DATASHEET

CORERO SMARTWALL®

THE DDoS PROTECTION SPECIALISTS

Distributed Denial of Service (DDoS) attacks are typically viewed as just the very large attacks that grab the headlines, after taking down high-profile targets with immense volumes of junk traffic. These attacks are in fact the exception, with only a handful occurring globally in any single year. The rarity of these largest attacks can lead to a sense that DDoS is not an issue for most organizations.

However, when viewed through the lens of real-time DDoS protection, the picture is very different – with tens of thousands of attacks occurring globally, every day. The vast majority of these attacks are, in fact, small (less than ten gigabits per second) and short (less than ten minutes in duration). Only a percent, or two, are classed as large.

Without a dedicated DDoS solution in place these daily attacks result in slow applications and failed services, impacting business continuity. DDoS attacks often get mistakenly attributed to some other IT issue, tying up valuable resources to investigate, when in fact, they are wholly preventable.

Addressing the DDoS threat isn't a one-size-its-all approach. Corero specializes in delivering flexible solutions that achieve business and revenue goals. We do this by delivering comprehensive visibility into DDoS attacks, with flexible, multi-layer protection options that meet your needs.

DDoS attacks hurt business – damaging brands, frustrating customers and impacting revenue

SmartWall is the DDoS Protection solution, whatever your size or network architecture

Flexible
From simple DDoS visibility to complete protection or delivery as a value-add service, our services are designed to meet your needs

Scalable
Whatever your network topology; appliance-based or software-only, we deliver the DDoS solution you need today, to scale with ease and evolve with your future needs

Visibility
Quickly understand unexplained increases in traffic levels - with dashboards, alerting and reporting visibility into whether DDoS is the root cause

Real-Time
With the ability to detect and block DDoS attacks in under a second, our solutions prevent application and service downtime to maximize business continuity

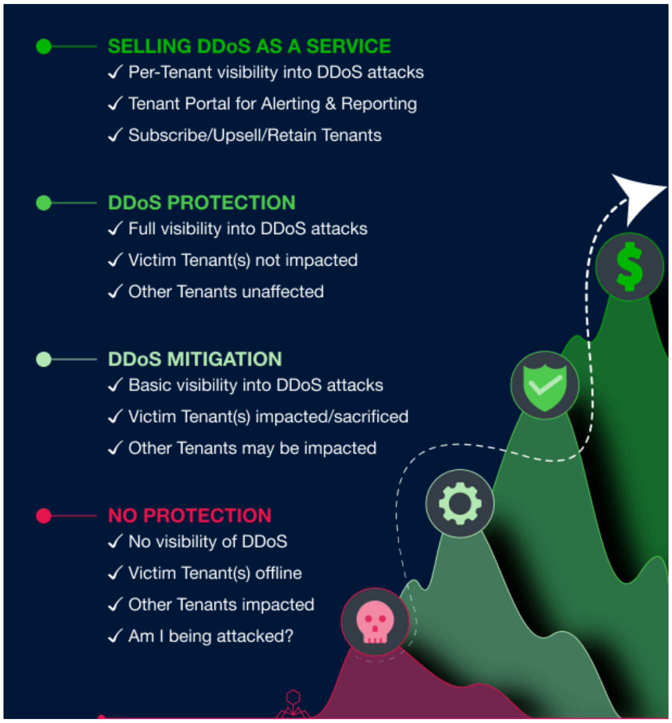
Automatic
With protection that's typically over 95% automatic and dynamic enough to prevent zero-day attacks our solutions ensure that IT and Security staff can remain focused on other critical tasks

From basic mitigation, that maximises your infrastructure investment, to advanced protection that keeps applications and services running at peak performance, Corero's SmartWall has the solution. We specialize in providing best-in-class DDoS protection, so you get the most innovative, precise and seamless solution without wasting time, money, or resources.

Real-Time DDoS Protection

Corero SmartWall leads the industry with real-time automatic protection that keeps DDoS attacks at bay, without any of the downtime associated with other solutions.

