward revisions to previous quarters. Growth is expected to remain modest at 0.5% in 2024 due to tighter fiscal policies, but is projected to gain momentum in 2025, reaching about 1.4%. Overall, advanced economies (excluding the EU) are forecasted to grow by 2.1% in both 2024 and 2025, slightly down from 2.2% in 2023.

TABLE 161 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	209.2	242.2	283.5	329.7	380.2	435.5	15.8%
Software Solutions	258.5	301.7	355.9	417.3	485.3	560.4	16.7%
Services	147.7	173.8	206.8	244.5	286.6	333.7	17.7%
Total	615.4	717.7	846.3	991.5	1,152.1	1,329.6	16.7%

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

TABLE 162 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	496.2	563.0	634.9	709.7	784.9	857.3	11.6%
Software Solutions	644.0	736.8	838.0	944.8	1,054.0	1,161.2	12.5%
Services	386.6	445.8	511.1	580.7	652.8	724.8	13.4%
Total	1,526.8	1,745.7	1,984.0	2,235.2	2,491.8	2,743.3	12.4%

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

TABLE 163 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	81.8	94.9	111.2	129.6	149.7	171.8	16.0%
Intrusion Detection & Prevention Systems	54.4	62.5	72.5	83.6	95.7	108.6	14.8%
Load Balancers	40.4	47.2	55.8	65.5	76.3	88.2	16.9%
Other Hardware Solutions	32.6	37.7	43.9	50.9	58.5	66.8	15.4%
Total	209.2	242.2	283.5	329.7	380.2	435.5	15.8%

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

TABLE 164 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	196.1	222.9	251.8	282.0	312.4	341.8	11.8%
Intrusion Detection & Prevention Systems	122.8	138.1	154.4	171.1	187.6	203.1	10.6%
Load Balancers	101.4	116.1	132.2	149.1	166.4	183.4	12.6%
Other Hardware Solutions	75.9	85.9	96.5	107.5	118.5	129.0	11.2%
Total	496.2	563.0	634.9	709.7	784.9	857.3	11.6%

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

TABLE 165 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	81.2	95.4	113.1	133.4	155.9	181.1	17.4%
Managed Services	66.5	78.5	93.7	111.1	130.7	152.7	18.1%
Total	147.7	173.8	206.8	244.5	286.6	333.7	17.7%

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

TABLE 166 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	209.1	240.5	275.0	311.6	349.3	386.7	13.1%
Managed Services	177.4	205.3	236.1	269.2	303.6	338.1	13.8%
Total	386.6	445.8	511.1	580.7	652.8	724.8	13.4%

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

TABLE 167 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	25.6	29.9	35.3	41.4	48.2	55.7	16.8%
Consulting and Advisory	20.6	24.5	29.4	35.1	41.5	48.7	18.7%
Training and Education	16.7	19.7	23.5	27.9	32.7	38.2	18.0%
Support and Maintenance	18.3	21.2	24.9	29.0	33.5	38.5	16.1%
Total	81.2	95.4	113.1	133.4	155.9	181.1	17.4%

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

TABLE 168 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	64.0	73.2	83.3	93.9	104.8	115.4	12.5%
Consulting and Advisory	56.9	66.1	76.4	87.5	99.2	111.0	14.3%
Training and Education	44.3	51.2	58.8	67.0	75.4	83.9	13.6%
Support and Maintenance	43.9	49.9	56.4	63.1	69.9	76.4	11.7%
Total	209.1	240.5	275.0	311.6	349.3	386.7	13.1%

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

TABLE 169 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	90.2	105.5	124.7	146.5	170.7	197.6	17.0%
Threat Mitigation Systems	75.5	87.9	103.4	121.0	140.3	161.7	16.5%
Botnet Detection & Management	55.1	64.8	77.0	91.0	106.7	124.1	17.7%
Other Solution Types	37.7	43.5	50.8	58.8	67.5	77.1	15.3%
Total	258.5	301.7	355.9	417.3	485.3	560.4	16.7%

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

TABLE 170 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	227.5	260.8	297.2	335.7	375.2	414.2	12.7%
Threat Mitigation Systems	185.3	211.5	240.0	269.9	300.4	330.1	12.2%
Botnet Detection & Management	143.7	165.7	189.9	215.7	242.4	269.1	13.4%
Other Solution Types	87.5	98.8	111.0	123.5	136.0	147.8	11.1%
Total	644.0	736.8	838.0	944.8	1,054.0	1,161.2	12.5%

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

TABLE 171 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	210.5	243.5	284.7	330.8	381.1	436.1	15.7%
Application Security	240.6	282.8	336.0	396.6	464.3	539.8	17.5%
Endpoint Security	76.9	89.3	104.8	122.2	141.2	162.2	16.1%
Cloud Security	87.4	102.2	120.8	142.0	165.4	191.5	17.0%
Total	615.4	717.7	846.3	991.5	1,152.1	1,329.6	16.7%

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

TABLE 172 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	496.5	562.8	634.1	708.1	782.4	853.7	11.4%
Application Security	624.4	719.2	823.3	934.3	1,049.0	1,163.1	13.2%
Endpoint Security	185.3	210.9	238.5	267.3	296.5	324.8	11.9%
Cloud Security	220.5	252.8	288.1	325.4	363.8	401.6	12.7%
Total	1,526.8	1,745.7	1,984.0	2,235.2	2,491.8	2,743.3	12.4%

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

TABLE 173 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	272.0	315.8	370.7	432.3	500.0	574.4	16.1%
Cloud	343.4	401.9	475.6	559.2	652.1	755.2	17.1%
Total	615.4	717.7	846.3	991.5	1,152.1	1,329.6	16.7%

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

TABLE 174 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	656.5	747.1	845.2	947.7	1,051.5	1,152.2	11.9%
Cloud	870.2	998.5	1,138.8	1,287.5	1,440.3	1,591.1	12.8%
Total	1,526.8	1,745.7	1,984.0	2,235.2	2,491.8	2,743.3	12.4%

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

TABLE 175 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	215.4	254.1	303.0	358.9	421.7	492.0	18.0%
Large Enterprises	400.0	463.7	543.3	632.6	730.4	837.7	15.9%
Total	615.4	717.7	846.3	991.5	1,152.1	1,329.6	16.7%

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

TABLE 176 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	571.0	659.9	757.9	862.8	971.8	1,080.8	13.6%
Large Enterprises	955.7	1,085.8	1,226.1	1,372.4	1,520.0	1,662.4	11.7%
Total	1,526.8	1,745.7	1,984.0	2,235.2	2,491.8	2,743.3	12.4%

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

TABLE 177 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	116.9	139.4	167.9	200.9	238.3	280.6	19.1%
Government & Defense	89.2	101.9	117.6	134.8	153.2	172.9	14.1%
IT & ITeS	49.2	57.6	68.0	79.9	93.1	107.7	16.9%
Telecom	45.5	53.8	64.3	76.3	89.9	105.0	18.2%
Manufacturing	67.7	78.1	91.1	105.5	121.2	138.3	15.4%
Energy and Utilities	30.2	34.5	39.9	45.9	52.3	59.2	14.4%
Healthcare	79.4	93.3	110.9	130.9	153.2	178.2	17.5%
Retail	64.0	74.5	87.7	102.5	118.9	137.0	16.4%
Education	33.8	39.3	46.0	53.6	62.0	71.1	16.0%
Other Verticals	39.4	45.4	52.8	61.1	70.0	79.8	15.2%
Total	615.4	717.7	846.3	991.5	1,152.1	1,329.6	16.7%

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

TABLE 178 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	328.6	383.0	443.6	509.2	578.1	648.0	14.5%
Government & Defense	193.9	216.5	240.1	263.8	286.6	307.2	9.6%
IT & ITeS	124.0	142.1	161.9	182.8	204.3	225.5	12.7%
Telecom	122.1	141.4	162.7	185.5	209.3	233.2	13.8%
Manufacturing	157.0	177.4	199.2	221.7	244.2	265.5	11.1%
Energy and Utilities	66.6	74.5	82.9	91.4	99.7	107.3	10.0%
Healthcare	206.1	237.4	271.8	308.5	346.4	384.1	13.3%
Retail	157.0	179.1	203.2	228.4	254.2	279.3	12.2%
Education	81.2	92.3	104.4	116.9	129.6	141.8	11.8%
Other Verticals	90.4	101.9	114.3	127.0	139.5	151.4	10.9%
Total	1,526.8	1,745.7	1,984.0	2,235.2	2,491.8	2,743.3	12.4%

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

TABLE 179 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)

Country	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
UK	133.9	153.9	178.5	206.0	235.8	268.1	14.9%
Germany	149.7	173.0	202.2	234.8	270.3	308.9	15.6%
Rest of Europe	331.8	390.9	465.5	550.7	646.0	752.6	17.8%
Total	615.4	717.7	846.3	991.5	1,152.1	1,329.6	16.7%

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

TABLE 180 EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)

Country	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
UK	303.3	341.5	382.1	423.8	464.9	503.4	10.7%
Germany	351.2	397.6	447.3	498.7	550.1	599.1	11.3%
Rest of Europe	872.3	1,006.6	1,154.6	1,312.7	1,476.8	1,640.7	13.5%
Total	1,526.8	1,745.7	1,984.0	2,235.2	2,491.8	2,743.3	12.4%

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

15.3.2 UK

15.3.2.1 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 security 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 security 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 Counsel 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 181 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	44.9	51.2	58.9	67.5	76.6	86.5	14.0%
Software Solutions	55.7	64.1	74.4	85.9	98.4	111.9	15.0%
Services	33.3	38.6	45.2	52.6	60.8	69.7	15.9%
Total	133.9	153.9	178.5	206.0	235.8	268.1	14.9%

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

TABLE 182 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	97.0	108.4	120.4	132.4	144.1	154.8	9.8%
Software Solutions	126.7	142.8	159.9	177.4	194.8	211.1	10.7%
Services	79.5	90.3	101.9	113.9	126.0	137.5	11.6%
Total	303.3	341.5	382.1	423.8	464.9	503.4	10.7%

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

TABLE 183 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	17.1	19.6	22.6	25.9	29.5	33.3	14.2%
Intrusion Detection & Prevention Systems	11.7	13.2	15.1	17.2	19.4	21.7	13.1%
Load Balancers	8.7	10.0	11.6	13.5	15.5	17.6	15.1%
Other Hardware Solutions	7.3	8.3	9.5	10.9	12.3	13.9	13.7%
Total	44.9	51.2	58.9	67.5	76.6	86.5	14.0%

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

TABLE 184 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	37.5	41.9	46.7	51.4	56.1	60.3	10.0%
Intrusion Detection & Prevention Systems	24.1	26.7	29.4	32.1	34.6	36.8	8.8%
Load Balancers	19.9	22.5	25.2	28.0	30.7	33.3	10.8%
Other Hardware Solutions	15.5	17.3	19.1	21.0	22.8	24.4	9.4%
Total	97.0	108.4	120.4	132.4	144.1	154.8	9.8%

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

TABLE 185 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	18.3	21.2	24.7	28.7	33.1	37.8	15.6%
Managed Services	15.0	17.5	20.5	23.9	27.7	31.9	16.3%
Total	33.3	38.6	45.2	52.6	60.8	69.7	15.9%

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

TABLE 186 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	43.0	48.7	54.8	61.1	67.4	73.4	11.3%
Managed Services	36.5	41.6	47.1	52.8	58.6	64.2	11.9%
Total	79.5	90.3	101.9	113.9	126.0	137.5	11.6%

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

TABLE 187 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	5.8	6.6	7.7	8.9	10.2	11.6	15.0%
Consulting and Advisory	5.0	5.8	6.9	8.0	9.4	10.8	16.8%
Training and Education	3.9	4.5	5.3	6.2	7.1	8.2	16.1%
Support and Maintenance	3.7	4.2	4.9	5.6	6.4	7.2	14.1%
Total	18.3	21.2	24.7	28.7	33.1	37.8	15.6%

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

TABLE 188 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	13.2	14.8	16.6	18.4	20.2	21.9	10.7%
Consulting and Advisory	12.4	14.2	16.2	18.2	20.3	22.3	12.4%
Training and Education	9.4	10.7	12.1	13.5	15.0	16.4	11.8%
Support and Maintenance	8.0	9.0	10.0	11.0	11.9	12.8	9.7%
Total	43.0	48.7	54.8	61.1	67.4	73.4	11.3%

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

TABLE 189 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	18.4	21.2	24.7	28.6	32.8	37.4	15.2%
Threat Mitigation Systems	16.1	18.5	21.4	24.6	28.2	32.0	14.7%
Botnet Detection & Management	12.0	13.9	16.2	18.9	21.8	25.0	15.9%
Other Solution Types	9.2	10.5	12.0	13.7	15.6	17.5	13.8%
Total	55.7	64.1	74.4	85.9	98.4	111.9	15.0%

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

TABLE 190 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	42.5	48.0	53.8	59.8	65.8	71.5	11.0%
Threat Mitigation Systems	36.1	40.6	45.3	50.2	54.9	59.4	10.5%
Botnet Detection & Management	28.5	32.4	36.5	40.9	45.2	49.3	11.6%
Other Solution Types	19.6	21.9	24.2	26.6	28.8	30.9	9.5%
Total	126.7	142.8	159.9	177.4	194.8	211.1	10.7%

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

TABLE 191 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	46.3	52.8	60.8	69.5	79.0	89.0	14.0%
Application Security	51.8	60.0	70.1	81.6	94.1	107.8	15.8%
Endpoint Security	16.6	19.0	21.9	25.2	28.7	32.4	14.3%
Cloud Security	19.1	22.1	25.7	29.7	34.1	38.9	15.2%
Total	133.9	153.9	178.5	206.0	235.8	268.1	14.9%

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

TABLE 192 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	99.8	111.5	123.7	135.9	147.8	158.7	9.7%
Application Security	122.8	139.3	157.0	175.4	193.8	211.4	11.5%
Endpoint Security	36.5	40.9	45.5	50.3	54.9	59.1	10.1%
Cloud Security	44.1	49.8	55.9	62.1	68.3	74.2	11.0%
Total	303.3	341.5	382.1	423.8	464.9	503.4	10.7%

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

TABLE 193 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	57.2	65.4	75.5	86.7	98.8	111.8	14.4%
Cloud	76.7	88.5	103.0	119.3	137.0	156.3	15.3%
Total	133.9	153.9	178.5	206.0	235.8	268.1	14.9%

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

TABLE 194 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	125.9	141.0	157.0	173.3	189.2	203.9	10.1%
Cloud	177.4	200.4	225.1	250.4	275.7	299.6	11.0%
Total	303.3	341.5	382.1	423.8	464.9	503.4	10.7%

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

TABLE 195 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	44.2	51.4	60.3	70.4	81.6	93.8	16.3%
Large Enterprises	89.7	102.5	118.2	135.5	154.2	174.3	14.2%
Total	133.9	153.9	178.5	206.0	235.8	268.1	14.9%

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

TABLE 196 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	107.4	122.2	138.3	155.1	172.0	188.3	11.9%
Large Enterprises	195.9	219.2	243.8	268.7	292.9	315.2	10.0%
Total	303.3	341.5	382.1	423.8	464.9	503.4	10.7%

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

TABLE 197 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	26.4	31.0	36.7	43.2	50.4	58.5	17.2%
Government & Defense	19.3	21.7	24.6	27.8	31.1	34.6	12.4%
IT & ITeS	10.4	12.0	14.0	16.2	18.6	21.2	15.2%
Telecom	8.6	10.0	11.8	13.8	16.0	18.5	16.6%
Manufacturing	14.6	16.6	19.0	21.7	24.6	27.6	13.6%
Energy and Utilities	6.4	7.2	8.2	9.3	10.5	11.7	12.7%
Healthcare	17.7	20.5	23.9	27.8	32.1	36.7	15.8%
Retail	15.8	18.1	21.0	24.2	27.6	31.4	14.7%
Education	6.7	7.6	8.8	10.1	11.5	13.0	14.2%
Other Verticals	8.0	9.1	10.4	11.9	13.4	15.0	13.3%
Total	133.9	153.9	178.5	206.0	235.8	268.1	14.9%

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

TABLE 198 UK: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	67.4	77.3	88.1	99.5	111.1	122.4	12.7%
Government & Defense	38.2	42.0	45.9	49.6	53.0	55.9	7.9%
IT & ITeS	24.0	27.1	30.4	33.8	37.2	40.4	10.9%
Telecom	21.2	24.2	27.5	30.9	34.4	37.8	12.2%
Manufacturing	30.9	34.4	38.0	41.6	45.1	48.2	9.3%
Energy and Utilities	12.9	14.2	15.6	16.9	18.1	19.2	8.2%
Healthcare	41.9	47.5	53.5	59.7	66.0	72.0	11.5%
Retail	35.4	39.8	44.5	49.2	53.9	58.3	10.5%
Education	14.6	16.4	18.2	20.0	21.8	23.5	10.0%
Other Verticals	16.7	18.6	20.5	22.4	24.2	25.8	9.0%
Total	303.3	341.5	382.1	423.8	464.9	503.4	10.7%

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

15.3.3 GERMANY

15.3.3.1 Increasing investments in DDoS protection and mitigation solutions to drive market

Germany is the second-largest market for DDoS protection and mitigation security in Europe. In June 2021, a DDoS attack disrupted more than 800 financial institutions in Germany. The networks were flooded with high volumes of data traffic. It became a serious issue overnight, shutting down or slowing the websites of cooperative banks nationwide. 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 199 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	52.5	60.3	70.0	80.7	92.2	104.6	14.8%
Software Solutions	62.6	72.4	84.7	98.4	113.3	129.6	15.7%
Services	34.6	40.3	47.6	55.8	64.8	74.8	16.7%
Total	149.7	173.0	202.2	234.8	270.3	308.9	15.6%

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

TABLE 200 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	118.0	132.6	148.1	163.8	179.3	193.8	10.4%
Software Solutions	147.4	167.0	188.0	209.8	231.6	252.4	11.3%
Services	85.8	98.0	111.2	125.1	139.2	152.9	12.3%
Total	351.2	397.6	447.3	498.7	550.1	599.1	11.3%

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

TABLE 201 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	20.0	23.0	26.8	30.9	35.4	40.2	15.0%
Intrusion Detection & Prevention Systems	14.1	16.1	18.5	21.2	24.0	27.0	13.9%
Load Balancers	10.0	11.6	13.6	15.8	18.2	20.9	15.9%
Other Hardware Solutions	8.4	9.6	11.1	12.8	14.6	16.5	14.4%
Total	52.5	60.3	70.0	80.7	92.2	104.6	14.8%

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

TABLE 202 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	45.5	51.2	57.2	63.5	69.6	75.3	10.6%
Intrusion Detection & Prevention Systems	30.3	33.7	37.3	41.0	44.5	47.7	9.5%
Load Balancers	23.8	27.0	30.4	33.9	37.5	40.9	11.5%
Other Hardware Solutions	18.5	20.8	23.1	25.5	27.8	29.9	10.1%
Total	118.0	132.6	148.1	163.8	179.3	193.8	10.4%

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

TABLE 203 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	21.4	25.0	29.4	34.3	39.8	45.8	16.4%
Managed Services	13.1	15.4	18.2	21.5	25.0	29.0	17.1%
Total	34.6	40.3	47.6	55.8	64.8	74.8	16.7%

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

TABLE 204 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	52.4	59.7	67.6	75.9	84.2	92.3	12.0%
Managed Services	33.4	38.3	43.6	49.2	55.0	60.6	12.7%
Total	85.8	98.0	111.2	125.1	139.2	152.9	12.3%

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

TABLE 205 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	6.8	7.9	9.3	10.8	12.4	14.2	15.8%
Consulting and Advisory	5.7	6.7	8.0	9.4	11.0	12.8	17.7%
Training and Education	4.4	5.2	6.1	7.2	8.4	9.7	17.0%
Support and Maintenance	4.5	5.2	6.1	7.0	8.0	9.1	15.0%
Total	21.4	25.0	29.4	34.3	39.8	45.8	16.4%

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

TABLE 206 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	16.2	18.4	20.7	23.1	25.5	27.8	11.4%
Consulting and Advisory	14.8	17.1	19.5	22.2	24.8	27.5	13.1%
Training and Education	11.1	12.7	14.5	16.3	18.2	20.0	12.5%
Support and Maintenance	10.3	11.6	12.9	14.3	15.7	16.9	10.5%
Total	52.4	59.7	67.6	75.9	84.2	92.3	12.0%

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

TABLE 207 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	20.6	23.9	28.0	32.6	37.6	43.1	15.9%
Threat Mitigation Systems	17.7	20.4	23.8	27.6	31.7	36.2	15.4%
Botnet Detection & Management	13.1	15.3	18.1	21.2	24.6	28.3	16.6%
Other Solution Types	11.1	12.8	14.8	17.0	19.4	22.0	14.6%
Total	62.6	72.4	84.7	98.4	113.3	129.6	15.7%

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

TABLE 208 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	49.1	55.8	62.9	70.4	77.8	85.0	11.6%
Threat Mitigation Systems	41.1	46.5	52.2	58.1	63.9	69.5	11.1%
Botnet Detection & Management	32.5	37.1	42.0	47.3	52.6	57.7	12.2%
Other Solution Types	24.7	27.7	30.9	34.1	37.3	40.2	10.2%
Total	147.4	167.0	188.0	209.8	231.6	252.4	11.3%

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

TABLE 209 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	51.9	59.5	69.0	79.5	90.8	102.9	14.6%
Application Security	57.9	67.4	79.4	92.9	107.8	124.1	16.5%
Endpoint Security	18.6	21.3	24.8	28.7	32.9	37.4	15.0%
Cloud Security	21.3	24.7	28.9	33.7	38.9	44.6	15.9%
Total	149.7	173.0	202.2	234.8	270.3	308.9	15.6%

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

TABLE 210 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	116.0	130.2	145.2	160.5	175.5	189.4	10.3%
Application Security	142.1	162.1	183.7	206.3	229.2	251.4	12.1%
Endpoint Security	42.3	47.6	53.3	59.2	64.9	70.3	10.7%
Cloud Security	50.8	57.7	65.1	72.8	80.5	87.9	11.6%
Total	351.2	397.6	447.3	498.7	550.1	599.1	11.3%

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

TABLE 211 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	62.7	72.1	83.9	97.0	111.1	126.3	15.0%
Cloud	87.0	100.9	118.3	137.8	159.2	182.6	16.0%
Total	149.7	173.0	202.2	234.8	270.3	308.9	15.6%

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

TABLE 212 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	143.0	161.0	180.3	200.0	219.5	237.8	10.7%
Cloud	208.3	236.6	267.0	298.7	330.6	361.2	11.6%
Total	351.2	397.6	447.3	498.7	550.1	599.1	11.3%

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

TABLE 213 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	53.9	63.0	74.4	87.3	101.6	117.4	16.9%
Large Enterprises	95.8	110.0	127.8	147.5	168.6	191.5	14.9%
Total	149.7	173.0	202.2	234.8	270.3	308.9	15.6%

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

TABLE 214 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	134.9	154.3	175.3	197.5	220.0	242.0	12.4%
Large Enterprises	216.4	243.3	272.0	301.2	330.1	357.0	10.5%
Total	351.2	397.6	447.3	498.7	550.1	599.1	11.3%

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

TABLE 215 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	28.3	33.4	39.9	47.3	55.6	64.9	18.1%
Government & Defense	22.0	24.9	28.5	32.4	36.5	40.8	13.1%
IT & ITeS	11.8	13.7	16.1	18.7	21.6	24.7	15.9%
Telecom	10.9	12.8	15.2	17.8	20.8	24.1	17.1%
Manufacturing	16.6	19.0	22.0	25.2	28.7	32.4	14.3%
Energy and Utilities	7.2	8.1	9.3	10.6	12.0	13.4	13.3%
Healthcare	19.6	22.8	26.9	31.5	36.5	42.0	16.5%
Retail	16.3	18.8	22.0	25.5	29.2	33.4	15.4%
Education	7.2	8.3	9.6	11.1	12.6	14.4	14.9%
Other Verticals	9.7	11.1	12.8	14.7	16.7	18.8	14.1%
Total	149.7	173.0	202.2	234.8	270.3	308.9	15.6%

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

TABLE 216 GERMANY: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	75.2	86.8	99.6	113.1	127.1	140.9	13.4%
Government & Defense	45.3	50.1	55.0	59.8	64.4	68.3	8.6%
IT & ITeS	28.2	32.0	36.1	40.3	44.6	48.6	11.5%
Telecom	27.7	31.8	36.2	40.9	45.7	50.3	12.6%
Manufacturing	36.5	40.8	45.4	50.0	54.5	58.6	10.0%
Energy and Utilities	15.0	16.6	18.2	19.9	21.5	22.8	8.8%
Healthcare	48.1	54.9	62.2	69.8	77.6	85.1	12.1%
Retail	37.9	42.8	48.0	53.5	58.9	64.0	11.1%
Education	16.2	18.2	20.4	22.6	24.8	26.8	10.5%
Other Verticals	21.1	23.6	26.2	28.8	31.4	33.7	9.7%
Total	351.2	397.6	447.3	498.7	550.1	599.1	11.3%

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

15.3.4 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 217 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	113.5	132.7	156.9	184.2	214.5	248.0	16.9%
Software Solutions	137.0	161.5	192.5	227.9	267.6	312.0	17.9%
Services	81.3	96.6	116.1	138.6	164.0	192.7	18.8%
Total	331.8	390.9	465.5	550.7	646.0	752.6	17.8%

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

TABLE 218 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	285.2	326.6	371.8	419.4	468.2	516.0	12.6%
Software Solutions	361.8	417.8	479.6	545.7	614.4	683.0	13.6%
Services	225.2	262.1	303.2	347.6	394.3	441.7	14.4%
Total	872.3	1,006.6	1,154.6	1,312.7	1,476.8	1,640.7	13.5%

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

TABLE 219 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	43.3	50.8	60.1	70.8	82.5	95.6	17.1%
Intrusion Detection & Prevention Systems	29.5	34.2	40.1	46.7	54.0	61.9	16.0%
Load Balancers	22.0	26.0	31.0	36.8	43.2	50.5	18.0%
Other Hardware Solutions	18.6	21.7	25.6	29.9	34.7	40.0	16.6%
Total	113.5	132.7	156.9	184.2	214.5	248.0	16.9%

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

TABLE 220 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	110.2	126.4	144.1	162.9	182.1	201.1	12.8%
Intrusion Detection & Prevention Systems	70.6	80.1	90.4	101.1	111.9	122.2	11.6%
Load Balancers	58.6	67.7	77.8	88.5	99.7	110.9	13.6%
Other Hardware Solutions	45.9	52.4	59.5	66.9	74.4	81.8	12.2%
Total	285.2	326.6	371.8	419.4	468.2	516.0	12.6%

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

TABLE 221 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	52.8	62.7	75.1	89.4	105.6	123.8	18.6%
Managed Services	28.5	34.0	41.0	49.1	58.4	68.9	19.3%
Total	81.3	96.6	116.1	138.6	164.0	192.7	18.8%

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

TABLE 222 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	144.4	167.6	193.4	221.3	250.4	279.8	14.2%
Managed Services	80.9	94.5	109.8	126.4	143.9	161.9	14.9%
Total	225.2	262.1	303.2	347.6	394.3	441.7	14.4%

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

TABLE 223 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	16.6	19.6	23.4	27.8	32.6	38.1	18.0%
Consulting and Advisory	14.0	16.8	20.4	24.5	29.2	34.7	19.9%
Training and Education	10.7	12.7	15.3	18.3	21.8	25.6	19.1%
Support and Maintenance	11.5	13.5	16.0	18.8	22.0	25.4	17.2%
Total	52.8	62.7	75.1	89.4	105.6	123.8	18.6%

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

TABLE 224 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	44.2	51.0	58.6	66.7	75.1	83.5	13.6%
Consulting and Advisory	40.9	47.9	55.9	64.6	73.9	83.4	15.3%
Training and Education	30.0	35.0	40.6	46.7	53.1	59.6	14.7%
Support and Maintenance	29.3	33.6	38.3	43.3	48.3	53.3	12.7%
Total	144.4	167.6	193.4	221.3	250.4	279.8	14.2%

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

TABLE 225 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	45.1	53.3	63.6	75.5	88.8	103.7	18.1%
Threat Mitigation Systems	38.4	45.1	53.6	63.3	74.2	86.3	17.6%
Botnet Detection & Management	29.7	35.3	42.4	50.6	59.9	70.3	18.8%
Other Solution Types	23.8	27.8	32.8	38.5	44.7	51.6	16.7%
Total	137.0	161.5	192.5	227.9	267.6	312.0	17.9%

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

TABLE 226 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	120.6	139.5	160.5	183.0	206.4	230.0	13.8%
Threat Mitigation Systems	99.8	114.9	131.6	149.4	167.7	186.0	13.3%
Botnet Detection & Management	82.2	95.6	110.6	126.8	143.8	161.0	14.4%
Other Solution Types	59.3	67.7	76.9	86.6	96.5	106.1	12.3%
Total	361.8	417.8	479.6	545.7	614.4	683.0	13.6%

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

TABLE 227 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	115.8	135.3	159.9	187.6	218.2	252.1	16.8%
Application Security	128.4	152.4	183.0	218.1	257.8	302.5	18.7%
Endpoint Security	40.8	47.8	56.7	66.7	77.9	90.3	17.2%
Cloud Security	46.8	55.3	66.0	78.3	92.1	107.6	18.1%
Total	331.8	390.9	465.5	550.7	646.0	752.6	17.8%

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

TABLE 228 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	289.8	331.6	377.1	425.1	474.1	522.1	12.5%
Application Security	353.3	410.7	474.5	543.5	615.8	689.1	14.3%
Endpoint Security	104.1	119.6	136.5	154.4	172.8	191.0	12.9%
Cloud Security	125.1	144.7	166.5	189.8	214.1	238.6	13.8%
Total	872.3	1,006.6	1,154.6	1,312.7	1,476.8	1,640.7	13.5%

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

TABLE 229 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	139.7	163.8	194.1	228.6	266.8	309.3	17.2%
Cloud	192.1	227.1	271.4	322.2	379.2	443.3	18.2%
Total	331.8	390.9	465.5	550.7	646.0	752.6	17.8%

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

TABLE 230 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	356.8	409.7	467.6	529.0	592.2	654.7	12.9%
Cloud	515.5	596.9	687.0	783.7	884.6	986.1	13.9%
Total	872.3	1,006.6	1,154.6	1,312.7	1,476.8	1,640.7	13.5%

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

TABLE 231 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	118.5	141.1	169.9	203.2	241.0	283.7	19.1%
Large Enterprises	213.4	249.8	295.6	347.5	405.0	468.9	17.1%
Total	331.8	390.9	465.5	550.7	646.0	752.6	17.8%

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

TABLE 232 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	332.3	387.5	449.1	515.9	586.3	657.9	14.6%
Large Enterprises	539.9	619.1	705.4	796.8	890.5	982.8	12.7%
Total	872.3	1,006.6	1,154.6	1,312.7	1,476.8	1,640.7	13.5%

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

TABLE 233 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	62.0	74.7	91.0	109.9	131.7	156.5	20.3%
Government & Defense	48.1	55.5	64.7	74.9	85.9	97.8	15.3%
IT & ITeS	26.2	31.0	37.0	43.8	51.6	60.2	18.1%
Telecom	24.6	29.3	35.4	42.4	50.4	59.5	19.3%
Manufacturing	36.2	42.1	49.6	58.0	67.3	77.5	16.5%
Energy and Utilities	16.3	18.8	22.0	25.5	29.3	33.5	15.5%
Healthcare	42.5	50.4	60.5	72.1	85.3	100.1	18.7%
Retail	34.8	41.0	48.7	57.5	67.3	78.3	17.6%
Education	17.6	20.6	24.4	28.7	33.5	38.8	17.1%
Other Verticals	23.6	27.4	32.3	37.8	43.8	50.4	16.4%
Total	331.8	390.9	465.5	550.7	646.0	752.6	17.8%

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

TABLE 234 REST OF EUROPE: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	185.1	217.8	254.7	295.1	338.2	382.6	15.6%
Government & Defense	110.8	124.8	139.7	154.9	169.8	183.8	10.7%
IT & ITeS	70.0	80.9	93.1	106.1	119.6	133.2	13.8%
Telecom	69.8	81.5	94.7	109.0	124.1	139.5	14.9%
Manufacturing	88.8	101.3	114.8	128.9	143.3	157.2	12.1%
Energy and Utilities	38.0	43.0	48.3	53.7	59.1	64.2	11.0%
Healthcare	116.9	135.9	157.0	179.8	203.8	228.1	14.3%
Retail	90.5	104.3	119.4	135.5	152.1	168.7	13.3%
Education	44.7	51.2	58.4	66.0	73.8	81.5	12.8%
Other Verticals	57.7	65.8	74.6	83.8	93.0	102.1	12.1%
Total	872.3	1,006.6	1,154.6	1,312.7	1,476.8	1,640.7	13.5%

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 security. 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 cyber-attacks, the data security concerns of businesses in the region have further heightened. According to 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. According to a report by Imperva, Asia Pacific was the target of network DDOS attacks in the first half of 2021, which was 46% of all the attacks.

15.4.1 ASIA PACIFIC: MACROECONOMIC OUTLOOK

- The East Asia and Pacific (EAP) region is expanding at a pace faster than the global average, though still slower than its pre-pandemic performance. According to the World Bank, EAP's growth is expected to moderate to 4.0% in 2025.
- Country-specific forecasts for 2025 include China and Cambodia at 4.0%, Indonesia at 4.7%, Malaysia at 3.9%, Mongolia at 6.3%, Lao PDR at 3.5%, the Philippines at 5.3%, Thailand at 1.6%, and Vietnam at 5.8%.
- Growth among the Pacific Island countries is projected at 2.5%. However, these projections are subject to considerable uncertainty and are expected to be influenced by both global trends and domestic policy decisions.

- In 2025, more accommodative monetary conditions are expected to support the growth activity, resulting in a slight upward growth revision to 4.4% from 4.3% in April. Inflation has retreated in much of the region.

