corero
[NETWORK SECURITY]

SOLUTION BRIEF

Stop Encrypted Attacks Before They Reach Your Applications

The only DDoS defense that sees threats hiding in TLS—without becoming the bottleneck

SMARTWALL ONE™

The Encryption Paradox

We fought for years to encrypt the internet, and we won. Today, over 85% of web traffic flows through HTTPS/TLS, shielding data from prying eyes. But that same shield has created the largest blind spot in modern cybersecurity.

Attackers now use encrypted tunnels as the perfect hiding place. They launch devastating HTTP floods, abuse APIs, and probe for vulnerabilities—all while traditional security tools see nothing but an encrypted blur. The attacks are sophisticated, the damage is immediate, and most defenses are completely blind.

> ⚠️ **The cost of this blindness is staggering.** E-commerce sites lose as much as $300,000 per hour during downtime. Service providers lose customers to competitors who can prove they stop encrypted threats. And worse, many organizations don't realize that the application-layer flood hammering their login page isn't the real attack—it's the distraction covering data exfiltration happening in the background.

If you can't see inside SSL/TLS traffic, you're not just blind to DDoS. You're blind to the opening move of a breach.

Why Traditional Defenses Bottleneck Under Encrypted Attacks

Three conventional approaches consistently fail when faced with modern encrypted threats, and each failure stems from a fundamental architectural flaw.

1 Legacy DDoS Tools

Measuring Volume, Missing Intent

Traditional DDoS solutions were built to count packets, not understand behavior. They can tell you a pipe is full but have no idea what's flowing through it. This makes them completely unable to distinguish a malicious botnet from a legitimate traffic spike during a flash sale. When attacks hide inside encrypted sessions, these tools are reduced to blind traffic cops guessing at intent.

2 Web Application Firewalls

The Serial Inspection Trap

To inspect encrypted traffic, WAFs must decrypt everything, typically in a single processing queue. If you're relying on your WAF to also handle high-volume attack conditions, this creates a catastrophic bottleneck. It's like forcing every person in a stadium to wait in a single-file line for security screening—the WAF itself becomes the point of failure. Latency skyrockets for legitimate users before the system crashes entirely, taking your application down with it.

