DATASHEET

CORERO SMARTWALL® ONE

EDGE MITIGATION: EMPOWERING THE NETWORK EDGE

Corero SmartWall ONE delivers full edge protection for even the largest provider networks.

Powering the filtering capabilities increasingly built into modern edge routers, SmartWall ONE scales to tens-of-terabits per second of protection, without the need to deploy dedicated appliances at the edge or needing to back-haul large volumes of attack traffic to scrubbing centers.

The DDoS threat landscape continues to have businesses and government agencies around the world concerned about outages of their online services which could impact customers, impact operations, and result in major economic losses.

Well-publicized volumetric attacks that harness vulnerable IoT devices have recently raised awareness of the scale of the DDoS problem. This has pushed maximum, and average, attack sizes up, as well as significantly increasing their frequency, due to the ease with which they can now be launched, by anyone with a motive.

The sophistication of DDoS also continues to evolve each year. These attacks make detection and protection more challenging due to their varying amplitudes, ports, and protocols. The average attack is short, meaning real-time detection and mitigation are an essential requirement for comprehensive protection.

Avoid the Protection Gap of Legacy DDoS Solutions

SmartWall ONE delivers intelligent DDoS defense that inspects packets directly and automatically defends against attacks, with the speed and accuracy to prevent the damaging downtime from a successful attack.

Uptime Assurance

DDoS attacks are a security and availability issue. SmartWall ONE ensures continuity for organizations that require SLAs for service uptime and availability without latency or service interruptions.

Granular Visibility

Industry-leading analytics drill down on attacks so you can better understand them and deliver increased threat intelligence.

Comprehensive Defense

Protection from volumetric, state exhaustion, short duration, IoT botnets, carpet bomb/spread spectrum, and pulsing attacks with available cloud hybrid protection to guard against the largest saturating attacks.

Advanced Protection

We protect against multi-vector, attacks, which combine one or more volumetric, or state exhaustion techniques sequentially, in an attempt to evade detection or mitigation.

On-Premises DDoS Protection without Dedicated Appliances

SmartWall ONE, coupled with the high-performance packet filtering of smart infrastructure devices, for mitigation, deliver our award-winning protection at unprecedented scale and simplicity of deployment.

The solution includes the SmartWall ONE Management engine, which offers multiple options for managing, configuring, and monitoring our detection appliances, including a flexible browser-based GUI, a full SSH CLI, and powerful REST API that supports open integration with existing management frameworks. The management engine is delivered as a virtual appliance to run on customer-provided hardware.

SmartWall ONE also includes the SmartWall ONE Analytics engine, a powerful security analytics tool that delivers comprehensive and easy-to-read dashboards, as well as enabling sophisticated forensics. Our analytics capability is driven by security event and traffic flow feeds from our detection appliances and supported infrastructure device telemetry.

Our solution leverages Splunk software for big data analytics and advanced visualization capabilities to transform sophisticated security event data into dashboards that deliver actionable intelligence before, during, and after an attack.

N Network Defense Device | M Provider Service Management | P Service Portal

Infrastructure	Devices monitor ingress traffic via sampled mirrors that include both header and payload to accurately identify the threat.
Visibility	SmartWall ONE inspects every packet in the sample feeds to detect any DDoS attack traffic quickly and accurately.
Mitigation	SmartWall ONE dynamically generates surgical filters to mitigate attacks directly on the supported infrastructure devices.
Automation	SmartWall ONE automatically configures infrastructure devices using the NETCONF to install filters which block DDoS packets directly at network ingress points.
Simplicity	Telemetry, machine analytics, and network programmability make the detection and mitigation process more intelligent, automated, and adaptable.

Key Benefits

Comprehensive Visibility

SmartWall leverages data analytics to deliver sophisticated and comprehensive visibility, reporting, and alerting capabilities for clear, actionable intelligence on the DDoS attack activity happening across the network.