SmartWall uses a patented, innovative, and automated, multi-stage detection and mitigation pipeline to ensure the highest possible efficacy. Protection is achieved while maintaining line-rate performance, to ensure legitimate traffic is not impacted by damaging false-positives, or a significant increase in latency.



SELLING DDoS AS A SERVICE
- ✓ Per-Tenant visibility into DDoS attacks
- ✓ Tenant Portal for Alerting & Reporting
- ✓ Subscribe/Upsell/Retain Tenants

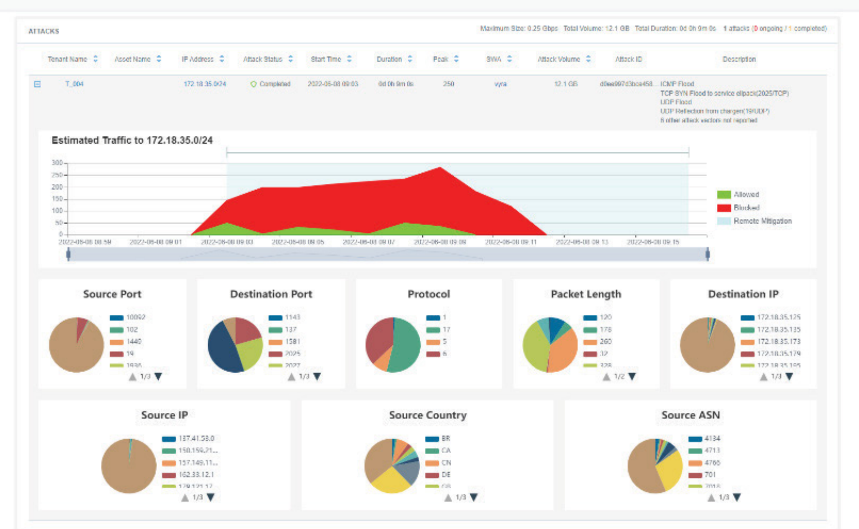
DDoS PROTECTION
- ✓ Full visibility into DDoS attacks
- ✓ Victim Tenant(s) not impacted
- ✓ Other Tenants unaffected

DDoS MITIGATION
- ✓ Basic visibility into DDoS attacks
- ✓ Victim Tenant(s) impacted/sacrificed
- ✓ Other Tenants may be impacted

NO PROTECTION
- ✓ No visibility of DDoS
- ✓ Victim Tenant(s) offline
- ✓ Other Tenants impacted
- ✓ Am I being attacked?

The Service Protection Maturity Journey

Unlike other DDoS protection solutions, which rely on header-based 5-tuple flow information, SmartWall's Deep Packet Inspection covers every bit of the packet header, plus the first 128-bytes of the payload, to deliver the most advanced DDoS attack detection, with surgical mitigation.



ATTACKS

Maximum Size: 0.25 Gbps Total Volume: 12.1 GB Total Duration: 0d 0h 9m 0s 1 attacks (0 ongoing / 1 completed)

Tenant Name	Asset Name	IP Address	Attack Status	Start Time	Duration	Peak	SWA	Attack Volume	Attack ID	Description
T_004		172.18.35.0/24	Completed	2022-06-08 09:03	0d 0h 9m 0s	250	vyra	12.1 GB	d0ee997d3bce458...	ICMP Flood TCP SYN Flood to service dlpack(2025/TCP) UDP Flood UDP Reflection from chargen(19/UDP) 8 other attack vectors not reported

Comprehensive dashboards deliver insights into blocked DDoS attacks

The first step in dealing with the DDoS threat is visibility. A comprehensive understanding of whether an increase in network traffic is legitimate, or a result of DDoS activity, is essential, whether you need basic mitigation or advanced protection. SmartWall's deep packet inspection ensures that headers and payloads are considered when determining if any received traffic is the result of a DDoS attack.

