DDoS attacks are a serious concern for both businesses and governments. They cause outages of online services, impacting customers, crippling operations and causing huge economic loss. Well publicized volumetric attacks that harness vulnerable IoT devices have recently raised awareness of the scale of the DDoS problem but the majority of modern DDoS attacks actually last less than 10 minutes in duration, are less than 5Gbps 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 have 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 under a second.

Uptime Assurance
DDoS attacks are a security and availability issue. SmartWall ensures continuity for organizations that require SLAs 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, Carpet Bomb, and pulsing attacks with available cloud hybrid protection, to 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.
Proactive DDoS Protection with Comprehensive Attack Visibility

ETD is part of the SmartWall® Threat Defense System which delivers DDoS protection best aligned to the needs of digital enterprises, service providers and hosting providers with real-time, automated traffic inspection and mitigation. Corero’s solution does this in seconds, compared to the minutes, or tens of minutes experienced with legacy solutions. Our purpose-built DDoS defense can be deployed centrally or distributed.

Proactive DDoS defense is a critical part of cybersecurity best practice and vital for organizations looking to protect against loss of service availability. DDoS attack methods are constantly evolving, as cyber criminals develop increasingly sophisticated ways to gain entry to networks and cause disruption. With attacks becoming increasingly frequent, many businesses are hit multiple times a day. Traditional Internet gateway security solutions, such as firewalls and Intrusion Prevention Systems are not enough. Similarly, cloud-based DDoS protection services alone cannot achieve successful mitigation of today’s frequent, short-duration attacks.

Business Growth and DDoS Defense
As a business grows, so do the requirements for DDoS protection. Corero supports you on the journey from not being aware that your network has been attacked, with no intelligence on service disruption or downtime, to having full visibility of attacks, with alerts and automatic edge-blocking. Our solutions are designed to support you through all stages in your DDoS defense journey and are built on an architecture that has the flexibility to grow with you, as the needs of your business evolve.
**SmartWall DDoS protection delivers**

» **Accurate detection**: Intelligent deep packet inspection that accurately identifies known and zero-day volumetric and state exhaustion attacks.

» **Threat Intel Expertise**: Protection is continually enhanced as our SOC team analyze real-world attacks across our diverse customer base.

» **Comprehensive visibility and analytics capabilities**, enriched using behavioral and machine analysis.

» **Multiple deployment options**: Designed to best suit your business needs and specific network environment.

» **Fast, effective, protection**: With always-on coverage at all ingress points to the network so attacks can be blocked without any downtime.

» **Flexibility**: Whether you require in-line with Internet connections, in-datapath, connected to edge routers with inbound traffic diverted via the SmartWall appliances, or out-ofband with edge or scrubbing mitigation.

» **Supports traditional scrubbing deployments**, with built-in flow-based detection and traffic redirection capabilities.

**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 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.

- **Hybrid DDoS Protection**

  Enhances cloud-only solutions with highly accurate, real-time, on-premis-es protection.
Centralized Management and Analytics
Corero SecureWatch Analytics delivers visibility into detected DDoS events with easy-to-read dashboards delivering actionable intelligence.

ETD Security Coverage
Detection Capabilities
- Advanced packet sample or sFlow detection, plus traditional NetFlow
- Attacks to Single/Multiple IPs and Subnets
- Smart-Rules – Patented high-performance heuristics-based engine that automatically detects volumetric DDoS attacks, including zero-day
- Flex-Rules - Programmable detection 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
- IP Address, Country and AS Number Block/Allow Lists
- TCP/UDP port-based
- Cloud Mitigation and BGP RTBH/FlowSpec signaling

Reflective Amplification DDoS
- NTP Monlist Response Amplification
- Connectionless LDAP (CLLDAP)
- SSDP/UPnP Responses
- SNMP Inbound Responses
- Chargen Responses
- DNS

Volumetric DDoS
- TCP Flood
- UDP Flood
- UDP Fragmentation
- SYN Flood
- ICMP Floods
- Carpet Bombing

Monitor in Real-Time
Information is presented in real-time or historical charts and tables

Analyze Attacks
Analyze the blocked and allowed traffic seen during attacks

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

Enhance Threat Intelligence
All events are stored and indexed in web-based application and available externally, via syslog
## Technical Specifications

<table>
<thead>
<tr>
<th>Management</th>
<th>Centralized Object-Oriented Management from a Separate Virtual (VMware/KVM) Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>1 x 10/100/1000 Virtual Ethernet</td>
</tr>
<tr>
<td>Web-Base GUI</td>
<td>HTTP(S) Access Through the Management Station</td>
</tr>
<tr>
<td>Command Line Interface</td>
<td>SSH Access Through the Management Station</td>
</tr>
<tr>
<td>Programmatic API</td>
<td>JSON-Based REST Through the Management Station</td>
</tr>
<tr>
<td>Remote Monitoring</td>
<td>SNMP v2/v3* Standard MIB GETs, SYSLOG</td>
</tr>
<tr>
<td>Security Dashboards</td>
<td>Link utilization (Gbps/PPS), Attack Targets, Attack Vectors, Alerts, Detailed Drill Downs, Top IP's/Ports/TTLs/Packet Sizes</td>
</tr>
<tr>
<td>Reporting &amp; 3rd Party Integration</td>
<td>SYSLOG for Traffic and Security Events with REST API for SIEM Integration. Corero Analysis Application for Splunk Integration</td>
</tr>
<tr>
<td>User Authentication</td>
<td>Role-Based Access Control (LDAP/Active Directory and RADIUS)</td>
</tr>
</tbody>
</table>

### Performance

**Maximum Throughput per Detector** (Packet/sFlow samples or NetFlow records)

- 0.5 Million/sec

**Attack Detection Time**

- Sub-Second (typical)

### Physical Environment

**Hypervisors**

- KVM running on Redhat Enterprise 7+, CentOS 7+ or Ubuntu 16.04+
- VMware ESXi 6.5+

**Minimum Requirements**

- 44GB Memory, 210GB Disk

### NTD Virtual Edition

**Network Interfaces**

- 1G - Virtio
- 10G - XL710 NIC
- 100G - E810 NIC

**Management Port**

- 1 x 10/100/1000 Virtual Ethernet