QKS Group | corero [NETWORK SECURITY]

Protecting Availability at Scale; Real-Time DDoS Defense as the Cornerstone of Business Continuity

Andrew Aken
AVP - Research

Sofia Ali
Practice Director & Principal Analyst

Sujit Dubal
Principal Analyst

TABLE OF CONTENTS

Executive Summary

Digital availability has become a strategic business imperative. Revenue generation, customer trust, regulatory standing, and operational resilience are now directly tied to uninterrupted application and network performance. Yet the threat landscape has evolved in ways that expose the limits of traditional DDoS defenses.

Volumetric Layer 3 and Layer 4 floods remain a persistent danger, but attackers have increasingly shifted toward subtler, harder-to-detect methods: application-layer assaults targeting HTTPS endpoints, API exhaustion campaigns, and short-burst attacks designed to evade threshold-based detection. Corero Network Security's threat intelligence drawn from inline deployment data across global ISP and enterprise environments consistently shows that application-layer and encrypted attacks now constitute the majority of observed DDoS activity by event count.

The near-universal adoption of TLS encryption across web and API traffic has created a structural visibility gap that legacy defenses cannot close. Malicious activity concealed inside encrypted sessions can silently degrade application performance without triggering volumetric alarms, and this silent degradation is increasingly more operationally damaging than dramatic bandwidth floods.

Key Finding: *Organizations relying on diversion-based scrubbing models are architecturally exposed to encrypted, low-volume, and short-burst attack vectors that operate below traditional detection thresholds. Inline, TLS-aware mitigation is no longer optional it is foundational to modern continuity strategy.*

This paper examines the architectural shift from reactive DDoS mitigation to continuity-driven defense and evaluates how Corero Network Security's SmartWall ONE™ platform enhanced by CORE centralized intelligence addresses the full spectrum of modern availability threats.

1. Availability as a Strategic Control Objective

Historically, DDoS defense was treated as a network hygiene function: absorb excess bandwidth, restore service, move on. That paradigm is no longer sufficient.

In modern digital enterprises and service provider environments, application responsiveness drives revenue conversion. API stability underpins entire digital ecosystems. Milliseconds of latency affect customer experience and downstream SLAs. Regulatory frameworks including the EU's Digital Operational Resilience Act (DORA), the NIS2 Directive, and the SEC's cybersecurity disclosure rules increasingly require demonstrable resilience under adverse conditions.

Availability is no longer measured solely by uptime. It is measured by performance stability under stress. A service that technically remains online but responds with degraded latency during an attack has failed its availability obligations.

Security leaders must therefore evaluate DDoS defense not as an isolated network function but as a core architectural safeguard for business continuity one that is measurable, reportable, and aligned to organizational risk appetite.

2. The Expanding Multi-Layer Threat Landscape

Modern DDoS campaigns rarely rely on a single attack vector. Sophisticated threat actors orchestrate multi-layer assaults that simultaneously pressure infrastructure, application logic, and encrypted traffic channels.

2.1 Layer 3 and Layer 4 Volumetric Threats

Infrastructure-layer attacks continue to target bandwidth saturation, amplification vectors (DNS, NTP, CLDAP reflection), connection state exhaustion, and routing infrastructure limits. These attacks can overwhelm links within seconds. Recent industry incidents have demonstrated volumetric attacks scaling into the terabit-per-second range a trajectory that continues to rise as botnet infrastructure grows in scale and sophistication.

Immediate automated suppression is non-negotiable at this layer. Any diversion-introduced delay compounds downstream impact.

2.2 Layer 7 Application-Layer Disruption

Layer 7 DDoS represents a more operationally nuanced threat. Rather than saturating bandwidth, attackers generate high volumes of seemingly legitimate HTTPS requests, exhaust API endpoints, manipulate session state, and exploit resource-intensive application logic such as search, authentication, and database queries.

Corero-observed data shows that the majority of attack events handled inline are under 10 minutes in duration precisely the window in which diversion-based models fail to respond before damage is done. Application-layer attack methodologies continue to evolve in both sophistication and volume.