Rapidly Detect DDoS Attacks of all Size

SmartWall fills the protection gap, by not only blocking the large volumetric attacks commonly associated with DDoS, but also detecting and surgically blocking the more common and smaller attacks which use the same vectors - many of which are too small or short in duration to be mitigated by legacy solutions.

Accurately and Automatically Allows the Good and Stops the Bad

Good traffic is able to flow uninterrupted, enabling services and applications to stay online, while DDoS traffic is surgically blocked before it has the chance to cause any damaging effects.

Reduced Operating Costs

Automated DDoS response from Corero significantly decreases human intervention and false positives for reduced operation-al costs and lowest TCO.

Automatic Protection

Automatically mitigates a wide range of DDoS attacks, without operator intervention, maintaining full connectivity to avoid disrupting the delivery of legitimate traffic – stopping attacks faster.

Hybrid DDoS Protection

Enhances cloud-only solutions with highly accurate, real-time, on-premises protection.

Always-On or Scrubbing Deployment

Physical or virtual appliance flexibility in-line, or in the data path, at the edge, or out-of-band scrubbing with fast and accurate sampled packet, or flow-based detection that redirects attack traffic for mitigation.

Managed Services Enabler

Hosting Providers, MSPs, MSSPs and ISPs can enhance security service offerings by delivering real-time automatic DDoS protection as-a-service to their customers with upstream signaling capabilities enabling them to protect their customers without "blackholing" or disrupting legitimate traffic.

Security Policy Enforcement

Always-on traffic inspection, and real-time mitigation enforces security policies that prevent volumetric layers 3-7 DDoS attacks for both IPv4 and IPv6 traffic.

DDoS Mitigation Coverage

Custom Protection

» Defends attacks to single/multiple IPs and Subnets

» Smart-Rules – Patented high-performance heuristics-based engine that automatically detects and blocks volumetric DDoS attacks, including zero-day.

» Flex-Rules - Programmable filters using the Berkeley Packet Filter (BPF) syntax with Corero enhancements

- Address a variety of volumetric attack vectors, from reflective through to those leveraging specific payloads (TeamSpeak, RIPv1, NetBIOS)

» Botnet/source flood detection and blocking

» Intelligent automatic fragment blocking

» TCP/UDP port-based

» Rate limiting policies

» Cloud mitigation and BGP RTBH/FlowSpec signaling

Resource Exhaustion

» Malformed and Truncated Packets (e.g. UDP bombs)

» IP fragmentation/segmentation AETs

» Invalid TCP segment IDs

» Bad checksums and illegal flags in TCP/UDP frames

» Invalid TCP/UDP port numbers

Volumetric DDoS

» TCP flood

» UDP flood

» UDP fragmentation

» SYN flood

» ICMP floods

» Carpet bombing

Reflective Amplification DDoS

» NTP monlist response amplification

» Connectionless LDAP (CLDAP)

» SSDP/UPnP responses

» SNMP inbound responses

» CHARGEN responses

» DNS

Monitor in Real-Time

Information is presented in real-time or historical charts and dashboards.

Analyze Attacks

Drill down into blocked and allowed traffic seen an attack.

Optimize Protection

Gather traffic information to help you fine-tune policies.

Enhance Threat Intelligence

All events are stored and indexed in the analytics and available to other security solutions.

Technical Specifications

Performance

Maximum Throughput
40 Terabits per Second

Maximum Throughput
60 Billion Packets per Second

Time to Mitigation
<10 Seconds (Typical)

Physical Environment

Hypervisors
KVM running on Red Hat Enterprise 7+, CentOS 7+ or Ubuntu 16.04+
VMware ESXi 6.5+

Minimum Requirements
16GB Memory, 20GB Disk

Network Interfaces
10G - XL710 NIC
100G - E810 NIC

Integrated Devices
Juniper MX Series Routers
(Junos OS 17R4, or later)

Juniper PTX Series Routers
(Junos EVO 22.3 and later versions)

Generic Mitigation
All BGP FlowSpec-enabled routers and L3 switches

US HEADQUARTERS info@corero.com
EMEA HEADQUARTERS info_uk@corero.com
corero.com