corero
[NETWORK SECURITY]

WHITEPAPER

2026 Budget Defense: The 90-Day Roadmap

Why Q1 Determines Whether You Control Your Security Spend—or It Controls You

A strategic guide for enterprise leaders to eliminate the "Reactive Premium" and secure comprehensive DDoS protection before procurement windows close.

Corero Network Security
www.corero.com

January 2026

Executive Summary

For enterprise leaders, Q1 2026 is the only quiet period you will get. By April 1st, procurement processes lock, discretionary budgets freeze, and the seasonal attack volume begins its climb.

But while budgets are static, the threat landscape has shifted. The era of focusing solely on massive, headline-grabbing volumetric attacks is over. The real threat to your network availability isn't the 100Gbps tsunami you see coming—it's the traffic you don't.

The Invisible Threat: What Your Dashboard Isn't Showing You

82% of all DDoS attacks now remain under 1Gbps. These attacks are surgically engineered to slip under the detection thresholds of legacy cloud scrubbers and ISP filters. While your dashboard shows "All Green," these sub-saturation attacks are silently exhausting your firewall state tables, degrading API performance, and eroding customer experience.

The Financial Reality: The "Reactive Premium"

63% of organizations only increase security spending AFTER a breach. Emergency procurement forces you to buy at premium rates, pay for rush implementation, and suffer the reputational damage of an outage.

This document is your 90-day execution guide. It is designed to help you utilize the Q1 window to shift your posture from "Firefighting" to "Strategic Defense."

Inside This Guide

This whitepaper provides a 90-day execution roadmap designed to help you shift your posture from "Firefighting" to "Strategic Defense" before Q2 budget locks.

The Risk Calculator

Quantify the cost of the "Reactive Premium" for your CFO—incident costs, team overtime, revenue loss, and compliance penalties.

The Blind Spot Analysis

Why 11 attacks per day are hitting your network unnoticed. 82% of attacks remain under 1Gbps—engineered to evade legacy detection.

The 90-Day Roadmap

Week-by-week plan from January assessment through March validation to deploy protection before Q2 budget locks.

Inside This Guide

Budget justification tools, technology evaluation checklist, and ROI calculations to secure executive approval.

Q1 is the window. This is the map. After April 1st, procurement processes lock and discretionary budgets freeze. Organizations that secure their networks in Q1 control their security spend. Those that wait pay the "Reactive Premium."

What You'll Learn:

- How to calculate the true cost of delayed security investment for your organization
- Why your current defenses are missing 82% of attacks and what that means for risk exposure
- A practical, week-by-week implementation plan to achieve full protection by March 31st
- ROI calculations and budget justification tools to secure executive buy-in

The Q1 Imperative

Why January-March Determines Your Year

For calendar-year organizations, January through March is the execution window. Budgets approved in Q4 get converted into vendor contracts, technology investments, and resource allocations. After Q1, budget flexibility decreases dramatically.

> **The "Reactive Premium" Tax**
>
> Organizations that wait until after an incident to invest in protection pay multiple premiums: the incident itself ($500K average), emergency procurement markups, and lost productivity.

Proactive vs. Reactive: The Comparison

✓ Q1 Proactive Strategy:

- → Full 12-month protection coverage
- → High negotiation leverage and discount opportunities
- → Planned implementation during normal hours
- → Optimized ROI through strategic spend

✕ Reactive (Post-Incident):

- → Partial year coverage with exposure gaps
- → Zero leverage—emergency pricing + rush fees
- → Crisis implementation causing team burnout
- → The "Reactive Premium"—high cost, low ROI

Bottom Line: Q1 2026 is when you eliminate the recurring cost of reactive security spending and establish peace of mind for the entire year.