2.3 The Encryption Blind Spot

The structural challenge of the current threat landscape is that most malicious traffic now arrives encrypted. Traditional inspection methods that rely on packet-level analysis are largely ineffective against threats embedded in HTTPS sessions.

Attackers exploit this systematically: malicious request patterns are concealed within encrypted flows, attack traffic blends with legitimate sessions, and signature-based controls are evaded entirely. Without TLS-aware inspection capabilities, organizations face a growing blind spot one that enables silent service degradation without any volumetric alarm being triggered.

Corero Threat Intelligence Note: *Analysis of attack patterns observed across SmartWall ONE deployments shows a growing incidence of encrypted application-layer attacks used in combination with other threat vectors leveraging availability degradation to create operational pressure that exposes additional attack surface.*

3. Why Traditional Scrubbing Models Fall Short

Centralized scrubbing architectures have provided effective defense against volumetric floods for over a decade. However, their design assumptions are increasingly misaligned with the current threat environment.

Traffic diversion models introduce latency through routing reconfiguration and require operational coordination before mitigation begins. For short-duration bursts which can

degrade service significantly within 30 to 60 seconds diversion-based response arrives too late. In Corero deployments, the overwhelming majority of attacks are suppressed automatically in under one second; a diversion model cannot approach that response window.

Beyond latency, scrubbing centers have limited capacity for Layer 7 inspection and minimal visibility into encrypted traffic streams. They are structurally designed to handle volumetric floods, not the nuanced application-layer and encrypted attack campaigns that now dominate the threat landscape.

In high-performance environments ISPs managing peering exchanges, financial institutions operating under strict SLA obligations, 5G core networks handling latency-sensitive signaling even brief diversion introduces performance trade-offs that undermine the case for scrubbing-based models.

As network infrastructure decentralizes across multi-site enterprises, hybrid cloud environments, and edge data centers, the architectural requirement shifts decisively: mitigation must occur closer to ingress points, inline, and without diversion delay.

4. Architecting for Continuity: Design Principles

A continuity-driven DDoS architecture is distinguished from a reactive mitigation model by a fundamental shift in objective: availability becomes a preserved state rather than a restored outcome.

This architectural shift requires several specific design properties working in concert. Inline deployment within the network path eliminates diversion latency and ensures mitigation begins at the first packet of an attack. Sub-second automated response removes human decision cycles from the critical path during fast-moving attacks. Multi-layer inspection across L3, L4, and L7 addresses the full spectrum of attack vectors without requiring separate tooling per layer. TLS-aware traffic analysis closes the encrypted traffic blind spot that legacy tools cannot address. Horizontal scalability across distributed sites enables consistent protection across enterprise branches, ISP points of presence, and edge deployments. And centralized governance and telemetry provides executive visibility, compliance reporting, and coordinated policy management.

Organizations that embed these principles into their infrastructure architecture achieve a fundamentally different risk posture one in which DDoS attacks are absorbed operationally rather than triggering reactive incident response cycles.

5. SmartWall ONE: Inline Multi-Layer Mitigation in Practice

Corero Network Security's SmartWall ONE platform is engineered around the continuity-driven design principles outlined above. The following sections examine each architectural dimension and its operational implications.

5.1 Always-On Inline Deployment

SmartWall ONE operates directly within the network path not as a diversion-capable appliance that activates on alert, but as a continuously active mitigation layer. This eliminates the diversion latency window that creates exposure in legacy models.

For ISPs and carriers, this means immediate suppression of L3 and L4 floods at peering edges, preserving throughput and routing integrity under attack conditions. For enterprise deployments, it means application performance is protected continuously, without requiring an operations team to initiate a mitigation workflow. Carrier-grade scalability enables SmartWall ONE to operate effectively at the throughput volumes characteristic of modern internet exchange points and high-bandwidth enterprise environments.

5.2 TLS-Aware Layer 7 Detection

The most operationally significant capability differentiating SmartWall ONE in the current threat environment is its encrypted traffic visibility. SmartWall ONE incorporates TLS-aware inspection techniques including behavioral fingerprinting and anomalous request pattern analysis within encrypted HTTPS sessions that allow detection and mitigation of threats that are invisible to traditional packet inspection tools.