Architecture that meets your needs

The way DDoS protection is deployed depends on what is being protected, the unique topology of your IT environment as well as a clear understanding of the DDoS threat landscape relates to your business.

Key considerations:

» Are you looking to protect your infrastructure?

» Do you need to keep customer applications and services running?

» Is creating a new revenue generating, value-add service top of your list?

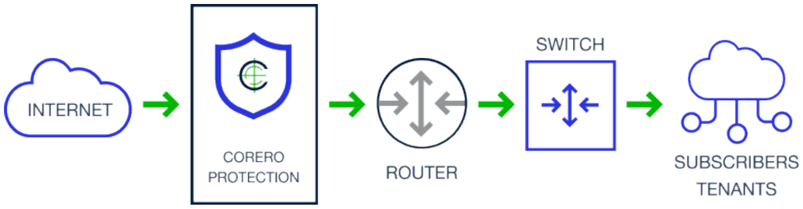
The type of organization, number of locations, geographic distribution, network topology and aggregate Internet bandwidth, all influence the techniques required to provide the most effective DDoS protection.

Flexible Deployment Options

SmartWall is built on three key pillars of protection:

1. Distributed intelligence built into physical or virtual appliances deployed in the network's Internet data path
2. Central intelligence that powers the line-rate filtering capabilities of the latest generation of network infrastructure devices
3. Cloud-based mitigation for link saturation protection

In many cases, always-on appliance protection at the network edge is the optimum combination of simplest to deploy, most effective and accurate.



Appliances

Always-on physical or software appliances that inspect every packet to surgically block DDoS

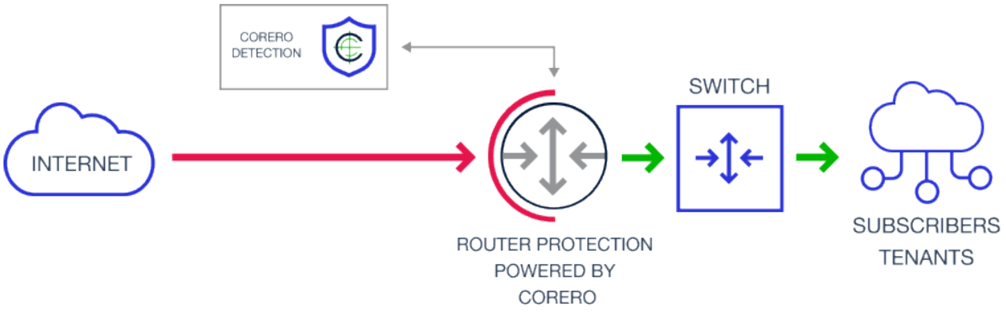
Infrastructure

Router and FlowSpec integration enable large-scale filtering of DDoS attacks without the need for appliances at the edge

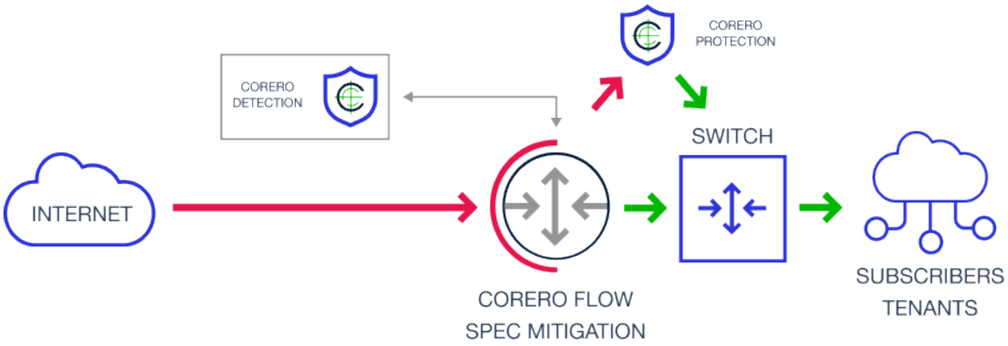
Cloud

Protect Internet connections from saturation by blocking larger attacks in the cloud