Proactive vs. Reactive

The True Cost of Delayed Decision-Making

CRITERIA	✓ Q1 PROACTIVE STRATEGY	✕ REACTIVE (POST-INCIDENT)
Coverage Duration	✓ **Full 12 Months** You are protected all year	✕ **Partial Year** You are exposed until the contract is signed
Negotiation Power	✓ **High Leverage** You can shop around and negotiate discounts	✕ **Zero Leverage** Emergency procurement means paying list price + rush fees
Team Impact	✓ **Planned Implementation** Install during normal hours, low stress	✕ **Crisis Firefighting** Install during an outage, high burnout
Financial Outcome	✓ **Optimized ROI** Strategic Spend	✕ **The "Reactive Premium"** High Cost / Low ROI

Why Q1 Matters: For calendar-year organizations, budgets approved in Q4 get converted into vendor contracts and technology investments during Q1. After Q1, budget flexibility decreases dramatically, and discretionary spending gets committed. Procurement processes lock in, and IT roadmaps freeze.

The 2025-2026 Threat Landscape

The Silent Killer: Why Your ISP and Firewall Are Missing 82% of Attacks

11 Attacks Per Day

Organizations face an average of 11 DDoS attacks per day. However, the nature of these attacks has changed. If you're relying on your ISP or a standard Next-Gen Firewall for protection, you're likely blind to the majority of traffic hitting your network.

The Attack Profile

Sub-Threshold Evasion

82% of attacks remain under 1Gbps—specifically designed to evade the volumetric thresholds set by most ISPs. Your service provider likely won't even see the attack until it's too late.

The "State Exhaustion" Trap

While the attack is too small to trigger an ISP alert, it's large enough to fill your firewall's connection tables. Attackers aim to exhaust the state tables of your firewalls and load balancers, causing them to drop legitimate users.

The Result: Your bandwidth looks fine (green on the ISP dashboard), but your firewall CPU spikes and applications fail. You're left troubleshooting "network ghosts" while the attack continues.

The Enterprise Reality:
With 11 attacks per day and a $500K average cost per damaging incident, even a 99% mitigation rate leaves you exposed to 40 incidents a year. That represents a theoretical $20M+ annual exposure.

The 90-Day Action Plan

From Vulnerable to Validated by March 31st

JANUARY

Assessment & Planning

Week 1

Inventory Assets & Benchmark Visibility

Week 2

Define Requirements & Update RFPs

Week 3

Vendor Evaluation & POC

Week 4

Business Case Presentation

FEBRUARY

Procurement & Preparation

Week 1

Finalize Contracts & Service Model

Week 2

Architecture Review & Traffic Routing

Week 3

Pre-Deployment Testing

Week 4

Stakeholder Briefing

MARCH

Deployment & Validation

Week 1

Deploy & Enable Visibility

Week 2

Activate Automated Mitigation

Week 3

SOC Integration (if applicable)

Week 4

"Hands-Off" Validation

Key Evaluation Criteria

- ✓ Sub-threshold detection (82% of attacks)
- ✓ Multi-vector auto-response capability
- ✓ Encrypted traffic inspection
- ✓ Zero-touch automation

Success Metrics

- ✓ Visibility into all 11 daily attacks
- ✓ Sub-second automated mitigation
- ✓ Zero alert fatigue for security team
- ✓ Protection ready for Q3/Q4 peaks

🎯 TARGET STATE: MARCH 31, 2026

Full production deployment with automated protection tuned for sub-1Gbps attacks and large-scale campaigns. Your team is equipped to handle 4,015 annual attacks without manual intervention.

2,007
Hours Reclaimed Annually

$301K
Team Efficiency Savings

100%
Coverage for Q3/Q4 Peaks

Calculate Your Reactive Cost

Use this formula to demonstrate the cost of delay to internal stakeholders

☐ **Incident Response:**

(Avg. cost per incident) _____ × (Potential incidents) _____ = $ _____

☐ **Team Overtime:**

(Emergency response hours) _____ × (Fully-loaded labor rate) _____ = $ _____

☐ **Revenue Loss:**

(Downtime hours) _____ × (Hourly revenue rate) _____ = $ _____

☐ **Compliance Penalties:**

(Fines from inadequate protection) _____ = $ _____

TOTAL COST OF DELAY:

$ _____

This total is your penalty for delayed decision-making. Q1 2026 is when you eliminate this recurring cost. With an average of $500K per damaging incident and 11 attacks per day, the exposure adds up quickly.

Regional & Industry Exposure

Understanding Your Attack Surface

Attack patterns vary significantly by geography and industry vertical. Understanding your specific exposure profile is critical for accurate budget planning and resource allocation.