FIGURE 36 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET SNAPSHOT



Source: Interviews with Experts and MarketsandMarkets Analysis

TABLE 235 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	156.8	186.0	223.4	266.9	316.5	373.5	19.0%
Software Solutions	187.2	223.9	271.1	326.4	390.2	464.3	19.9%
Services	103.9	125.4	153.1	185.9	224.2	268.9	20.9%
Total	447.9	535.4	647.7	779.3	930.9	1,106.8	19.8%

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

TABLE 236 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	438.7	513.3	597.1	688.9	786.9	888.1	15.1%
Software Solutions	549.8	648.5	760.7	885.0	1,019.3	1,160.2	16.1%
Services	321.1	381.9	451.7	529.7	615.0	705.5	17.0%
Total	1,309.7	1,543.8	1,809.5	2,103.6	2,421.2	2,753.8	16.0%

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

TABLE 237 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	59.9	71.2	85.7	102.5	121.8	144.0	19.2%
Intrusion Detection & Prevention Systems	41.4	48.7	58.1	68.8	80.9	94.7	18.0%
Load Balancers	30.6	36.6	44.4	53.6	64.1	76.4	20.1%
Other Hardware Solutions	24.9	29.5	35.3	42.0	49.7	58.5	18.6%
Total	156.8	186.0	223.4	266.9	316.5	373.5	19.0%

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

TABLE 238 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	169.4	198.6	231.5	267.5	306.1	346.1	15.4%
Intrusion Detection & Prevention Systems	110.3	128.0	147.6	168.9	191.2	213.9	14.2%
Load Balancers	90.6	106.9	125.5	146.1	168.4	191.7	16.2%
Other Hardware Solutions	68.4	79.8	92.6	106.4	121.2	136.3	14.8%
Total	438.7	513.3	597.1	688.9	786.9	888.1	15.1%

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

TABLE 239 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	64.4	77.5	94.5	114.4	137.6	164.7	20.7%
Managed Services	39.5	47.8	58.6	71.5	86.5	104.2	21.4%
Total	103.9	125.4	153.1	185.9	224.2	268.9	20.9%

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

TABLE 240 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	196.2	232.8	274.6	321.3	372.1	425.8	16.8%
Managed Services	124.9	149.1	177.0	208.4	242.9	279.7	17.5%
Total	321.1	381.9	451.7	529.7	615.0	705.5	17.0%

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

TABLE 241 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	20.3	24.3	29.5	35.5	42.5	50.7	20.1%
Consulting and Advisory	17.0	20.7	25.5	31.2	38.0	46.0	22.0%
Training and Education	13.1	15.8	19.4	23.6	28.5	34.3	21.2%
Support and Maintenance	14.0	16.7	20.1	24.1	28.6	33.9	19.2%
Total	64.4	77.5	94.5	114.4	137.6	164.7	20.7%

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

TABLE 242 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	60.0	70.9	83.2	96.9	111.6	127.1	16.2%
Consulting and Advisory	55.3	66.3	79.1	93.5	109.4	126.5	18.0%
Training and Education	41.0	48.9	57.9	68.1	79.3	91.1	17.3%
Support and Maintenance	39.8	46.7	54.4	62.8	71.8	81.1	15.3%
Total	196.2	232.8	274.6	321.3	372.1	425.8	16.8%

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

TABLE 243 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	62.5	75.0	90.9	109.7	131.4	156.7	20.2%
Threat Mitigation Systems	52.4	62.5	75.5	90.7	108.2	128.4	19.6%
Botnet Detection & Management	39.9	48.1	58.7	71.2	85.8	102.8	20.9%
Other Solution Types	32.4	38.4	46.0	54.8	64.9	76.4	18.7%
Total	187.2	223.9	271.1	326.4	390.2	464.3	19.9%

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

TABLE 244 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	185.9	219.8	258.3	301.2	347.6	396.4	16.3%
Threat Mitigation Systems	151.6	178.4	208.7	242.2	278.3	315.9	15.8%
Botnet Detection & Management	122.7	145.9	172.4	202.0	234.4	268.8	17.0%
Other Solution Types	89.5	104.5	121.3	139.6	159.0	179.0	14.9%
Total	549.8	648.5	760.7	885.0	1,019.3	1,160.2	16.1%

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

TABLE 245 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	155.0	183.7	220.5	263.1	311.7	367.4	18.8%
Application Security	173.3	208.8	254.5	308.6	371.4	444.9	20.7%
Endpoint Security	55.1	65.5	78.9	94.4	112.3	132.8	19.2%
Cloud Security	64.5	77.3	93.8	113.1	135.5	161.6	20.2%
Total	447.9	535.4	647.7	779.3	930.9	1,106.8	19.8%

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

TABLE 246 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	431.1	503.9	585.6	674.8	769.9	868.0	15.0%
Application Security	530.4	629.9	743.7	870.9	1,009.6	1,156.6	16.9%
Endpoint Security	156.4	183.4	213.9	247.4	283.3	320.5	15.4%
Cloud Security	191.7	226.6	266.4	310.5	358.3	408.7	16.3%
Total	1,309.7	1,543.8	1,809.5	2,103.6	2,421.2	2,753.8	16.0%

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

TABLE 247 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	190.3	226.5	272.7	326.5	388.2	459.3	19.3%
Cloud	257.5	308.9	375.0	452.8	542.7	647.4	20.2%
Total	447.9	535.4	647.7	779.3	930.9	1,106.8	19.8%

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

TABLE 248 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	540.9	634.5	740.1	856.2	980.6	1,109.8	15.5%
Cloud	768.8	909.3	1,069.4	1,247.5	1,440.6	1,644.0	16.4%
Total	1,309.7	1,543.8	1,809.5	2,103.6	2,421.2	2,753.8	16.0%

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

TABLE 249 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	154.1	186.3	228.0	277.4	335.1	402.9	21.2%
Large Enterprises	293.8	349.1	419.7	501.8	595.8	703.9	19.1%
Total	447.9	535.4	647.7	779.3	930.9	1,106.8	19.8%

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

TABLE 250 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	482.0	574.3	680.4	799.4	929.7	1,068.5	17.3%
Large Enterprises	827.7	969.5	1,129.1	1,304.3	1,491.5	1,685.3	15.3%
Total	1,309.7	1,543.8	1,809.5	2,103.6	2,421.2	2,753.8	16.0%

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

TABLE 251 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	82.9	101.3	125.3	154.0	187.8	228.0	22.4%
Government & Defense	63.6	74.4	88.1	103.6	121.0	140.6	17.2%
IT & ITeS	36.3	43.5	52.7	63.6	76.1	90.8	20.1%
Telecom	32.7	39.6	48.6	59.2	71.7	86.3	21.4%
Manufacturing	49.3	58.2	69.7	82.9	97.9	115.1	18.5%
Energy and Utilities	25.5	30.0	35.8	42.3	49.7	58.1	17.9%
Healthcare	58.2	70.1	85.5	103.6	124.7	149.4	20.7%
Retail	52.8	63.1	76.2	91.5	109.1	129.5	19.6%
Education	18.8	22.3	26.8	32.0	38.0	44.8	19.0%
Other Verticals	27.8	32.8	39.1	46.4	54.7	64.2	18.2%
Total	447.9	535.4	647.7	779.3	930.9	1,106.8	19.8%

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

TABLE 252 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	275.3	331.0	395.6	468.7	549.6	636.7	18.3%
Government & Defense	162.4	186.8	213.5	241.9	271.2	300.2	13.1%
IT & ITeS	107.7	127.2	149.5	174.2	201.0	229.1	16.3%
Telecom	103.5	123.5	146.6	172.5	201.0	231.3	17.5%
Manufacturing	134.6	156.8	181.7	208.7	237.3	266.6	14.6%
Energy and Utilities	67.6	78.3	90.1	102.9	116.2	129.7	13.9%
Healthcare	178.1	211.5	249.7	292.4	339.0	388.3	16.9%
Retail	153.0	180.0	210.6	244.4	280.9	318.9	15.8%
Education	52.6	61.6	71.7	82.7	94.4	106.6	15.1%
Other Verticals	74.9	87.1	100.6	115.3	130.7	146.5	14.4%
Total	1,309.7	1,543.8	1,809.5	2,103.6	2,421.2	2,753.8	16.0%

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

TABLE 253 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)

Country	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
China	159.8	187.1	221.7	261.1	305.3	355.0	17.3%
India	68.7	84.6	105.3	130.4	160.2	195.9	23.3%
Japan	39.9	48.6	60.0	73.6	89.7	108.7	22.2%
Rest of Asia Pacific	179.5	215.1	260.7	314.1	375.7	447.1	20.0%
Total	447.9	535.4	647.7	779.3	930.9	1,106.8	19.8%

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

TABLE 254 ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)

Country	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
China	410.8	473.2	541.8	615.0	690.6	765.9	13.3%
India	238.4	289.0	348.2	416.1	492.3	575.5	19.3%
Japan	131.1	157.4	188.0	222.6	260.8	302.1	18.2%
Rest of Asia Pacific	529.4	624.1	731.5	850.0	977.5	1,110.4	16.0%
Total	1,309.7	1,543.8	1,809.5	2,103.6	2,421.2	2,753.8	16.0%

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

15.4.2 CHINA

15.4.2.1 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 Services 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 255 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	58.1	67.6	79.6	93.1	108.1	124.8	16.5%
Software Solutions	64.4	75.4	89.5	105.5	123.4	143.6	17.4%
Services	37.2	44.0	52.6	62.6	73.8	86.6	18.4%
Total	159.8	187.1	221.7	261.1	305.3	355.0	17.3%

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

TABLE 256 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	143.4	164.0	186.4	210.0	234.1	257.7	12.4%
Software Solutions	166.3	191.7	219.7	249.5	280.4	311.2	13.4%
Services	101.1	117.5	135.8	155.5	176.1	197.0	14.3%
Total	410.8	473.2	541.8	615.0	690.6	765.9	13.3%

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

TABLE 257 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	22.8	26.6	31.3	36.7	42.7	49.4	16.7%
Intrusion Detection & Prevention Systems	15.3	17.6	20.6	23.9	27.5	31.5	15.6%
Load Balancers	11.5	13.5	16.0	18.9	22.1	25.8	17.6%
Other Hardware Solutions	8.6	10.0	11.7	13.6	15.8	18.2	16.1%
Total	58.1	67.6	79.6	93.1	108.1	124.8	16.5%

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

TABLE 258 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	56.8	65.1	74.1	83.6	93.4	103.0	12.6%
Intrusion Detection & Prevention Systems	35.9	40.7	45.9	51.3	56.7	61.8	11.5%
Load Balancers	29.9	34.5	39.6	45.0	50.6	56.2	13.5%
Other Hardware Solutions	20.8	23.7	26.8	30.1	33.5	36.7	12.1%
Total	143.4	164.0	186.4	210.0	234.1	257.7	12.4%

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

TABLE 259 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	26.1	30.7	36.7	43.5	51.2	60.0	18.2%
Managed Services	11.2	13.3	15.9	19.1	22.6	26.6	19.0%
Total	37.2	44.0	52.6	62.6	73.8	86.6	18.4%

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

TABLE 260 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	69.9	81.0	93.4	106.7	120.6	134.6	14.0%
Managed Services	31.2	36.5	42.4	48.7	55.5	62.3	14.8%
Total	101.1	117.5	135.8	155.5	176.1	197.0	14.3%

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

TABLE 261 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	7.9	9.3	11.1	13.1	15.3	17.8	17.6%
Consulting and Advisory	7.1	8.5	10.2	12.3	14.6	17.3	19.4%
Training and Education	5.1	6.1	7.3	8.7	10.2	12.1	18.7%
Support and Maintenance	5.9	6.9	8.1	9.5	11.1	12.8	16.8%
Total	26.1	30.7	36.7	43.5	51.2	60.0	18.2%

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

TABLE 262 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	20.7	23.9	27.4	31.1	35.0	38.8	13.4%
Consulting and Advisory	20.3	23.8	27.7	32.0	36.6	41.2	15.2%
Training and Education	14.1	16.5	19.1	21.9	24.9	27.9	14.6%
Support and Maintenance	14.7	16.9	19.2	21.7	24.2	26.7	12.6%
Total	69.9	81.0	93.4	106.7	120.6	134.6	14.0%

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

TABLE 263 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	22.0	25.9	30.7	36.3	42.5	49.6	17.6%
Threat Mitigation Systems	19.0	22.2	26.3	30.9	36.1	41.9	17.1%
Botnet Detection & Management	13.8	16.3	19.5	23.2	27.4	32.1	18.3%
Other Solution Types	9.5	11.0	12.9	15.1	17.4	20.0	16.0%
Total	64.4	75.4	89.5	105.5	123.4	143.6	17.4%

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

TABLE 264 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	57.6	66.5	76.4	86.9	97.9	108.8	13.6%
Threat Mitigation Systems	48.4	55.6	63.6	72.0	80.8	89.4	13.1%
Botnet Detection & Management	37.4	43.5	50.2	57.5	65.0	72.7	14.2%
Other Solution Types	22.9	26.1	29.5	33.1	36.7	40.2	11.9%
Total	166.3	191.7	219.7	249.5	280.4	311.2	13.4%

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

TABLE 265 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	56.4	65.5	77.0	90.0	104.3	120.4	16.4%
Application Security	61.4	72.5	86.5	102.7	121.0	141.8	18.2%
Endpoint Security	16.5	19.2	22.6	26.4	30.7	35.5	16.6%
Cloud Security	25.5	29.9	35.6	42.0	49.2	57.4	17.6%
Total	159.8	187.1	221.7	261.1	305.3	355.0	17.3%

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

TABLE 266 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	138.1	157.8	179.1	201.6	224.4	246.8	12.3%
Application Security	165.3	191.8	221.2	252.9	286.1	319.6	14.1%
Endpoint Security	40.8	46.8	53.2	60.0	67.0	73.8	12.6%
Cloud Security	66.6	76.9	88.3	100.4	113.1	125.7	13.5%
Total	410.8	473.2	541.8	615.0	690.6	765.9	13.3%

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

TABLE 267 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	70.3	81.9	96.7	113.3	131.9	152.7	16.8%
Cloud	89.5	105.1	125.0	147.8	173.4	202.4	17.7%
Total	159.8	187.1	221.7	261.1	305.3	355.0	17.3%

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

TABLE 268 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	175.8	201.6	229.7	259.5	290.1	320.1	12.7%
Cloud	235.0	271.6	312.1	355.4	400.6	445.7	13.7%
Total	410.8	473.2	541.8	615.0	690.6	765.9	13.3%

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

TABLE 269 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	54.3	64.4	77.1	91.9	108.7	127.8	18.7%
Large Enterprises	105.4	122.7	144.5	169.2	196.6	227.2	16.6%
Total	159.8	187.1	221.7	261.1	305.3	355.0	17.3%

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

TABLE 270 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	149.5	174.1	201.6	231.2	262.4	294.1	14.5%
Large Enterprises	261.2	299.1	340.3	383.7	428.2	471.8	12.5%
Total	410.8	473.2	541.8	615.0	690.6	765.9	13.3%

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

TABLE 271 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	29.9	35.8	43.3	52.1	62.2	73.8	19.8%
Government & Defense	23.6	27.1	31.5	36.3	41.5	47.2	14.8%
IT & ITeS	12.8	15.0	17.8	21.0	24.7	28.8	17.6%
Telecom	11.5	13.7	16.4	19.6	23.2	27.3	18.9%
Manufacturing	17.6	20.4	23.9	27.8	32.1	36.9	16.0%
Energy and Utilities	8.9	10.3	12.0	13.9	16.0	18.3	15.4%
Healthcare	21.2	25.1	29.9	35.5	41.8	49.0	18.2%
Retail	19.5	22.8	27.0	31.7	37.0	43.0	17.1%
Education	6.4	7.4	8.7	10.2	11.8	13.7	16.4%
Other Verticals	8.3	9.6	11.2	13.0	14.9	17.0	15.5%
Total	159.8	187.1	221.7	261.1	305.3	355.0	17.3%

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

TABLE 272 CHINA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	87.2	102.4	119.5	138.2	158.1	178.6	15.4%
Government & Defense	53.4	60.1	67.2	74.4	81.5	88.1	10.5%
IT & ITeS	33.4	38.5	44.2	50.3	56.6	63.0	13.5%
Telecom	32.0	37.4	43.3	49.8	56.6	63.6	14.7%
Manufacturing	42.2	48.1	54.4	61.0	67.7	74.1	11.9%
Energy and Utilities	20.8	23.5	26.4	29.5	32.5	35.3	11.2%
Healthcare	57.1	66.2	76.4	87.3	98.8	110.3	14.1%
Retail	49.6	57.1	65.2	73.9	82.9	91.8	13.1%
Education	15.7	17.9	20.4	22.9	25.6	28.1	12.4%
Other Verticals	19.4	22.0	24.7	27.6	30.4	33.1	11.3%
Total	410.8	473.2	541.8	615.0	690.6	765.9	13.3%

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

15.4.3 JAPAN

15.4.3.1 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 security 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 273 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	13.6	16.5	20.2	24.6	29.8	35.8	21.3%
Software Solutions	16.9	20.7	25.5	31.4	38.2	46.4	22.3%
Services	9.3	11.4	14.2	17.6	21.7	26.5	23.4%
Total	39.9	48.6	60.0	73.6	89.7	108.7	22.2%

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

TABLE 274 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	42.9	51.1	60.5	71.1	82.7	95.0	17.3%
Software Solutions	55.9	67.2	80.3	95.2	111.6	129.4	18.3%
Services	32.3	39.1	47.1	56.3	66.5	77.7	19.2%
Total	131.1	157.4	188.0	222.6	260.8	302.1	18.2%

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

TABLE 275 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	5.3	6.4	7.8	9.6	11.6	13.9	21.5%
Intrusion Detection & Prevention Systems	3.6	4.3	5.2	6.3	7.6	9.0	20.3%
Load Balancers	2.6	3.2	3.9	4.8	5.9	7.1	22.5%
Other Hardware Solutions	2.2	2.6	3.2	3.9	4.7	5.7	20.9%
Total	13.6	16.5	20.2	24.6	29.8	35.8	21.3%

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

TABLE 276 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	16.7	20.0	23.7	27.9	32.5	37.4	17.5%
Intrusion Detection & Prevention Systems	10.7	12.7	14.9	17.4	20.0	22.8	16.3%
Load Balancers	8.6	10.4	12.4	14.7	17.3	20.0	18.3%
Other Hardware Solutions	6.8	8.0	9.5	11.1	12.9	14.8	16.9%
Total	42.9	51.1	60.5	71.1	82.7	95.0	17.3%

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

TABLE 277 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	5.8	7.1	8.8	10.9	13.3	16.2	23.1%
Managed Services	3.5	4.4	5.5	6.8	8.4	10.3	23.8%
Total	9.3	11.4	14.2	17.6	21.7	26.5	23.4%

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

TABLE 278 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	19.7	23.8	28.6	34.1	40.2	46.9	18.9%
Managed Services	12.6	15.3	18.5	22.1	26.3	30.8	19.7%
Total	32.3	39.1	47.1	56.3	66.5	77.7	19.2%

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

TABLE 279 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	1.8	2.2	2.7	3.4	4.1	5.0	22.5%
Consulting and Advisory	1.5	1.9	2.4	3.0	3.7	4.6	24.4%
Training and Education	1.2	1.5	1.8	2.3	2.8	3.5	23.6%
Support and Maintenance	1.2	1.5	1.8	2.2	2.7	3.2	21.6%
Total	5.8	7.1	8.8	10.9	13.3	16.2	23.1%

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

TABLE 280 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	6.0	7.2	8.6	10.3	12.0	13.9	18.3%
Consulting and Advisory	5.6	6.8	8.3	10.0	11.9	14.0	20.1%
Training and Education	4.2	5.1	6.2	7.4	8.8	10.3	19.5%
Support and Maintenance	3.9	4.6	5.5	6.5	7.5	8.7	17.4%
Total	19.7	23.8	28.6	34.1	40.2	46.9	18.9%

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

TABLE 281 JAPAN DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	5.6	6.9	8.5	10.5	12.8	15.6	22.6%
Threat Mitigation Systems	4.8	5.9	7.3	8.9	10.8	13.1	22.0%
Botnet Detection & Management	3.6	4.5	5.6	6.9	8.5	10.4	23.3%
Other Solution Types	2.8	3.4	4.2	5.1	6.1	7.3	21.0%
Total	16.9	20.7	25.5	31.4	38.2	46.4	22.3%

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

TABLE 282 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	18.8	22.7	27.1	32.2	37.8	43.9	18.5%
Threat Mitigation Systems	15.8	18.9	22.5	26.6	31.1	36.0	18.0%
Botnet Detection & Management	12.6	15.3	18.4	21.9	25.9	30.2	19.1%
Other Solution Types	8.8	10.4	12.3	14.4	16.7	19.2	16.9%
Total	55.9	67.2	80.3	95.2	111.6	129.4	18.3%

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

TABLE 283 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	13.6	16.4	20.1	24.4	29.5	35.4	21.2%
Application Security	15.7	19.4	24.1	29.7	36.5	44.6	23.1%
Endpoint Security	4.8	5.9	7.2	8.8	10.6	12.8	21.6%
Cloud Security	5.7	7.0	8.7	10.7	13.1	15.9	22.6%
Total	39.9	48.6	60.0	73.6	89.7	108.7	22.2%

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

TABLE 284 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	42.4	50.4	59.7	70.1	81.4	93.4	17.1%
Application Security	54.1	65.5	78.8	93.9	110.9	129.3	19.0%
Endpoint Security	15.4	18.4	21.8	25.7	30.0	34.6	17.6%
Cloud Security	19.2	23.1	27.7	32.9	38.6	44.8	18.5%
Total	131.1	157.4	188.0	222.6	260.8	302.1	18.2%

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

TABLE 285 JAPAN DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	15.9	19.4	23.8	29.0	35.2	42.4	21.6%
Cloud	23.9	29.3	36.2	44.6	54.5	66.3	22.6%
Total	39.9	48.6	60.0	73.6	89.7	108.7	22.2%

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

TABLE 286 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	50.9	60.8	72.2	85.0	99.1	114.2	17.6%
Cloud	80.2	96.7	115.8	137.5	161.7	187.9	18.6%
Total	131.1	157.4	188.0	222.6	260.8	302.1	18.2%

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

TABLE 287 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	14.0	17.3	21.6	26.8	33.0	40.4	23.6%
Large Enterprises	25.8	31.3	38.4	46.8	56.7	68.3	21.5%
Total	39.9	48.6	60.0	73.6	89.7	108.7	22.2%

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

TABLE 288 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	49.3	59.8	72.2	86.4	102.3	119.6	19.4%
Large Enterprises	81.8	97.6	115.8	136.2	158.6	182.4	17.4%
Total	131.1	157.4	188.0	222.6	260.8	302.1	18.2%

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

TABLE 289 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	7.3	9.1	11.4	14.3	17.8	22.1	24.9%
Government & Defense	5.9	7.1	8.6	10.3	12.3	14.6	19.7%
IT & ITeS	3.2	3.9	4.8	5.9	7.2	8.8	22.5%
Telecom	2.8	3.5	4.4	5.4	6.7	8.3	23.9%
Manufacturing	3.9	4.7	5.7	7.0	8.4	10.0	20.7%
Energy and Utilities	2.0	2.3	2.8	3.4	4.1	4.8	19.9%
Healthcare	5.2	6.4	8.0	9.9	12.1	14.8	23.1%
Retail	4.7	5.8	7.1	8.7	10.6	12.8	22.0%
Education	1.8	2.2	2.7	3.2	3.9	4.7	21.4%
Other Verticals	3.0	3.7	4.5	5.4	6.5	7.8	20.9%
Total	39.9	48.6	60.0	73.6	89.7	108.7	22.2%

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

TABLE 290 JAPAN: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	27.2	33.3	40.5	48.9	58.4	68.9	20.5%
Government & Defense	17.2	20.2	23.5	27.2	31.0	35.0	15.3%
IT & ITeS	10.6	12.8	15.3	18.2	21.4	24.8	18.5%
Telecom	10.1	12.3	14.8	17.8	21.1	24.8	19.7%
Manufacturing	11.9	14.1	16.6	19.4	22.4	25.6	16.6%
Energy and Utilities	5.7	6.7	7.9	9.1	10.4	11.8	15.6%
Healthcare	18.0	21.7	26.1	31.2	36.8	42.9	19.0%
Retail	15.4	18.5	22.1	26.1	30.5	35.3	18.0%
Education	5.7	6.8	8.0	9.4	11.0	12.6	17.3%
Other Verticals	9.3	11.1	13.1	15.3	17.7	20.3	16.8%
Total	131.1	157.4	188.0	222.6	260.8	302.1	18.2%

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

15.4.4 INDIA

15.4.4.1 Increasing DDoS attacks leading to adoption of DDoS protection and mitigation security solutions

India is one of the leading markets for DDoS protection and mitigation security 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 security 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 291 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	22.2	27.1	33.5	41.1	50.1	60.8	22.3%
Software Solutions	30.6	37.7	46.9	58.1	71.5	87.5	23.4%
Services	15.9	19.8	24.9	31.1	38.6	47.6	24.5%
Total	68.7	84.6	105.3	130.4	160.2	195.9	23.3%

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

TABLE 292 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	73.4	88.3	105.5	125.1	146.7	170.1	18.3%
Software Solutions	106.5	129.2	155.8	186.3	220.6	258.0	19.4%
Services	58.5	71.5	86.9	104.8	125.0	147.4	20.3%
Total	238.4	289.0	348.2	416.1	492.3	575.5	19.3%

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

TABLE 293 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	8.6	10.5	13.0	16.0	19.5	23.8	22.6%
Intrusion Detection & Prevention Systems	6.5	7.9	9.6	11.7	14.2	17.1	21.5%
Load Balancers	4.1	5.1	6.3	7.8	9.7	11.8	23.6%
Other Hardware Solutions	3.0	3.7	4.5	5.5	6.7	8.1	21.9%
Total	22.2	27.1	33.5	41.1	50.1	60.8	22.3%

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

TABLE 294 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	28.7	34.6	41.4	49.2	57.8	67.1	18.5%
Intrusion Detection & Prevention Systems	20.5	24.5	29.0	34.2	39.8	45.7	17.4%
Load Balancers	14.4	17.5	21.1	25.3	29.9	35.0	19.4%
Other Hardware Solutions	9.8	11.7	13.9	16.4	19.2	22.2	17.8%
Total	73.4	88.3	105.5	125.1	146.7	170.1	18.3%

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

TABLE 295 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	11.2	13.8	17.3	21.6	26.8	33.0	24.2%
Managed Services	4.8	6.0	7.5	9.5	11.8	14.6	25.1%
Total	15.9	19.8	24.9	31.1	38.6	47.6	24.5%

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

TABLE 296 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	40.4	49.3	59.8	71.9	85.7	100.8	20.1%
Managed Services	18.1	22.2	27.1	32.9	39.4	46.7	20.9%
Total	58.5	71.5	86.9	104.8	125.0	147.4	20.3%

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

TABLE 297 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	3.4	4.1	5.2	6.4	7.9	9.7	23.6%
Consulting and Advisory	3.0	3.8	4.8	6.1	7.6	9.5	25.5%
Training and Education	2.3	2.8	3.6	4.5	5.5	6.9	24.8%
Support and Maintenance	2.5	3.1	3.8	4.7	5.7	7.0	22.8%
Total	11.2	13.8	17.3	21.6	26.8	33.0	24.2%

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

TABLE 298 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	11.8	14.3	17.3	20.7	24.5	28.7	19.4%
Consulting and Advisory	11.7	14.4	17.7	21.5	25.9	30.7	21.3%
Training and Education	8.4	10.4	12.6	15.3	18.2	21.6	20.6%
Support and Maintenance	8.4	10.2	12.2	14.5	17.0	19.8	18.6%
Total	40.4	49.3	59.8	71.9	85.7	100.8	20.1%

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

TABLE 299 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	9.8	12.1	15.1	18.8	23.1	28.4	23.7%
Threat Mitigation Systems	9.0	11.0	13.7	17.0	20.8	25.4	23.1%
Botnet Detection & Management	6.8	8.5	10.6	13.3	16.4	20.3	24.3%
Other Solution Types	5.0	6.0	7.4	9.1	11.1	13.4	22.1%
Total	30.6	37.7	46.9	58.1	71.5	87.5	23.4%

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

TABLE 300 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	34.6	42.1	50.9	61.0	72.3	84.8	19.6%
Threat Mitigation Systems	30.9	37.4	44.9	53.6	63.3	73.9	19.1%
Botnet Detection & Management	24.8	30.4	36.9	44.4	52.9	62.4	20.2%
Other Solution Types	16.2	19.4	23.1	27.3	32.0	37.0	18.0%
Total	106.5	129.2	155.8	186.3	220.6	258.0	19.4%

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

TABLE 301 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	24.0	29.3	36.2	44.4	54.1	65.6	22.3%
Application Security	26.5	32.8	41.2	51.4	63.6	78.4	24.3%
Endpoint Security	8.4	10.3	12.7	15.7	19.2	23.3	22.7%
Cloud Security	9.9	12.2	15.2	18.9	23.3	28.6	23.7%
Total	68.7	84.6	105.3	130.4	160.2	195.9	23.3%

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

TABLE 302 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	79.2	95.2	113.7	134.7	158.0	183.1	18.2%
Application Security	96.1	117.3	142.4	171.5	204.3	240.6	20.1%
Endpoint Security	28.2	34.0	40.8	48.5	57.1	66.4	18.7%
Cloud Security	34.9	42.4	51.3	61.4	72.9	85.4	19.6%
Total	238.4	289.0	348.2	416.1	492.3	575.5	19.3%

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

TABLE 303 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	32.6	39.9	49.5	61.0	74.7	90.9	22.8%
Cloud	36.1	44.7	55.8	69.3	85.5	105.0	23.8%
Total	68.7	84.6	105.3	130.4	160.2	195.9	23.3%

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

TABLE 304 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	110.2	132.9	159.5	189.8	223.5	260.1	18.7%
Cloud	128.3	156.1	188.7	226.4	268.8	315.4	19.7%
Total	238.4	289.0	348.2	416.1	492.3	575.5	19.3%

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

TABLE 305 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	21.6	27.0	34.0	42.6	53.0	65.6	24.8%
Large Enterprises	47.1	57.6	71.3	87.7	107.2	130.3	22.6%
Total	68.7	84.6	105.3	130.4	160.2	195.9	23.3%

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

TABLE 306 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	80.8	99.1	120.8	146.1	174.8	206.6	20.6%
Large Enterprises	157.6	189.9	227.4	270.1	317.5	368.9	18.5%
Total	238.4	289.0	348.2	416.1	492.3	575.5	19.3%

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

TABLE 307 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	12.2	15.4	19.6	24.8	31.2	39.0	26.1%
Government & Defense	9.4	11.3	13.8	16.7	20.0	23.9	20.5%
IT & ITeS	5.7	7.0	8.8	10.9	13.4	16.5	23.6%
Telecom	6.0	7.4	9.4	11.7	14.6	18.0	24.7%
Manufacturing	6.7	8.2	10.1	12.3	14.9	18.0	21.8%
Energy and Utilities	3.3	4.0	4.9	5.9	7.1	8.5	20.9%
Healthcare	8.7	10.8	13.6	16.9	21.0	25.9	24.3%
Retail	8.0	9.9	12.3	15.2	18.6	22.7	23.1%
Education	3.3	4.0	5.0	6.1	7.5	9.1	22.5%
Other Verticals	5.3	6.4	7.9	9.7	11.8	14.3	22.0%
Total	68.7	84.6	105.3	130.4	160.2	195.9	23.3%

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

TABLE 308 INDIA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	48.5	59.9	73.7	89.8	108.3	129.0	21.6%
Government & Defense	28.4	33.5	39.4	45.8	52.7	59.9	16.1%
IT & ITeS	20.1	24.4	29.5	35.3	41.8	49.0	19.6%
Telecom	22.2	27.2	33.1	39.9	47.8	56.4	20.5%
Manufacturing	21.7	25.9	30.8	36.3	42.3	48.8	17.7%
Energy and Utilities	10.2	12.1	14.2	16.6	19.2	21.9	16.6%
Healthcare	31.7	38.7	47.0	56.6	67.4	79.4	20.2%
Retail	27.6	33.4	40.2	47.9	56.6	66.1	19.1%
Education	11.0	13.3	15.9	18.9	22.2	25.7	18.5%
Other Verticals	17.2	20.6	24.6	29.0	34.0	39.2	17.9%
Total	238.4	289.0	348.2	416.1	492.3	575.5	19.3%

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

15.4.5 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 309 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	32.1	38.2	45.9	54.9	65.2	77.0	19.1%
Software Solutions	38.8	46.5	56.5	68.1	81.5	97.0	20.1%
Services	21.5	26.0	31.9	38.8	46.8	56.2	21.1%
Total	92.4	110.7	134.2	161.7	193.4	230.2	20.0%

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

TABLE 310 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	90.5	105.9	123.1	142.0	162.0	182.7	15.1%
Software Solutions	115.0	135.6	159.1	185.0	212.9	242.0	16.1%
Services	67.1	79.8	94.4	110.6	128.3	147.0	17.0%
Total	272.5	321.3	376.6	437.6	503.2	571.7	16.0%

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

TABLE 311 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	12.3	14.7	17.7	21.2	25.2	29.8	19.4%
Intrusion Detection & Prevention Systems	8.6	10.1	12.1	14.3	16.9	19.7	18.2%
Load Balancers	6.2	7.4	9.0	10.9	13.0	15.5	20.3%
Other Hardware Solutions	5.0	6.0	7.2	8.5	10.1	11.9	18.8%
Total	32.1	38.2	45.9	54.9	65.2	77.0	19.1%

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

TABLE 312 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	35.1	41.2	48.0	55.4	63.4	71.5	15.3%
Intrusion Detection & Prevention Systems	23.0	26.7	30.8	35.2	39.9	44.5	14.1%
Load Balancers	18.4	21.7	25.5	29.7	34.2	38.9	16.1%
Other Hardware Solutions	13.9	16.3	18.8	21.7	24.6	27.7	14.7%
Total	90.5	105.9	123.1	142.0	162.0	182.7	15.1%

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

TABLE 313 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	12.9	15.6	19.0	23.1	27.8	33.3	20.8%
Managed Services	8.6	10.5	12.8	15.7	19.0	22.9	21.6%
Total	21.5	26.0	31.9	38.8	46.8	56.2	21.1%

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

TABLE 314 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	39.7	47.1	55.5	64.9	75.1	85.8	16.7%
Managed Services	27.4	32.8	38.9	45.7	53.3	61.2	17.4%
Total	67.1	79.8	94.4	110.6	128.3	147.0	17.0%

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

TABLE 315 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	4.0	4.8	5.9	7.1	8.5	10.1	20.2%
Consulting and Advisory	3.5	4.2	5.2	6.4	7.8	9.5	22.1%
Training and Education	2.7	3.2	4.0	4.8	5.8	7.0	21.4%
Support and Maintenance	2.8	3.3	4.0	4.7	5.6	6.7	19.4%
Total	12.9	15.6	19.0	23.1	27.8	33.3	20.8%

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

TABLE 316 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	12.0	14.2	16.6	19.4	22.3	25.4	16.1%
Consulting and Advisory	11.4	13.6	16.3	19.2	22.4	25.9	17.9%
Training and Education	8.4	10.0	11.9	13.9	16.2	18.6	17.2%
Support and Maintenance	7.9	9.2	10.7	12.4	14.1	15.9	15.2%
Total	39.7	47.1	55.5	64.9	75.1	85.8	16.7%

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

TABLE 317 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	12.6	15.1	18.4	22.2	26.6	31.8	20.4%
Threat Mitigation Systems	10.9	13.0	15.8	19.0	22.7	26.9	19.8%
Botnet Detection & Management	8.2	9.9	12.0	14.6	17.7	21.2	21.1%
Other Solution Types	7.2	8.5	10.3	12.2	14.5	17.1	19.0%
Total	38.8	46.5	56.5	68.1	81.5	97.0	20.1%

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

TABLE 318 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	37.7	44.6	52.4	61.1	70.5	80.3	16.3%
Threat Mitigation Systems	31.8	37.4	43.8	50.8	58.3	66.1	15.8%
Botnet Detection & Management	25.3	30.1	35.6	41.7	48.3	55.3	16.9%
Other Solution Types	20.1	23.5	27.3	31.4	35.8	40.2	14.9%
Total	115.0	135.6	159.1	185.0	212.9	242.0	16.1%

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

TABLE 319 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	31.6	37.6	45.2	54.0	64.0	75.5	19.0%
Application Security	36.1	43.6	53.3	64.7	78.0	93.5	20.9%
Endpoint Security	11.5	13.7	16.5	19.8	23.5	27.9	19.4%
Cloud Security	13.2	15.9	19.3	23.3	28.0	33.4	20.4%
Total	92.4	110.7	134.2	161.7	193.4	230.2	20.0%

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

TABLE 320 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	88.6	103.6	120.4	138.6	158.0	177.9	15.0%
Application Security	111.5	132.4	156.3	182.9	211.9	242.4	16.8%
Endpoint Security	32.8	38.5	44.9	51.9	59.4	67.1	15.4%
Cloud Security	39.6	46.8	55.1	64.2	74.0	84.3	16.3%
Total	272.5	321.3	376.6	437.6	503.2	571.7	16.0%

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

TABLE 321 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	38.1	45.4	54.8	65.7	78.1	92.5	19.4%
Cloud	54.4	65.3	79.5	96.1	115.3	137.7	20.4%
Total	92.4	110.7	134.2	161.7	193.4	230.2	20.0%

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

TABLE 322 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	109.0	127.9	149.1	172.4	197.3	223.0	15.4%
Cloud	163.5	193.4	227.5	265.2	306.0	348.7	16.4%
Total	272.5	321.3	376.6	437.6	503.2	571.7	16.0%

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

TABLE 323 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	32.4	39.2	48.1	58.5	70.8	85.2	21.4%
Large Enterprises	60.1	71.5	86.2	103.2	122.6	145.0	19.3%
Total	92.4	110.7	134.2	161.7	193.4	230.2	20.0%

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

TABLE 324 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	101.9	121.5	143.9	168.9	196.3	225.2	17.2%
Large Enterprises	170.6	199.9	232.7	268.7	307.0	346.4	15.2%
Total	272.5	321.3	376.6	437.6	503.2	571.7	16.0%

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

TABLE 325 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	16.8	20.6	25.6	31.5	38.5	46.7	22.7%
Government & Defense	12.9	15.2	18.0	21.2	24.8	28.8	17.3%
IT & ITeS	7.3	8.8	10.7	12.9	15.4	18.4	20.3%
Telecom	6.4	7.8	9.5	11.6	14.1	17.0	21.7%
Manufacturing	9.7	11.5	13.8	16.4	19.4	22.8	18.6%
Energy and Utilities	5.0	5.9	7.0	8.3	9.7	11.4	17.9%
Healthcare	11.6	14.0	17.0	20.7	25.0	29.9	21.0%
Retail	10.4	12.5	15.1	18.2	21.7	25.8	19.8%
Education	3.7	4.4	5.3	6.3	7.5	8.9	19.1%
Other Verticals	8.6	10.2	12.3	14.7	17.4	20.5	19.0%
Total	92.4	110.7	134.2	161.7	193.4	230.2	20.0%

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

TABLE 326 REST OF ASIA PACIFIC: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	56.5	67.9	81.2	96.2	112.7	130.5	18.2%
Government & Defense	33.2	38.2	43.7	49.4	55.4	61.2	13.0%
IT & ITeS	21.9	25.8	30.4	35.4	40.8	46.4	16.3%
Telecom	20.4	24.4	29.0	34.1	39.8	45.7	17.5%
Manufacturing	26.7	31.0	35.9	41.2	46.8	52.5	14.5%
Energy and Utilities	13.2	15.3	17.6	20.1	22.6	25.2	13.7%
Healthcare	35.7	42.4	50.1	58.6	67.9	77.7	16.8%
Retail	30.5	35.9	42.0	48.7	55.9	63.3	15.8%
Education	10.4	12.2	14.2	16.3	18.6	21.0	15.0%
Other Verticals	24.0	28.1	32.6	37.5	42.8	48.1	14.9%
Total	272.5	321.3	376.6	437.6	503.2	571.7	16.0%

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 security solutions and services, although its DDoS protection and mitigation security 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.