This supports identification of anomalous request behavior within encrypted flows, mitigation of encrypted API endpoint exhaustion attacks, protection of

web services that operate exclusively over HTTPS, and a significant reduction in the encrypted traffic blind spot that has become the primary concealment vector for sophisticated attackers.

Effective TLS inspection in an inline context requires architectural care: inspection must be conducted with minimal latency overhead to avoid becoming a performance bottleneck. Corero's approach relies on behavioral and statistical analysis rather than full TLS termination for all traffic, enabling inspection at scale without introducing the latency penalties associated with full decryption architectures.

5.3 Sub-Second Automated Mitigation

In SLA-sensitive environments, mitigation speed is a continuity metric in its own right. SmartWall ONE's automated response capability reduces exposure windows to sub-second timescales a critical capability for short-burst attacks that can cause measurable service degradation within tens of seconds.

Automation also removes the operational burden of human-in-the-loop mitigation decisions during fast-moving attack events, enabling security teams to focus on investigation and reporting rather than real-time triage.

Operational Impact: *In ISP deployments, sub-second mitigation directly translates to preserved customer SLAs and reduced support escalation volumes during attack events measurable improvements to operational efficiency and customer retention.*

6. CORE: Centralized Intelligence and Governance

While SmartWall ONE executes inline mitigation at network ingress points, CORE provides the centralized visibility and orchestration layer that transforms distributed mitigation into a governable, reportable capability.

For organizations with multi-site deployments, CORE aggregates telemetry across all SmartWall ONE instances, enabling correlation of attack patterns that span multiple locations. A low-volume Layer 7 campaign targeting an organization's API infrastructure simultaneously across four regional sites each instance below the threshold of local alerting becomes visible as a coordinated campaign when viewed

through CORE's aggregated telemetry. Without cross-site correlation, these attacks can persist undetected.

CORE's governance capabilities align directly with the reporting requirements of modern regulatory frameworks. DORA, for instance, requires financial entities to maintain documented evidence of resilience testing and incident response. CORE's audit trails, availability KPI dashboards, and executive-level reporting provide the structured data necessary to satisfy these requirements.

Board-level oversight of cybersecurity resilience is increasingly mandated both by regulation and by investor and customer expectations. CORE enables security leaders to translate technical mitigation performance into the business continuity metrics that board-level governance demands.

7. Protecting Distributed and Edge Architectures

Digital infrastructure no longer resides primarily in centralized data centers. Modern organizations span multi-site enterprise networks, ISP peering exchanges, 5G core infrastructure, edge data centers, and hybrid cloud environments. Each point of presence represents both a potential attack surface and an opportunity for proximity-based mitigation.

Inline, multi-layer mitigation deployed at distributed ingress points provides several architectural advantages over centralized models. Attack traffic is contained at the point of entry rather than traversing internal network segments before mitigation begins. Performance integrity is maintained locally, reducing the blast radius of volumetric attacks that would otherwise saturate transit links. And customer-facing DDoS protection services an increasing revenue opportunity for ISPs and managed security providers become feasible to deliver at scale.

As 5G network rollouts accelerate, the signaling plane of core networks becomes an increasingly attractive target. Inline mitigation at 5G infrastructure ingress points addresses a threat vector that traditional perimeter-based architectures are poorly positioned to handle.

8. Measuring Business Continuity Outcomes

The business case for modern DDoS defense must be expressed in continuity outcomes, not technical specifications. Security leaders evaluating availability platforms should establish measurable baselines and track improvement across the following dimensions: downtime frequency per quarter measured against pre-deployment baseline; mean time to mitigate from attack onset to service restoration; operational intervention rate reflecting the proportion of attacks requiring human escalation; SLA compliance rate during active attack periods; and compliance audit readiness in the form of documented evidence for DORA, NIS2, and SEC reporting obligations.

Inline, TLS-aware, automated mitigation directly improves each of these metrics. The investment case for continuity-driven DDoS defense is therefore expressible in the language of operational and regulatory risk accessible to finance, legal, and board-level stakeholders, not only to security teams.

