Corero SmartWall® TDC

DDoS Defense Cloud

SmartWall Threat Defense Cloud (TDC) solutions guard against large attacks that would saturate your Internet connections and overwhelm all legitimate traffic. Protection is available by directly connecting to a SmartWall powered service, from a supported provider, or as a Hybrid DDoS protection cloud service in combination with SmartWall TDS, or TDD, deployed on-premises.

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, cripple 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, with the ability to launch attacks at a scale which can only be effecively dealt with by the addition of cloud-scale protection, but the majority of modern DDoS attacks actually last less than 10 minutes in duration, are less than 10Gbps in size and can hit networks with multiple vectors. These more sophisticated attacks can be just as damaging and slip under the radar of legacy DDoS protection that can only detect traditional attacks and has limited visibility into the latest DDoS vectors.

The sophistication of DDoS also continues to evolve each year. These attacks present a more challenging detection and mitigation task due to their varying amplitude, 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® delivers intelligent DDoS mitigation that inspects traffic and automatically defends against DDoS attacks, typically in seconds.

Uptime Assurance
DDoS attacks are a security and availability issue. SmartWall ensures continuity for organizations that require SLA's for service uptime and availability and cannot afford latency or outages related to DDoS.

Granular Visibility
Industry-leading analytics drill down on attacks so you can better understand the types of attacks and deliver increased threat intelligence.

Comprehensive Defense
Protection from volumetric, state exhaustion, short duration, IoT Botnet, and pulsing attacks with cloud scale defenses that guard against the largest saturating attacks.

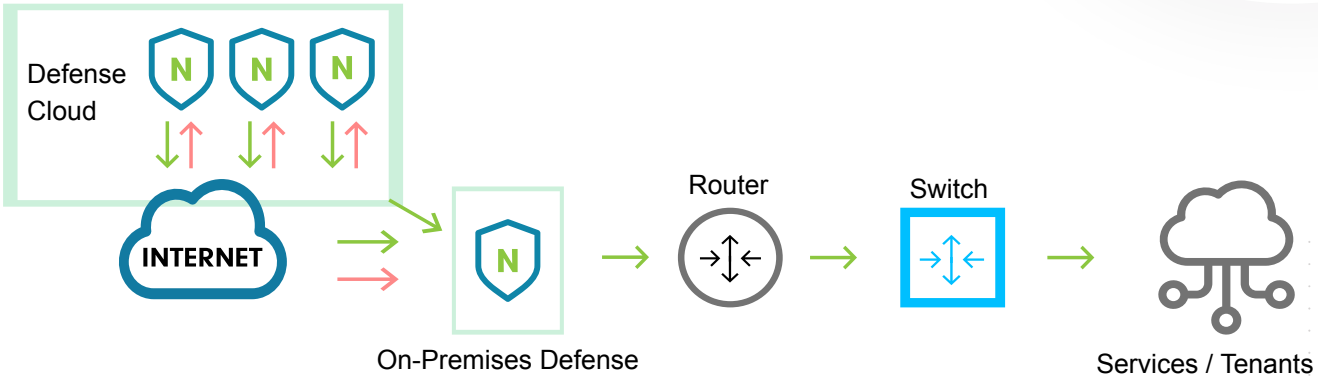
Advanced Protection
Many attacks that Corero mitigates are now multi-vector, where attackers combine one or more volumetric, or state exhaustion techniques sequentially, in an attempt to evade detection or mitigation.

corero

Flexible Hybrid or Provider-Based Protection

Organizations can benefit from SmartWall cloud protection either; connecting directly through a supported Service Provider, or using a hybrid SmartWall deployment with on-premises plus cloud protection. The SmartWall DDoS protection solution delivers 24/7 visibility and surgical mitigation of volumetric DDoS attacks at layers 3 thru 7, for both IPv4 and IPv6 traffic, without impacting the performance or connectivity of physical or virtualized networks.

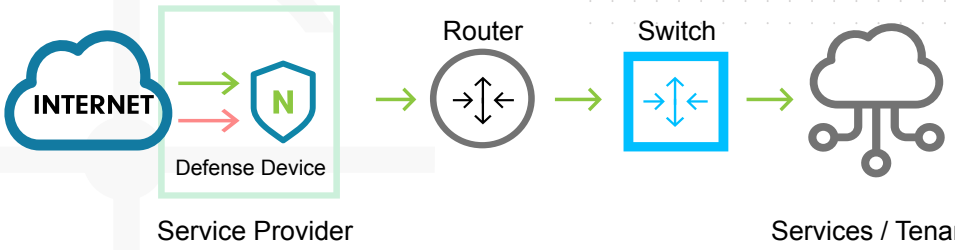
Hybrid Cloud DDoS Protection



SmartWall TDC	Threat Defense Cloud
Scrubbing Capacity	> 11 Tbps
Scrubbing Centers	14, Globally Distributed
Redirection Method	BGP, Signalled automatically from on-premises TDS/TDD

Direct-Connect Cloud DDoS Protection

SmartWall Direct-Connect Threat Defense Cloud protection is available to customers of Corero's Service Provider partners. Organizations using a Corero Partner as their Internet Service Provider can subscribe to DDoS protection powered by Corero's real-time automatic SmartWall solution. The direct-connect cloud delivers all the benefits of SmartWall protection, without the need to deploy or manage the system locally.