15.5.1 MIDDLE EAST & AFRICA: MACROECONOMIC OUTLOOK

- The global economy is grappling with increased uncertainty, making economic forecasts more difficult. In 2024, growth in the Middle East and North Africa (MENA) region averaged a modest 1.9%. As of April 2025, it is projected to rise moderately to 2.6% in 2025 and 3.7% in 2026. However, these projections remain uncertain due to the potential effects of shifting trade dynamics on global growth, inflation, and oil markets.
- As of April 2025, regional GDP growth is projected to average 2.6% in 2025 and 3.7% in 2026. Oil-exporting countries in the region are expected to benefit from a gradual rise in oil production, while oil-importing countries may see gains driven by robust private consumption and declining inflation. Nonetheless, these forecasts are clouded by significant uncertainty. Risks include global policy unpredictability, weak global demand, oil market volatility, and underlying economic fragility.

- A slowdown in global demand could reduce oil export revenues, putting pressure on the fiscal and external accounts of oil exporters. Meanwhile, oil importers may benefit from lower oil prices, but declines in remittances, weakening consumer confidence, and deteriorating investor sentiment could trigger capital outflows, straining their external balances.
- Heightened trade policy uncertainty can have real effects. It could negatively impact private sector decisions, especially regarding investments, market entry and exit, and productivity.

TABLE 327 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	84.1	98.5	116.5	137.0	159.7	184.9	17.1%
Software Solutions	101.6	119.9	143.1	169.6	199.4	232.8	18.0%
Services	60.9	72.5	87.2	104.2	123.4	145.2	19.0%
Total	246.6	290.9	346.9	410.9	482.6	562.9	17.9%

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

TABLE 328 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	213.0	244.3	278.4	314.6	351.7	390.0	12.9%
Software Solutions	270.4	312.7	359.4	409.6	461.9	516.7	13.8%
Services	170.0	198.1	229.5	263.5	299.4	337.4	14.7%
Total	653.4	755.1	867.4	987.8	1,113.1	1,244.1	13.7%

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

TABLE 329 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	32.6	38.3	45.4	53.5	62.4	72.4	17.3%
Intrusion Detection & Prevention Systems	22.2	25.8	30.3	35.3	40.8	46.9	16.1%
Load Balancers	16.3	19.3	23.1	27.4	32.2	37.6	18.2%
Other Hardware Solutions	13.0	15.1	17.8	20.9	24.3	28.0	16.7%
Total	84.1	98.5	116.5	137.0	159.7	184.9	17.1%

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

TABLE 330 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	83.5	96.0	109.6	124.0	138.9	154.3	13.1%
Intrusion Detection & Prevention Systems	53.5	60.9	68.8	77.1	85.5	94.0	11.9%
Load Balancers	43.7	50.6	58.2	66.4	74.9	83.8	13.9%
Other Hardware Solutions	32.2	36.8	41.8	47.0	52.4	57.9	12.5%
Total	213.0	244.3	278.4	314.6	351.7	390.0	12.9%

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

TABLE 331 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	35.2	41.8	50.1	59.8	70.6	82.9	18.7%
Managed Services	25.7	30.7	37.1	44.4	52.8	62.4	19.4%
Total	60.9	72.5	87.2	104.2	123.4	145.2	19.0%

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

TABLE 332 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	96.7	112.4	129.9	148.8	168.6	189.4	14.4%
Managed Services	73.3	85.7	99.6	114.8	130.8	147.9	15.1%
Total	170.0	198.1	229.5	263.5	299.4	337.4	14.7%

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

TABLE 333 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	10.5	12.4	14.8	17.6	20.7	24.2	18.1%
Consulting and Advisory	9.3	11.2	13.5	16.3	19.5	23.1	20.0%
Training and Education	7.1	8.5	10.2	12.2	14.5	17.2	19.2%
Support and Maintenance	8.3	9.7	11.5	13.6	15.9	18.4	17.4%
Total	35.2	41.8	50.1	59.8	70.6	82.9	18.7%

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

TABLE 334 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	28.1	32.4	37.3	42.5	47.9	53.5	13.8%
Consulting and Advisory	27.3	32.0	37.4	43.3	49.6	56.3	15.6%
Training and Education	20.1	23.5	27.3	31.4	35.7	40.4	14.9%
Support and Maintenance	21.3	24.5	27.9	31.6	35.4	39.3	13.1%
Total	96.7	112.4	129.9	148.8	168.6	189.4	14.4%

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

TABLE 335 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	32.9	38.9	46.6	55.3	65.2	76.2	18.3%
Threat Mitigation Systems	29.9	35.2	41.9	49.5	58.1	67.6	17.7%
Botnet Detection & Management	21.5	25.6	30.8	36.8	43.6	51.3	19.0%
Other Solution Types	17.3	20.2	23.8	28.0	32.5	37.6	16.8%
Total	101.6	119.9	143.1	169.6	199.4	232.8	18.0%

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

TABLE 336 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	88.7	102.8	118.5	135.3	152.9	171.4	14.1%
Threat Mitigation Systems	78.4	90.4	103.7	117.8	132.6	147.9	13.6%
Botnet Detection & Management	60.1	70.0	81.1	93.1	105.8	119.2	14.7%
Other Solution Types	43.2	49.4	56.2	63.4	70.7	78.2	12.6%
Total	270.4	312.7	359.4	409.6	461.9	516.7	13.8%

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

TABLE 337 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	83.4	97.5	115.3	135.4	157.7	182.4	17.0%
Application Security	95.6	113.7	136.6	163.0	192.9	226.8	18.8%
Endpoint Security	30.6	36.0	42.7	50.3	58.8	68.2	17.4%
Cloud Security	37.0	43.7	52.3	62.1	73.2	85.6	18.3%
Total	246.6	290.9	346.9	410.9	482.6	562.9	17.9%

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

TABLE 338 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	209.9	240.4	273.7	309.0	345.0	382.2	12.7%
Application Security	265.1	308.7	357.2	409.7	465.0	523.5	14.6%
Endpoint Security	78.8	90.6	103.6	117.3	131.6	146.3	13.2%
Cloud Security	99.6	115.4	132.9	151.7	171.4	192.1	14.0%
Total	653.4	755.1	867.4	987.8	1,113.1	1,244.1	13.7%

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

TABLE 339 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	101.6	119.3	141.5	166.8	195.0	226.3	17.4%
Cloud	145.0	171.6	205.3	244.0	287.6	336.6	18.3%
Total	246.6	290.9	346.9	410.9	482.6	562.9	17.9%

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

TABLE 340 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	261.3	300.5	343.5	389.2	436.3	485.2	13.2%
Cloud	392.0	454.6	523.9	598.6	676.7	758.9	14.1%
Total	653.4	755.1	867.4	987.8	1,113.1	1,244.1	13.7%

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

TABLE 341 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	84.6	100.9	121.7	145.9	173.2	204.3	19.3%
Large Enterprises	162.0	189.9	225.1	265.0	309.3	358.6	17.2%
Total	246.6	290.9	346.9	410.9	482.6	562.9	17.9%

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

TABLE 342 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	239.8	280.1	325.3	374.4	426.3	481.4	15.0%
Large Enterprises	413.6	474.9	542.1	613.4	686.8	762.6	13.0%
Total	653.4	755.1	867.4	987.8	1,113.1	1,244.1	13.7%

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

TABLE 343 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	46.1	55.6	67.8	82.0	98.3	117.1	20.5%
Government & Defense	36.0	41.6	48.6	56.3	64.7	73.7	15.4%
IT & ITeS	18.7	22.2	26.5	31.5	37.1	43.3	18.3%
Telecom	17.3	20.7	25.0	30.0	35.7	42.2	19.6%
Manufacturing	24.4	28.4	33.5	39.2	45.5	52.4	16.5%
Energy and Utilities	14.8	17.2	20.2	23.5	27.2	31.2	16.1%
Healthcare	31.3	37.2	44.7	53.4	63.2	74.3	18.9%
Retail	24.7	29.0	34.5	40.8	47.9	55.7	17.7%
Education	9.9	11.5	13.7	16.1	18.7	21.7	17.0%
Other Verticals	23.4	27.4	32.4	38.0	44.3	51.2	16.9%
Total	246.6	290.9	346.9	410.9	482.6	562.9	17.9%

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

TABLE 344 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	138.6	163.4	191.3	222.0	254.9	290.1	15.9%
Government & Defense	83.6	94.4	105.8	117.5	129.1	140.6	10.9%
IT & ITeS	50.4	58.4	67.3	76.8	86.8	97.3	14.0%
Telecom	49.7	58.1	67.7	78.0	89.0	100.8	15.2%
Manufacturing	60.0	68.4	77.5	87.1	96.8	106.7	12.2%
Energy and Utilities	35.7	40.5	45.8	51.3	56.8	62.3	11.8%
Healthcare	86.9	101.2	117.1	134.3	152.5	171.7	14.6%
Retail	64.6	74.5	85.4	97.0	109.1	121.7	13.5%
Education	25.0	28.6	32.6	36.8	41.2	45.7	12.8%
Other Verticals	58.9	67.5	76.9	86.7	96.8	107.2	12.7%
Total	653.4	755.1	867.4	987.8	1,113.1	1,244.1	13.7%

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

TABLE 345 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)

Country	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
GCC Countries	143.8	169.8	202.8	240.5	282.8	330.4	18.1%
South Africa	22.9	27.4	33.1	39.7	47.3	55.9	19.5%
Rest of Middle East & Africa	79.9	93.7	111.0	130.6	152.4	176.7	17.2%
Total	246.6	290.9	346.9	410.9	482.6	562.9	17.9%

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

TABLE 346 MIDDLE EAST & AFRICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)

Country	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
GCC Countries	383.9	444.3	511.0	582.6	657.3	732.4	13.8%
South Africa	65.7	77.0	89.6	103.4	118.1	134.5	15.4%
Rest of Middle East & Africa	203.7	233.9	266.8	301.8	337.7	377.2	13.1%
Total	653.4	755.1	867.4	987.8	1,113.1	1,244.1	13.7%

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

15.5.2 KSA

15.5.2.1 Increasing investments in mitigation security 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 security 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 e-commerce, 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 347 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	22.8	26.8	31.9	37.7	44.2	51.5	17.7%
Software Solutions	27.5	32.6	39.2	46.7	55.2	64.7	18.7%
Services	16.3	19.5	23.6	28.4	33.8	40.0	19.6%
Total	66.6	79.0	94.7	112.8	133.2	156.2	18.6%

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

TABLE 348 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	59.6	68.7	78.8	89.5	100.6	111.7	13.4%
Software Solutions	75.6	87.9	101.6	116.4	132.0	147.8	14.4%
Services	47.1	55.2	64.2	74.2	84.7	95.6	15.2%
Total	182.3	211.8	244.6	280.1	317.4	355.1	14.3%

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

TABLE 349 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	8.9	10.4	12.5	14.8	17.3	20.2	17.9%
Intrusion Detection & Prevention Systems	6.0	7.0	8.3	9.7	11.3	13.0	16.8%
Load Balancers	4.4	5.3	6.3	7.6	9.0	10.5	18.8%
Other Hardware Solutions	3.5	4.1	4.8	5.7	6.7	7.7	17.3%
Total	22.8	26.8	31.9	37.7	44.2	51.5	17.7%

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

TABLE 350 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	23.4	27.1	31.1	35.4	39.8	44.3	13.6%
Intrusion Detection & Prevention Systems	14.9	17.1	19.4	21.8	24.3	26.8	12.4%
Load Balancers	12.3	14.3	16.6	19.0	21.5	24.1	14.4%
Other Hardware Solutions	8.9	10.3	11.7	13.3	14.9	16.5	13.0%
Total	59.6	68.7	78.8	89.5	100.6	111.7	13.4%

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

TABLE 351 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	9.5	11.3	13.6	16.3	19.4	22.9	19.3%
Managed Services	6.9	8.2	10.0	12.0	14.4	17.1	20.1%
Total	16.3	19.5	23.6	28.4	33.8	40.0	19.6%

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

TABLE 352 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	26.9	31.4	36.5	42.0	47.9	53.9	14.9%
Managed Services	20.2	23.7	27.8	32.2	36.9	41.7	15.6%
Total	47.1	55.2	64.2	74.2	84.7	95.6	15.2%

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

TABLE 353 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	2.9	3.5	4.2	5.0	5.9	6.9	18.7%
Consulting and Advisory	2.5	3.0	3.7	4.4	5.3	6.4	20.7%
Training and Education	1.9	2.3	2.8	3.4	4.0	4.8	19.9%
Support and Maintenance	2.1	2.5	3.0	3.5	4.2	4.8	18.0%
Total	9.5	11.3	13.6	16.3	19.4	22.9	19.3%

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

TABLE 354 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	8.1	9.4	10.9	12.5	14.1	15.8	14.3%
Consulting and Advisory	7.6	8.9	10.5	12.2	14.0	15.9	16.1%
Training and Education	5.6	6.6	7.7	8.9	10.2	11.5	15.5%
Support and Maintenance	5.6	6.5	7.4	8.5	9.5	10.6	13.5%
Total	26.9	31.4	36.5	42.0	47.9	53.9	14.9%

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

TABLE 355 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	8.9	10.6	12.8	15.3	18.1	21.3	18.9%
Threat Mitigation Systems	8.0	9.5	11.4	13.5	16.0	18.7	18.4%
Botnet Detection & Management	5.9	7.0	8.5	10.2	12.2	14.4	19.6%
Other Solution Types	4.6	5.5	6.5	7.6	8.9	10.4	17.5%
Total	27.5	32.6	39.2	46.7	55.2	64.7	18.7%

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

TABLE 356 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	24.9	29.0	33.6	38.6	43.8	49.2	14.6%
Threat Mitigation Systems	21.8	25.2	29.1	33.3	37.6	42.0	14.1%
Botnet Detection & Management	17.0	19.9	23.1	26.7	30.5	34.4	15.2%
Other Solution Types	12.0	13.8	15.8	17.9	20.1	22.2	13.1%
Total	75.6	87.9	101.6	116.4	132.0	147.8	14.4%

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

TABLE 357 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	22.6	26.6	31.7	37.4	43.8	50.9	17.6%
Application Security	25.7	30.7	37.1	44.5	53.0	62.6	19.5%
Endpoint Security	8.2	9.7	11.5	13.7	16.1	18.7	18.0%
Cloud Security	10.1	12.0	14.4	17.2	20.3	23.9	18.9%
Total	66.6	79.0	94.7	112.8	133.2	156.2	18.6%

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

TABLE 358 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	58.9	67.9	77.7	88.2	99.0	109.8	13.3%
Application Security	73.6	86.2	100.3	115.7	132.0	148.8	15.1%
Endpoint Security	21.8	25.2	28.9	32.9	37.1	41.3	13.7%
Cloud Security	28.0	32.6	37.7	43.3	49.2	55.2	14.6%
Total	182.3	211.8	244.6	280.1	317.4	355.1	14.3%

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

TABLE 359 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	27.8	32.8	39.1	46.3	54.5	63.6	18.0%
Cloud	38.8	46.2	55.6	66.4	78.7	92.6	19.0%
Total	66.6	79.0	94.7	112.8	133.2	156.2	18.6%

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

TABLE 360 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	73.8	85.4	98.1	111.8	126.0	140.3	13.7%
Cloud	108.5	126.5	146.5	168.4	191.4	214.9	14.7%
Total	182.3	211.8	244.6	280.1	317.4	355.1	14.3%

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

TABLE 361 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	22.8	27.4	33.2	40.0	47.8	56.7	19.9%
Large Enterprises	43.7	51.6	61.4	72.7	85.4	99.5	17.9%
Total	66.6	79.0	94.7	112.8	133.2	156.2	18.6%

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

TABLE 362 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	66.9	78.6	91.7	106.2	121.6	137.4	15.5%
Large Enterprises	115.4	133.2	152.9	174.0	195.8	217.7	13.5%
Total	182.3	211.8	244.6	280.1	317.4	355.1	14.3%

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

TABLE 363 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	12.4	15.1	18.5	22.5	27.1	32.5	21.1%
Government & Defense	9.8	11.4	13.3	15.6	18.0	20.6	16.1%
IT & ITeS	5.3	6.3	7.5	9.0	10.6	12.5	18.9%
Telecom	4.9	5.8	7.1	8.6	10.3	12.2	20.2%
Manufacturing	6.5	7.6	9.0	10.5	12.3	14.2	17.1%
Energy and Utilities	4.0	4.7	5.5	6.5	7.5	8.7	16.8%
Healthcare	8.8	10.5	12.7	15.2	18.1	21.4	19.5%
Retail	7.0	8.3	9.9	11.8	13.9	16.2	18.4%
Education	2.5	3.0	3.5	4.2	4.9	5.7	17.6%
Other Verticals	5.5	6.4	7.6	9.0	10.5	12.2	17.4%
Total	66.6	79.0	94.7	112.8	133.2	156.2	18.6%

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

TABLE 364 KSA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	38.7	45.8	54.0	63.0	72.7	82.8	16.4%
Government & Defense	23.5	26.7	30.1	33.6	37.1	40.5	11.5%
IT & ITeS	14.6	17.0	19.7	22.6	25.7	28.8	14.6%
Telecom	14.4	16.9	19.8	23.0	26.3	29.8	15.7%
Manufacturing	16.4	18.8	21.4	24.1	27.0	29.8	12.7%
Energy and Utilities	10.0	11.4	12.9	14.5	16.2	17.8	12.3%
Healthcare	25.2	29.4	34.3	39.5	45.1	50.8	15.1%
Retail	18.9	21.9	25.3	28.9	32.7	36.5	14.0%
Education	6.6	7.6	8.7	9.9	11.1	12.3	13.3%
Other Verticals	14.1	16.2	18.5	21.0	23.5	26.0	13.1%
Total	182.3	211.8	244.6	280.1	317.4	355.1	14.3%

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

15.5.3 UAE

15.5.3.1 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 security. The DDoS protection and mitigation security 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.

15.5.4 SOUTH AFRICA

15.5.4.1 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 security 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.

15.5.5 REST OF MIDDLE EAST & AFRICA

Israel, Turkey, and the remaining countries are considered in the rest of Middle East & Africa. The DDoS protection & mitigation security 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.

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, cyber-attacks, misuse due to unauthorized access, and theft-related losses has driven the adoption of DDoS protection and mitigation solutions in 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 security 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.

15.6.1 LATIN AMERICA: MACROECONOMIC OUTLOOK

- The economic growth in the Latin American and Caribbean (LAC) region is expected to be 2.1% in 2025 and 2.4% in 2026, making it the slowest-growing region worldwide. Low investment, high debt, and a shifting external environment pose significant barriers to the region's development.
- Brazil's growth is expected to moderate to 2.2% in 2025 and to converge to 2.3% in the medium term, reflecting the effect of past and ongoing structural reforms. Inflation is projected to gradually converge toward 3.8% by 2025, within the Central Bank's target range. However, a recent deterioration of inflation expectations is expected to slow the pace of the monetary easing, which is expected to contribute to moderate growth.
- According to a report by the IMF, headline inflation in the region was expected to end 2024 at 4.3%, then fall further to 3.4% in 2025. Core inflation also continues to decline, currently standing at 4%.

TABLE 365 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	35.6	41.6	49.2	57.8	67.2	77.8	16.9%
Software Solutions	41.8	49.3	58.8	69.6	81.7	95.2	17.9%
Services	26.6	31.6	38.0	45.3	53.6	63.0	18.8%
Total	104.0	122.5	145.9	172.7	202.6	236.0	17.8%

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

TABLE 366 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	89.5	102.5	116.7	131.7	147.2	162.9	12.7%
Software Solutions	110.5	127.6	146.6	166.9	188.0	209.9	13.7%
Services	73.7	85.7	99.2	113.7	129.0	145.1	14.5%
Total	273.6	315.9	362.5	412.4	464.2	518.0	13.6%

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

TABLE 367 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	13.7	16.0	19.0	22.3	26.0	30.1	17.1%
Intrusion Detection & Prevention Systems	9.7	11.2	13.2	15.3	17.7	20.3	16.0%
Load Balancers	6.9	8.2	9.8	11.6	13.6	15.9	18.0%
Other Hardware Solutions	5.3	6.2	7.3	8.5	9.9	11.4	16.5%
Total	35.6	41.6	49.2	57.8	67.2	77.8	16.9%

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

TABLE 368 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	34.7	39.9	45.5	51.4	57.5	63.8	12.9%
Intrusion Detection & Prevention Systems	23.2	26.4	29.8	33.3	36.9	40.5	11.8%
Load Balancers	18.5	21.4	24.5	27.9	31.5	35.2	13.8%
Other Hardware Solutions	13.1	14.9	16.9	19.0	21.2	23.4	12.3%
Total	89.5	102.5	116.7	131.7	147.2	162.9	12.7%

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

TABLE 369 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	17.3	20.5	24.6	29.3	34.5	40.5	18.5%
Managed Services	9.3	11.1	13.4	16.1	19.1	22.5	19.3%
Total	26.6	31.6	38.0	45.3	53.6	63.0	18.8%

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

TABLE 370 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	47.2	54.8	63.3	72.4	81.9	91.9	14.3%
Managed Services	26.4	30.9	35.9	41.3	47.1	53.2	15.0%
Total	73.7	85.7	99.2	113.7	129.0	145.1	14.5%

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

TABLE 371 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	5.3	6.3	7.5	8.9	10.4	12.2	17.9%
Consulting and Advisory	4.6	5.5	6.6	8.0	9.5	11.3	19.8%
Training and Education	3.5	4.2	5.0	6.0	7.2	8.4	19.1%
Support and Maintenance	3.9	4.6	5.4	6.4	7.5	8.6	17.2%
Total	17.3	20.5	24.6	29.3	34.5	40.5	18.5%

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

TABLE 372 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	14.1	16.3	18.7	21.3	24.0	26.8	13.7%
Consulting and Advisory	13.3	15.6	18.2	21.0	24.0	27.2	15.5%
Training and Education	9.9	11.5	13.4	15.3	17.5	19.7	14.8%
Support and Maintenance	10.0	11.4	13.0	14.7	16.5	18.3	12.9%
Total	47.2	54.8	63.3	72.4	81.9	91.9	14.3%

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

TABLE 373 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	13.4	15.8	18.9	22.4	26.4	30.8	18.1%
Threat Mitigation Systems	11.7	13.8	16.4	19.3	22.6	26.3	17.6%
Botnet Detection & Management	8.9	10.6	12.8	15.2	18.0	21.2	18.8%
Other Solution Types	7.8	9.1	10.7	12.6	14.6	16.9	16.8%
Total	41.8	49.3	58.8	69.6	81.7	95.2	17.9%

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

TABLE 374 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	35.8	41.5	47.7	54.5	61.5	68.8	13.9%
Threat Mitigation Systems	30.5	35.1	40.2	45.7	51.3	57.2	13.4%
Botnet Detection & Management	24.8	28.8	33.4	38.3	43.4	48.9	14.5%
Other Solution Types	19.4	22.2	25.3	28.5	31.8	35.1	12.6%
Total	110.5	127.6	146.6	166.9	188.0	209.9	13.7%

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

TABLE 375 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	36.1	42.2	49.8	58.5	68.0	78.6	16.8%
Application Security	40.7	48.3	57.9	69.1	81.6	95.8	18.7%
Endpoint Security	11.7	13.7	16.2	19.1	22.2	25.8	17.2%
Cloud Security	15.6	18.4	22.0	26.1	30.7	35.8	18.1%
Total	104.0	122.5	145.9	172.7	202.6	236.0	17.8%

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

TABLE 376 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	90.4	103.4	117.7	132.7	148.1	163.8	12.6%
Application Security	111.9	130.1	150.4	172.4	195.4	219.6	14.4%
Endpoint Security	29.7	34.1	38.9	44.0	49.3	54.7	13.0%
Cloud Security	41.6	48.2	55.5	63.3	71.4	79.9	13.9%
Total	273.6	315.9	362.5	412.4	464.2	518.0	13.6%

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

TABLE 377 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	44.3	52.0	61.6	72.5	84.7	98.2	17.2%
Cloud	59.7	70.6	84.4	100.1	117.9	137.8	18.2%
Total	104.0	122.5	145.9	172.7	202.6	236.0	17.8%

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

TABLE 378 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	113.3	130.1	148.6	168.2	188.5	209.3	13.1%
Cloud	160.3	185.7	213.9	244.1	275.7	308.7	14.0%
Total	273.6	315.9	362.5	412.4	464.2	518.0	13.6%

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

TABLE 379 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	34.5	41.2	49.6	59.4	70.5	83.1	19.2%
Large Enterprises	69.5	81.4	96.3	113.3	132.1	152.9	17.1%
Total	104.0	122.5	145.9	172.7	202.6	236.0	17.8%

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

TABLE 380 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	97.4	113.7	131.9	151.7	172.7	194.8	14.9%
Large Enterprises	176.2	202.2	230.5	260.6	291.5	323.2	12.9%
Total	273.6	315.9	362.5	412.4	464.2	518.0	13.6%

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

TABLE 381 **LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)**

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	19.6	23.6	28.7	34.7	41.6	49.4	20.3%
Government & Defense	14.4	16.6	19.3	22.4	25.6	29.1	15.1%
IT & ITeS	8.1	9.5	11.4	13.5	15.9	18.5	18.1%
Telecom	7.2	8.6	10.4	12.4	14.8	17.5	19.5%
Manufacturing	11.0	12.8	15.0	17.6	20.4	23.5	16.4%
Energy and Utilities	5.5	6.4	7.5	8.7	10.0	11.4	15.7%
Healthcare	13.2	15.7	18.8	22.4	26.5	31.2	18.7%
Retail	11.5	13.6	16.1	19.1	22.3	26.0	17.6%
Education	4.5	5.2	6.2	7.3	8.5	9.8	17.0%
Other Verticals	9.1	10.6	12.5	14.6	17.0	19.6	16.7%
Total	104.0	122.5	145.9	172.7	202.6	236.0	17.8%

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

TABLE 382 **LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)**

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	58.5	68.8	80.5	93.3	107.0	121.6	15.8%
Government & Defense	33.0	37.1	41.5	46.0	50.4	54.6	10.6%
IT & ITeS	21.5	24.9	28.7	32.7	36.9	41.3	13.9%
Telecom	20.5	24.0	27.9	32.2	36.7	41.4	15.1%
Manufacturing	26.9	30.7	34.8	39.1	43.4	47.8	12.2%
Energy and Utilities	13.0	14.8	16.6	18.5	20.4	22.3	11.4%
Healthcare	36.4	42.3	48.9	56.1	63.6	71.5	14.5%
Retail	30.0	34.6	39.7	45.0	50.6	56.4	13.4%
Education	11.3	12.9	14.7	16.6	18.6	20.6	12.8%
Other Verticals	22.5	25.7	29.2	32.9	36.7	40.5	12.5%
Total	273.6	315.9	362.5	412.4	464.2	518.0	13.6%

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

TABLE 383 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2019–2024 (USD MILLION)

Country	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Brazil	43.2	50.3	59.3	69.5	80.7	93.0	16.6%
Mexico	37.2	44.1	52.8	62.8	74.0	86.6	18.4%
Rest of Latin America	23.6	28.1	33.8	40.4	47.9	56.3	19.0%
Total	104.0	122.5	145.9	172.7	202.6	236.0	17.8%

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

TABLE 384 LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY COUNTRY, 2025–2030 (USD MILLION)

Country	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Brazil	106.7	121.9	138.3	155.6	173.2	192.2	12.5%
Mexico	100.9	117.1	135.0	154.3	174.5	194.9	14.1%
Rest of Latin America	66.0	76.9	89.2	102.5	116.5	130.8	14.7%
Total	273.6	315.9	362.5	412.4	464.2	518.0	13.6%

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

15.6.2 BRAZIL

15.6.2.1 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 385 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	14.8	17.1	20.0	23.2	26.8	30.7	16.1%
Software Solutions	17.4	20.3	23.9	28.0	32.5	37.5	17.0%
Services	11.1	13.0	15.5	18.3	21.4	24.8	17.9%
Total	43.2	50.3	59.3	69.5	80.7	93.0	16.9%

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

TABLE 386 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	34.9	39.5	44.5	49.7	54.9	60.5	12.4%
Software Solutions	43.1	49.2	55.9	63.0	70.1	77.9	13.3%
Services	28.7	33.1	37.8	42.9	48.1	53.9	14.2%
Total	106.7	121.9	138.3	155.6	173.2	192.2	13.2%

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

TABLE 387 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	5.7	6.6	7.7	9.0	10.4	11.9	16.3%
Intrusion Detection & Prevention Systems	4.0	4.6	5.4	6.2	7.1	8.0	15.2%
Load Balancers	2.9	3.4	4.0	4.7	5.4	6.3	17.2%
Other Hardware Solutions	2.2	2.5	3.0	3.4	3.9	4.5	15.7%
Total	14.8	17.1	20.0	23.2	26.8	30.7	16.1%

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

TABLE 388 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	13.5	15.4	17.4	19.4	21.5	23.7	12.6%
Intrusion Detection & Prevention Systems	9.1	10.2	11.4	12.6	13.8	15.0	11.4%
Load Balancers	7.2	8.2	9.4	10.5	11.7	13.1	13.4%
Other Hardware Solutions	5.1	5.8	6.5	7.2	7.9	8.7	12.0%
Total	34.9	39.5	44.5	49.7	54.9	60.5	12.4%

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

TABLE 389 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	7.2	8.4	10.0	11.8	13.8	16.0	17.6%
Managed Services	3.9	4.6	5.5	6.5	7.6	8.9	18.4%
Total	11.1	13.0	15.5	18.3	21.4	24.8	17.9%

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

TABLE 390 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	18.4	21.2	24.1	27.3	30.6	34.1	13.9%
Managed Services	10.3	11.9	13.7	15.6	17.6	19.7	14.6%
Total	28.7	33.1	37.8	42.9	48.1	53.9	14.2%

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

TABLE 391 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	2.2	2.6	3.0	3.6	4.2	4.8	17.1%
Consulting and Advisory	1.9	2.2	2.7	3.2	3.8	4.4	19.0%
Training and Education	1.5	1.7	2.0	2.4	2.8	3.3	18.2%
Support and Maintenance	1.6	1.9	2.2	2.6	3.0	3.4	16.3%
Total	7.2	8.4	10.0	11.8	13.8	16.0	17.6%

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

TABLE 392 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	5.5	6.3	7.1	8.0	9.0	9.9	13.3%
Consulting and Advisory	5.2	6.0	6.9	7.9	9.0	10.1	15.1%
Training and Education	3.8	4.4	5.1	5.8	6.5	7.3	14.4%
Support and Maintenance	3.9	4.4	5.0	5.6	6.1	6.8	12.5%
Total	18.4	21.2	24.1	27.3	30.6	34.1	13.9%

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

TABLE 393 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	5.6	6.5	7.7	9.0	10.5	12.1	17.3%
Threat Mitigation Systems	4.9	5.7	6.7	7.8	9.0	10.4	16.7%
Botnet Detection & Management	3.7	4.4	5.2	6.1	7.2	8.4	17.9%
Other Solution Types	3.2	3.7	4.4	5.1	5.8	6.7	15.9%
Total	17.4	20.3	23.9	28.0	32.5	37.5	17.0%

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

TABLE 394 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	14.0	16.0	18.2	20.5	22.9	25.5	13.6%
Threat Mitigation Systems	11.9	13.5	15.3	17.2	19.1	21.2	13.0%
Botnet Detection & Management	9.7	11.1	12.7	14.4	16.2	18.1	14.2%
Other Solution Types	7.6	8.6	9.6	10.7	11.9	13.0	12.2%
Total	43.1	49.2	55.9	63.0	70.1	77.9	13.3%

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

TABLE 395 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	15.0	17.3	20.3	23.5	27.1	31.0	16.0%
Application Security	16.9	19.8	23.6	27.8	32.5	37.8	17.8%
Endpoint Security	4.7	5.5	6.5	7.5	8.7	10.0	16.3%
Cloud Security	6.6	7.7	9.1	10.6	12.4	14.3	17.2%
Total	43.2	50.3	59.3	69.5	80.7	93.0	16.9%

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

TABLE 396 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	35.2	39.9	44.9	50.1	55.2	60.8	12.3%
Application Security	43.6	50.2	57.4	65.0	72.9	81.5	14.1%
Endpoint Security	11.4	12.9	14.6	16.3	18.0	19.9	12.6%
Cloud Security	16.5	18.9	21.5	24.2	27.0	30.1	13.5%
Total	106.7	121.9	138.3	155.6	173.2	192.2	13.2%

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

TABLE 397 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	18.6	21.5	25.3	29.5	34.1	39.1	16.4%
Cloud	24.6	28.8	34.1	40.0	46.6	54.0	17.3%
Total	43.2	50.3	59.3	69.5	80.7	93.0	16.9%

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

TABLE 398 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	44.6	50.7	57.3	64.1	71.0	78.4	12.7%
Cloud	62.1	71.2	81.1	91.5	102.2	113.8	13.6%
Total	106.7	121.9	138.3	155.6	173.2	192.2	13.2%

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

TABLE 399 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	15.0	17.7	21.1	25.0	29.4	34.2	18.2%
Large Enterprises	28.1	32.6	38.2	44.5	51.3	58.8	16.2%
Total	43.2	50.3	59.3	69.5	80.7	93.0	16.9%