3 Cloud Scrubbing Services

Always Late to the Fight

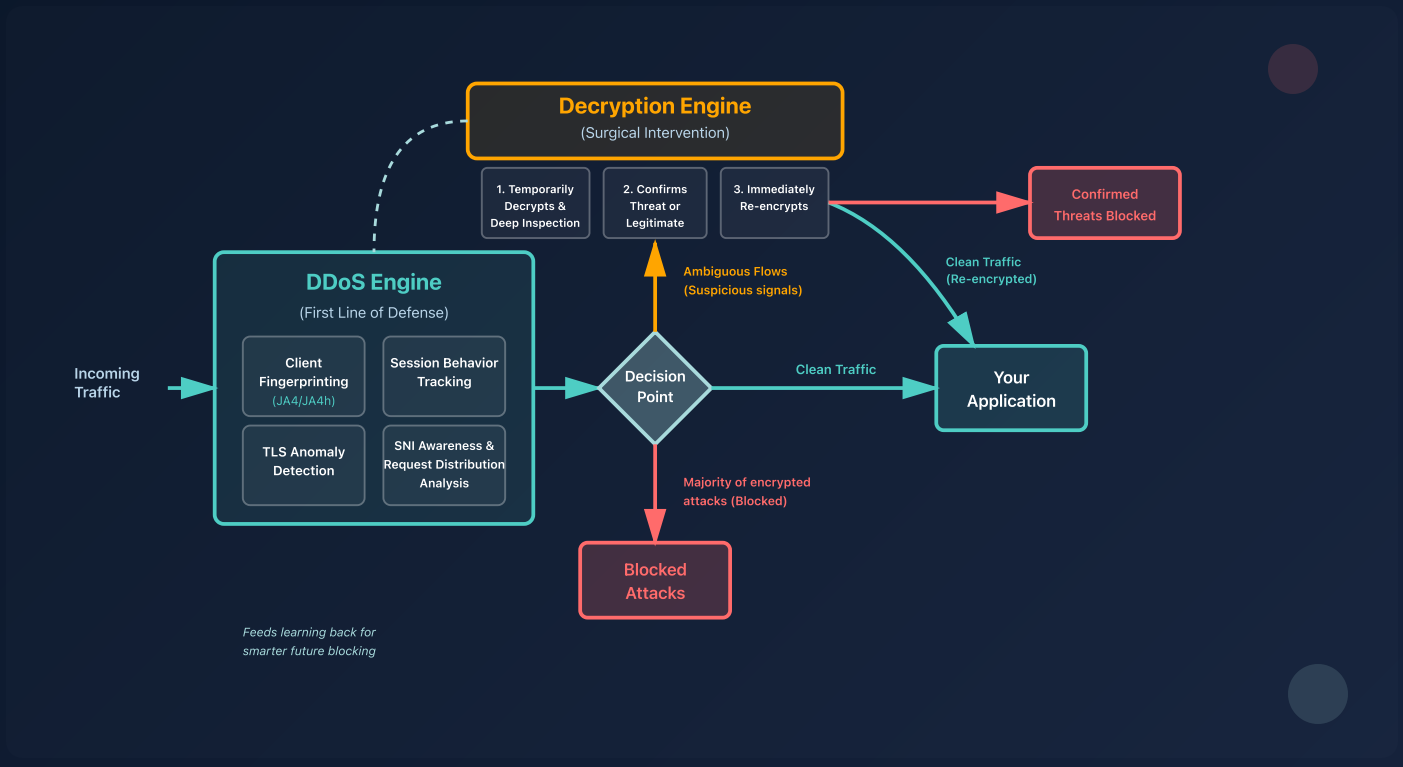
The fundamental flaw here is time. When an attack is detected, traffic must be rerouted to an off-site scrubbing center. This BGP redirection and stabilization process takes minutes to activate. By the time mitigation begins, 5 to 15 minutes have passed, an e-commerce site has already lost $50,000 to $75,000, customer trust has evaporated, and the damage is irreversible.

The pattern is clear: solutions that can't intelligently analyze encrypted traffic in real-time, inline, will always arrive too late or collapse under the load.

The Smarter Architecture: Integrated Intelligence + Surgical Precision

SmartWall ONE takes a fundamentally different approach. Instead of forcing all traffic through a serial decryption bottleneck, we use an integrated dual-engine architecture that stops most attacks without ever decrypting them—and only applies surgical decryption when truly necessary.

How It Works: Two Engines, One Seamless Defense



The DDoS Engine (First Line of Defense)

Handles volumetric attacks and behavioral analysis at wire speed. This engine processes traffic using multiple intelligence layers:

- **Client Fingerprinting (JA4/JA4h):** Every connection announces itself through a TLS handshake. Legitimate browsers from Chrome, Firefox, and Safari have predictable, standardized fingerprints. Bots reveal themselves through anomalous or outdated TLS implementations—no decryption needed.
- **Session Behavior Tracking:** We monitor patterns over time. Low-and-slow attacks that open thousands of connections and keep them barely alive? Instantly identified and blocked. Connection rate anomalies that indicate reconnaissance? Stopped before they become breaches.
- **TLS Anomaly Detection:** Unusual handshake errors, suspicious renegotiation attempts, and protocol violations flag malicious actors before they ever reach your application.
- **SNI Awareness and Request Distribution Analysis:** We analyze metadata within TLS handshakes and observe how requests distribute across resources to spot patterns invisible to volume-based tools.

The majority of attacks are stopped here—at line rate, with zero decryption overhead.