9. Vertical Use Cases: Tailored Value by Sector

ISPs and Carriers: Primary risk profile centers on peering exchange floods and customer SLA breach. SmartWall ONE delivers inline mitigation at the edge and enables customer-facing DDoS protection as a managed service revenue stream.

Financial Services: Application-layer exhaustion and regulatory scrutiny under DORA and NIS2 represent the dominant risk factors. SmartWall ONE provides sub-second L7 response, while CORE delivers the audit trails and availability reporting that compliance frameworks require.

5G and Telco: Core network flooding and signaling plane attacks are the critical threat vectors. Carrier-grade throughput and proximity-based containment ensure mitigation does not introduce latency into latency-sensitive network functions.

Enterprise and Multi-site: Encrypted attack campaigns coordinated across distributed branches require cross-site visibility. CORE's centralized governance combined with per-site inline enforcement addresses this architecture directly.

Edge and Cloud Hybrid: Attack propagation across hybrid boundaries requires distributed inline deployment with coordinated cross-site policy precisely the architecture SmartWall ONE and CORE provide together.

10. Strategic Evaluation Framework

When assessing DDoS defense platforms for continuity-grade protection, security leaders should evaluate candidates against the following criteria: whether the deployment model is inline and always-on versus out-of-path and diversion-based; the breadth of coverage across L3, L4, and L7; the depth of HTTPS and TLS inspection capability; mitigation speed under active attack conditions; scalability across distributed and edge environments; and the quality of centralized governance, executive reporting, and compliance documentation.

Architectural design now outweighs raw bandwidth absorption capacity as the primary determinant of resilience maturity. The question is no longer how much traffic can be scrubbed it is how quickly, accurately, and continuously mitigation operates across the full attack surface.

11. The Road Ahead: Emerging Threat Dimensions

The threat landscape will continue to evolve in ways that amplify the importance of the architectural properties described in this paper.

AI-generated attack traffic is an emerging concern: generative models are increasingly capable of producing attack patterns that mimic legitimate user behavior more accurately than rule-based tools, raising the sophistication ceiling for Layer 7 evasion. Mitigation platforms that rely on static signatures will be increasingly outpaced; behavioral and statistical detection methods gain importance correspondingly.

Post-quantum cryptography transitions will affect TLS inspection architectures. As quantum-resistant cipher suites are adopted, organizations will need to ensure their

inspection capabilities keep pace with new cryptographic handshake patterns a consideration for both procurement timelines and vendor roadmap evaluation.

Link speeds continue to scale. 400Gbps and 800Gbps interfaces are becoming standard at major internet exchange points, and attack tooling scales proportionally with available botnet infrastructure. Mitigation platforms must demonstrate a credible scalability roadmap to remain relevant at the throughput volumes that the next three to five years will normalize.

Organizations that invest in inline, TLS-aware, behavioral detection architectures today are building the foundation that will remain valid as these pressures intensify.

Conclusion

The DDoS threat landscape has shifted decisively: from pure bandwidth floods to multi-layer campaigns, from visible volumetric spikes to encrypted concealment, from reactive scrubbing to the requirement for always-on inline mitigation. The organizations most exposed are those whose defense architectures were designed for the previous generation of attacks.

Business continuity in the current environment depends on multi-layer detection across L3, L4, and L7; genuine visibility into encrypted HTTPS traffic streams; sub-second automated response that removes human latency from the mitigation path; inline deployment that eliminates diversion delays; and centralized governance that makes resilience performance measurable and reportable at the executive level.

Corero's SmartWall ONE platform, enhanced by CORE centralized intelligence, reflects this architectural evolution. For ISPs, financial institutions, 5G operators, and enterprises operating distributed digital infrastructure, it provides a continuity-grade foundation that addresses both today's threat landscape and the architectural pressures of the years ahead.

In an increasingly encrypted and application-centric threat environment, real-time TLS-aware inline DDoS defense is not an enhancement to existing security architecture. It is the foundation on which meaningful availability assurance is built.

QKS Group | corero [NETWORK SECURITY]

www.qksgroup.com