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

TABLE 400 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	39.7	45.8	52.6	59.8	67.2	75.4	14.4%
Large Enterprises	67.0	76.0	85.8	95.9	106.0	116.9	12.5%
Total	106.7	121.9	138.3	155.6	173.2	192.2	13.2%

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

TABLE 401 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	8.1	9.7	11.7	13.9	16.5	19.4	19.5%
Government & Defense	6.0	6.8	7.8	9.0	10.2	11.4	14.3%
IT & ITeS	3.4	4.0	4.7	5.5	6.4	7.4	17.2%
Telecom	3.0	3.6	4.3	5.1	6.0	7.0	18.6%
Manufacturing	4.7	5.4	6.3	7.3	8.3	9.5	15.6%
Energy and Utilities	2.3	2.7	3.1	3.6	4.1	4.6	14.9%
Healthcare	5.4	6.3	7.5	8.9	10.4	12.1	17.8%
Retail	4.9	5.7	6.7	7.8	9.1	10.4	16.7%
Education	1.7	2.0	2.3	2.7	3.1	3.6	16.0%
Other Verticals	3.7	4.2	4.9	5.7	6.6	7.5	15.8%
Total	43.2	50.3	59.3	69.5	80.7	93.0	16.9%

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

TABLE 402 BRAZIL: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	22.8	26.5	30.6	35.1	39.8	45.0	15.4%
Government & Defense	12.8	14.3	15.8	17.3	18.7	20.2	10.3%
IT & ITeS	8.6	9.8	11.1	12.6	14.0	15.6	13.5%
Telecom	8.1	9.4	10.8	12.3	13.9	15.6	14.7%
Manufacturing	10.8	12.1	13.6	15.1	16.6	18.2	11.9%
Energy and Utilities	5.2	5.8	6.5	7.1	7.8	8.5	11.1%
Healthcare	14.0	16.1	18.4	20.9	23.4	26.1	14.1%
Retail	11.9	13.6	15.4	17.3	19.2	21.3	13.0%
Education	4.1	4.6	5.2	5.8	6.4	7.1	12.3%
Other Verticals	8.6	9.7	10.9	12.1	13.3	14.6	12.1%
Total	106.7	121.9	138.3	155.6	173.2	192.2	13.2%

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

15.6.3 MEXICO

15.6.3.1 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 security 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 403 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	12.7	14.9	17.7	20.9	24.5	28.5	17.5%
Software Solutions	15.7	18.6	22.3	26.5	31.2	36.6	18.5%
Services	8.9	10.6	12.8	15.4	18.3	21.6	19.5%
Total	37.2	44.1	52.8	62.8	74.0	86.6	18.4%

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

TABLE 404 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	32.9	37.9	43.3	49.1	55.2	61.1	13.2%
Software Solutions	42.7	49.5	57.2	65.4	74.0	82.7	14.2%
Services	25.4	29.7	34.5	39.8	45.4	51.1	15.1%
Total	100.9	117.1	135.0	154.3	174.5	194.9	14.1%

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

TABLE 405 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	4.9	5.7	6.8	8.1	9.5	11.0	17.7%
Intrusion Detection & Prevention Systems	3.4	4.0	4.7	5.5	6.3	7.3	16.6%
Load Balancers	2.4	2.9	3.5	4.1	4.9	5.7	18.7%
Other Hardware Solutions	2.0	2.3	2.8	3.3	3.8	4.4	17.1%
Total	12.7	14.9	17.7	20.9	24.5	28.5	17.5%

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

TABLE 406 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	12.8	14.7	16.9	19.2	21.6	23.9	13.4%
Intrusion Detection & Prevention Systems	8.4	9.6	10.8	12.2	13.6	14.9	12.2%
Load Balancers	6.7	7.8	9.0	10.3	11.6	13.0	14.2%
Other Hardware Solutions	5.1	5.8	6.6	7.5	8.4	9.3	12.8%
Total	32.9	37.9	43.3	49.1	55.2	61.1	13.2%

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

TABLE 407 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	5.3	6.3	7.6	9.1	10.8	12.8	19.2%
Managed Services	3.5	4.3	5.2	6.2	7.4	8.8	19.9%
Total	8.9	10.6	12.8	15.4	18.3	21.6	19.5%

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

TABLE 408 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	15.0	17.5	20.3	23.3	26.5	29.8	14.8%
Managed Services	10.4	12.2	14.2	16.4	18.8	21.3	15.5%
Total	25.4	29.7	34.5	39.8	45.4	51.1	15.1%

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

TABLE 409 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	1.7	2.0	2.4	2.8	3.3	3.9	18.6%
Consulting and Advisory	1.4	1.7	2.1	2.5	3.0	3.6	20.5%
Training and Education	1.1	1.3	1.6	1.9	2.3	2.7	19.7%
Support and Maintenance	1.1	1.3	1.6	1.9	2.2	2.6	17.7%
Total	5.3	6.3	7.6	9.1	10.8	12.8	19.2%

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

TABLE 410 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	4.5	5.3	6.1	7.0	7.9	8.8	14.2%
Consulting and Advisory	4.3	5.1	5.9	6.9	7.9	9.0	15.9%
Training and Education	3.2	3.7	4.3	5.0	5.7	6.5	15.3%
Support and Maintenance	3.0	3.4	3.9	4.4	5.0	5.5	13.3%
Total	15.0	17.5	20.3	23.3	26.5	29.8	14.8%

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

TABLE 411 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	5.1	6.0	7.2	8.6	10.2	12.0	18.7%
Threat Mitigation Systems	4.4	5.2	6.2	7.4	8.7	10.2	18.2%
Botnet Detection & Management	3.3	3.9	4.7	5.7	6.8	8.0	19.4%
Other Solution Types	2.9	3.4	4.0	4.8	5.6	6.5	17.4%
Total	15.7	18.6	22.3	26.5	31.2	36.6	18.5%

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

TABLE 412 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	14.0	16.3	18.8	21.6	24.5	27.4	14.4%
Threat Mitigation Systems	11.8	13.7	15.7	18.0	20.3	22.6	13.9%
Botnet Detection & Management	9.4	11.0	12.8	14.7	16.8	18.9	15.0%
Other Solution Types	7.5	8.6	9.8	11.1	12.4	13.8	13.0%
Total	42.7	49.5	57.2	65.4	74.0	82.7	14.2%

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

TABLE 413 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	12.7	15.0	17.8	20.9	24.5	28.4	17.4%
Application Security	14.6	17.4	21.0	25.1	29.8	35.2	19.3%
Endpoint Security	4.6	5.4	6.5	7.7	9.0	10.5	17.8%
Cloud Security	5.3	6.3	7.6	9.0	10.7	12.6	18.7%
Total	37.2	44.1	52.8	62.8	74.0	86.6	18.4%

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

TABLE 414 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	32.8	37.7	43.1	48.9	54.8	60.7	13.1%
Application Security	41.3	48.2	56.0	64.5	73.5	82.7	14.9%
Endpoint Security	12.2	14.0	16.1	18.3	20.6	22.9	13.5%
Cloud Security	14.7	17.1	19.7	22.6	25.7	28.7	14.4%
Total	100.9	117.1	135.0	154.3	174.5	194.9	14.1%

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

TABLE 415 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	16.4	19.3	23.0	27.2	32.0	37.3	17.9%
Cloud	20.9	24.8	29.8	35.5	42.0	49.4	18.8%
Total	37.2	44.1	52.8	62.8	74.0	86.6	18.4%

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

TABLE 416 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	43.2	49.9	57.2	65.1	73.3	81.5	13.5%
Cloud	57.7	67.2	77.8	89.2	101.2	113.5	14.5%
Total	100.9	117.1	135.0	154.3	174.5	194.9	14.1%

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

TABLE 417 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	12.9	15.4	18.7	22.5	26.8	31.7	19.7%
Large Enterprises	24.4	28.7	34.1	40.3	47.2	54.9	17.7%
Total	37.2	44.1	52.8	62.8	74.0	86.6	18.4%

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

TABLE 418 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	37.3	43.8	51.0	58.9	67.4	76.0	15.3%
Large Enterprises	63.6	73.3	84.0	95.4	107.2	118.9	13.3%
Total	100.9	117.1	135.0	154.3	174.5	194.9	14.1%

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

TABLE 419 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	7.0	8.5	10.4	12.7	15.2	18.2	20.9%
Government & Defense	5.2	6.0	7.0	8.2	9.4	10.7	15.7%
IT & ITeS	2.8	3.4	4.0	4.8	5.7	6.7	18.7%
Telecom	2.5	3.0	3.7	4.5	5.3	6.3	20.1%
Manufacturing	3.8	4.5	5.3	6.2	7.3	8.4	17.0%
Energy and Utilities	1.9	2.3	2.6	3.1	3.6	4.1	16.3%
Healthcare	4.8	5.7	6.9	8.3	9.8	11.6	19.3%
Retail	4.1	4.8	5.7	6.8	8.0	9.4	18.2%
Education	1.6	1.8	2.2	2.6	3.0	3.5	17.5%
Other Verticals	3.5	4.1	4.8	5.7	6.6	7.7	17.4%
Total	37.2	44.1	52.8	62.8	74.0	86.6	18.4%

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

TABLE 420 MEXICO: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	21.6	25.6	30.1	35.0	40.3	45.9	16.2%
Government & Defense	12.2	13.8	15.5	17.3	19.0	20.7	11.1%
IT & ITeS	7.8	9.1	10.5	12.0	13.6	15.2	14.4%
Telecom	7.5	8.8	10.3	11.9	13.6	15.4	15.6%
Manufacturing	9.7	11.1	12.6	14.2	15.9	17.5	12.6%
Energy and Utilities	4.7	5.4	6.0	6.8	7.5	8.2	11.8%
Healthcare	13.6	15.9	18.5	21.3	24.3	27.3	14.9%
Retail	10.9	12.6	14.5	16.5	18.7	20.8	13.9%
Education	4.1	4.7	5.3	6.1	6.8	7.5	13.2%
Other Verticals	8.9	10.2	11.7	13.2	14.8	16.4	13.0%
Total	100.9	117.1	135.0	154.3	174.5	194.9	14.1%

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

15.6.4 REST OF LATIN AMERICA

The rest of Latin America includes Argentina, Peru, Chile, and the remaining countries. The DDoS protection and mitigation security 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 e-commerce 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 421 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Hardware Solutions	8.3	9.8	11.7	13.8	16.3	19.0	18.1%
Software Solutions	9.9	11.8	14.2	16.9	20.1	23.6	19.1%
Services	5.5	6.6	8.0	9.6	11.5	13.7	20.1%
Total	23.6	28.1	33.8	40.4	47.9	56.3	19.0%

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

TABLE 422 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Hardware Solutions	22.1	25.6	29.4	33.6	37.9	42.2	13.8%
Software Solutions	27.7	32.3	37.5	43.1	49.0	55.1	14.8%
Services	16.2	19.0	22.3	25.8	29.6	33.5	15.7%
Total	66.0	76.9	89.2	102.5	116.5	130.8	14.7%

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

TABLE 423 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2019–2024 (USD MILLION)

Hardware Solution	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Firewalls	3.2	3.8	4.6	5.5	6.4	7.5	18.3%
Intrusion Detection & Prevention Systems	2.2	2.6	3.0	3.6	4.2	4.8	17.2%
Load Balancers	1.6	1.9	2.3	2.7	3.2	3.8	19.3%
Other Hardware Solutions	1.2	1.5	1.7	2.1	2.4	2.8	17.7%
Total	8.3	9.8	11.7	13.8	16.3	19.0	18.1%

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

TABLE 424 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY HARDWARE SOLUTION, 2025–2030 (USD MILLION)

Hardware Solution	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Firewalls	8.8	10.2	11.7	13.4	15.1	16.9	14.0%
Intrusion Detection & Prevention Systems	5.6	6.4	7.3	8.3	9.2	10.2	12.8%
Load Balancers	4.5	5.3	6.1	7.0	8.0	9.0	14.8%
Other Hardware Solutions	3.3	3.8	4.3	4.9	5.5	6.1	13.4%
Total	22.1	25.6	29.4	33.6	37.9	42.2	13.8%

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

TABLE 425 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2019–2024 (USD MILLION)

Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Professional Services	3.4	4.0	4.9	5.9	7.0	8.3	19.8%
Managed Services	2.1	2.6	3.1	3.8	4.5	5.4	20.6%
Total	5.5	6.6	8.0	9.6	11.5	13.7	20.1%

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

TABLE 426 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SERVICE, 2025–2030 (USD MILLION)

Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Professional Services	9.8	11.4	13.4	15.4	17.7	20.0	15.4%
Managed Services	6.4	7.6	8.9	10.4	11.9	13.6	16.1%
Total	16.2	19.0	22.3	25.8	29.6	33.5	15.7%

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

TABLE 427 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2019–2024 (USD MILLION)

Professional Service	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Design and Implementation	1.0	1.2	1.5	1.7	2.1	2.4	19.2%
Consulting and Advisory	0.9	1.1	1.3	1.6	2.0	2.4	21.1%
Training and Education	0.7	0.8	1.0	1.2	1.5	1.7	20.4%
Support and Maintenance	0.8	0.9	1.1	1.3	1.5	1.8	18.4%
Total	3.4	4.0	4.9	5.9	7.0	8.3	19.8%

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

TABLE 428 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY PROFESSIONAL SERVICE, 2025–2030 (USD MILLION)

Professional Service	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Design and Implementation	2.8	3.3	3.9	4.4	5.1	5.7	14.8%
Consulting and Advisory	2.8	3.3	3.9	4.6	5.3	6.0	16.6%
Training and Education	2.1	2.4	2.9	3.3	3.8	4.3	15.9%
Support and Maintenance	2.0	2.4	2.7	3.1	3.5	3.9	14.0%
Total	9.8	11.4	13.4	15.4	17.7	20.0	15.4%

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

TABLE 429 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Traffic Analyzers	3.2	3.8	4.6	5.5	6.5	7.7	19.3%
Threat Mitigation Systems	2.8	3.3	3.9	4.7	5.6	6.5	18.8%
Botnet Detection & Management	2.1	2.5	3.0	3.7	4.4	5.2	20.0%
Other Solution Types	1.8	2.2	2.6	3.0	3.6	4.2	18.0%
Total	9.9	11.8	14.2	16.9	20.1	23.6	19.1%

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

TABLE 430 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Traffic Analyzers	9.1	10.6	12.3	14.2	16.2	18.2	15.0%
Threat Mitigation Systems	7.6	8.9	10.3	11.8	13.4	15.0	14.5%
Botnet Detection & Management	6.2	7.2	8.5	9.8	11.2	12.7	15.6%
Other Solution Types	4.8	5.6	6.4	7.3	8.2	9.2	13.6%
Total	27.7	32.3	37.5	43.1	49.0	55.1	14.8%

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

TABLE 431 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2019–2024 (USD MILLION)

Application Area	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	8.1	9.5	11.4	13.5	15.8	18.5	18.0%
Application Security	9.2	11.1	13.4	16.2	19.3	22.9	19.9%
Endpoint Security	2.9	3.5	4.2	4.9	5.8	6.8	18.4%
Cloud Security	3.4	4.0	4.9	5.8	6.9	8.2	19.3%
Total	23.6	28.1	33.8	40.4	47.9	56.3	19.0%

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

TABLE 432 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY APPLICATION AREA, 2025–2030 (USD MILLION)

Application Area	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	21.5	24.8	28.5	32.5	36.6	40.7	13.7%
Application Security	27.0	31.7	37.0	42.8	49.0	55.5	15.5%
Endpoint Security	7.9	9.2	10.6	12.2	13.7	15.4	14.1%
Cloud Security	9.6	11.2	13.0	15.0	17.1	19.3	15.0%
Total	66.0	76.9	89.2	102.5	116.5	130.8	14.7%

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

TABLE 433 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	10.5	12.5	14.9	17.8	21.0	24.6	18.5%
Cloud	13.1	15.6	18.9	22.6	26.9	31.8	19.4%
Total	23.6	28.1	33.8	40.4	47.9	56.3	19.0%

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

TABLE 434 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	28.6	33.2	38.3	43.8	49.6	55.5	14.1%
Cloud	37.3	43.7	50.8	58.6	66.9	75.3	15.1%
Total	66.0	76.9	89.2	102.5	116.5	130.8	14.7%

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

TABLE 435 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
SMEs	7.8	9.4	11.5	13.9	16.7	19.8	20.4%
Large Enterprises	15.8	18.7	22.3	26.5	31.2	36.5	18.3%
Total	23.6	28.1	33.8	40.4	47.9	56.3	19.0%

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

TABLE 436 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
SMEs	23.5	27.7	32.5	37.7	43.3	49.2	15.9%
Large Enterprises	42.5	49.2	56.7	64.7	73.2	81.6	13.9%
Total	66.0	76.9	89.2	102.5	116.5	130.8	14.7%

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

TABLE 437 REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
BFSI	4.4	5.4	6.6	8.1	9.8	11.7	21.6%
Government & Defense	3.1	3.7	4.3	5.0	5.8	6.6	16.2%
IT & ITeS	1.8	2.1	2.5	3.1	3.6	4.3	19.3%
Telecom	1.6	1.9	2.4	2.9	3.4	4.1	20.7%
Manufacturing	2.5	2.9	3.5	4.1	4.8	5.6	17.6%
Energy and Utilities	1.2	1.4	1.7	2.0	2.3	2.7	16.9%
Healthcare	3.0	3.6	4.3	5.2	6.2	7.4	19.9%
Retail	2.6	3.1	3.7	4.4	5.2	6.1	18.8%
Education	1.0	1.2	1.4	1.7	2.0	2.3	18.2%
Other Verticals	2.4	2.8	3.4	4.0	4.7	5.5	18.0%
Total	23.6	28.1	33.8	40.4	47.9	56.3	19.0%

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

TABLE 438 **REST OF LATIN AMERICA: DDOS PROTECTION AND MITIGATION SECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)**

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
BFSI	14.0	16.6	19.7	23.0	26.7	30.5	16.9%
Government & Defense	7.6	8.6	9.7	10.9	12.0	13.1	11.5%
IT & ITeS	5.0	5.9	6.8	7.9	9.0	10.1	15.0%
Telecom	4.9	5.8	6.8	7.9	9.1	10.3	16.2%
Manufacturing	6.5	7.4	8.5	9.7	10.8	12.0	13.2%
Energy and Utilities	3.1	3.5	4.0	4.5	5.0	5.5	12.4%
Healthcare	8.7	10.2	11.9	13.8	15.8	17.9	15.5%
Retail	7.1	8.3	9.6	11.0	12.5	14.0	14.5%
Education	2.7	3.1	3.6	4.1	4.7	5.2	13.8%
Other Verticals	6.4	7.4	8.5	9.7	10.9	12.2	13.7%
Total	66.0	76.9	89.2	102.5	116.5	130.8	14.7%

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 security market. It includes a trend analysis based on the revenue of various business segments of key market players. Additionally, benchmarking of the growth strategies adopted by key players was also carried out. 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

The key players have adopted organic and inorganic growth strategies to expand their global presence, which has helped them increase their 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 439 DDOS PROTECTION AND MITIGATION SECURITY 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 discover and mitigate large DDoS attacks, implement defense measures for 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 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 capability of Akamai Prolexic allowed customers to define and manage their own access control lists (ACLs) while enabling greater flexibility to secure their own 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 DefensePro DDoS Protection to offer customers a DDoS scrubbing service designed to combat today's increasingly complex threats.	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 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.	The Americas contribute about 38% to the company's revenue.

Source: Annual Reports, Press Releases, and MarketsandMarkets Analysis

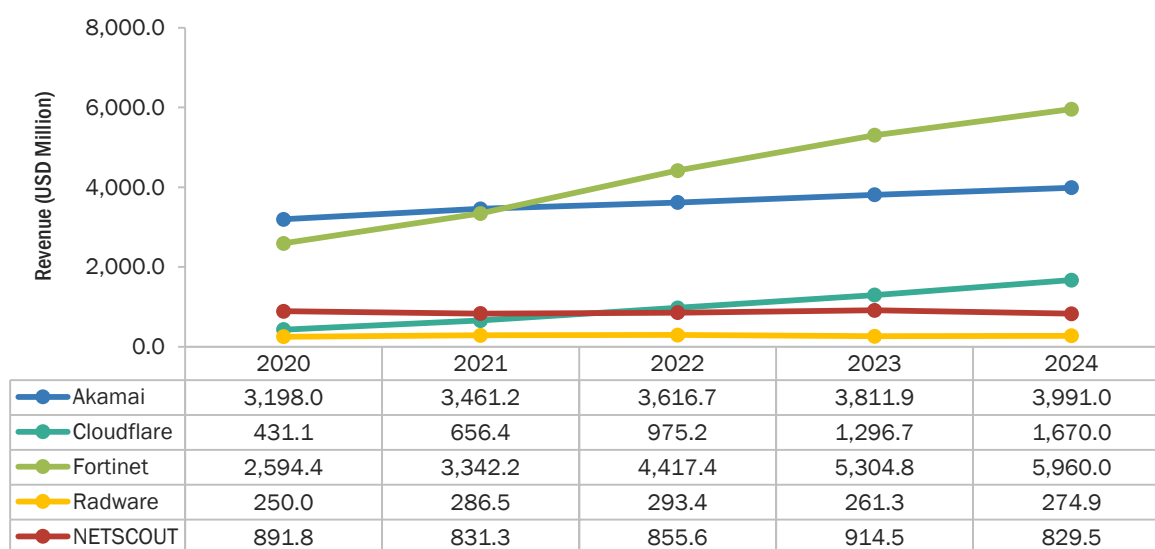
Strategies of various DDoS protection and mitigation security vendors have been assessed, along with the strategies they have adopted:

- **Product Type:** Key players in the DDoS protection and mitigation security market offer a comprehensive product portfolio that includes DDoS protection and mitigation security 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, 2020–2024

Players in the DDoS protection and mitigation security 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 37 DDoS PROTECTION AND MITIGATION SECURITY MARKET: REVENUE ANALYSIS OF FIVE KEY PLAYERS, 2020–2024



Source: Company Websites and Annual Reports

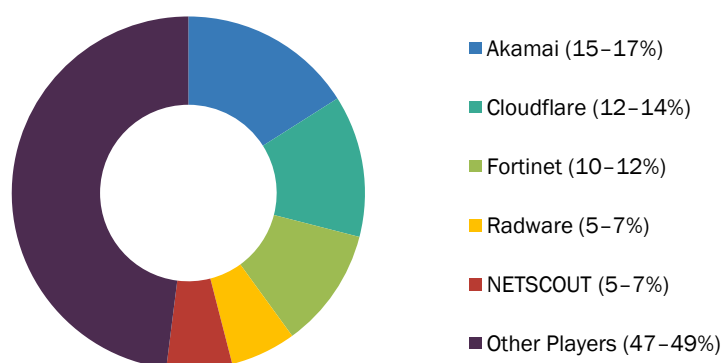
The revenue analysis of five key players in the DDoS protection and mitigation security market from 2020 to 2024 highlights consistent overall growth driven by rising attack frequency and demand for advanced mitigation capabilities. Akamai and Fortinet remain the leading contributors, showing steady year-on-year increases as enterprises expand their cloud and edge-security investments. Cloudflare demonstrates strong momentum with sharp revenue acceleration, reflecting rapid customer acquisition and its expanding DDoS-as-a-Service portfolio. Radware maintains stable revenues, supported by its enterprise-focused mitigation appliances, while NETSCOUT shows moderate but steady performance in line with its traditional telecom and network visibility strengths. Collectively, the upward trend across vendors illustrates a maturing yet rapidly scaling market as organizations prioritize resilience, automated, and scalable DDoS defense solutions.

16.4 MARKET SHARE ANALYSIS, 2024

Key players in the DDoS protection and mitigation security 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 security market in 2024.

FIGURE 38 SHARE ANALYSIS OF LEADING COMPANIES IN DDOS PROTECTION AND MITIGATION SECURITY MARKET, 2024



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

TABLE 440 DDOS PROTECTION AND MITIGATION SECURITY MARKET: DEGREE OF COMPETITION, 2024

DEGREE OF COMPETITION	CONSOLIDATED
Total Market Share of Top 5 players	50-55%
Akamai	15-17%
Cloudflare	12-14%
Fortinet	10-12%
Radware	5-7%
NETSCOUT	5-7%

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 competitive, and the top five players constitute 50-55% of the DDoS protection and mitigation security market, with other dominant players accounting for 45-49% of the global market. In addition, the market is witnessing new entrants and comprises a relatively small number of small and medium-sized DDoS protection and mitigation security players, leading to noticeable market competition. However, the market is expected to remain competitive in the coming years due to multiple players coming into the market.

NETSCOUT

NETSCOUT is one of the leading providers of application and network performance management solutions and products. Its product portfolio comprises business assurance, service assurance, and security assurance, along with advanced DDoS attack and threat solutions and business intelligence (BI) solutions. It offers various technology-based solutions, such as Network Functions Virtualization (NFV), Software-defined Networking (SDN), core network, Information Management System (IMS) monitoring, and radio access. It caters to a wide range of industry verticals, including government, retail banking, healthcare, pharmaceuticals, utilities, manufacturing, BFSI, education, and transportation. Arbor Networks is a security division of NETSCOUT that provides leading products and services in the DDoS protection and mitigation market. It has an extensive DDoS protection and mitigation product portfolio, including Arbor Networks APS, Arbor Cloud, and Arbor Networks TMS. Arbor Networks APS is an on-premises solution that helps in the decryption and analysis of encrypted traffic.

AKAMAI TECHNOLOGIES

Akamai Technologies 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 Technologies 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.

RADWARE

Radware specializes in application delivery and load balancing, as well as application and network security, and cloud security. It offers a variety of products for DDoS protection and mitigation, including DefensePro, Cloud DDoS Protection Service, and DefenseFlow. The company serves multiple industry sectors, including e-commerce, financial services, education, government, and healthcare. The company is focused on application integration with leading companies, such as Cisco, Citrix Systems, Microsoft, Oracle, SAP, and VMware. Its R&D centers are located in the US, Israel, and India. 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.

CLOUDFLARE

Cloudflare is a company that focuses on internet security and performance. It creates solutions to enhance the speed and protection of millions of websites, APIs, SaaS services, e-commerce platforms, and mobile applications. It offers services in CDN, DDoS protection, secure DNS, and security and web optimization. The company also provides enterprise-grade security and performance management solutions for large enterprises.

Cloudflare's global network spans more than 180 cities. It has the capacity to handle 15 Tbps of throughput, thus helping deliver better security and performance to customers. Some of its customers include NASDAQ, Cisco, Zendesk, Quizlet, and DigitalOcean. The company provides various pricing plans for personal, professional, e-commerce, and business websites targeting SMEs and larger organizations. Its offices are in North America, South America, Europe, Asia Pacific, and MEA.

FORTINET

Fortinet is a leading provider of cybersecurity solutions to various businesses, such as enterprises, communication service providers, and small businesses. Its flagship product, FortiGate firewall, is renowned for advanced threat protection and secure access. The company's offerings extend to endpoint and cloud security, secure access technologies like VPN and ZTNA, and threat intelligence through integrated solutions. The company operates under four business areas: network security, Fortinet security fabric, cloud security, and IoT and operational technology.

The company provides a comprehensive range of solutions for small and medium-sized enterprises (SMEs). Fortinet also offers products tailored for carriers, cloud service providers, and managed security service providers (MSSPs). Its offerings cater to various industry sectors, including government, education, financial services, retail, and healthcare. With over 330,000 customers in 180 countries, the company has a broad customer base across the Americas, EMEA, and Asia Pacific.

16.4.1 MARKET RANKING ANALYSIS, 2024

FIGURE 39 MARKET RANKING ANALYSIS OF TOP FIVE PLAYERS



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

16.5 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2025

In this section, key players operating in the DDoS protection and mitigation security market have been mapped. These players have been ranked based on the market share/rank and the strength of the product footprint.

16.5.1 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 Technologies, Cloudflare, Fortinet, Radware, NETSCOUT, Nexusguard, NSFocus, A10 Networks, Corero and F5 are the vendors in this category.

16.5.2 EMERGING LEADERS

The key players involved in the development and innovation of new products in the DDoS protection and mitigation security 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. Imperva, Link11, and Fastly fall under this category.

16.5.3 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. BT, Lumen Technologies, and Huawei fall under this category.

16.5.4 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. Link11, AlloT, Stratacore, and Sucuri are placed in this quadrant.

FIGURE 40 DDOS PROTECTION AND MITIGATION SECURITY MARKET:
COMPANY EVALUATION MATRIX (KEY PLAYERS), 2025



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

16.5.5 COMPANY FOOTPRINT: KEY PLAYERS, 2025

16.5.5.1 Company footprint

FIGURE 41 DDOS PROTECTION AND MITIGATION SECURITY MARKET: COMPANY FOOTPRINT, 2025

COMPANY NAME	REGIONAL FOOTPRINT	OFFERING FOOTPRINT	VERTICAL FOOTPRINT	OVERALL FOOTPRINT
NETSCOUT	○○○○	○○○○	○○○	○○○○
Akamai	○○○○	○○○○	○○	○○○
Radware	○○○○	○○○○	○○○	○○○○
Huawei Technology	○○○○	○○○○	○	○○○
Fortinet	○○○○	○○○○	○○○○	○○○○
Link11	○○○○	○○○○	○○○	○○○○
Imperva	○○○○	○○○○	○	○○○
NSFocus	○○○○	○○○○	○○○○	○○○○
Cloudflare	○○○○	○○○○	○	○○○
BT	○○○○	○○○○	○○○○	○○○○
A10 Networks	○○○○	○○○○	○○○	○○○○
F5	○○○○	○○○	○	○○○
Fastly	○○	○	○○○	○○○
Nexusguard	○○○○	○○○○	○○○	○○○
Corero	○○○○	○○○○	○○○○	○○○○
RATING : ○○○○ EXCELLENT ○○○ GOOD ○○ AVERAGE ○ BELOW AVERAGE NOT APPLICABLE				

Source: Company Websites and MarketsandMarkets Analysis

16.5.5.2 Regional footprint

TABLE 441 DDOS PROTECTION AND MITIGATION SECURITY MARKET: REGIONAL FOOTPRINT, 2025

COMPANY	NORTH AMERICA	EUROPE	ASIA PACIFIC	MIDDLE EAST & AFRICA	LATIN AMERICA	REGION FOOTPRINT
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 Technology	Y	Y	Y	Y	Y	4.00
Fortinet	Y	Y	Y	Y	Y	4.00
Link11	Y	Y	Y	Y	Y	4.00
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
Nexusguard	Y	Y	N	Y	N	2.40
Corero	Y	Y	Y	Y	Y	4.00
RioRey	Y	Y	Y	N	N	2.40
PhoenixNAP	Y	Y	N	Y	Y	3.20
Allot	Y	N	N	N	N	0.80
StrataCore	Y	Y	Y	N	N	2.40
Sucuri	Y	Y	Y	Y	Y	4.00
Lumen Technologies	Y	Y	Y	Y	N	3.20
Seceon	Y	Y	Y	N	N	2.40
HaltDos	Y	N	Y	N	N	1.60
DDoS-Guard	Y	N	N	N	N	0.80
Indusface	N	Y	Y	N	N	1.60
Activereach	Y	Y	Y	Y	Y	4.00
Mlytics	Y	Y	Y	Y	Y	4.00
Comodo Security Solutions	Y	Y	N	N	Y	2.40

Source: Company Websites and MarketsandMarkets Analysis

16.5.5.3 Offering footprint

TABLE 442 DDOS PROTECTION AND MITIGATION SECURITY MARKET: OFFERING FOOTPRINT, 2025

COMPANY	HARDWARE SOLUTIONS	SOFTWARE SOLUTIONS	SERVICES	OFFERING FOOTPRINT
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
Link11	N	Y	Y	2.7
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
Nexusguard	N	Y	Y	2.7
Corero	Y	Y	Y	4.0
RioRey	N	Y	N	1.3
PhoenixNAP	N	Y	Y	2.7
Allot	N	Y	N	1.3
StrataCore	N	Y	N	1.3
Sucuri	N	Y	Y	2.7
Lumen Technologies	N	Y	N	1.3
Seceon	N	Y	Y	2.7
HaltDos	N	Y	Y	2.7
DDoS-Guard	N	Y	Y	2.7
Indusface	N	Y	Y	2.7
Activereach	N	Y	N	1.3
Mlytics	N	Y	N	1.3
Comodo Security Solutions	N	Y	N	1.3

Source: Company Websites and MarketsandMarkets Analysis

16.5.5.4 Vertical footprint

TABLE 443 DDOS PROTECTION AND MITIGATION SECURITY MARKET: VERTICAL FOOTPRINT, 2025

COMPANY	BFSI	HEALTHCARE	IT & ITES	VERTICAL FOOTPRINT
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
Link11	Y	N	N	1.33
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
Nexusguard	Y	Y	Y	4.00
Corero	Y	Y	Y	4.00
RioRey	N	N	Y	1.33
PhoenixNAP	N	N	Y	1.33
Allot	N	N	Y	1.33
StrataCore	Y	N	Y	2.67
Sucuri	Y	Y	N	2.67
Lumen Technologies	Y	Y	Y	4.00
Seceon	Y	N	N	1.33
HaltDos	N	N	Y	1.33
DDoS-Guard	Y	Y	N	2.67
Indusface	Y	Y	Y	4.00
Activereach	N	N	Y	1.33
Mlytics	N	N	Y	1.33
Comodo Security Solutions	N	N	Y	1.33

Source: Company Websites and MarketsandMarkets Analysis

16.6 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2025

16.6.1 PROGRESSIVE COMPANIES

Seceon, Haltdos, and Mlytics 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 security market.

16.6.2 RESPONSIVE COMPANIES

Activereach and RioRey are recognized as responsive companies in the DDoS protection and mitigation security market. Responsive companies provide innovative solutions to cater to future DDoS protection and mitigation security 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 security products and solutions to their customers to fulfill their demands.

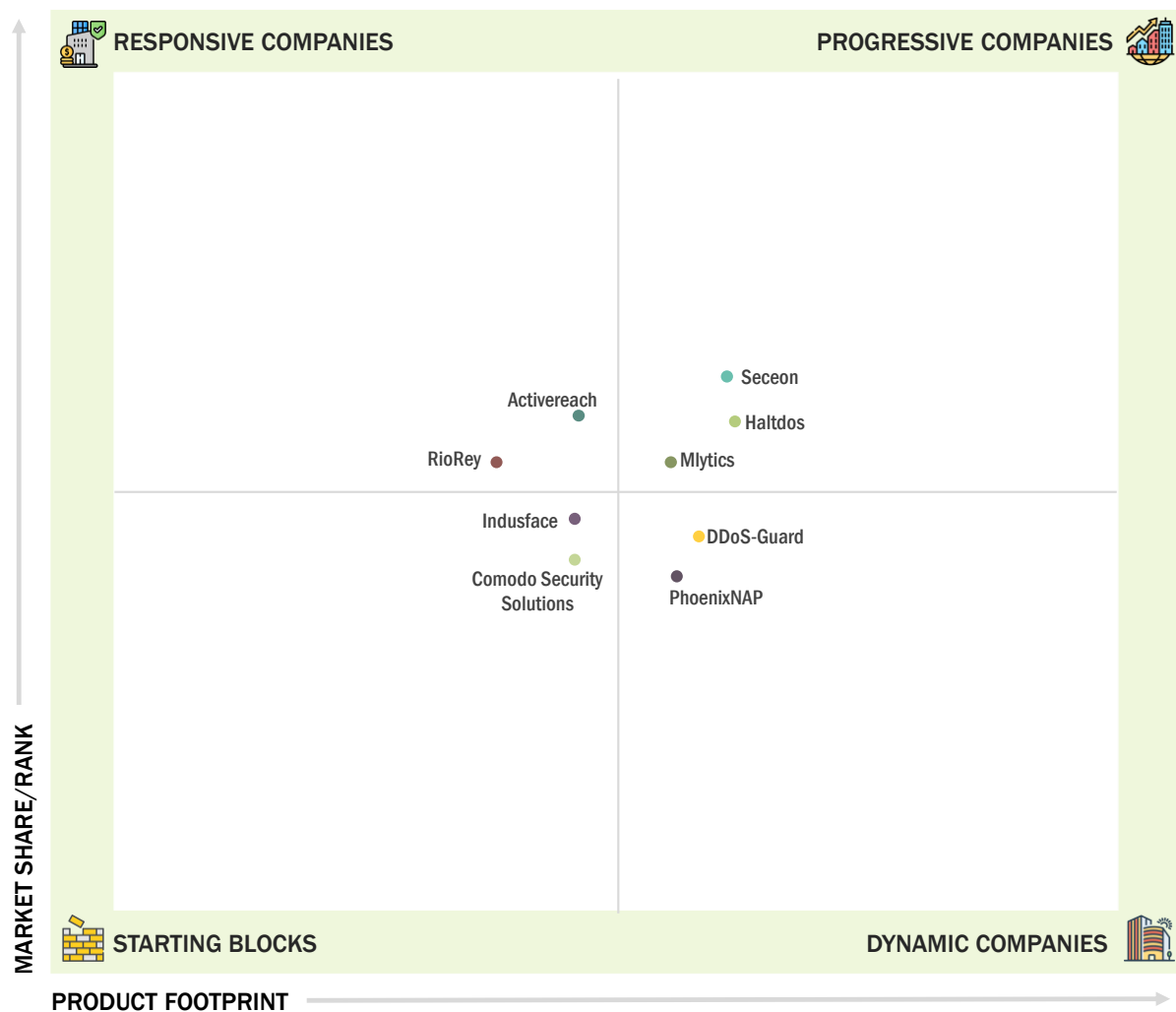
16.6.3 DYNAMIC COMPANIES

Dynamic companies such as DDoS-Guard and PhoenixNAP offer innovative solutions 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 security market, and organic and inorganic ventures have boosted their market position.