The Decryption Engine (Surgical Intervention)

When behavioral signals are suspicious but not conclusive, the DDoS engine steers only those ambiguous flows to the decryption engine. This secondary system:

- Temporarily decrypts the suspicious session
- Performs deep inspection to confirm threat or legitimate traffic
- Immediately re-encrypts and passes clean traffic through
- Feeds learning back to the DDoS engine for smarter future blocking

This selective approach reserves resource intensive decryption for the fraction of traffic that genuinely requires it. Your performance stays intact. Your security gets smarter with every attack.

Four Reasons This Architecture Outperforms Everything Else

1 Faster Mitigation

Sub-Second Blocking vs. Minutes of Damage

Because most attacks are identified and stopped locally by behavioral analysis, mitigation is nearly instantaneous. There's no waiting for BGP rerouting, no queue backlog, no "scrubbing center spin-up time." Attacks are blocked inline, in under a second, before they ever touch your application infrastructure. The difference between sub-second response and multi-minute response is the difference between zero revenue loss and catastrophic business impact.

2 Better Performance

No Decryption Bottleneck

By not decrypting everything, SmartWall ONE avoids the architectural chokepoint that cripples other solutions. Legitimate traffic flows through with no added latency. The system handles typical SSL/TLS connection rates without breaking stride—because intelligence, not brute-force processing, does the heavy lifting.

3 Higher Precision

Block Intent, Not Volume

Blocking based on malicious behavior detection, rather than traffic volume profiling, dramatically reduces false positives. Your marketing campaign drives a 10x traffic spike? SmartWall ONE recognizes this as legitimate user patterns, and your site keeps running smoothly. Meanwhile, a sophisticated low-volume bot attack that legacy tools would miss entirely gets identified and eliminated through behavioral fingerprinting, before your site is impacted.

4 Less Complexity

One Platform, L3 Through L7

SmartWall ONE provides unified protection from network-layer floods (L3/L4) all the way through encrypted application attacks (L7). Integrated L3-L7 DDoS defense leaves your WAF infrastructure to focus on protecting your applications from exploits. You don't need to manage multiple vendor relationships, or stitch together incompatible security telemetry. One platform, one management interface, complete visibility.

The Strategic Shift: From Volume to Intent

The most important advantage our architecture delivers is a fundamental change in how you understand your traffic.

Flow data only tells you how much is coming. SmartWall ONE also tells you what it's trying to do.

This shift from quantitative to qualitative threat analysis gives you four critical capabilities:

- **See Through the Encryption:** Attackers hide inside encrypted traffic because they assume you're blinded by it. Our behavioral analysis and selective decryption gives you vision, without the performance penalty of decrypting everything.
- **Reserve Heavy Processing for Real Threats:** Intelligence identifies attacks; decryption confirms them. This surgical approach preserves speed and system resources for legitimate traffic.
- **Stop Sophisticated Attacks Traditional Tools Miss:** Low-and-slow attacks, API abuse, and reconnaissance probes don't generate massive traffic spikes. They're invisible to volume-based defenses but immediately obvious to behavioral analysis.
- **Respond Inline, Not Off-Path:** Milliseconds matter. Routing traffic to an external scrubbing service means the first wave of an attack always succeeds. Inline defense means attacks are identified and blocked within the first few packets.

What Makes SmartWall ONE Architecturally Superior

Traditional approaches force ALL encrypted traffic through a single serial processing pipeline. This creates unavoidable bottlenecks under attack conditions. SmartWall ONE uses parallel processing with intelligent traffic steering—the DDoS engine handles volumetric defense and behavioral analysis simultaneously, only engaging the decryption engine for the fraction of traffic that requires deep inspection.

Key Architectural Differentiators:

- High-performance DDoS engine handles volumetric attacks first, steering suspicious flows (not all traffic) to decryption
- Decryption engine extracts features, detects attacks, closes the loop back to the DDoS engine
- Selective decryption with the explicit goal to "get out of the path" once a session is validated
- Integrated L3–L7 defense leaves your WAF to focus on application exploits

Is Your Current Defense Leaving You Exposed?

Use this framework to evaluate whether your existing security architecture can handle modern encrypted threats.