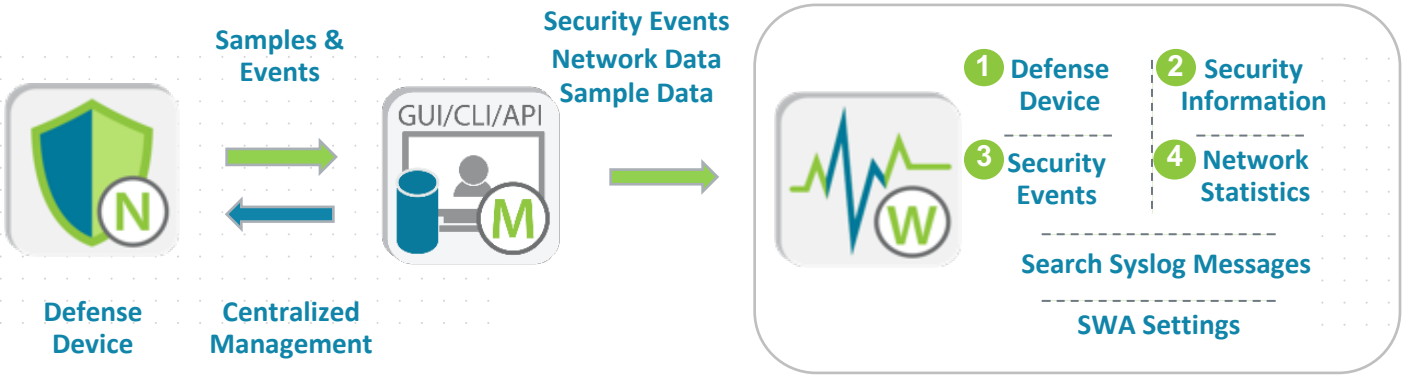


corero

Comprehensive Attack Visibility

Corero SmartWall delivers comprehensive visibility into DDoS attacks with easy-to-read dashboards and reporting that deliver actionable intelligence, from its on-premises SecureWatch Analytics and direct-connect Service Portal applications

1. **Monitor in Real-Time**
   Information is presented in real-time or historical charts and tables
2. **Analyze Attacks**
   Analyze the blocked and allowed traffic seen during attacks
3. **Optimize Protection**
   Detailed traffic information enables policies to be fine-tuned, if needed
4. **Enhance Threat Intelligence**
   All events are stored and indexed in a web-based application that enables DDoS attack detail to feed into a broader cybersecurity monitoring and protection activities.



TDC Security Coverage

Custom Protection

- 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)
- Smart-Rules – Patented high-performance heuristics-based engine that automatically detects & blocks volumetric DDoS attacks, including zero-day
- Botnet protection
- Blacklisting or Whitelisting of IP Addresses
- TCP/UDP port-based attacks
- Rate Limiting Policies
- Cloud Mitigation and RTBH signalling

Volumetric DDoS

- TCP Flood
- UDP Flood
- UDP Fragmentation
- SYN Flood
- ICMP Floods

Reflection DDoS

- NTP Monlist
- SSDP/UPnP
- SNMP Inbound
- Chargen
- DNS
- Connectionless LDAP (CLDAP)
- Memcached
- Portmapper
- Netbios
- RIP

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
- Use of reserved IP addresses

corero

Key Benefits

Comprehensive Visibility
SmartWall leverages big data analytics to deliver 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 Sizes
SmartWall fills the perception gap, by not only blocking the very large volumetric attacks commonly associated with DDoS, but also detecting and surgically blocking the more common and much smaller attacks, many of which are too small or short in duration to be detected 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 ties together attack events, significantly reducing human intervention and false positives for reduced operational 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.

Cloud/On-Premise Hybrid DDoS Protection Scalability
Cloud-scale defense against the largest attacks, with the speed and accuracy of always-on, automatic, real-time, on-premises protection. Can complement or replace legacy cloud-only mitigation solutions.

Security Policy Enforcement
With proactive traffic inspection, our detection and real-time mitigation solutions enforce security policies and prevent volumetric layers 3-7 DDoS attacks for both IPv4 and IPv6 traffic.

www.corero.com

US Headquarters
293 Boston Post Road
West Suite 310
Marlborough, MA 01752
Tel: +1 978 212 1500
Email: info@corero.com

EMEA Headquarters
Regus House, Highbridge,
Oxford Road Uxbridge,
England UB8 1HR, UK Tel:
+44 (0) 1895 876579
Email: info_uk@corero.com

Scotland Office
53 Hanover Rd
Edinburgh EH2 2PJ, UK
Email: info_uk@corero.com

corero