16.6.4 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. Indusface and Comodo Security Solutions are recognized as a starting block in the DDoS protection and mitigation security market.

FIGURE 42 DDOS PROTECTION AND MITIGATION SECURITY MARKET:
COMPANY EVALUATION MATRIX (STARTUPS/SMES), 2025



Source: Secondary Research and MarketsandMarkets Analysis

16.6.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2025

16.6.5.1 Detailed list of key startups/SMEs

TABLE 444 DDOS PROTECTION AND MITIGATION SECURITY MARKET: KEY STARTUPS/SMES, 2025

COMPANY	TYPE	CATEGORY	OWNERSHIP STATUS	HQ LOCATION	FOUNDED	EMPLOYEES	FINANCING STATUS	LATEST FUNDING ROUND	TOTAL FUNDING (USD MILLION)
Seceon	Startup	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
Activereach	SME	Solution/Services	Private	Buckinghamshire, UK	2008	51–200	Venture Capital	Series C	28.3
Mlytics	SME	Solution/Services	Private	Singapore	2017	51–200	Venture Capital	NA	NA
RioRey	Startup	Solution	Private	Maryland, US	2006	11–50	Venture Capital	Debt	0.29
PhoenixNAP	Startup	Solution	Private	Phoenix, US	2009	201–500	Venture Capital	NA	NA
Comodo Security Solutions	Startup	Solution	Private	Lasi, Romania	2005	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

16.6.5.2 Competitive benchmarking of key startups/SMEs

TABLE 445 DDOS PROTECTION AND MITIGATION SECURITY 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
Comodo Security Solutions	N	Y	N	N	N	Y	Y	Y	N	N	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

Source: Secondary Research and MarketsandMarkets Analysis

16.7 COMPETITIVE SCENARIO

Key market developments include the recent developments of the key players in the DDoS protection and mitigation security market. The market size analysis of the key industry players has been done based on various parameters, including the number of DDoS protection and mitigation security stakeholders, the depth of product offerings, and the revenue generated.

16.7.1 PRODUCT LAUNCHES & ENHANCEMENTS

The major companies that have incorporated product launch and product enhancement strategies include Akamai Technologies and Radware.

TABLE 446 DDOS PROTECTION AND MITIGATION SECURITY MARKET: PRODUCT LAUNCHES AND ENHANCEMENTS, APRIL 2023–AUGUST 2025

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (TYPE)	DESCRIPTION
August 2025	Program launch	Radware (Israel)	Cybersecurity Partner Program	Radware launched an enhanced Cybersecurity Partner Program to help MSSPs and channel partners scale managed security services, including DDoS protection, WAF, and application security offerings. The program introduced new incentives, onboarding tools, and training to strengthen its global managed security network.
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.
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.
April 2023	Product launch	Akamai Technologies (US)	Prolexic (Platform)	Akamai Technologies announced the launch of its Prolexic Network Cloud Firewall. This new capability of Akamai Prolexic allowed customers to define and manage their own access control lists (ACLs) while enabling greater flexibility to secure their own network edge.

Source: Press Releases

16.7.2 DEALS

The major companies that have incorporated deals, such as acquisitions, partnerships, and agreements, include NETSCOUT, Akamai Technologies, Radware, Huawei, Fortinet, Link11, Imperva, and BT.

TABLE 447 DDOS PROTECTION AND MITIGATION SECURITY MARKET: DEALS,
FEBRUARY 2022-MAY 2024

MONTH- & YEAR	DEAL TYPE	COMPANY 1 NAME	COMPANY 2 NAME	DESCRIPTION	DEAL SIZE
May 2024	Agreement	Radware (Israel)	Lightpath (US)	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 DefensePro DDoS Protection to offer customers a DDoS scrubbing service designed to combat today's increasingly complex threats.	NA
September 2023	Partnership	Akamai Technologies (US)	Corero Network Security (UK)	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.	NA
November 2022	Partnership	Link11 (Germany)	BSO (Ireland)	Link11 partnered with BSO, a global connectivity provider. Using BSO's infrastructure and stringent SLAs, LINK11 increased its network capacity to provide its customers with AI and machine-learning-powered DDoS mitigation.	NA
February 2022	Acquisition	Radware (Israel)	SecurityDAM (Israel)	Radware acquired cloud DDoS network operator SecurityDAM to accelerate the growth of its cloud security services business.	USD 30 Million
February 2022	Acquisition	Akamai Technologies (US)	Linode (US)	Akamai Technologies completed the acquisition of Linode to provide businesses with a developer-friendly and massively distributed platform to build, run, and secure applications.	USD 900 Million

Source: Press Releases

16.8 BRAND/PRODUCT COMPARISON

FIGURE 43 BRAND/PRODUCT COMPARISON

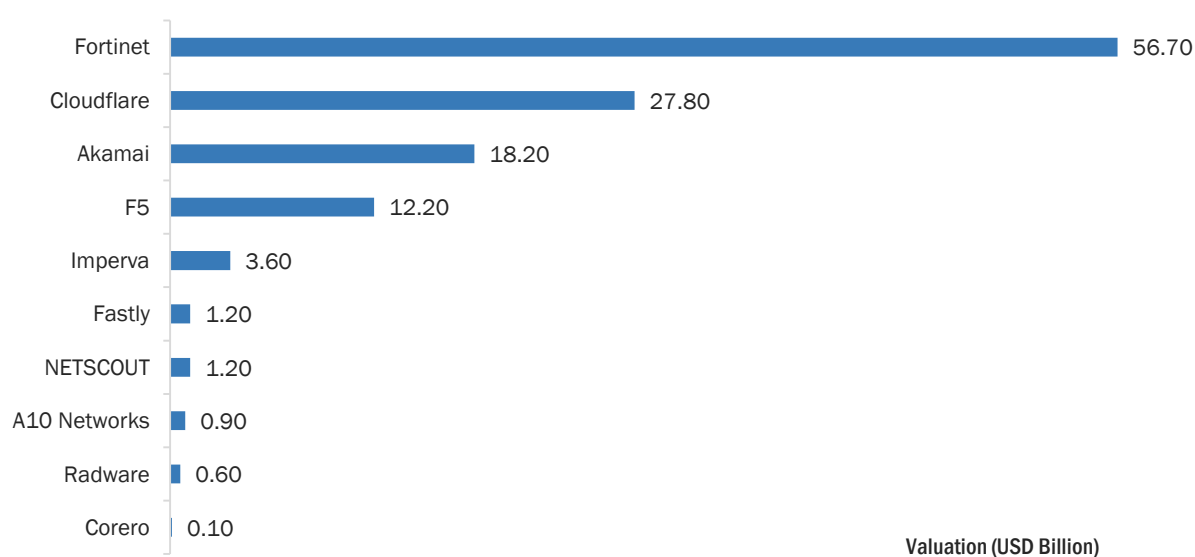
PARAMETERS	NETSCOUT	Akamai	radware	FORTINET	CLOUDFLARE
HARDWARE					
SOFTWARE					
SERVICES					
OFFERING	On-premises and Cloud-based	Cloud-based	On-premises and Cloud-based	On-premises and Cloud-based	Cloud-based
STRENGTHS	Deep packet inspection, real-time threat intelligence	Global network infrastructure, large-scale attack mitigation	Wide range of DDoS mitigation techniques, strong security features	Integrated security platform, performance optimization	Extensive global network, easy to use
WEAKNESSES	Can be complex to manage, may require significant upfront investment	Relies on cloud infrastructure, may have limitations for on-premises deployments	Can be expensive for large-scale deployments, may require specialized expertise	May be less flexible for custom configurations, focused on broader security solutions	Limited control over mitigation strategies, reliance on cloud infrastructure
 EXCELLENT  GOOD  FAIR  POOR					

Source: Secondary Research and MarketsandMarkets Analysis

16.9 COMPANY VALUATION AND FINANCIAL METRICS, 2025

16.9.1 COMPANY VALUATION

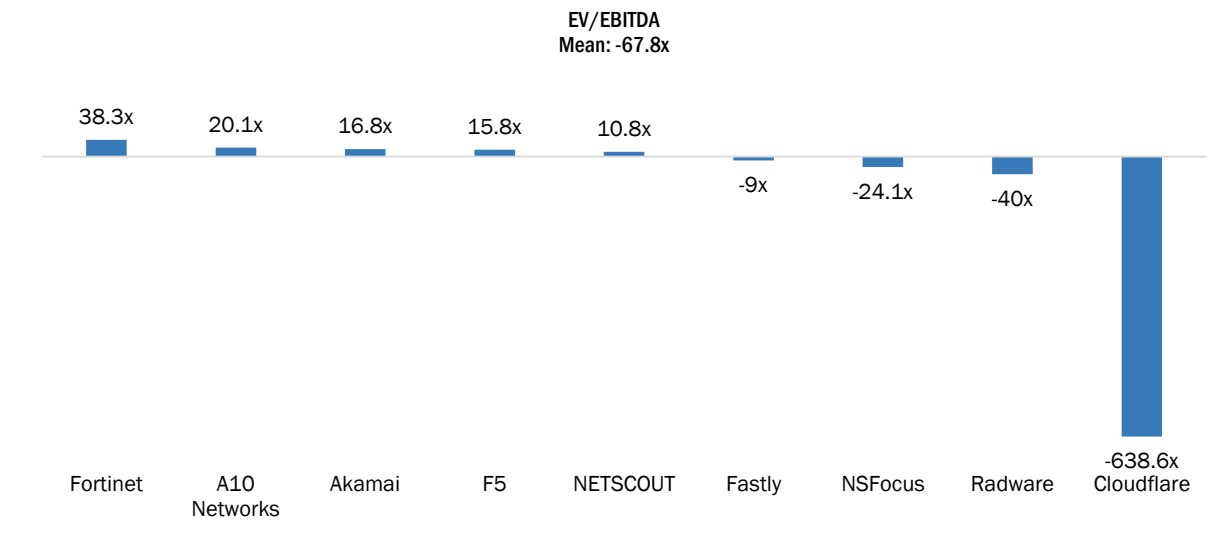
FIGURE 44 COMPANY VALUATION, 2025 (USD BILLION)



Source: Dealroom.co

16.9.2 FINANCIAL METRICS

FIGURE 45 FINANCIAL METRICS, 2025



Note: EV/EBITDA for all companies as of October 2025.

Source: Finbox.com

17 COMPANY PROFILES

17.1 KEY PLAYERS

17.1.1 NETSCOUT

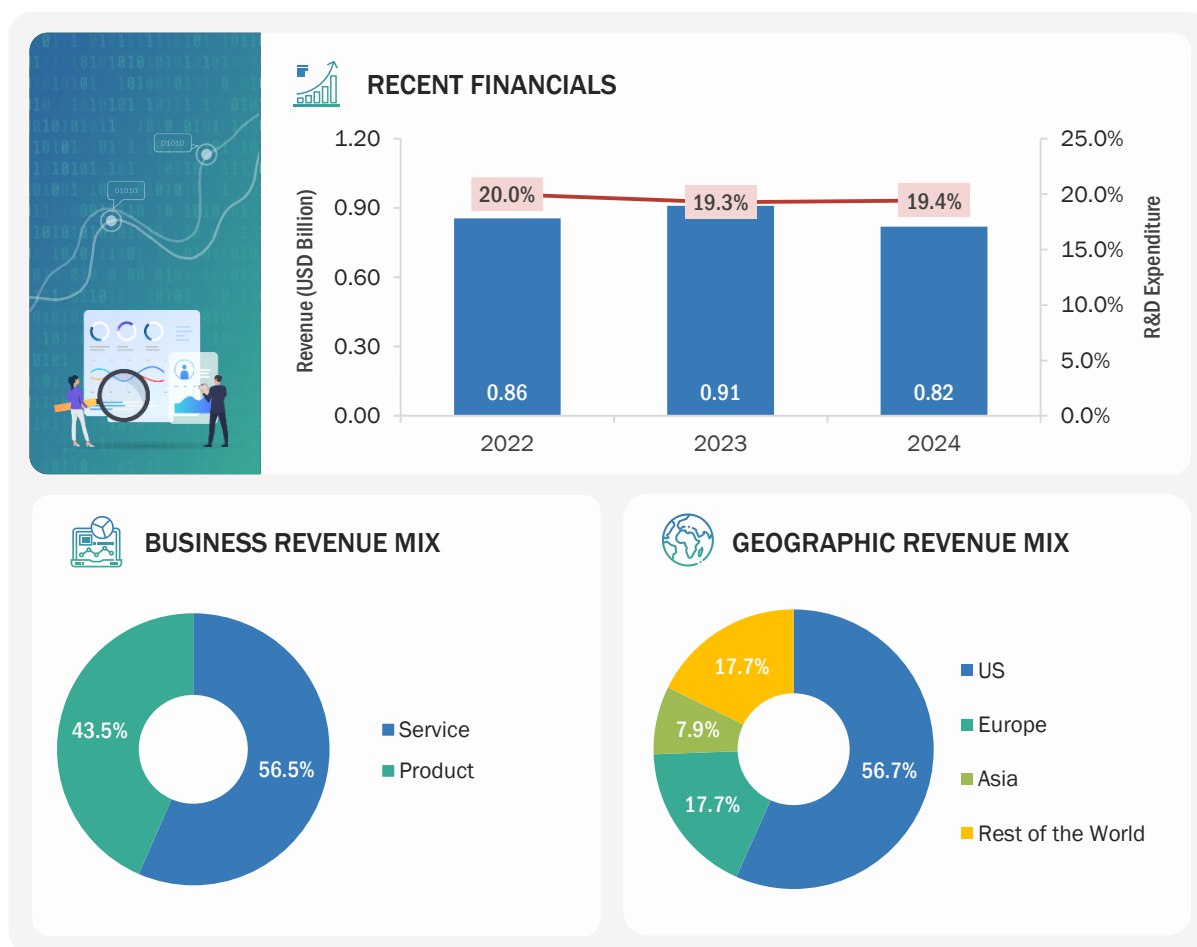
17.1.1.1 Business overview

NETSCOUT is one of the leading providers of application and network performance management solutions and products. Its product portfolio comprises business assurance, service assurance, and security assurance, along with advanced DDoS attack and threat solutions and business intelligence (BI) solutions. It offers various technology-based solutions, such as Network Functions Virtualization (NFV), Software-defined Networking (SDN), core network, Information Management System (IMS) monitoring, and radio access. It caters to a wide range of industry verticals, including government, retail banking, healthcare, pharmaceuticals, utilities, manufacturing, BFSI, education, and transportation. Arbor Networks is a security division of NETSCOUT that provides leading products and services in the DDoS protection and mitigation market. It has an extensive DDoS protection and mitigation product portfolio, including Arbor Networks APS, Arbor Cloud, and Arbor Networks TMS. Arbor Networks APS is an on-premises solution that helps in the decryption and analysis of encrypted traffic.

TABLE 448 NETSCOUT: COMPANY OVERVIEW

NETSCOUT	
Founded	1984
Country	US
City	Westford, Massachusetts
Ownership	Public (NASDAQ: NTCT)

Source: Company Website

FIGURE 46 NETSCOUT: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and MarketsandMarkets Analysis

17.1.1.2 Products/Solutions/Services offered

TABLE 449 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 offers over 11 Tbps of DDoS attack mitigation capacity via 14 worldwide scrubbing centers, providing global protection for organizations of any size.	Service	Security & Mitigation

Source: Company Website

17.1.1.3 Recent developments

17.1.1.3.1 Product launches & enhancements

TABLE 450 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

17.1.1.3.2 Deals

TABLE 451 NETSCOUT: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
September 2021	Collaboration	NETSCOUT (US)	NTT Communications (US)	NETSCOUT collaborated with NTT Communications on Threat Intelligence and DDoS Attack Resilience Research. The aim was to discover and mitigate large DDoS attacks, implement defense measures for application attacks, and identify new attacks before they became an issue.

Source: Press Releases

17.1.1.3.3 Expansions

TABLE 452 NETSCOUT: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
June 2024	Expansion	Facility	Canada	NETSCOUT (US)	NETSCOUT announced 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.

Source: Press Releases

17.1.1.4 MnM view

17.1.1.4.1 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.

17.1.1.4.2 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.

17.1.1.4.3 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.

17.1.2 AKAMAI TECHNOLOGIES

17.1.2.1 Business overview

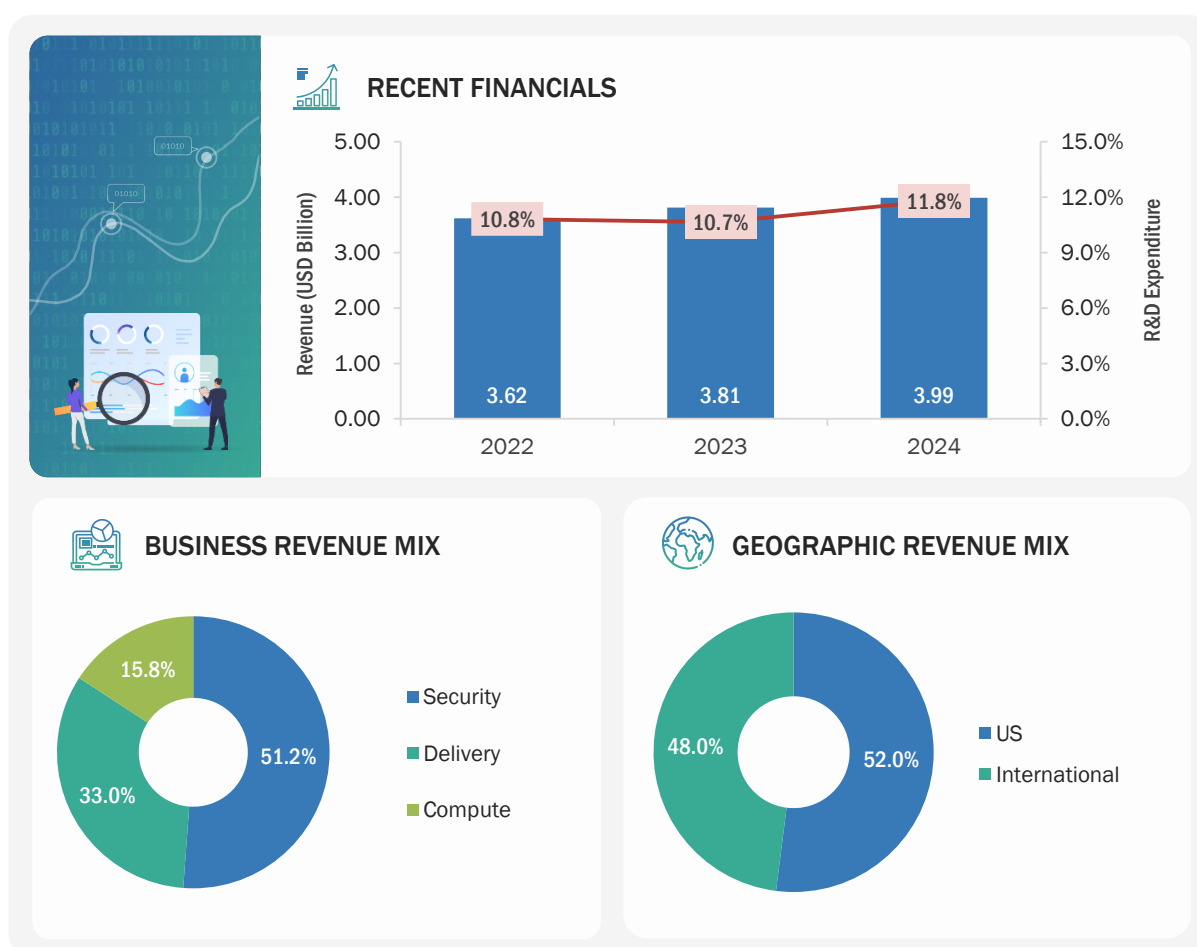
Akamai Technologies specializes in web and mobile acceleration, DNS and traffic management, media delivery, cloud security, and CDN. It offers security solutions, media delivery solutions, and network operator solutions. Its cloud security portfolio includes application protection, bot management, DDoS 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 Technologies 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 453 AKAMAI TECHNOLOGIES: COMPANY OVERVIEW

AKAMAI TECHNOLOGIES	
Founded	1998
Country	US
City	Cambridge, Massachusetts
Ownership	Public (NASDAQ: AKAM)

Source: Company Website

FIGURE 47 AKAMAI TECHNOLOGIES: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.2.2 Products/Solutions/Services offered**TABLE 454** AKAMAI TECHNOLOGIES: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/SOLUTION/SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Prolexic	It stops DDoS attacks with fast and effective defense at scale.	Software	Security
Kona Site Defender	Kona Site Defender protects websites and APIs against all types of sophisticated DDoS, web application, and direct-to-origin attacks, leveraging an always-on multilayered toolset. This solution blocks attacks at scale at the edge of Akamai's network and far away from your web server and applications.	Solution	Security
Web Application Protector	It protects web assets with less maintenance and fast activation.	Software	Security
Edge DNS	It is a cloud-based DNS solution that provides defense against DDoS attacks.	Software	Security

Source: Company Website

17.1.2.3 Recent developments

17.1.2.3.1 Product launches & enhancements

TABLE 455 AKAMAI TECHNOLOGIES: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
April 2023	Product launch	Akamai Technologies (US)	Prolexic (Platform)	Akamai Technologies announced the launch of its Prolexic Network Cloud Firewall. This new capability of Akamai Prolexic allowed customers to define and manage their own access control lists (ACLs) while enabling greater flexibility to secure their own network edge.
October 2022	Product enhancement	Akamai Technologies (US)	Prolexic (Platform)	Akamai's Prolexic launched a sixth-generation DDoS platform upgrade. This upgrade provided a strong foundation for future cybersecurity innovations, including enhanced detection and mitigation, deployment methodologies, expanded self-service controls, and other value-added capabilities beyond DDoS.

Source: Press Releases

17.1.2.3.2 Deals

TABLE 456 AKAMAI TECHNOLOGIES: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
September 2023	Partnership	Akamai Technologies (US)	Corero Network Security (UK)	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.	NA
February 2022	Acquisition	Akamai Technologies (US)	Linode (US)	Akamai Technologies completed the acquisition of Linode to provide businesses with a developer-friendly and massively distributed platform to build, run, and secure applications.	USD 900 Million
September 2021	Acquisition	Akamai Technologies (US)	Guardicore (US)	Akamai Technologies acquired Guardicore to expand its zero-trust technology solution with Guardicore's micro-segmentation technology.	USD 600 Million
February 2021	Acquisition	Akamai Technologies (US)	Inverse Inc. (US)	Akamai Technologies acquired Inverse Inc. to expand its zero-trust portfolio and IoT solutions.	NA

Source: Press Releases

17.1.2.3.3 Expansions

TABLE 457 AKAMAI TECHNOLOGIES: EXPANSIONS

MONTH & YEAR	DEVELOPMENT TYPE	EXPANSION TYPE	COUNTRY	COMPANY	DESCRIPTION
October 2023	Expansion	Facility	Canada	Akamai Technologies (US)	Akamai Technologies announced the launch of its latest Akamai Prolexic scrubbing centers in Toronto and Montreal. The new centers offered world-class DDoS protection to regional and global organizations, government institutions, and critical public infrastructure.
April 2023	Expansion	Facility	India	Akamai Technologies (US)	Akamai Technologies announced the deployment of two new scrubbing centers in Mumbai and Chennai, as part of its global infrastructure investment strategy to provide access to the strongest DDoS protections with increased performance for local businesses in India, as well as global organizations that have invested in the market in India.
February 2023	Expansion	Facility	Dubai	Akamai Technologies (US)	Akamai Technologies announced at the 2023 Gartner Security & Risk Management Summit the deployment of a new scrubbing center in Dubai, positioning its DDoS protection platform (Prolexic) to deliver the strongest security protections to organizations across the Middle East.

Source: Press Releases

17.1.2.4 MnM view

17.1.2.4.1 Right to win

Akamai Technologies 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.

17.1.2.4.2 Strategic choices

Akamai Technologies operates in three segments: performance and security solutions, media delivery solutions, and services and support 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.

17.1.2.4.3 Weaknesses and competitive threats

The company's primary revenue comes exclusively 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.

17.1.3 RADWARE

17.1.3.1 Business overview

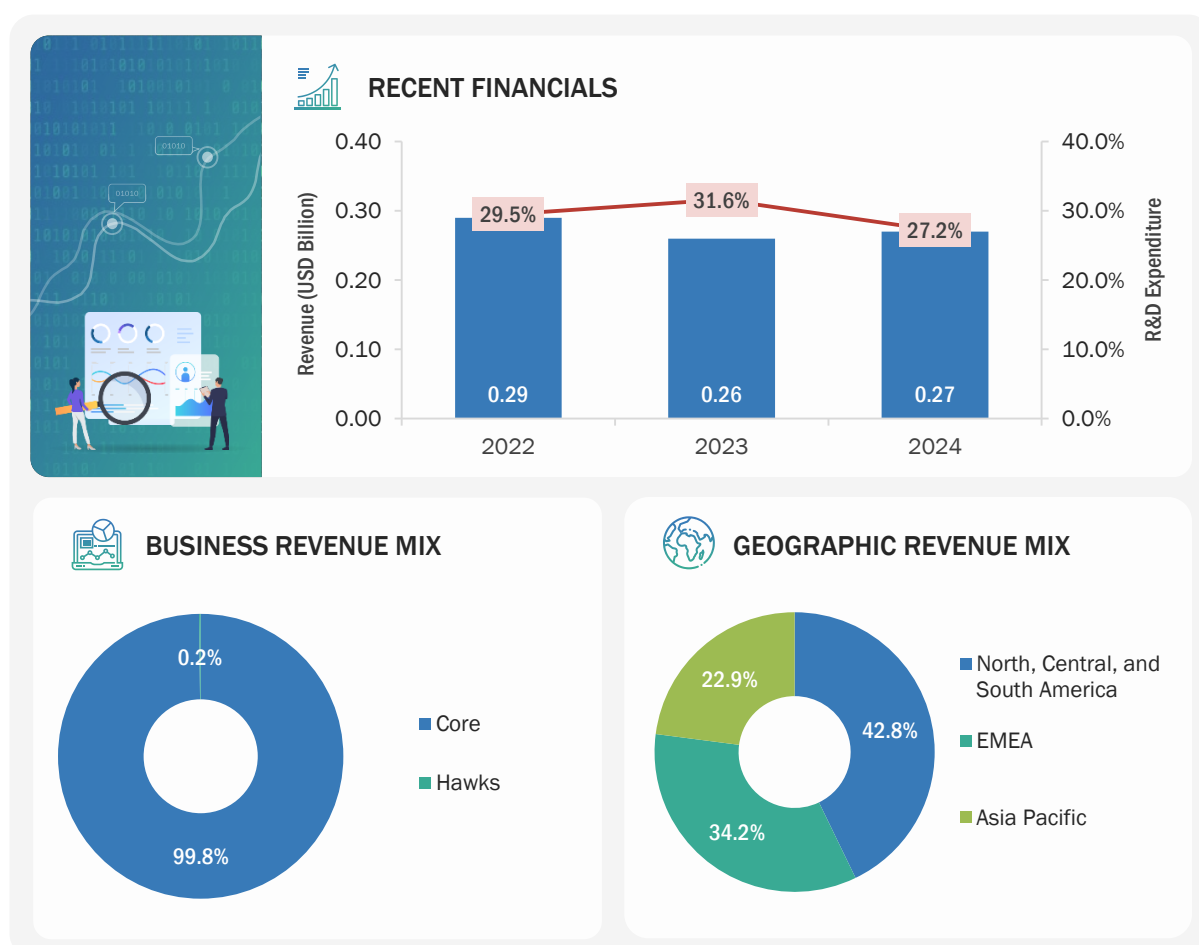
Radware specializes in application delivery and load balancing, as well as application and network security, and cloud security. It offers a variety of products for DDoS protection and mitigation, including DefensePro, Cloud DDoS Protection Service, and DefenseFlow. The company serves multiple industry sectors, including e-commerce, financial services, education, government, and healthcare. The company is focused on application integration with leading companies, such as Cisco, Citrix Systems, Microsoft, Oracle, SAP, and VMware. Its R&D centers are located in the US, Israel, and India. 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 458 RADWARE: COMPANY OVERVIEW

RADWARE	
Founded	1996
Country	Israel
City	Tel Aviv
Ownership	Public (NASDAQ: RDWR)

Source: Company Website

FIGURE 48 RADWARE: COMPANY SNAPSHOT



Source: Company Website and Annual Reports

17.1.3.2 Products/Solutions/Services offered

TABLE 459 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 enhance DDoS protection and extend its automated, real-time behavioral threat analysis for preemptive protection.	Service	Analysis & Security
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 460 RADWARE: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
August 2025	Program launch	Radware (Israel)	Cybersecurity Partner Program	Radware launched an enhanced Cybersecurity Partner Program to help MSSPs and channel partners scale managed security services, including DDoS protection, WAF, and application security offerings. The program introduced new incentives, onboarding tools, and training to strengthen its global managed security network.
April 2024	Product enhancement	Radware (Israel)	DNS DDoS Protection (Solution)	Radware introduced a new AI-powered, rule-free edition of its DNS DDoS Protection solution. Using Radware's patented algorithms, the enhanced version was designed to automatically distinguish between legitimate and actual attack traffic and instantly adapt DDoS defenses based on the specific attacker. For DNS service providers or companies that host their own DNS services, this could significantly shorten the time to resolution and reduce the total cost of ownership when countering even the most sophisticated DNS DDoS attack campaigns.
May 2023	Product launch	Radware (Israel)	Cloud Web DDoS Protection (Solution)	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 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.

Source: Press Releases

17.1.3.3.2 Deals

TABLE 461 RADWARE: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION	DEAL SIZE
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
May 2024	Partnership	Radware (Israel)	Lightpath (US)	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 DefensePro DDoS Protection to offer customers a DDoS scrubbing service designed to combat today's increasingly complex threats.	NA
February 2022	Acquisition	Radware (Israel)	SecurityDAM (Israel)	Radware acquired cloud DDoS network operator SecurityDAM to accelerate the growth of its cloud security services business.	USD 30 Million

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 CLOUDFLARE

17.1.4.1 Business overview

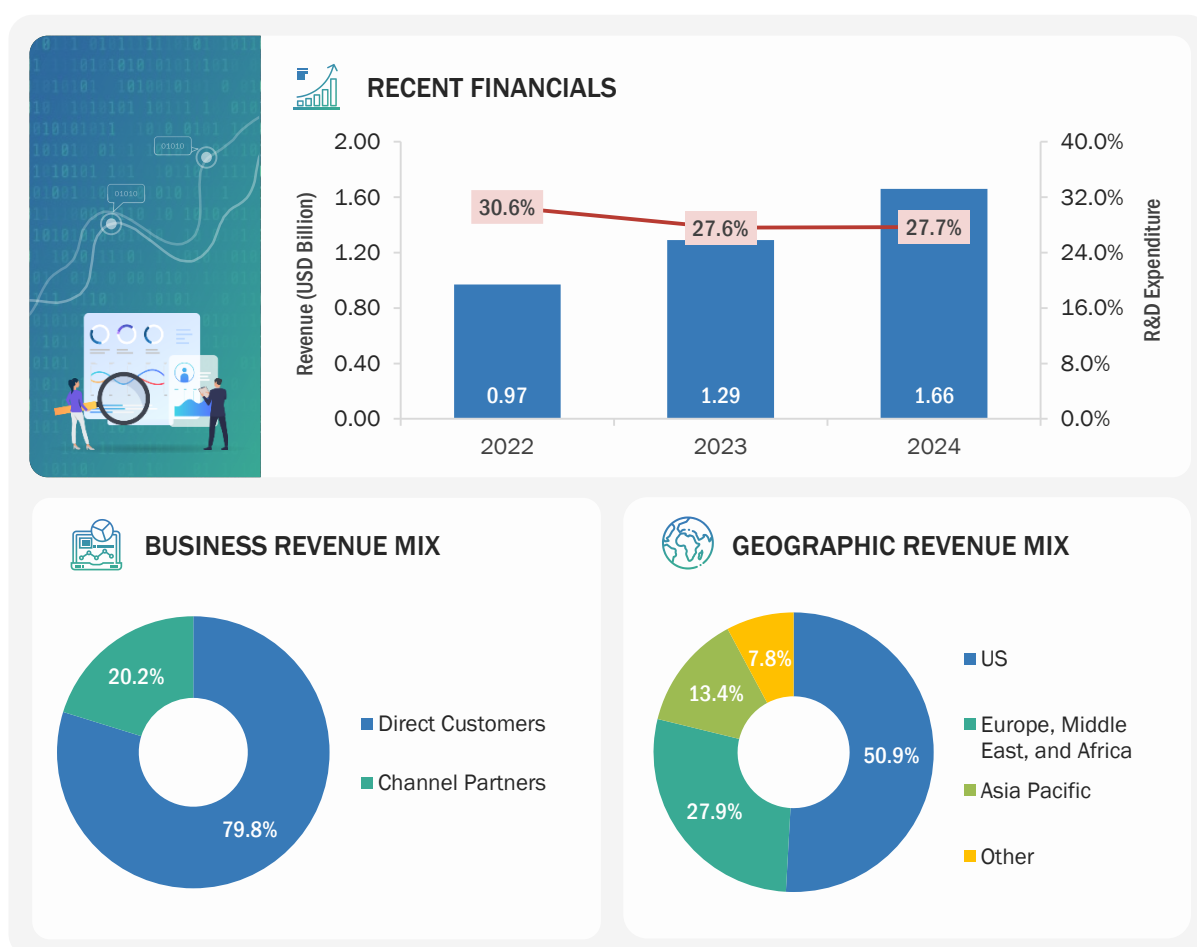
Cloudflare is a company that focuses on internet security and performance. It creates solutions to enhance the speed and protection of millions of websites, APIs, SaaS services, e-commerce platforms, and mobile applications. It offers services in CDN, DDoS protection, secure DNS, and security and web optimization. The company also provides enterprise-grade security and performance management solutions for large enterprises.