Question 1: Decryption Bottleneck Test

If you're currently just using a standalone WAF for L7 protection: What happens to inspection latency when you face a 50Gbps encrypted flood? Does your WAF have enough processing headroom to decrypt, inspect, block the bad packets, and re-encrypt the legitimate traffic volume without collapsing? Most don't.

What SmartWall ONE Does Differently:

We don't decrypt everything. We identify and block the majority of malicious traffic using behavioral analysis, before it ever reaches the decryption engine.

Question 2: Time-to-Mitigation Reality Check

If you're using cloud-based scrubbing services: Calculate this: [Your average online revenue per minute] × [10 minutes of BGP rerouting and scrubbing activation]. That's your guaranteed minimum loss from every attack, not including the time it takes to recover your applications and services after mitigation begins.

What SmartWall ONE Does Differently:

Inline, sub-second blocking means zero minutes of unprotected exposure. Attacks are stopped from the first few malicious packets; applications and services keep running—the revenue loss is zero.

Question 3: False Positive Cost Analysis

If you're using volume-based DDoS thresholds: Have you ever had a legitimate traffic surge (marketing campaign, product launch, viral content) trigger your DDoS protection and block real customers? Traffic volume-based networking and security tools can't distinguish a flash sale from a botnet.

What SmartWall ONE Does Differently:

Behavioral fingerprinting and intent analysis identify malicious patterns regardless of traffic volume. Legitimate spikes flow through; sophisticated volumetric attacks get blocked.

Question 4: The Hidden Cost of Complexity

If you're running separate solutions for L3/L4 DDoS and L7 application protection: How many hours per month does your team spend correlating data between systems, troubleshooting integration issues, and managing multi-vendor relationships? What's the total cost of ownership across those separate platforms?

What SmartWall ONE Does Differently:

A single unified platform that delivers complete L3–L7 visibility and protection. One vendor, one management interface, one source of truth for security telemetry.

What You Get With SmartWall ONE

Capability	SmartWall ONE	Cloud-Based Scrubbing	Standalone WAF	Legacy DDoS Tools
Sub-second inline mitigation	✓ Integrated	✕ 5–15 min BGP + mitigate delay	✕ Only if traffic reaches it	Δ 10s of seconds flow detect and redirect delays
TLS/HTTPS flood protection	✓ Behavioral + selective decryption	Δ Full decryption (bottleneck)	Δ Full decryption (bottleneck)	✕ Blind to encrypted attacks
Bot detection (JA4/JA4h)	✓ Included	✕ Separate bot mgmt fee	✕ Separate bot mgmt. fee	✕ Not available
No performance degradation under attack	✓ Parallel engines	✕ Off-path latency	✕ Serial decryption queue	Δ L3/L4 only
Unified L3–L7 platform	✓ Single system	✕ Multiple services	✕ Application-layer only	✕ Network-layer only
Session behavior tracking	✓ Built-in	Δ Limited visibility	Δ App-level only	✕ Volume-based only
Low-and-slow attack detection	✓ Behavioral analysis	✕ Missed entirely	Δ If traffic reaches WAF	✕ Below volume thresholds

The Real Question Isn't "Can We Afford This?"

It's "Can we afford NOT to see what's hiding in our encrypted traffic?"

What's the greater risk?

> The impact of a DDoS attack you can't see, because it's encrypted, could be the smokescreen that distracts you from a more damaging and costly data breach.

Most organizations discover their blind spots only after an incident. By then, the cost isn't just revenue loss—it's customer trust, regulatory scrutiny, incident response, and reputational damage that takes years to repair.

Next Step: See Your Blind Spots

We're not asking you to take our word for it. Send us your current architecture diagram, and we'll provide a no-obligation competitive threat assessment—a detailed analysis of exactly where your encrypted traffic blind spots exist, what attack types you're vulnerable to, and how SmartWall ONE addresses those gaps.

No sales pitch. Just engineering analysis from our team to yours.

The attacks hiding in your encrypted traffic aren't waiting. Your defenses shouldn't either.

Contact us today *to schedule your competitive threat assessment.*