40%+

of Layer 3/4 attacks specifically target US data centers

121%

increase in attack volume against Financial Services

2x

Attack volume doubled year-over-year for Technology/Internet sectors

11/day

Average number of DDoS attacks organizations face daily

High-Risk Industry Verticals

- **Financial Services:** Banking, fintech, payment processors facing 121% attack volume increase
- **Technology/Internet:** SaaS providers, hosting companies, cloud services with doubled attack rates
- **E-Commerce:** Online retailers facing $300K/hour revenue loss during downtime
- **Gaming:** High-profile targets for DDoS-for-hire services and competitors

North American organizations face a disproportionate share of sophisticated attacks. With 40%+ of Layer 3/4 attacks targeting US infrastructure, enterprises in this region must prioritize sub-threshold detection capabilities that legacy ISP filters cannot provide.

Enterprise Planning Guide

Budget for Peace, Not Panic

To secure the budget for proactive defense, you must demonstrate ROI not just in "security" terms, but in "efficiency" terms. Here's how to make the business case.

Team Efficiency ROI

Automating defense reclaims your team's time from manual response to 11 daily attacks.

$301K

Annual savings from reclaiming 2,007 hours at $150/hr fully-loaded cost

Insurance & Compliance

Proactive controls deliver measurable financial benefits beyond security.

15-30%

Insurance premium reductions plus avoidance of NIS2/DORA fines (€10M or 2% revenue)

Technology Evaluation Checklist

Does your proposed solution pass the "Q1 2026" standard?

- ✓ Sub-threshold detection for 82% of attacks under 1Gbps
- ✓ Multi-vector defense with automated response
- ✓ Encrypted traffic inspection without breaking standards
- ✓ Zero-Touch Automation for 11 daily attacks

The Choice

Budget for Peace or Pay the Panic Tax

The first quarter of 2026 will determine your security posture for the entire year. Organizations that act decisively in January-March secure comprehensive protection and establish peace of mind.

The Q1 Advantage

- ✓ Full 12-month protection against 4,015 annual attacks (11/day)
- ✓ Avoidance of the "Reactive Premium" on procurement
- ✓ Reclaim 2,007 hours of team productivity annually
- ✓ Protection that works while you sleep
- ✓ Strategic budget control vs. emergency spending

The question isn't whether you'll face DDoS attacks—it's whether you'll be protected when they arrive.

The window is open now. Don't wait until Q2 to find out what you missed.

SPEAK WITH A SPECIALIST

Q1 2026 is the execution window.
This is your roadmap to securing your year.

Sources & Citations

[1] *Corero Network Security.* **"2025 Threat Intelligence Report."** 2025.

[2] *IBM.* **"Cost of Data Breach Report 2024."** 2024.

[3] *IANS Research and Artico Search.* **"2024 Security Budget Benchmark Report."** September 2024.

[4] *MazeBolt.* **"Cost of Damaging DDoS Attacks in 2025: Annual Trends Report."** January 2025.

[5] *Golia, Nick.* **"Annual Budgeting Process: Tips & Tools for Finance Teams in 2025."** *Limelight.* October 2024.

[6] *IBM.* **"Cost of Data Breach Report 2024."** Staffing adequacy correlation. 2024.

[7] *Elisity.* **"2026 Cybersecurity Budget: Complete Enterprise Planning Guide."** September 2025.

[8] *G2.* **"45+ DDoS Attack Statistics: Key Data and Takeaways for 2025."** July 2025.

[9] *StormWall.* **"DDoS in 2024: Detailed Statistics."** April 2025.

[10] *Corero Network Security.* **"2025 Threat Intelligence Report."** Regional data. 2025.

[11] *G2.* **"45+ DDoS Attack Statistics."** Q1 2024 regional targeting. July 2025.

[12] *StationX.* **"Top +35 DDoS Statistics (2025)."** June 2025.

[13] *Gcore.* **"DDoS Attack Trends for Q1–Q2 2024."** 2024.

[14] *Elisity.* **"Cybersecurity Budget Benchmarks for 2026."** Insurance impact. November 2025.

[15] *Elisity.* **"2026 Cybersecurity Budget Guide."** Skills gap statistics. September 2025.