Cloudflare's global network spans more than 180 cities. It has the capacity to handle 15 Tbps of throughput, thus helping deliver better security and performance to customers. Some of its customers include NASDAQ, Cisco, Zendesk, Quizlet, and DigitalOcean. The company provides various pricing plans for personal, professional, e-commerce, and business websites targeting SMEs and larger organizations. Its offices are in North America, South America, Europe, Asia Pacific, and MEA.

TABLE 462 CLOUDFLARE: COMPANY OVERVIEW

CLOUDFLARE	
Founded	2009
Country	US
City	San Francisco, California
Ownership	Public (NYSE: NET)

Source: Company Website

FIGURE 49 CLOUDFLARE: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and MarketsandMarkets Analysis

17.1.4.2 Products/Solutions/Services offered

TABLE 463 CLOUDFLARE: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/SOLUTION/SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Cloudflare DDoS Protection	It secures websites, applications, and networks without compromising on legitimate traffic performance.	Software	DDoS Protection

Source: Company Website

17.1.4.3 MnM view

17.1.4.3.1 Key strengths

Cloudflare operates one of the world's largest DDoS mitigation networks, spanning more than 330 cities in over 120 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.

17.1.4.3.2 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.

17.1.4.3.3 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.

17.1.5 FORTINET

17.1.5.1 Business overview

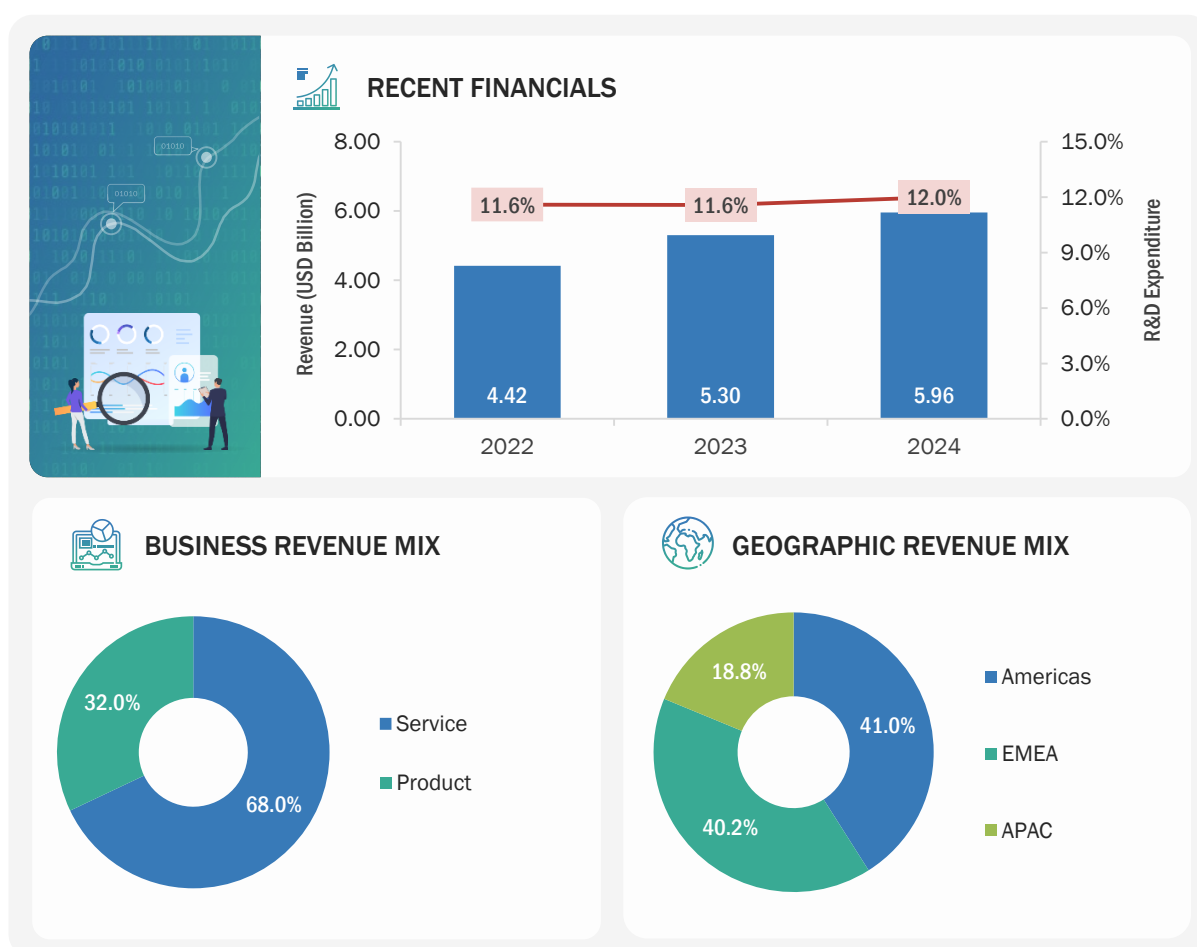
Fortinet is a leading provider of cybersecurity solutions to various businesses, such as enterprises, communication service providers, and small businesses. Its flagship product, FortiGate firewall, is renowned for advanced threat protection and secure access. The company's offerings extend to endpoint and cloud security, secure access technologies like VPN and ZTNA, and threat intelligence through integrated solutions. The company operates under four business areas: network security, Fortinet security fabric, cloud security, and IoT and operational technology.

The company provides a comprehensive range of solutions for small and medium-sized enterprises (SMEs). Fortinet also offers products tailored for carriers, cloud service providers, and managed security service providers (MSSPs). Its offerings cater to various industry sectors, including government, education, financial services, retail, and healthcare. With over 330,000 customers in 180 countries, the company has a broad customer base across the Americas, EMEA, and Asia Pacific.

TABLE 464 FORTINET: COMPANY OVERVIEW

FORTINET	
Founded	2000
Country	US
City	Sunnyvale, California
Ownership	Public (NASDAQ: FTNT)

Source: Company Website

FIGURE 50 FORTINET: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.5.2 Products/Solutions/Services offered**TABLE 465 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

17.1.5.3 Recent developments

17.1.5.3.1 Deals

TABLE 466 FORTINET: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
July 2021	Acquisition	Fortinet (US)	Sken.ai (US)	To accelerate DevSecOps, Fortinet acquired Sken.ai, an application security innovator.
March 2021	Acquisition	Fortinet (US)	ShieldX (US)	Fortinet acquired ShieldX, a cloud and network security provider.
January 2021	Agreement	Fortinet (US)	Savex (India)	As per an agreement, Fortinet appointed Savex as a value-added distributor in India.

Source: Press Releases

17.1.5.4 MnM view

17.1.5.4.1 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 security market.

17.1.5.4.2 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.

17.1.5.4.3 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 security market.

17.1.6 HUAWEI

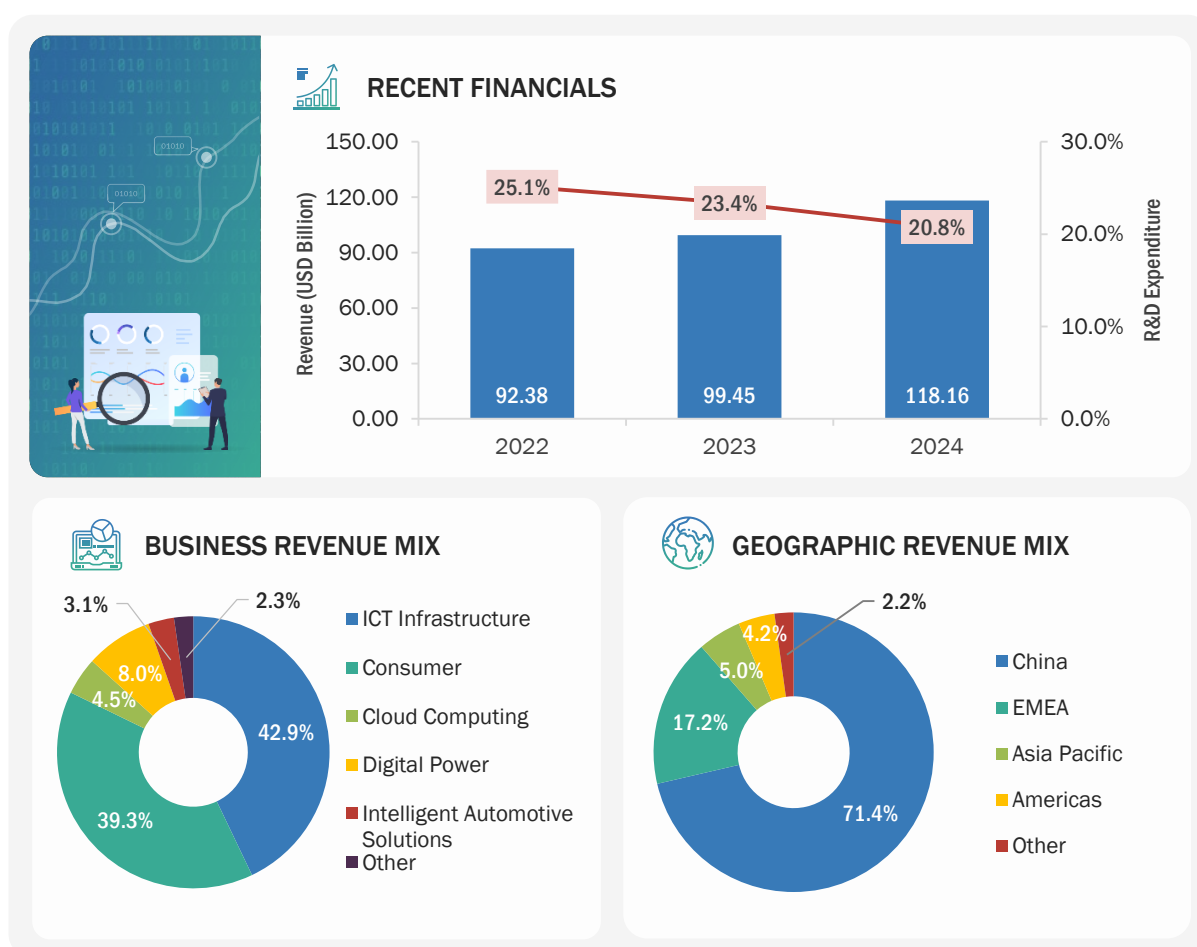
17.1.6.1 Business overview

Huawei is a privately owned global provider of information and communications technology (ICT) solutions, offering a comprehensive range of cybersecurity services across various industries. The company specializes in cloud computing, big data, connectivity, IoT, and artificial intelligence (AI) with integrated solutions across telecom networks, IT, smart devices, and cloud services. It operates in more than 170 countries. Its partner ecosystem comprises independent software vendors (ISVs), consulting companies, system integrators, independent hardware vendors (IHVs), channel partners, service partners, and talent alliance partners. The company has a global presence with offices in Asia Pacific, Europe, Latin America, the Middle East & Africa, and North America.

TABLE 467 HUAWEI: COMPANY OVERVIEW

HUAWEI	
Founded	1987
Country	China
City	Shenzhen
Ownership	Private

Source: Company Website

FIGURE 51 HUAWEI: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and MarketsandMarkets Analysis

17.1.6.2 Products/Solutions/Services offered

TABLE 468 HUAWEI: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
AntiDDoS8000 Series DDoS Protection System	It provides Terabit-level capacity, second-level response, precise protection, and value-added operations.	Hardware	Security
HiSecEngine AntiDDoS12000 Series Anti-DDoS system	It provides up to 2T+ security protection performance and service expansion capabilities, ideal for mitigating heavy-traffic DDoS attacks.	Hardware	Security & Mitigation

Source: Company Website

17.1.6.3 Recent developments

17.1.6.3.1 Deals

TABLE 469 HUAWEI: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
September 2021	Partnership	Huawei (China)	CloudExchange (Nigeria)	CloudExchange partnered with Huawei Cloud to expand data center infrastructure in Nigeria and West Africa.
June 2021	Partnership	Huawei (China)	Temenos (Switzerland)	Huawei partnered with Temenos to provide Temenos with cloud-native core banking solutions on Huawei's public cloud.

Source: Press Releases

17.1.7 LINK11

17.1.7.1 Business overview

Link11 is a leading cybersecurity provider specializing in DDoS protection for websites and IT infrastructures. Besides the patent-pending DDoS protection solution, the company offers additional services such as a WAF or a CDN, ensuring 360° protection and performance for its international customers.

The company was originally founded as a hosting provider and later developed a DDoS protection solution in 2011 to safeguard its customers and network. The company caters to Europe's large organizations across verticals such as media, financial, e-commerce, entertainment, and utilities. The company has a presence in Frankfurt, Amsterdam, London, Zurich, Los Angeles, Miami, New York, and Singapore, and further plans to expand its business functions across Asia and the Middle East. The company's AI-based DDoS protection solution is a part of the Link11 Cloud Security Platform and runs fully automated, ensuring real-time protection.

TABLE 470 LINK11: COMPANY OVERVIEW

LINK11	
Founded	2005
Country	Germany
City	Frankfurt
Ownership	Private

Source: Company Website

17.1.7.2 Products/Solutions/Services offered

TABLE 471 LINK11: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Infrastructure DDoS Protection	It is a cloud-based system that defends against DDoS attacks on applications and services. This system includes a globally distributed DDoS scrubbing center architecture.	Software	-
Web DDoS Protection	It is an automated protection solution that protects against potential online threats.	Software	-
Secure CDN	The Secure Content Delivery Network (CDN) is an addition to DDoS protection to increase security.	Software	-

Source: Company Website

17.1.7.3 Recent developments

17.1.7.3.1 Product launches & enhancements

TABLE 472 LINK11: PRODUCT LAUNCHES & ENHANCEMENTS

MONTH & YEAR	DEVELOPMENT TYPE	COMPANY NAME	PRODUCT NAME (PRODUCT TYPE)	DESCRIPTION
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

17.1.7.3.2 Deals

TABLE 473 LINK11: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
November 2022	Partnership	Link11 (Germany)	BSO (Ireland)	Link11 partnered with BSO, a global connectivity provider. Using BSO's infrastructure and stringent SLAs, LINK11 increased its network capacity to provide its customers with AI and machine-learning-powered DDoS mitigation.
January 2021	Acquisition	Link11 (Germany)	DOSarrest (Canada)	Link11 acquired DOSarrest to strengthen its customer base in Europe, North America, and Asia.

Source: Press Releases

17.1.8 IMPERVA (A THALES COMPANY)

17.1.8.1 Business overview

Imperva is a global provider of cybersecurity solutions and services that protect business-critical websites, applications, and databases. Imperva was acquired in October 2018 by Thoma Bravo, LLC, a leading private equity technology investment firm. It specializes in DDoS protection, application security, database security, file security, cloud security, breach prevention, and cybersecurity platforms. Imperva safeguards any critical data that is stored on-premises and in cloud environments. It has progressed in the DDoS protection and mitigation market by offering products like Website DDoS Protection, Name Server DDoS Protection, and Infrastructure DDoS Protection.

In December 2023, Thoma Bravo announced the completion of its sale of Imperva to Thales in an all-cash transaction that values Imperva at approximately USD 3.6 billion, creating a global leader in cybersecurity, with more than 5,800 cybersecurity experts across 68 countries. Thales completed the acquisition of Imperva in January 2024, marking a new step in the expansion of its global cybersecurity capabilities for enterprises and governments around the world.

TABLE 474 IMPERVA: COMPANY OVERVIEW

IMPERVA	
Founded	2000
Country	US
City	Seattle, Washington
Ownership	Subsidiary of Thales

Source: Company Website

17.1.8.2 Products/Solutions/Services offered

TABLE 475 IMPERVA: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Imperva DDoS Protection for Websites	It complements Imperva Cloud Web Application Firewall (WAF) to block malicious bot attacks and hacking attacks on websites.	Software	Security
Imperva DDoS Protection for Networks	The critical network assets are protected by DDoS protection for networks through DDoS mitigation.	Software	Security & Mitigation
Imperva DDoS Protection for Individual IPs	It provides an easy-to-manage solution and critical protection for any services exposed to the internet.	Software	Security
Imperva DDoS Protection for DNS	It is an always-on service that protects against DDoS targeting domain name servers.	Software	Security

Source: Company Website

17.1.8.3 Recent developments

17.1.8.3.1 Deals

TABLE 476 IMPERVA: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
May 2021	Acquisition	Imperva (US)	Cloud Vector (UK)	Imperva announced the acquisition of Cloud Vector to expand its web application and API protection services.

Source: Press Releases

17.1.9 BT

17.1.9.1 Business overview

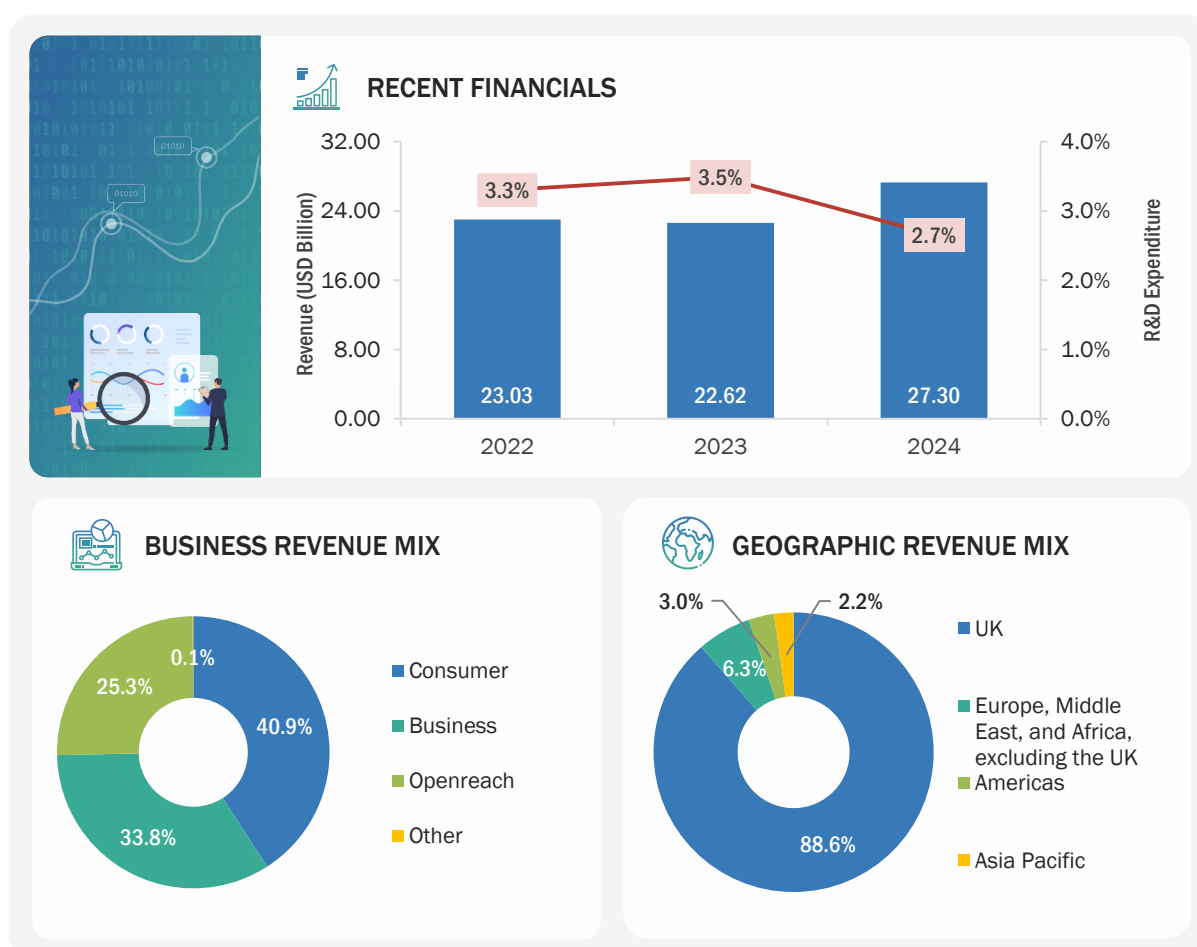
Formerly known as British Telecom, BT has established itself as a strong brand over its decades of legacy. BT has developed a broad portfolio of differentiated products. It provides managed DDoS protection, which handles internet traffic by sorting through normal and malicious requests. The protection system is activated if any suspicious traffic is detected, and a DDoS attack is separated from legitimate traffic.

In 2021, Altice, a French telecommunications company, acquired a 12% stake in BT. Its thousands of employees serve customers in around 180 countries. It is one of the largest providers of mobile services, broadband, and fixed-line services in the UK. It also provides IT services and subscription-based television that caters to around 18 million customers worldwide.

TABLE 477 BT: COMPANY OVERVIEW

BT	
Founded	1980
Country	England
City	London
Ownership	Public (LON: BT.A)

Source: Company Website

FIGURE 52 BT: COMPANY SNAPSHOT

Source: Company Website, Annual Reports, and Investor Presentations

17.1.9.2 Products/Solutions/Services offered**TABLE 478** BT: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Managed DDoS Protection	A platform for detection and mitigation, it detects rogue traffic.	Software	DDoS Protection & Mitigation

Source: Company Website

17.1.9.3 Recent developments**17.1.9.3.1** Deals**TABLE 479** BT: DEALS

MONTH & YEAR	DEAL TYPE	COMPANY 1	COMPANY 2	DESCRIPTION
November 2021	Partnership	BT (UK)	OneWeb (UK)	BT partnered with OneWeb to provide a low Earth orbit (LEO) satellite network and connectivity services.

Source: Press Releases

17.1.10 A10 NETWORKS

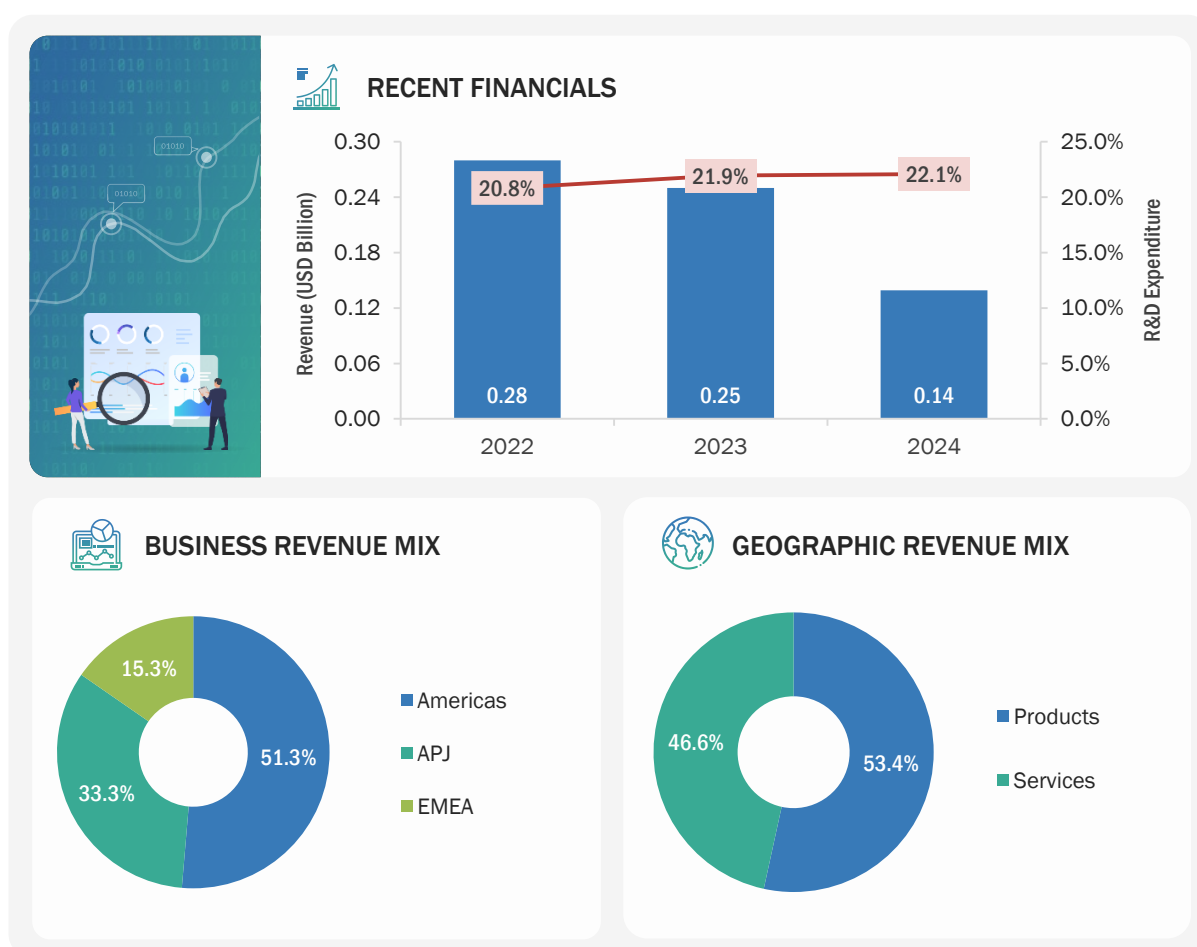
17.1.10.1 Business overview

A10 Networks is a US-based company specializing in networking and cybersecurity 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 480 **A10 NETWORKS: COMPANY OVERVIEW**

A10 NETWORKS	
Founded	2004
Country	US
City	San Jose, California
Ownership	Public (NYSE: ATEN)

Source: Company Website

FIGURE 53 A10 NETWORKS: COMPANY SNAPSHOT

Source: Company Website and Annual Reports

17.1.10.2 Products/Solutions/Services offered**TABLE 481** A10 NETWORKS: PRODUCTS/SOLUTIONS/SERVICES OFFERED

PRODUCT/ SOLUTION/ SERVICE	DESCRIPTION	PRODUCT TYPE	APPLICATION
Thunder Threat Protection Systems (TPS)	It is powered by advanced machine learning to provide scalable and automated DDoS protection.	Software	Security

Source: Company Website

17.1.11 NSFOCUS

17.1.11.1 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 482 NSFOCUS: COMPANY OVERVIEW

NSFOCUS	
Founded	2000
Country	US
City	Santa Clara, California
Ownership	Public (SHE: 300369)

Source: Company Website

17.1.11.2 Products/Solutions/Services offered

TABLE 483 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 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.	Solution	DDoS Protection & Mitigation
Services	NSFOCUS offers various services, such as product support services, professional services, and managed security services.	Services	NA

Source: Company Website

17.1.12 NEXUSGUARD

17.1.12.1 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 484 NEXUSGUARD: COMPANY OVERVIEW

NEXUSGUARD	
Founded	2008
Country	Singapore
City	Singapore
Ownership	Private

Source: Company Website

17.1.12.2 Products/Solutions/Services offered

TABLE 485 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

17.1.12.3 Recent developments

17.1.12.3.1 Deals

TABLE 486 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 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.
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 optimizes performance and reduces 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.
November 2021	Partnership	Nexusguard (Singapore)	RETN (England)	Nexusguard and RETN partnered via their Transformational Alliance Partner program to integrate advanced DDoS protection directly into its global IP Transit infrastructure. By deploying Nexusguard's Bastions technology, RETN transformed its service model from simple connectivity to a comprehensive security-as-a-service provider. This partnership significantly enhanced RETN's technical capabilities, resulting in a 5,000% increase in scrubbing capacity and a 54% reduction in latency. The partnership allowed RETN to differentiate its portfolio and provide superior, high-performance network security to its global enterprise clients.

Source: Press Releases

17.2 OTHER 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. Founded in 2002 and headquartered in California, 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 e-commerce, 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. While Fastly has faced challenges, such as service outages, it continues to focus on expanding its edge cloud infrastructure and enhancing security offerings to meet the growing demand for fast and secure content delivery.
Products/Solutions Offered	DDoS Protection and Mitigation Service
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

17.2.2 F5

Founded	1996
Country	US
City	Seattle, Washington
Ownership	Public (NASDAQ: FFIV)
Business Overview	F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. It specializes in multi-cloud security, application services, and delivery solutions that help enterprises enhance and secure digital experiences. The company focuses on optimizing the performance, security, and reliability of applications, whether deployed on-premises, in the cloud, or in hybrid environments. F5 offers services like load balancing, application firewalls, bot protection, and cloud-native solutions, addressing key areas such as application availability, scalability, and security. It partners with the world's largest, most advanced organizations to optimize and secure every app and API anywhere, including on-premises, in the cloud, or at the edge. The company enables organizations to provide exceptional, secure digital experiences for their customers and to continuously stay ahead of threats.
Products/Solutions Offered	Distributed Cloud Services Enterprise Application Security and Delivery Solutions
Geographic Presence	North America, Europe, Asia Pacific, the Middle East & Africa, and Latin America

Source: Company Website

17.2.3 CORERO

Founded	2011
Country	London, UK
Ownership Type	Public (LON: CNS)
Business Overview	Corero Network Security is a champion of service availability and business resiliency, delivered through its high-performance and real-time SmartWall ONE DDoS defense solutions and cloud-native observability and resiliency platform, CORE, to service providers, hosting providers, and digital enterprises. Corero has a global presence, with offices in London and Edinburgh in the UK, Massachusetts in the US, and focuses on growth strategies that deliver its solutions and related services through regional channel partners and global strategic alliances. Corero's SmartWall ONE is a fast, automatic, and accurate solution that can detect and block over 98% of DDoS attacks in under a second. Its behavioral-based protection defends against known and emerging attacks out of the box, without needing to be trained on peacetime traffic. It can handle network-based DDoS attacks, including those using multi-vector and spread spectrum evasion techniques, of all sizes, from the largest to those that can be too short or low to be detected by other solutions Corero's CORE (Observability & Resiliency Ecosystem) is a cloud-native, bring your own cloud (BYOC), platform that includes real-time visibility and automated protection against modern multi-vector and application-layer (Layer 7) DoS and DDoS attacks. It integrates seamlessly with Corero's SmartWall ONE solution and existing network infrastructure to eliminate security blind spots and reduce mitigation times from minutes to seconds. In addition, Corero offers SecureWatch Fully Managed Services, with 24/7 expert-led monitoring and mitigation that allows organizations to outsource their DDoS defense, fully or partially, to its Security Operations Center (SOC). It combines their automated protection technology with human intelligence to optimize security policies, manage incident responses, and provide detailed forensic reporting, without needing in-house DDoS expertise.
Products/Solutions Offered	▪ SmartWall ONE DDoS Protection ▪ CORE Cloud-native Business Continuity Platform ▪ SecureWatch Managed Services
Geographic Presence	North America, Europe, Asia Pacific, Middle East & Africa, and Latin America

Source: Company Website

17.2.4 ALLOT

Founded	1996
Country	Israel
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

17.2.5 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
Geographic Presence	North America

Source: Company Website

17.2.6 SUCURI

Founded	2010
Country	US
City	Menifee, California
Ownership Type	Private
Business Overview	Sucuri is a managed security service provider for websites. It also provides Content Distribution Network (CDN) services to websites. It helps websites load faster and increase their resilience to attacks from malware, DDoS attacks, and other hacker activities. Sucuri provides DDoS protection with all its products, including website security platforms, WordPress security, enterprise security, and website firewalls.
Products/Solutions Offered	▪ Website Security Platform ▪ WordPress Security ▪ Enterprise Security ▪ Website Firewall
Geographic Presence	North America, Europe, and Asia Pacific

Source: Company Website

17.2.7 LUMEN TECHNOLOGIES

Founded	2010
Country	US
City	Menifee, California
Ownership Type	Private
Business Overview	Lumen Technologies is a US-based telecommunications and technology company offering network connectivity, edge computing, cloud solutions, and cybersecurity services to global enterprises. The company operates one of the largest and most connected fiber networks in the world, supporting secure data transmission and digital transformation across industries. In the area of DDoS protection, Lumen provides a DDoS Mitigation Service designed to detect and mitigate large-scale and multi-vector attacks. The solution leverages Lumen's global scrubbing centers and Black Lotus Labs threat intelligence to filter malicious traffic and maintain network availability. It offers both on-demand and always-on deployment options, with a mitigation capacity exceeding 170 Tbps, ensuring continuous protection for enterprise networks and online applications.
Products/Solutions Offered	▪ Agile DDoS protection solutions ▪ Uses Black Lotus Labs threat intelligence ▪ Protects network & application layers ▪ 24/7 monitoring and rapid threat defense ▪ 170 Tbps global mitigation capacity ▪ Supports IPv4/IPv6 ▪ On-Demand or Always-On deployment ▪ Carrier-agnostic protection ▪ Add-ons: WAF and bot management ▪ Lumen DDoS Mitigation Service ▪ Automated detection and mitigation ▪ On-Demand or Always-On models ▪ Clean traffic return via GRE or Internet Direct ▪ Self-service portal for configuration ▪ Backed by Black Lotus Labs threat intel ▪ Supports IPv4/IPv6, up to 100 Gbps clean traffic return ▪ Optional: SOC advanced support, WAF/API/Bot protection
Geographic Presence	North America and Asia Pacific

Source: Company Website

17.3 SMES/STARTUPS

17.3.1 SECEON

Founded	2014
Country	US
City	Westford, Massachusetts
Ownership Type	Private
Business Overview	Seceon specializes in network security, DDoS protection and mitigation, data center security, cloud security, and security analytics. The company helps customers safeguard their entire infrastructure, which includes endpoints, cloud environments, servers, and mobile devices, from DDoS threats, malware, ransomware, and other known and unknown threats. It provides its products and services to large enterprises, SMEs, and MSPs in different industry verticals, such as government, finance, retail, education, healthcare, and IT and telecom. Seceon has an extensive partner ecosystem, which includes business and technology partners. Some of the significant partners of the company include Tech Mahindra, SonicWall, AWS, Paramount, TechLab Security, and Exertis.
Products/Solutions Offered	Seceon Open Threat Management (OTM)
Geographic Presence	North America, Europe, Asia Pacific, and the Middle East & Africa

Source: Company Website

17.3.2 HALTDOS

Founded	2015
Country	India
City	Noida
Ownership Type	Private
Business Overview	Haltdos provides intelligent, multi-layered security WAF and DDoS mitigation services to online businesses requiring zero management. It gives a self-learning solution to provide real-time and historical insights with visualizations. This solution continuously learns and adapts to network/website traffic. The company specializes in DDoS protection, mitigation, web application firewalls, and security. Its DDoS security solution provides attack notifications and alerts, attack signatures, and audit trails. Haltdos also provides an enterprise anti-DDoS solution, Haltdos-Falcon, which protects the enterprise from illegitimate traffic.
Products/Solutions Offered	- Haltdos DDoS Protection Service - Haltdos Falcon Enterprise Anti-DDoS Solution
Geographic Presence	North America and Asia Pacific

Source: Company Website

17.3.3 DDOS-GUARD

Founded	2011
Country	Rostov-on-Don, Russia
Ownership Type	Private
Business Overview	DDoS-Guard started providing Denial-of-Services protection to the Russian Ministry of Defense in 2016, and in 2018, it helped test the Russian state's deep packet inspection systems. Similarly, the Russian Central Bank cooperates closely with DDoS-Guard. DDoS-Guard provides DDoS protection along with its other services, such as website protection and optimization, protected and dedicated servers, network protection, bot mitigation, and web application firewall. The company uses proprietary software working with high-performance computing clusters for traffic scrubbing. The scrubbing centers are located in different places such as Russia, the US, Kazakhstan, Peru, Hong Kong, and the Netherlands.
Products/Solutions Offered	DDoS Website Protection and Optimization
Geographic Presence	North America, Europe, and Asia Pacific