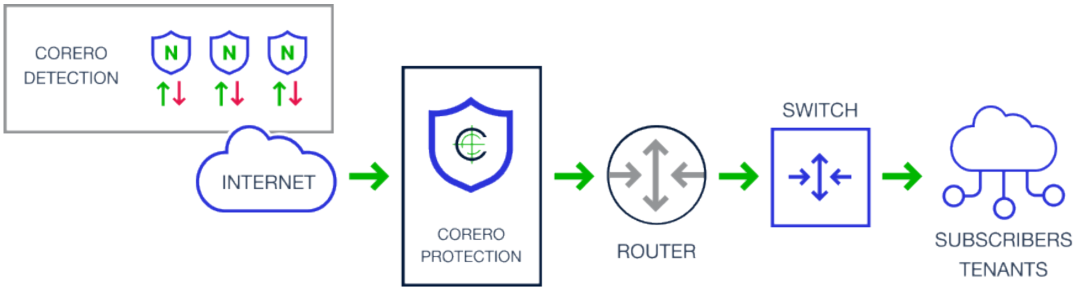
For Service and Hosting Provider business models, where Internet capacity is measured in hundreds of gigabits, edge protection remains the most effective approach. However, deploying appliances at every connection point can become unwieldy for larger and more distributed networks, where aggregate bandwidth is typically measured in terabits or tens of terabits. In these cases, a centralized DDoS detection approach using existing infrastructure-based filtering to block incoming attacks at the edge provides an effective alternative, trading some fine-grained efficacy for maximum scale and ease of deployment.



For deployments where router-integrated filtering is not available, BGP FlowSpec filtering can be used and combined with redirecting specific traffic to SmartWall appliances for fine-grained protection.



Where the total Internet bandwidth is measured in tens of gigabits, or less, typical DDoS attack sizes are more likely to overwhelm the available Internet capacity. In these cases, upstream blackholing of victim traffic may be used for basic mitigation, to prevent link saturation. For more advanced protection, the on-premises solution can be augmented with cloud-based protection, for the occasions when an attack is significantly larger than the available capacity.



Protect and Grow your Business

Corero solutions are designed to fit your specific requirements, irrespective of where your business is in terms of dealing with the threat from DDoS attacks. Whether you're considering a DDoS solution for the first time, and require basic mitigation with visibility of attacks, or looking for more advanced protection to ensure zero DDoS downtime and in-depth visibility into blocked attacks, we provide coordinated protection.

For businesses looking to sell value-add services, we also deliver options that include a bespoke web portal, giving per-tenant alerts, reporting and real-time visibility into blocked attacks.

Corero DDoS Solutions are specifically designed to meet the needs of:

» Service Providers » Hosting Providers » SaaS Enterprises

DDoS attacks typically target services hosted on IP based networks. Service providers, Hosting providers, and SaaS enterprises, whose businesses require guaranteed internet service uptime, need robust DDoS cybersecurity solutions to protect their digital environments from the threat of these attacks.

At Corero, our sole focus is providing comprehensive, scalable, DDoS solutions to support you in achieving business and revenue goals.
Our customers get direct access to our specialist DDoS Security Operations Centre (SOC) analysts, 24/7 and 365 days of the year. You can rest assured that Corero has your DDoS concerns covered, so you can focus on what you do best.

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 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.

About Corero Network Security

Corero Network Security are Distributed Denial of Service (DDoS) cyber protection specialists. We provide automatic attack detection and mitigation, coupled with network visibility, analytics and reporting tools. Corero's technology provides scalable protection capabilities against both external DDoS attackers and internal DDoS threats, in even the most complex edge and subscriber environments, ensuring internet service availability and uptime. Corero's key operational centers are in Marlborough, Massachusetts, USA and Edinburgh, UK, with the Company's headquarters in London, UK. The Company is listed on the London Stock Exchange's AIM market under the ticker CNS.

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