corero [NETWORK SECURITY]

SMARTWALL ONE™
DATASHEET _

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 under- stand 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.

AI-Assisted Threat Protection

Delivers predictive detection to block evolving and zero-day DDoS attacks before they impact service availability.

REMOTE MITIGATION

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 evolve, putting service availability and operational continuity at constant risk. While high-volume, headline-grabbing attacks raise awareness, they represent only part of the problem. In reality, most attacks are less than 1Gbps and often go undetected without the right visibility.

These smaller, short-burst attacks can still cause disruption, especially when they exploit different ports, protocols, and patterns. Their frequency and unpredictability require more than static defenses. Organizations need adaptive protection that evolves with the threat.

Our remote mitigation solution provides granular, real-time visibility and automatic mitigation. By inspecting traffic directly in the data path, it helps maintain service availability, avoid downtime, and respond to every threat, regardless of size or sophistication.

Software-Based 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.

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.
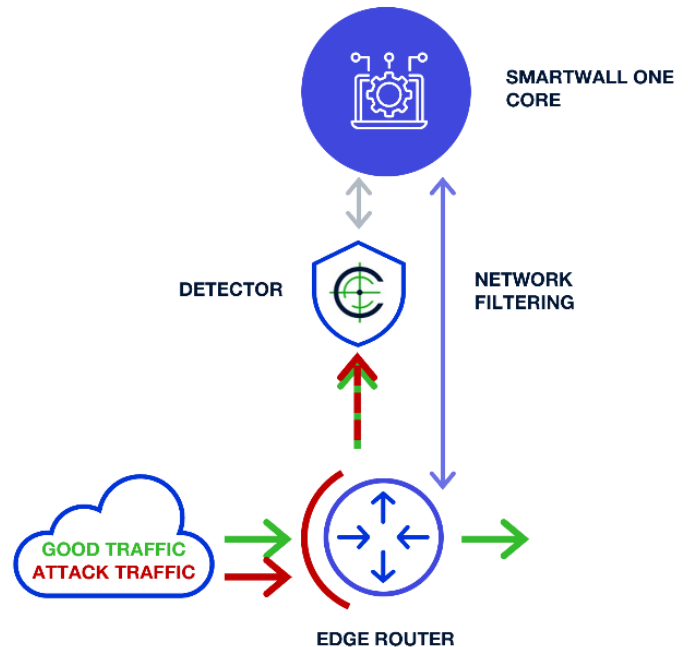
Mitigation

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.

SMARTWALL ONE CORE

DETECTOR

NETWORK FILTERING

GOOD TRAFFIC
ATTACK TRAFFIC

EDGE ROUTER

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.

Optimized Protection
Gather traffic information to help you fine-tune policies

Analyze Attacks
Drill down into blocked and allowed traffic seen an attack.

Enhanced Threat Intelligence
All events are stored and indexed in web-based applica- tion and available the analytics externally, to other security tools via syslog

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 Devices

All BGP FlowSpec-enabled routers and L3 switches including Cisco, Nokia, Huawei, and more

corero
[NETWORK SECURITY]