Source: Company Website

17.3.4 INDUSFACE

Founded	2012
Country	Maharashtra, India
Ownership Type	Private
Business Overview	Indusface is a SaaS company that offers security solutions through its platform, which combines web application scanners, web application firewalls, a content delivery network (CDN), and a threat information engine. Indusface's AppTrana provides fully managed protection for web applications and APIs, delivering real-time defense against OWASP exploits, DDoS attacks, bot mitigation, and zero-day vulnerabilities. Indusface's AppTrana is a total application security platform that detects, protects, and monitors applications. This solution is available on-premises, as a service, and through the AWS marketplace. Indusface serves more than 2,000 clients globally, including well-known brands like Tata Consultancy Services, HDFC Life, NASSCOM, Aegon Life, Crisil, and many more.
Products/Solutions Offered	▪ Indusface AppTrana ▪ Application Security ▪ Web Application Scanning ▪ WEB Application firewall
Geographic Presence	North America and Asia Pacific

Source: Company Website

17.3.5 ACTIVEREACH

Founded	2008
Country	UK
City	High Wycombe, Buckinghamshire
Ownership Type	Private (Subsidiary of Babble)
Business Overview	activereach serves in areas of security and connectivity with IT solutions and services. It helps organizations maximize business value from their technological investments with its independent consultative approach and provides a platform for businesses to grow, reinvent, and transform. The company offers the most innovative hosted, on-premises, and cloud-based services through partnerships and collaborations with many of the world's leading technology vendors and software providers. Hundreds of businesses have transformed with consultancy, technology, and services provided by activereach. activereach serves a diverse range of clients, including Fortune 500 companies, large corporations, and SMEs.
Products/Solutions Offered	▪ activeDEFENCE ▪ activeNETWORKS
Geographic Presence	North America

Source: Company Website

17.3.6 MLYTICS

Founded	2017
Country	Singapore
Ownership Type	Private
Business Overview	Mlytics builds a platform that monitors the internet and routes web traffic across multiple CDNs to avoid downtime and congestion with full security features built in. It offers unmetered, always-on DDoS protection for web assets through aggregated multi-CDNs, AI detection, and auto-switching between the CDN consortium and the largest number of nodes. Mlytics applies rate controls to API requests and inspects JSON and XML API calls to ensure that the web server remains available and the data is secure. Mlytics has developed a SaaS platform driven by machine learning technology that can help companies at different scales to optimize websites/web apps.
Products/Solutions Offered	▪ CDN DDoS Protection ▪ Mlytics Origin DDoS Protection
Geographic Presence	Europe and Asia Pacific

Source: Company Website

17.3.7 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

17.3.8 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 17 servers 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

17.3.9 COMODO SECURITY SOLUTIONS

Founded	2005
Country	Romania
City	Iasi
Ownership Type	Private
Business Overview	Comodo provides digital security, identity, and trust assurance services with a portfolio that includes digital certificates, managed PKI solutions, authentication, and network vulnerability scanning. In the area of DDoS protection, Comodo offers website and network security solutions that integrate a Web Application Firewall (WAF), Content Delivery Network (CDN), and traffic monitoring tools to identify and mitigate DDoS attacks. These offerings help maintain website uptime, ensure stable network performance, and protect against large-scale traffic disruptions across online platforms.
Products/Solutions Offered	▪ Web Application Firewall (WAF) ▪ Content Delivery Network (CDN)
Geographic Presence	Europe

Source: Company Website

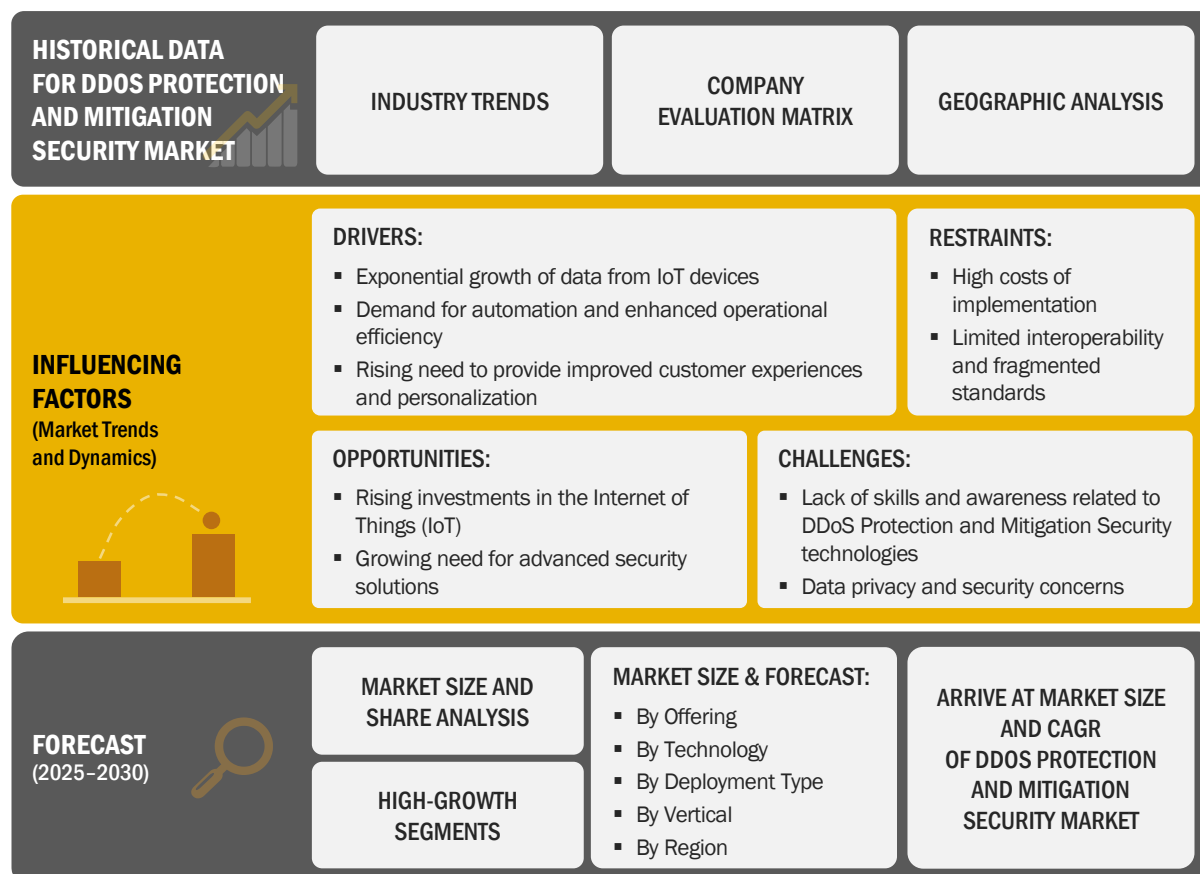
18 RESEARCH METHODOLOGY

18.1 RESEARCH DATA

The DDoS protection and mitigation security market study extensively used secondary sources, directories, and databases, such as D&B Hoovers, Bloomberg Businessweek, and Factiva. Other market-related sources, such as journals and white papers from industry associations, were also considered while conducting the secondary research. Primary sources were mainly industry experts from core and related industries, preferred system developers, service providers, system integrators, resellers, partners, and organizations related to the various segments of the industry's value chain. In-depth interviews were conducted with primary respondents to obtain and verify critical qualitative and quantitative information and assess the market's prospects. These respondents included key industry participants, subject matter experts, C-level executives of key market players, and industry consultants.

The figure below outlines the market research methodology used in preparing this report.

FIGURE 54 DDOS PROTECTION AND MITIGATION SECURITY MARKET: RESEARCH DESIGN



Source: Secondary Research, Industry Experts, and MarketsandMarkets Analysis

18.1.1 SECONDARY DATA

The market size of the companies offering DDoS protection and mitigation security software and services globally was based on the secondary data available through paid and unpaid sources. It was also arrived at by analyzing the product portfolios of the major companies and rating companies based on their performance and quality.

In the secondary research process, various secondary sources were referred to identify and collect information for the study. The secondary sources included annual reports, press releases, investor presentations of companies, white papers, certified publications, and articles from recognized associations and government publishing sources. Several journals and associations, such as DDoS white papers by Active Reach, AWS Best Practices for DDoS Resiliency, DDoS architecture and whitepaper by F5; journals such as An Effective Mechanism To mitigate Real-Time DDoS Attacks, DDoS Attacks Prevention and Mitigation Techniques, were also referred to. Secondary research was used to obtain key information about industry insights, the market's monetary chain, the overall pool of key players, market classification and segmentation according to industry trends to the bottom-most level, regional markets, and key developments from both the market and technology-oriented perspectives.

Secondary research was used to obtain key information about the industry's supply chain, the total pool of key players, market classification, and segmentation according to the industry trends to the bottom-most level, regional markets, and key developments from both market and technology-oriented perspectives, all of which were further validated by primary sources.

18.1.2 PRIMARY DATA

In the primary research process, various primary sources from both the supply and demand sides were interviewed to obtain qualitative and quantitative information for the report. The primary sources from the supply side included industry experts, such as chief executive officers (CEOs), chief technology officers (CTOs), chief operating officers (COOs), Vice Presidents (VPs), marketing directors, technology and innovation directors, and related key executives from various key companies and organizations operating in the DDoS protection and mitigation security market. The primary sources from the demand side included DDoS protection and mitigation security end users, consultants/specialists, chief information officers (CIOs), and subject-matter experts from enterprises and government associations.

After the complete market engineering process (including calculations for market statistics, market breakdown, market size estimations, market forecast, and data triangulation), extensive primary research was conducted to gather information and verify and validate the critical numbers arrived at. Primary research was also undertaken to identify and validate the segmentation types, industry trends, key players, the market's competitive landscape, and key market dynamics, such as drivers, restraints, opportunities, challenges, and key strategies.

In the complete market engineering process, the top-down and bottom-up approaches and data triangulation methods were used to estimate and forecast the overall market segments and subsegments listed in this report. Extensive qualitative and quantitative analysis was performed on the complete market engineering process to list the key information/insights throughout the report.

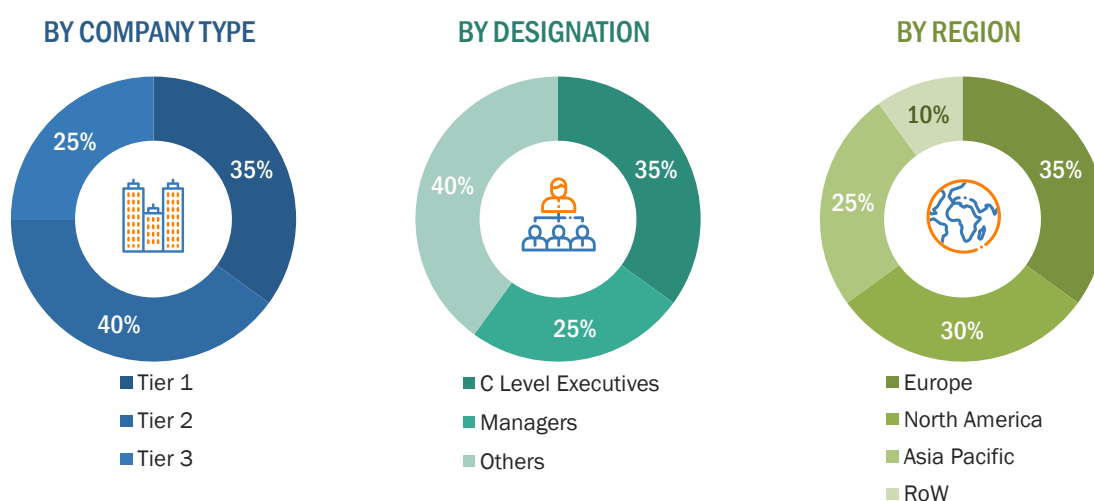
18.1.2.1 Primary interviews with experts

TABLE 487 PRIMARY INTERVIEWS WITH EXPERTS

PARTICULARS	INTENDED PARTICIPANTS/KEY OPINION LEADERS
Primary Interview Breakup	- DDoS protection and mitigation security providers - Academicians and research organizations - End users

18.1.2.2 Breakdown of primary profiles

FIGURE 55 BREAKDOWN OF PRIMARY INTERVIEWS, BY COMPANY TYPE, DESIGNATION, AND REGION



Notes: Tier-1 companies' revenue is more than USD 1 billion; Tier-2 companies' revenue ranges between USD 500 million and USD 1 billion; and Tier-3 companies' revenue ranges between USD 100 million and USD 500 million.

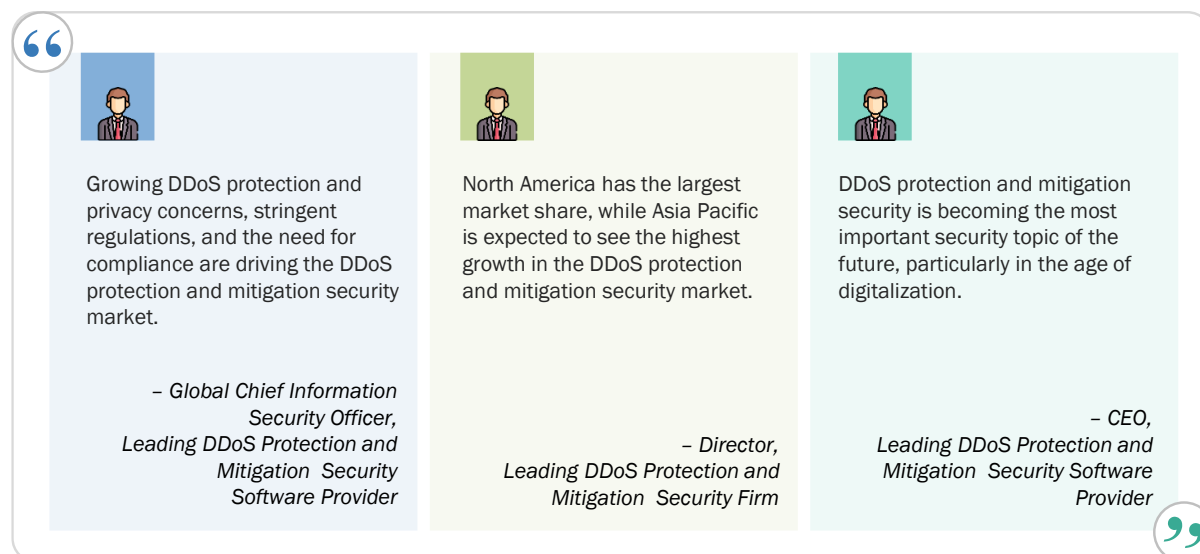
Other designations include sales, marketing, and product managers.

The rest of the world includes the Middle East & Africa and Latin America

Source: Industry Experts

18.1.2.3 Key insights from industry experts

FIGURE 56 KEY INSIGHTS FROM INDUSTRY EXPERTS



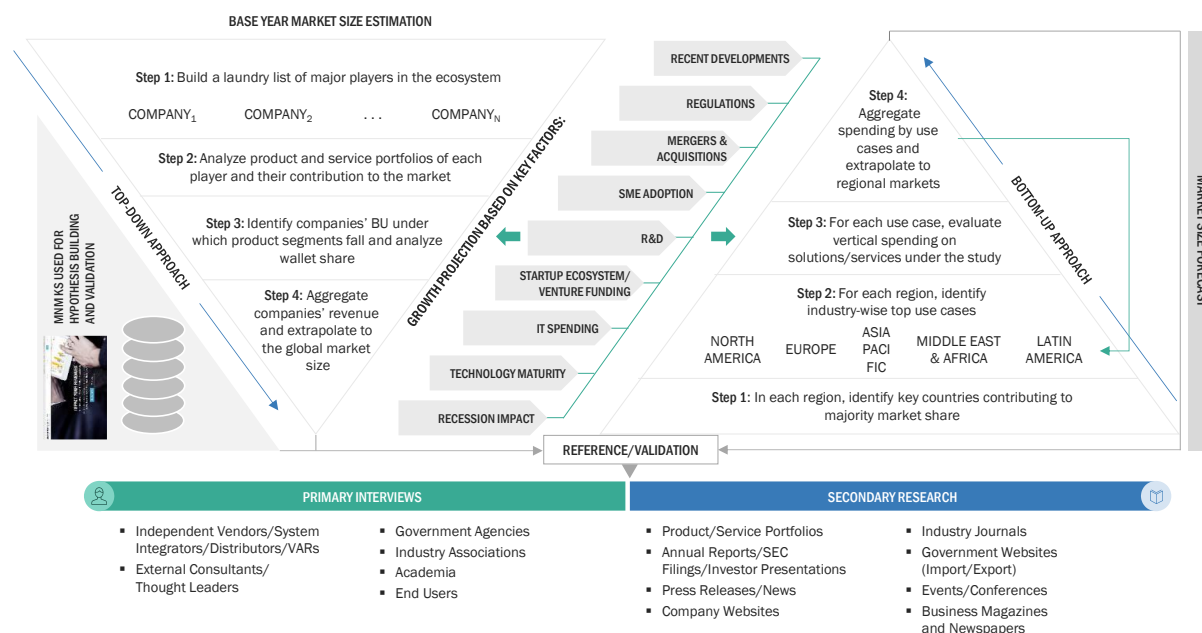
Source: Industry Experts

18.2 MARKET SIZE ESTIMATION

In the market engineering process, the top-down and bottom-up approaches and multiple data triangulation methods were used to estimate and validate the size of the DDoS protection and mitigation security market and other dependent submarkets. Key market players were identified through secondary research, and their market shares in the targeted regions were determined with the help of primary and secondary research. This entire research methodology included the study of annual and financial presentations of the top market players and interviews with experts for key insights (quantitative and qualitative).

The shares, splits, and breakdowns were determined using secondary sources and verified through primary research. All the possible parameters that affect the DDoS protection and mitigation security market were verified in detail with the help of primary sources and analyzed to obtain quantitative and qualitative data. This data was supplemented with detailed inputs and analysis from MarketsandMarkets and presented in the report.

FIGURE 57 DDOS PROTECTION AND MITIGATION SECURITY MARKET: TOP-DOWN AND BOTTOM-UP APPROACHES



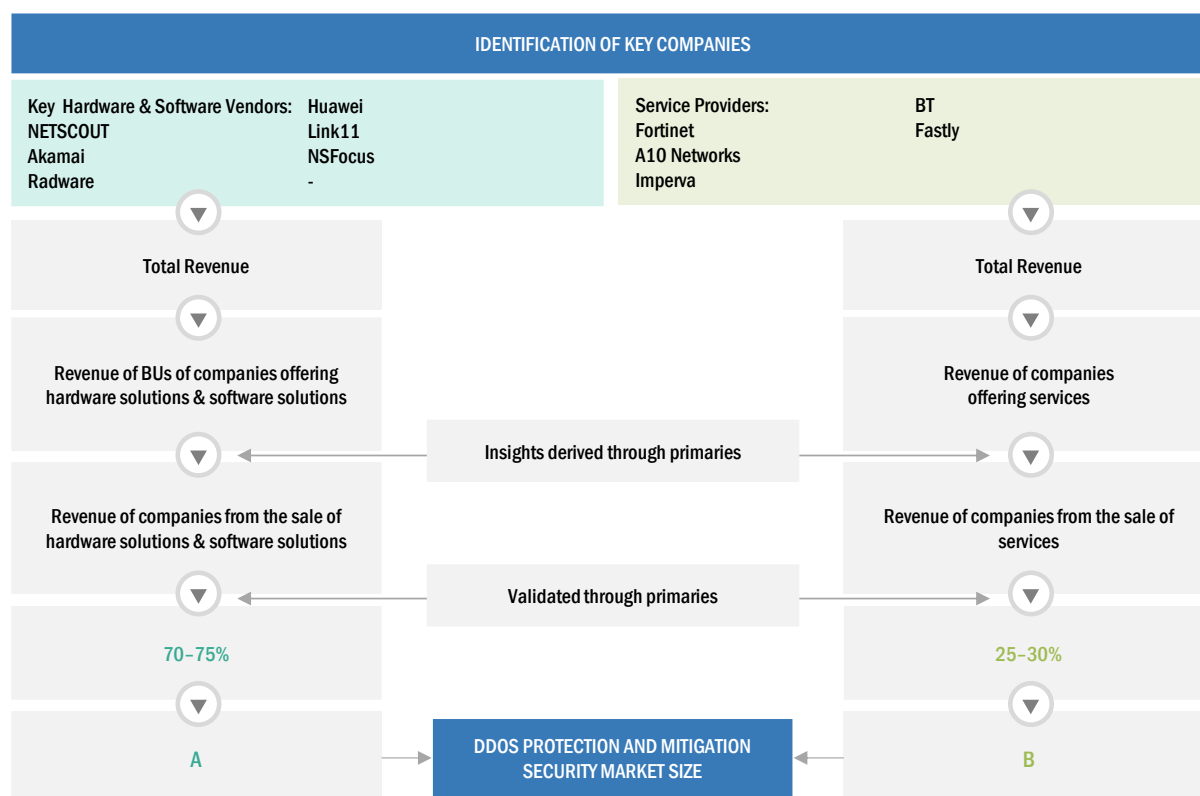
Source: Secondary Research and MarketsandMarkets Analysis

18.2.1 TOP-DOWN APPROACH

The top-down approach prepared an exhaustive list of vendors offering software and services in the DDoS protection and mitigation security market. The revenue contribution of all vendors in the market was estimated through annual reports, press releases, funding, investor presentations, paid databases, and primary interviews. Each vendor's offerings were evaluated based on breadth of software, modernization services, organization size, and verticals. The aggregate of all the companies' revenue 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 both primary and secondary research. The primary procedure included extensive interviews for key insights from the industry leaders, such as chief information officers (CIOs), CEOs, vice presidents (VPs), directors, and marketing executives. The market numbers were further triangulated with the existing MarketsandMarkets repository for validation.

The list of vendors considered for estimating the market is not limited to those profiled in the report. However, MarketsandMarkets prepares a laundry list of vendors operating in DDoS protection and mitigation security and their product mapping (related to DDoS protection & mitigation security) to identify the major vendors operating in the market.

FIGURE 58 **APPROACH 1 (SUPPLY SIDE): REVENUE OF VENDORS IN DDOS PROTECTION AND MITIGATION SECURITY MARKET**



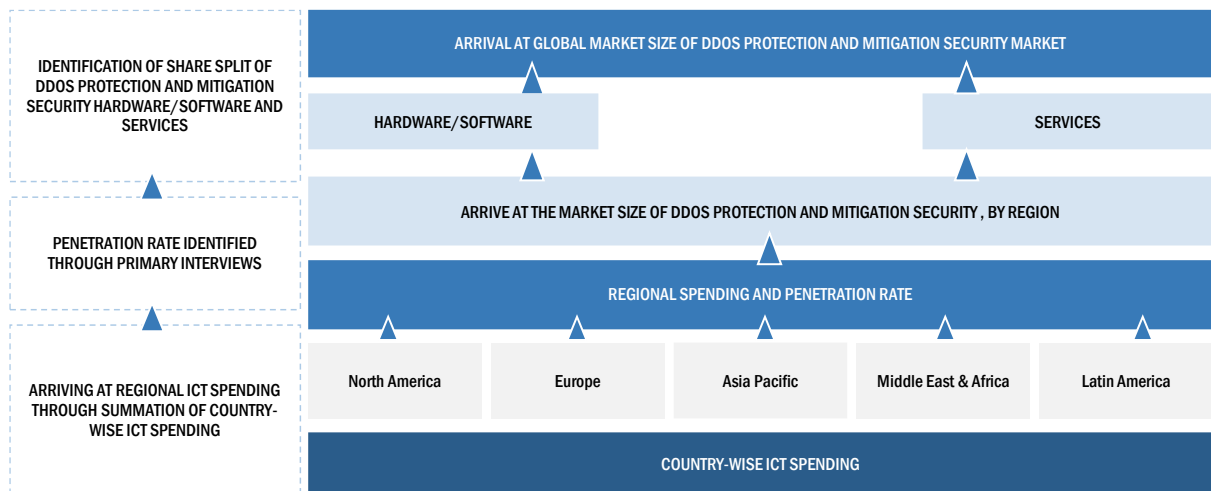
Source: Secondary Research and MarketsandMarkets Analysis

18.2.2 BOTTOM-UP APPROACH

In this approach, the adoption of DDoS protection and mitigation security for different applications in key countries was identified with respect to their region, contributing to most of the market share. The adoption of DDoS protection and mitigation security in different applications and use cases concerning their region was identified and extrapolated for cross-validation. In addition, weightage was 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 the regional penetration of the DDoS protection and mitigation security market. Based on secondary research, the regional spending on information and communications technology (ICT), socioeconomic analysis of each country, strategic vendor analysis of the major DDoS protection and mitigation security providers, and organic and inorganic business development activities of regional and global players were estimated. With the data triangulation procedure and data validation through primary interviews, this study determined and confirmed the exact values of the overall DDoS protection and mitigation security market size and its segments' market size.

FIGURE 59 **APPROACH 2 (DEMAND SIDE): DDOS PROTECTION AND MITIGATION SECURITY MARKET**

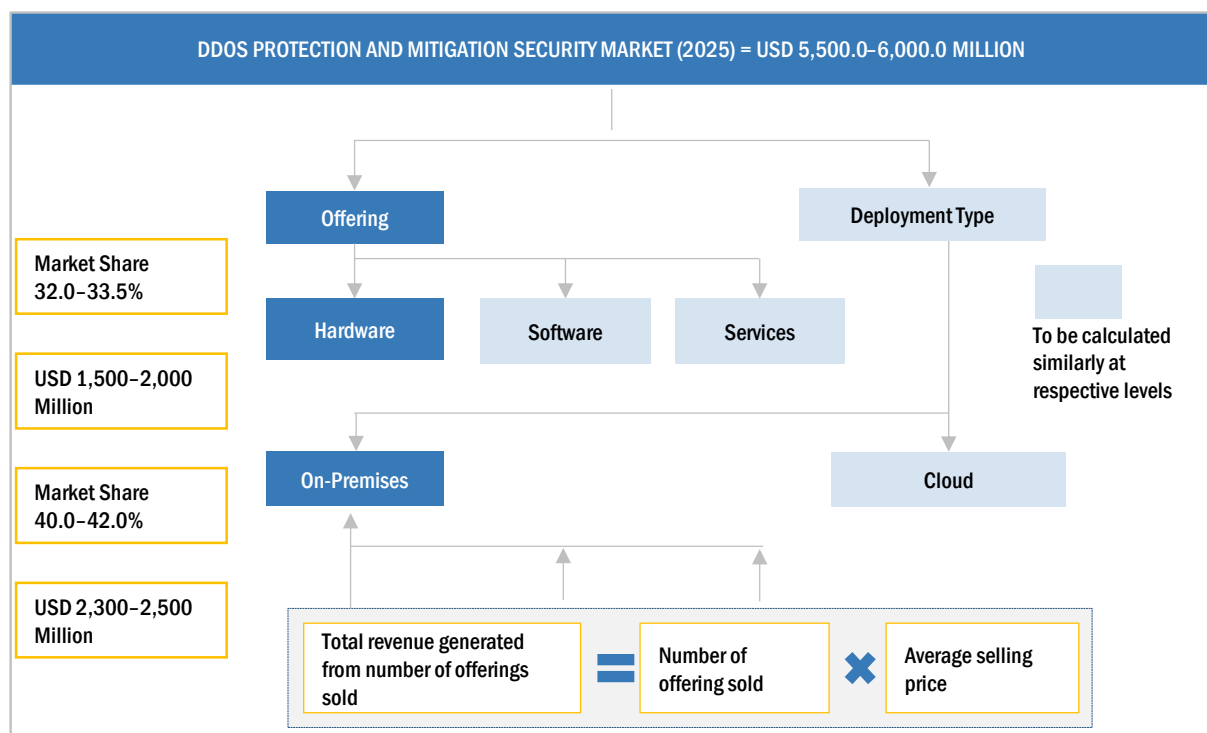


Source: Secondary Research and MarketsandMarkets

18.2.3 DDOS PROTECTION AND MITIGATION SECURITY MARKET ESTIMATION: DEMAND-SIDE ANALYSIS

The demand-side approach involved estimating the DDoS protection and mitigation security market. The demand-side analysis of the market was described in the figure provided below:

FIGURE 60 **MARKET SIZE ESTIMATION METHODOLOGY: DEMAND-SIDE ANALYSIS**



Source: Secondary Research and MarketsandMarkets Analysis

FIGURE 61 TECHNOLOGY/PRODUCT ROADMAP

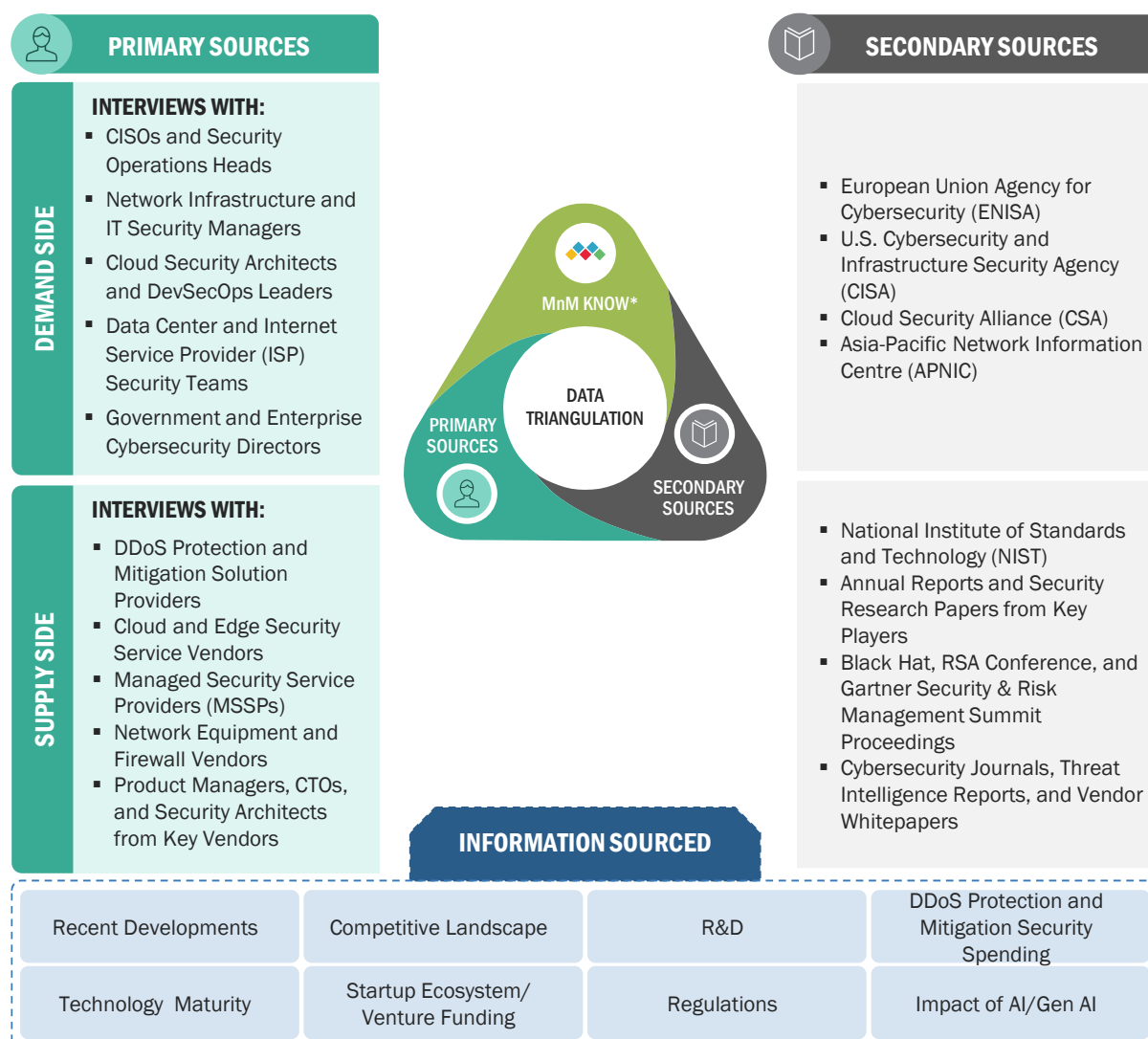
STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Identification of 18–20 major DDoS Protection and Mitigation Security companies, such as NETSCOUT, Akamai, Radware, NSFocus, Huawei, Fortinet, Link11, Imperva, CloudFlare, BT, A10 Networks, Fastly, Nexusguard, Corero, RioRey, PhoenixNAP, Allot, StrataCore, Sucuri, Seceon, HaltDos, DDoS-Guard, Indusface, Activereach, Mlytics, F5	Estimation of top players' potential revenue from their respective BUs that offer DDoS Protection and Mitigation Security hardware, solutions & software solutions, and services	Identification of the revenue contribution of DDoS Protection and Mitigation Security hardware, solutions & software solutions, and services to the relevant BU/BUs	Calculation of the total market size of DDoS Protection and Mitigation Security 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 Security managers, COOs, and CSOs)

Source: Secondary Research and MarketsandMarkets Analysis

18.3 DATA TRIANGULATION

After arriving at the overall market size, the DDoS protection and mitigation security market was divided into several segments and subsegments. A data triangulation procedure was used to complete the overall market engineering process and arrive at the exact statistics for all segments and subsegments, wherever applicable. The data was triangulated by studying various factors and trends from the demand and supply sides. Along with data triangulation and market breakdown, the market size was validated by the top-down and bottom-up approaches.

FIGURE 62 DDoS PROTECTION AND MITIGATION SECURITY MARKET: DATA TRIANGULATION



*MnM KNOW stands for MarketsandMarkets' "Knowledge Asset Management" framework. It refers to 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 and the Security-as-a-Service market, have been referred to for making this report.

Source: Secondary Research and MarketsandMarkets Analysis

18.4 RISK ASSESSMENT

TABLE 488 RISK ASSESSMENT

FACTOR	INFERENCE	IMPACT
Regulations	Some regulatory and compliance requirements in the areas of socioeconomic concerns are supposed to affect the DDoS protection and mitigation security ecosystem.	High
Government Initiatives	China, South Korea, Japan, the UK, and the US have aggressively and actively promoted SDN, NFV, 5G, broadband, and cloud computing. Also, they have taken several initiatives, such as the 13th Five Year plan referring to 5G and broadband strategy (China); Japan e-Government; Master Plan for Intelligent Information Society (South Korea); 5G Strategy for the UK; and Digital Government Strategy (US). Other key initiatives include the availability of unlicensed spectrum (Citizens Broadband Radio Service [CBRS] and MulteFire), heavy investment in digital transformation, and national broadband plans.	Medium
Recent Developments	Major vendors contribute to more than 60% of the developments in the market.	Low
R&D Spending	Overall, companies are spending approximately 10% of their total revenue on their R&D activities. The share of R&D in the DDoS protection and mitigation security market is assumed to be 0.5–1.0% of the actual revenue. With the emergence of innovative technologies such as blockchain, IoT, and 5G, key vendors are expected to invest heavily in R&D. Key vendors have planned to use most of their R&D spending to develop innovative solutions across technologies.	High
Startup Ecosystem	The market is controlled by major key vendors such as NETSCOUT, Akamai, Radware, NSFocus, Huawei Technologies, and Fortinet. There are a few startup players in the market. Because of the strong merger and acquisition strategy, there is significantly less space for startup players to grow in the market. Hence, startups existing in the ecosystem seem to be very low, less than 2–5%.	Low

Source: Secondary Research and MarketsandMarkets Analysis

18.5 RESEARCH ASSUMPTIONS

The following global economic assumptions were taken into consideration to complete the overall engineering of the DDoS protection and mitigation security market:

PARAMETER	ASSUMPTION
Global DDoS Protection and Mitigation Security Market Size	Market size estimates are conservative/realistic as opposed to optimistic/aggressive.
Quantitative Assumption	The market sizes may not add up to the total due to rounding off of values.
Economy	According to the January 2025 World Economic Outlook (WEO) growth projections, global growth is forecasted to stay at 3.3% in 2025 and 2026, and the economy is assumed to be stable in 2025 and 2026.
Financial Statistics	All the revenue and financial insights were extracted from company websites or annual reports. The report assumes the authenticity of the financials of the companies operating in the market.

Source: Secondary Research and MarketsandMarkets Analysis

18.6 RESEARCH LIMITATIONS

- The market size estimation is based on the approximation of the market share of vendors.
- Vertical spending was considered only to estimate the trend and not for sizing.
- Due to varied and fluctuating pricing models, the global DDoS protection and mitigation security market can deviate from the current assumptions during the forecast period.

19 ADJACENT AND RELATED MARKETS

19.1 INTRODUCTION

This chapter explores the role of DDoS protection and mitigation security in other markets. Using the MarketsandMarkets KnowledgeStore, it identifies retail markets related to DDoS protection and mitigation security and provides an abridged analysis of the key related markets, such as the cybersecurity market and Security-as-a-Service market.

This section provides a holistic overview of the growth of markets adjacent/related to DDoS protection and mitigation security. The MarketsandMarkets studies published separately and identified as related markets in this chapter are given below.

STUDY NAME	PUBLICATION YEAR	BASE YEAR	FORECAST PERIOD
Cybersecurity Market	2025	2024	2025–2030
Security as a Service Market	2021	2020	2021–2026

Source: Secondary Research and MarketsandMarkets Analysis

19.2 CYBERSECURITY MARKET

19.2.1 MARKET DEFINITION

Cybersecurity protects critical systems and sensitive information from digital attacks. Also known as Information Technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether they originate from inside or outside an organization.

(Source: IBM)

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks aim to access, change, or destroy sensitive information, extort money from users, or interrupt normal business processes.

(Source: Cisco)

According to MarketsandMarkets, cybersecurity is a set of technologies, processes, and practices to fortify critical systems, such as networks, physical devices, programs, and information, from unauthorized access, insider threats, and malicious attacks. These cyberattacks can affect data transmission across the networks, cause operational disruptions, and result in money extortion/ransomware. Cybersecurity, or information security, can be provided through hardware, software, and services. Cybersecurity encompasses a range of technologies, processes, and practices designed to protect critical systems, including networks, physical devices, programs, and information, from unauthorized access, insider threats, and malicious attacks. These cyberattacks can disrupt data transmission across networks, lead to operational interruptions, and result in financial loss through extortion or ransomware. Cybersecurity, also known as information security, can be achieved through hardware, software, and services.

TABLE 489 CYBERSECURITY MARKET, BY OFFERING, 2019–2024 (USD MILLION)

Offering	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Solutions	72,776.2	81,704.3	90,014.2	98,096.6	106,561.7	115,572.7	9.7%
Services	52,881.8	60,510.7	67,901.4	75,248.0	83,418.6	92,350.6	11.8%
Total	125,658.0	142,215.0	157,915.6	173,344.6	189,980.4	207,923.3	10.6%

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

TABLE 490 CYBERSECURITY MARKET, BY OFFERING, 2025–2030 (USD MILLION)

Offering	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Solutions	125,321.8	135,746.3	147,112.4	159,102.6	172,179.4	186,171.8	8.2%
Services	102,272.0	113,112.6	124,685.7	137,467.1	151,018.0	165,745.3	10.1%
Total	227,593.8	248,858.9	271,798.1	296,569.7	323,197.4	351,917.1	9.1%

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

TABLE 491 CYBERSECURITY MARKET, BY SOLUTION TYPE, 2019–2024 (USD MILLION)

Solution Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
IAM	10,538.7	11,914.9	13,206.4	14,671.0	16,126.2	17,633.7	10.8%
Antivirus/Antimalware	4,791.6	5,295.6	5,741.6	6,153.9	6,573.9	7,009.0	7.9%
Log Management & SIEM	17,780.0	20,420.1	23,000.6	25,614.0	28,420.8	31,467.2	12.1%
Firewall & VPN	9,293.4	10,345.7	11,300.9	12,207.3	13,143.5	14,128.1	8.7%
DLP, Encryption, and Tokenization	8,975.3	9,874.3	10,658.4	11,370.6	12,089.5	12,826.9	7.4%
Compliance & Policy Management	5,597.2	6,347.4	7,062.8	7,772.9	8,526.1	9,335.4	10.8%
Patch Management	3,068.9	3,349.1	3,583.0	3,784.8	3,982.6	4,178.6	6.4%
Other Solution Types	12,731.0	14,157.2	15,460.5	16,522.1	17,699.0	18,993.6	8.3%
Total	72,776.2	81,704.3	90,014.2	98,096.6	106,561.7	115,572.7	9.7%

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

TABLE 492 CYBERSECURITY MARKET, BY SOLUTION TYPE, 2025–2030 (USD MILLION)

Solution Type	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
IAM	19,197.3	20,792.4	22,404.2	24,014.4	26,055.8	28,241.2	8.0%
Antivirus/Antimalware	7,469.5	7,947.2	8,457.8	8,982.1	9,545.8	10,134.8	6.3%
Log Management & SIEM	34,836.8	38,494.3	42,540.3	46,949.4	51,724.3	57,385.3	10.5%
Firewall & VPN	15,181.6	16,293.5	17,495.0	18,746.6	20,104.3	21,541.3	7.2%
DLP, Encryption, and Tokenization	13,603.2	14,396.6	15,234.3	16,087.2	16,996.2	17,934.7	5.7%
Compliance & Policy Management	10,220.4	11,175.3	12,224.8	13,344.2	14,570.8	15,896.9	9.2%
Patch Management	4,379.7	4,576.5	4,779.7	4,978.3	5,185.4	5,392.3	4.2%
Other Solution Types	20,433.3	22,070.5	23,976.4	26,000.4	27,996.8	29,645.2	7.7%
Total	125,321.8	135,746.3	147,112.4	159,102.6	172,179.4	186,171.8	8.2%

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

TABLE 493 CYBERSECURITY MARKET, BY SECURITY TYPE, 2019–2024 (USD MILLION)

Security Type	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Network Security	50,969.6	56,826.2	62,230.3	67,282.2	72,677.6	78,409.7	9.0%
Endpoint & IoT Security	27,740.3	31,764.9	35,691.0	39,616.6	43,945.3	48,699.7	11.9%
Cloud Security	27,645.3	31,582.7	35,366.1	39,008.5	42,882.6	47,038.0	11.2%
Application Security	19,302.8	22,041.2	24,628.1	27,437.3	30,474.9	33,775.9	11.8%
Total	125,658.0	142,215.0	157,915.6	173,344.6	189,980.4	207,923.3	10.6%

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

TABLE 494 CYBERSECURITY MARKET, BY SECURITY TYPE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Network Security	84,501.4	90,878.7	97,564.5	104,636.1	113,206.7	122,360.3	7.7%
Endpoint & IoT Security	53,939.6	59,669.3	65,930.3	72,653.5	79,398.9	86,707.5	10.0%
Cloud Security	51,676.8	56,799.1	62,381.0	68,657.8	75,491.5	82,937.2	9.9%
Application Security	37,476.0	41,511.9	45,922.3	50,622.2	55,100.3	59,912.1	9.8%
Total	227,593.8	248,858.9	271,798.1	296,569.7	323,197.4	351,917.1	9.1%

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

TABLE 495 CYBERSECURITY MARKET, BY DEPLOYMENT MODE, 2019–2024 (USD MILLION)

Deployment Mode	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
On-premises	74,828.6	84,055.2	92,638.0	101,113.4	109,881.9	119,228.5	9.8%
Cloud	32,704.6	37,608.1	42,430.5	47,274.8	52,664.1	58,582.8	12.4%
Hybrid	18,124.8	20,551.7	22,847.1	24,956.4	27,434.4	30,112.1	10.7%
Total	125,658.0	142,215.0	157,915.6	173,344.6	189,980.4	207,923.3	10.6%

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

TABLE 496 CYBERSECURITY MARKET, BY DEPLOYMENT MODE, 2025–2030 (USD MILLION)

Deployment Mode	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
On-premises	129,363.5	140,163.8	151,648.8	163,957.0	177,943.4	192,937.1	8.3%
Cloud	65,180.8	72,445.7	80,429.6	89,186.4	97,678.6	106,888.6	10.4%
Hybrid	33,049.5	36,249.4	39,719.7	43,426.2	47,575.4	52,091.3	9.5%
Total	227,593.8	248,858.9	271,798.1	296,569.7	323,197.4	351,917.1	9.1%

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

TABLE 497 CYBERSECURITY MARKET, BY ORGANIZATION SIZE, 2019–2024 (USD MILLION)

Organization Size	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Large Enterprises	79,527.2	88,756.0	97,163.1	105,165.4	114,700.1	124,921.3	9.5%
SMEs	46,130.8	53,459.0	60,752.5	68,179.2	75,280.3	83,002.0	12.5%
Total	125,658.0	142,215.0	157,915.6	173,344.6	189,980.4	207,923.3	10.6%

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

TABLE 498 CYBERSECURITY MARKET, BY ORGANIZATION SIZE, 2025–2030 (USD MILLION)

Organization Size	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Large Enterprises	136,017.3	147,948.6	160,728.9	174,410.2	189,059.3	204,749.3	8.5%
SMEs	91,576.5	100,910.3	111,069.2	122,159.4	134,138.1	147,167.8	10.0%
Total	227,593.8	248,858.9	271,798.1	296,569.7	323,197.4	351,917.1	9.1%

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

TABLE 499 CYBERSECURITY MARKET, BY VERTICAL, 2019–2024 (USD MILLION)

Vertical	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
Government	22,463.7	24,805.0	26,869.3	28,977.1	31,297.0	33,779.8	8.5%
BFSI	19,598.7	22,305.7	24,911.3	27,592.1	30,583.9	33,857.6	11.6%
IT & ITeS	10,880.2	12,509.8	14,111.5	15,863.7	17,939.1	20,261.9	13.2%
Healthcare & Life Sciences	10,367.4	12,146.3	13,954.1	15,966.2	18,289.2	20,921.3	15.1%
Aerospace & Defense	9,785.0	11,001.2	12,142.7	13,255.8	14,410.0	15,648.4	9.8%
Retail & eCommerce	6,200.9	7,035.0	7,833.4	8,617.7	9,505.5	10,475.4	11.1%
Manufacturing	5,670.5	6,503.3	7,315.9	8,136.6	8,995.9	9,933.7	11.9%
Energy & Utilities	8,683.2	9,824.7	10,909.9	11,946.6	13,081.3	14,300.7	10.5%
Telecommunications	6,503.1	7,281.2	7,976.8	8,599.9	9,280.4	10,000.1	9.0%
Transportation & Logistics	7,163.3	8,089.0	8,954.4	9,799.8	10,585.9	11,407.8	9.8%
Media & Entertainment	3,431.6	3,813.2	4,162.6	4,421.3	4,748.6	5,029.6	7.9%
Other Verticals	14,910.3	16,900.7	18,773.5	20,167.8	21,263.4	22,306.9	8.4%
Total	125,658.0	142,215.0	157,915.6	173,344.6	189,980.4	207,923.3	10.6%

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

TABLE 500 CYBERSECURITY MARKET, BY VERTICAL, 2025–2030 (USD MILLION)

Vertical	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
Government	36,374.5	39,108.9	41,892.4	44,805.6	48,187.6	51,784.7	7.3%
BFSI	37,463.6	41,426.3	45,761.6	50,513.8	55,276.1	60,436.5	10.0%
IT & ITeS	22,870.6	25,803.5	29,084.9	32,754.0	36,139.7	39,839.1	11.7%
Healthcare & Life Sciences	23,917.9	27,324.5	31,181.5	35,548.0	39,370.2	43,565.1	12.7%
Aerospace & Defense	17,006.6	18,451.1	19,993.9	21,641.0	23,408.6	25,296.8	8.3%
Retail & eCommerce	11,568.5	12,741.9	14,026.8	15,423.1	16,837.0	18,365.7	9.7%
Manufacturing	10,971.8	12,090.0	13,313.1	14,610.5	15,951.2	17,397.0	9.7%
Energy & Utilities	15,628.6	17,060.5	18,594.2	19,961.6	21,670.0	23,504.3	8.5%
Telecommunications	10,779.0	11,605.1	12,480.4	13,410.0	14,473.7	15,607.8	7.7%
Transportation & Logistics	12,316.1	13,255.1	14,227.7	15,243.5	16,483.7	17,807.3	7.7%
Media & Entertainment	5,329.8	5,622.7	5,898.3	6,196.3	6,584.3	6,991.5	5.6%
Other Verticals	23,366.8	24,369.3	25,343.3	26,462.3	28,815.2	31,321.2	6.0%
Total	227,593.8	248,858.9	271,798.1	296,569.7	323,197.4	351,917.1	9.1%

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

TABLE 501 CYBERSECURITY MARKET, BY REGION, 2019–2024 (USD MILLION)

Region	2019	2020	2021	2022	2023	2024	CAGR (2019–2024)
North America	53,680.7	60,008.5	65,736.1	71,117.5	76,789.5	82,783.1	9.0%
Europe	31,026.6	34,985.0	38,682.1	42,268.6	46,132.8	50,217.3	10.1%
Asia Pacific	21,626.1	25,241.8	28,887.9	32,671.0	36,903.3	41,597.9	14.0%
Middle East & Africa	12,985.4	14,779.5	16,590.5	18,461.1	20,451.7	22,666.7	11.8%
Latin America	6,339.3	7,200.2	8,019.0	8,826.4	9,703.1	10,658.3	11.0%
Total	125,658.0	142,215.0	157,915.6	173,344.6	189,980.4	207,923.3	10.6%

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

TABLE 502 CYBERSECURITY MARKET, BY REGION, 2025–2030 (USD MILLION)

Region	2025	2026	2027	2028	2029	2030	CAGR (2025–2030)
North America	89,156.7	95,840.2	102,824.5	110,330.7	118,274.5	126,790.3	7.3%
Europe	54,766.3	59,666.8	64,938.3	70,561.3	76,629.6	83,143.1	8.7%
Asia Pacific	46,943.7	52,919.5	59,591.2	66,920.9	74,884.5	83,571.1	12.2%
Middle East & Africa	25,021.5	27,589.6	30,367.9	33,345.2	36,548.5	39,984.3	9.8%
Latin America	11,705.6	12,842.8	14,076.2	15,411.6	16,860.3	18,428.3	9.5%
Total	227,593.8	248,858.9	271,798.1	296,569.7	323,197.4	351,917.1	9.1%

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

19.3 SECURITY AS A SERVICE MARKET

19.3.1 MARKET DEFINITION

Security as a service is a cloud-based model wherein security vendors secure and maintain the enterprise network, application, and data over the cloud and in an on-premise environment. It is a security management approach that enables the provisioning of security solutions and services from the cloud. Security as a service is an outsourcing service that benefits an organization in several ways, such as reduced costs, ease of IT security, scalable security services, and continuous support. It enables organizations to access and implement robust security practices. Security services are integrated with the enterprise infrastructure, safeguarding enterprises' essential assets from external and internal threats.

According to McAfee, Software-as-a-Service (SaaS) is an on-demand, cloud-based software delivery model, which enables organizations to subscribe to applications they need without hosting them in-house.

According to Forcepoint, Security-as-a-Service (SECaaS) can most easily be described as a cloud-delivered model for outsourcing cybersecurity services. Much like software-as-a-service, SECaaS provides security services on a subscription basis hosted by cloud providers.

TABLE 503 SECURITY AS A SERVICE MARKET SIZE, BY COMPONENT, 2016–2020 (USD MILLION)

Component	2016	2017	2018	2019	2020	CAGR (2016–2020)
Solutions	4,083	4,973	5,978	7,121	8,353	15.4%
Services	1,011	1,271	1,574	1,900	2,296	17.8%
Total	5,095	6,244	7,552	9,021	10,649	15.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 504 SECURITY AS A SERVICE MARKET SIZE, BY COMPONENT, 2021–2026 (USD MILLION)

Component	2021-e	2022-p	2023-p	2024-p	2025-p	2026-p	CAGR (2021–2026)
Solutions	9,694	11,140	12,690	14,459	16,222	18,082	13.3%
Services	2,743	3,245	3,802	4,302	4,966	5,693	15.7%
Total	12,437	14,385	16,493	18,760	21,188	23,775	13.8%

e: estimated; p: projected

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 505 SECURITY AS A SERVICE MARKET SIZE, BY SOLUTION, 2016–2020 (USD MILLION)

Solution	2016	2017	2018	2019	2020	CAGR (2016–2020)
Business Continuity and Disaster Management	293	360	435	520	614	15.9%
Continuous Monitoring	341	413	494	586	684	14.9%
DLP	580	697	826	978	1,130	14.3%
Encryption	495	618	762	917	1,101	17.3%
IAM	1,383	1,692	2,042	2,437	2,870	15.7%
Intrusion Management	367	440	520	614	708	14.1%
SIEM	245	304	371	445	531	16.7%
Vulnerability Scanning	200	239	281	332	381	13.7%
Other Solutions	177	211	248	292	334	13.5%
Total	4,083	4,973	5,978	7,121	8,353	15.4%

Other solutions include security assessment, DDoS mitigation services, and firewall services.

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 506 SECURITY AS A SERVICE MARKET SIZE, BY SOLUTION, 2021–2026 (USD MILLION)

Solution	2021-e	2022-p	2023-p	2024-p	2025-p	2026-p	CAGR (2021–2026)
Business Continuity and Disaster Management	717	830	951	1,087	1,227	1,377	13.9%
Continuous Monitoring	788	901	1,020	1,158	1,292	1,431	12.7%
DLP	1,292	1,463	1,642	1,859	2,053	2,253	11.8%
Encryption	1,308	1,537	1,790	2,058	2,358	2,684	15.5%
IAM	3,344	3,859	4,414	5,037	5,675	6,351	13.7%
Intrusion Management	808	912	1,020	1,153	1,270	1,388	11.4%
SIEM	626	730	844	968	1,102	1,247	14.8%
Vulnerability Scanning	432	485	540	609	667	726	10.9%
Other Solutions	378	423	470	529	577	625	10.6%
Total	9,694	11,140	12,690	14,459	16,222	18,082	13.3%

e: estimated; p: projected

Other solutions include security assessment, DDoS mitigation services, and firewall services

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 507 SECURITY AS A SERVICE MARKET SIZE, BY SERVICE, 2016–2020 (USD MILLION)

Service	2016	2017	2018	2019	2020	CAGR (2016–2020)
Training and Education	152	186	225	267	314	15.5%
Consulting	405	505	622	747	896	17.2%
Support and Maintenance	454	579	728	886	1,086	19.1%
Total	1,011	1,271	1,574	1,900	2,296	17.8%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 508 SECURITY AS A SERVICE MARKET SIZE, BY SERVICE, 2021–2026 (USD MILLION)

Service	2021-e	2022-p	2023-p	2024-p	2025-p	2026-p	CAGR (2021–2026)
Training and Education	364	417	473	525	586	649	12.3%
Consulting	1,063	1,248	1,451	1,634	1,871	2,129	14.9%
Support and Maintenance	1,317	1,580	1,878	2,143	2,508	2,915	17.2%
Total	2,743	3,245	3,802	4,302	4,966	5,693	15.7%

e: estimated; p: projected

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 509 SECURITY AS A SERVICE MARKET SIZE, BY APPLICATION, 2016–2020 (USD MILLION)

Application	2016	2017	2018	2019	2020	CAGR (2016–2020)
Network Security	1,296	1,588	1,921	2,303	2,718	16.0%
Endpoint Security	789	950	1,129	1,330	1,543	14.4%
Application Security	695	871	1,077	1,318	1,588	18.0%
Cloud Security	451	560	684	829	989	17.0%
Other Applications	853	1,004	1,166	1,341	1,515	12.2%
Total	4,083	4,973	5,978	7,121	8,353	15.4%

Other applications include email security, web security, and database security.

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 510 SECURITY AS A SERVICE MARKET SIZE, BY APPLICATION, 2021–2026 (USD MILLION)

Application	2021-e	2022-p	2023-p	2024-p	2025-p	2026-p	CAGR (2021–2026)
Network Security	3,174	3,670	4,206	4,821	5,442	6,102	14.0%
Endpoint Security	1,770	2,010	2,263	2,548	2,825	3,111	11.9%
Application Security	1,891	2,229	2,602	3,036	3,487	3,977	16.0%
Cloud Security	1,167	1,363	1,577	1,826	2,080	2,354	15.1%
Other Applications	1,692	1,869	2,042	2,227	2,388	2,538	8.4%
Total	9,694	11,140	12,690	14,459	16,222	18,082	13.3%

e: estimated; p: projected

Other applications include email security, web security, and database security.

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 511 SECURITY AS A SERVICE MARKET SIZE, BY ORGANIZATION SIZE, 2016–2020 (USD MILLION)

Organization Size	2016	2017	2018	2019	2020	CAGR (2016–2020)
SMEs	1,324	1,654	2,039	2,481	2,983	17.6%
Large Enterprises	3,771	4,589	5,513	6,540	7,666	15.2%
Total	5,095	6,244	7,552	9,021	10,649	15.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 512 SECURITY AS A SERVICE MARKET SIZE, BY ORGANIZATION SIZE, 2021–2026 (USD MILLION)

Organization Size	2021-e	2022-p	2023-p	2024-p	2025-p	2026-p	CAGR (2021–2026)
SMEs	3,546	4,174	4,854	5,617	6,451	7,359	15.7%
Large Enterprises	8,891	10,211	11,638	13,144	14,737	16,416	13.0%
Total	12,437	14,385	16,493	18,760	21,188	23,775	13.8%

e: estimated; p: projected

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 513 SECURITY AS A SERVICE MARKET SIZE, BY VERTICAL, 2016–2020 (USD MILLION)

Vertical	2016	2017	2018	2019	2020	CAGR (2016–2020)
BFSI	1,139	1,394	1,685	2,011	2,371	15.8%
Government and Defense	949	1,167	1,416	1,696	2,007	16.2%
Retail and eCommerce	441	560	703	869	1,061	19.2%
Healthcare and Life Sciences	623	774	950	1,151	1,377	17.2%
IT and Telecom	737	899	1,082	1,286	1,511	15.4%
Energy and Utilities	413	499	595	701	815	14.6%
Manufacturing	390	470	560	658	765	14.4%
Other Verticals	404	480	562	650	742	12.9%
Total	5,095	6,244	7,552	9,021	10,649	15.9%

Other verticals include media and entertainment, education, and travel and hospitality.

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 514 SECURITY AS A SERVICE MARKET SIZE, BY VERTICAL, 2021–2026 (USD MILLION)

Vertical	2021-e	2022-p	2023-p	2024-p	2025-p	2026-p	CAGR (2021–2026)
BFSI	2,766	3,196	3,661	4,160	4,693	5,260	13.7%
Government and Defense	2,351	2,727	3,135	3,575	4,048	4,554	14.1%
Retail and eCommerce	1,280	1,529	1,808	2,119	2,464	2,845	17.3%
Healthcare and Life Sciences	1,630	1,911	2,220	2,558	2,926	3,325	15.3%
IT and Telecom	1,756	2,021	2,306	2,610	2,933	3,274	13.3%
Energy and Utilities	938	1,069	1,207	1,352	1,503	1,660	12.1%
Manufacturing	879	1,000	1,127	1,260	1,399	1,542	11.9%
Other Verticals	837	933	1,030	1,127	1,222	1,315	9.5%
Total	12,437	14,385	16,493	18,760	21,188	23,775	13.8%

e: estimated; p: projected

Other verticals include media and entertainment, education, and travel and hospitality.

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 515 SECURITY AS A SERVICE MARKET SIZE, BY REGION, 2016–2020 (USD MILLION)

Country	2016	2017	2018	2019	2020	CAGR (2016–2020)
North America	1,772	2,183	2,653	3,185	3,778	16.3%
Europe	1,401	1,745	2,145	2,603	3,120	17.4%
APAC	949	1,158	1,394	1,658	1,949	15.5%
MEA	548	657	776	906	1,044	13.7%
Latin America	424	501	583	670	758	12.3%
Total	5,095	6,244	7,552	9,021	10,649	15.9%

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

TABLE 516 SECURITY AS A SERVICE MARKET SIZE, BY REGION, 2021–2026 (USD MILLION)

Country	2021-e	2022	2023	2024	2025	2026-p	CAGR (2021–2026)
North America	4,434	5,154	5,938	6,787	7,701	8,683	14.4%
Europe	3,700	4,344	5,055	5,834	6,685	7,608	15.5%
APAC	2,266	2,609	2,978	3,372	3,792	4,235	13.3%
MEA	1,189	1,341	1,498	1,658	1,822	1,988	10.8%
Latin America	848	937	1,025	1,109	1,188	1,261	8.3%
Total	12,437	14,385	16,493	18,760	21,188	23,775	13.8%

e: estimated; p: projected

Note: Numbers are rounded off to the nearest integer, resulting in rounding-off errors

Source: Secondary Literature, Expert Interviews, and MarketsandMarkets Analysis

20 APPENDIX

20.1 DISCUSSION GUIDE

We are conducting a global study on the DDoS protection and mitigation security market. It features a detailed analysis of opportunities, market drivers, restraints, competitive landscape, and key industry players' profiles.

Name:

Designation:

Company Name:

Phone No:

Email ID:

Fax No:

Q. 1. What are the top three drivers, restraints, opportunities, and challenges for your company in the DDoS protection and mitigation security market?

SR. NO.	DRIVERS	RESTRAINTS	OPPORTUNITIES	CHALLENGES
1				
2				
3				

Comments: _____

Q. 2. Which region, according to you, is expected to offer maximum market opportunities for DDoS protection and mitigation security vendors? Kindly provide a market share.

SR. NO.	REGION	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2025	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2030
1	North America		
2	Europe		
3	Asia Pacific		
4	Middle East & Africa		
5	Latin America		

Comments: _____

Q. 3. Which offering, according to you, is expected to provide the maximum opportunities in the DDoS protection and mitigation security market? Please mention its market share.

SR. NO.	OFFERING	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2025	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2030
1	Hardware Solutions		
2	Software Solutions		
3	Services		

Comments: _____

Q. 4. Which solution type, according to you, is expected to offer maximum opportunities in the DDoS protection and mitigation security market? Please provide their respective market share.

SR. NO.	SOLUTION TYPE	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2025	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2030
1	Network Traffic Analyzers		
2	Threat Mitigation Systems		
3	Botnet Detection & Management		
4	Other Solution Types		

Comments: _____

Q. 5. Which application area, according to you, is expected to offer maximum opportunities in the DDoS protection and mitigation security market? Kindly provide its market share.

SR. NO.	APPLICATION AREA	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2025	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2030
1	Network Security		
2	Application Security		
3	Cloud Security		
4	Endpoint Security		

Comments: _____

Q. 6. Which deployment mode, according to you, is expected to offer maximum opportunities in the DDoS protection and mitigation security market? Kindly provide its market share.

SR. NO.	DEPLOYMENT MODE	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2025	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2030
1	On-Premises		
2	Cloud		

Comments: _____

Q. 7. Which organization size, according to you, is expected to offer maximum opportunities in the DDoS protection and mitigation security market? Kindly provide its market share.

SR. NO.	ORGANIZATION SIZE	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2025	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2030
1	Large Enterprises		
2	Small & Medium-sized Enterprises		

Comments: _____

Q. 8. Which vertical, according to you, is expected to offer maximum opportunities in the DDoS protection and mitigation security market? Kindly provide its market share.

SR. NO.	VERTICAL	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2025	ATTRACTIVENESS OF OPPORTUNITY (MARKET SHARE OUT OF 100%) - 2030
1	Government and Defense		
2	Banking, Financial Services, and Insurance (BFSI)		
3	Manufacturing		
4	Energy & Utilities		
5	IT & ITES		
6	Telecom		
7	Healthcare		
8	Education		
9	Retail		
10	Other Verticals		

Comments: _____

Q. 9. Please name your competitors in the DDoS protection and mitigation security market.

Comments: _____

Q. 10. What are expected to be the key development strategies of your company in the near future?

Comments: _____

Q. 11. Please help us understand the product portfolio of your organization in the DDoS protection and mitigation security market. Also, please tell us how your organization's products differ from those of other major competitors in the market.

Comments: _____

Q. 12. According to you, what are the technological changes/innovations that would significantly impact the DDoS protection and mitigation security market?

Comments: _____

Q. 13. Lastly, we would like to add your statement/paragraph about the DDoS protection and mitigation security market as a quote in the report. Can we use it?

Comments: _____

20.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL

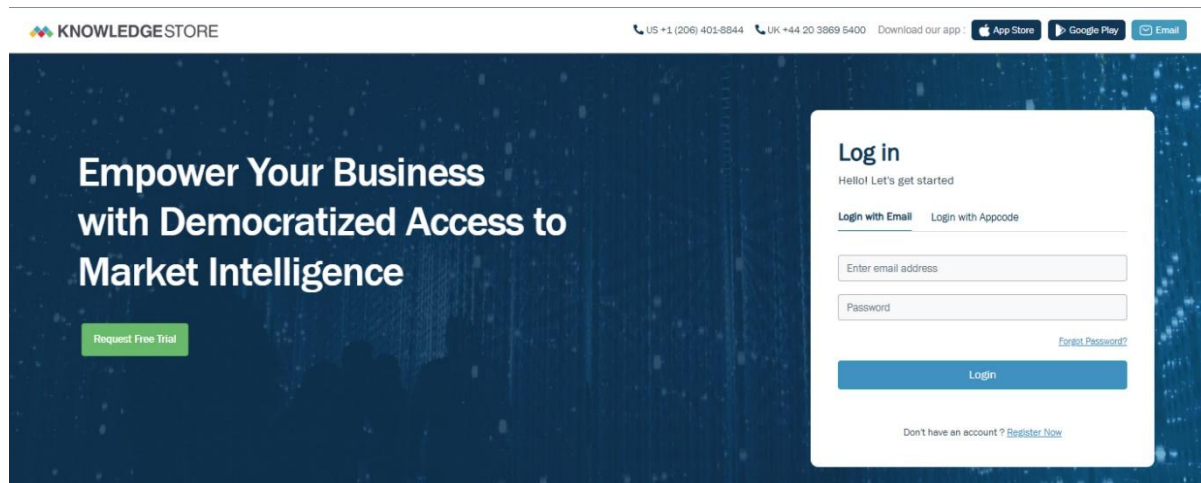
KnowledgeStore contains unique market insights of MarketsandMarkets. As a subscriber, you have access to all of the published titles and any new ones added over the course of the subscription period. You can subscribe to a specific number of reports or domains of your interest.

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

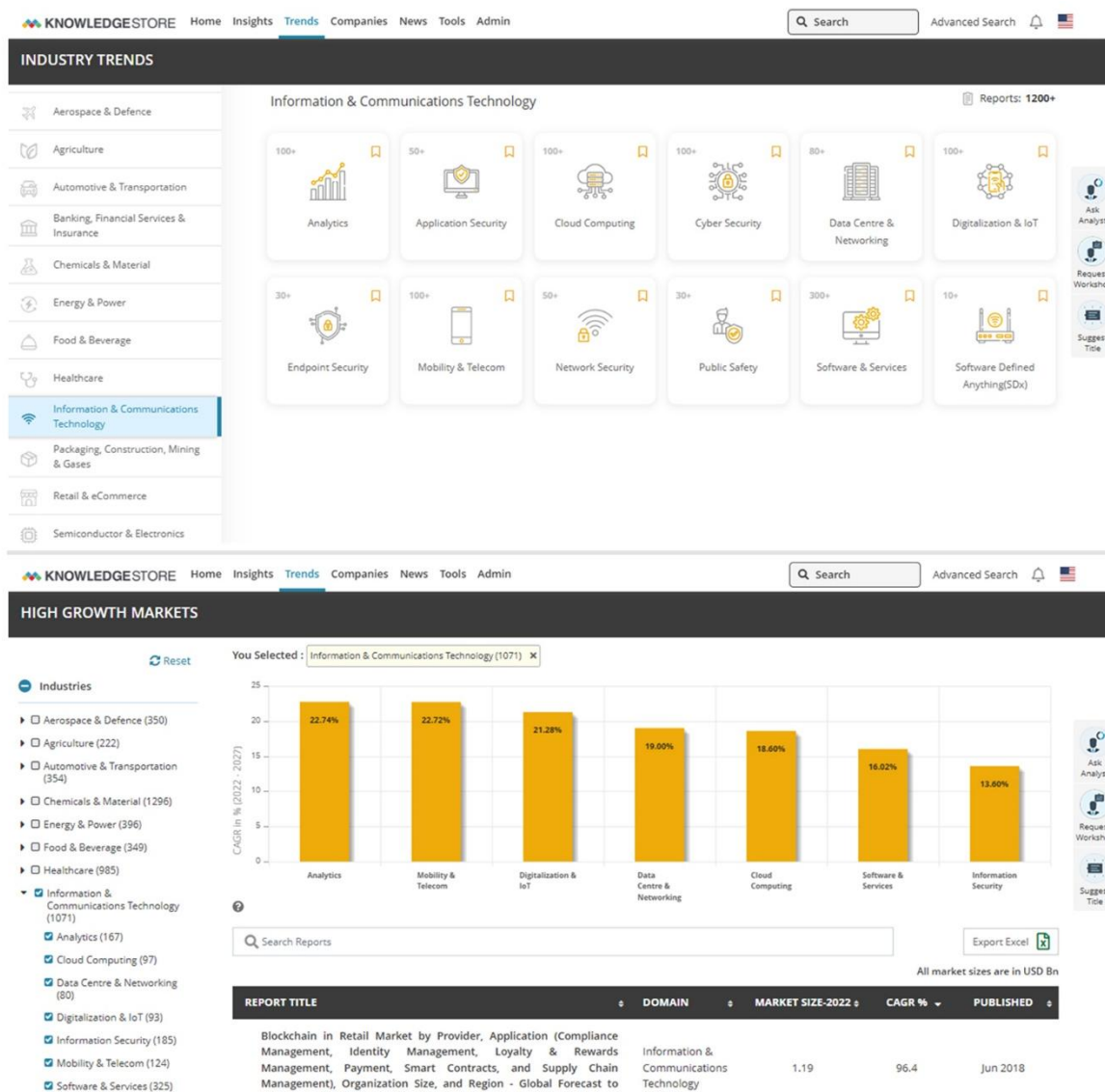
Get started now by requesting a demo and learning more about KnowledgeStore www.mnmks.com

MARKETSANDMARKETS KNOWLEDGESTORE SNAPSHOT



The screenshot shows the KnowledgeStore login interface. The header includes the KnowledgeStore logo, contact numbers for US (+1 206 401-8844) and UK (+44 20 3869 5400), and links to download the app on the App Store and Google Play, along with an email link. The main content area has a dark blue background with the text "Empower Your Business with Democratized Access to Market Intelligence" and a green "Request Free Trial" button. On the right, there is a white login box titled "Log in" with the text "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



20.3 CUSTOMIZATION OPTIONS

With the given market data, MarketsandMarkets offers customizations per the company's specific needs. The following customization options are available for the report:

PRODUCT ANALYSIS

- Product Matrix, which gives a detailed comparison of the product portfolio of each company

COMPANY INFORMATION

- Detailed analysis and profiling of additional market players (up to five)

20.4 RELATED REPORTS

SR. NO	REPORT TITLE	PUBLISHED DATE
1	CYBERSECURITY MARKET - GLOBAL FORECAST TO 2030 Cybersecurity Market by Solution Type (IAM, Firewall & VPN, Log Management & SIEM, Antivirus/Antimalware), Service (Professional (Risk & Threat Assessment, Training & Education), Managed), Security Type (Cloud, Application) https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html	June 2025
2	SECURITY AS A SERVICE MARKET - GLOBAL FORECAST TO 2026 Security as a Service Market by Component (Solution and Service), Application (Network Security, Endpoint Security, Application Security, and Cloud), Organization Size (SMEs, Large Enterprises), Vertical, and Region https://www.marketsandmarkets.com/Market-Reports/security-as-a-service-market-132531603.html	October 2021

20.5 AUTHOR DETAILS

Vivek Ravichandran

*Senior Research Manager,
Information and
Communications Technology*

14+ 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 ever-changing revenue mix, use 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

Sagar Khanivadekar

Associate Manager

Aditi Kapil

Research Analyst

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 is 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