corero [THE DDoS PROTECTION SPECIALISTS]

SMARTWALL® ONE
OVERVIEW _

Key capabilities and differentiators

Flexibility

All SmartWall ONE modules are available as hardware and software appliances.

Flexible deployment models adapt to your network, risk tolerance, and business requirements.

Edge router integrations turn your routers into DDoS attack sensors without changing your network.

Intelligent, automated protection

Defend your business against the latest DDoS threats with protections based on our latest threat research.

Header and payload inspection at line speeds give us a more complete analysis of potential threats to your network without latency.

Attacks are detected and blocked within seconds, or less.

DDoS protection that pays you back

Leverage your DDoS protection investment to offer DDoS protection-as-a-service to your subscribers to:

- Create additional revenue streams.
- Improve customer experience.
- Differentiate from your competitors.

What is Corero SmartWall ONE?

Every year it's the same. IT and security budgets are flat or reduced; headcount is static while there are more vendors to manage; and the mantra to do more with less is, well… you know the drill. And yet, every year, vendors roll in with their latest-and-greatest widget that they expect these teams to instantly adopt as if none of these challenges exist.

We like to think that we have a good sense of the challenges our customers face. Our goal is to meet our customers where they are on their DDoS protection journey with everything they need and nothing they don't. With more than a decade of dedicating ourselves to on-prem DDoS protection, we continue to evolve our industry-leading SmartWall technology to achieve this goal.

SmartWall ONE is a modular, platform-based, on-premises DDoS protection solution. It has been designed for flexible, adaptable deployment options that meet today's business and network needs and grows with you based on your needs.

The Realities of DDoS

There's no denying that massive attacks can have an enormous impact. But it's the constant, daily drip of smaller attacks that causes the most harm over time. Like waves crashing on the shore, this steady barrage wears down defenses gradually.

While headline-grabbing, tsunami-scale attacks are rare, most real-world DDoS attacks are quick strikes under 10 minutes and under 10 Gbps. They evade legacy systems lacking intelligence to detect multi-vector assaults. By the time humans respond, it's too late. Only an intelligent, automated solution can act swiftly enough to stop today's attacks from inflicting damage.

The DDoS Protection Journey

Every organization is at a different stage in their DDoS protection journey. Their needs evolve based on business priorities, technical challenges, budgets, and more. We've seen this progression first-hand with our customers over the years. Some start with no protection. Others achieve complete protection. And some offer DDoS protection as a service.

That's why we built a flexible solution that adapts to any phase of the journey. Whether you're just getting started or want the latest managed services, our technology can meet you where you are and grow with your needs.

No protection

Let's face it. There are no regulations, no laws, no compliance mandates that state that anyone must have DDoS protection. So, it's understandable that organizations prioritize compliance requirements ahead of DDoS protection… that is, until they are attacked. Unfortunately, this is when we most often hear from prospective customers.

Detection

It's common for an organization to start with some form of DDoS detection. Doing so provides visibility as to where their trouble spots may be so that they can better prioritize how and where to roll out some form of defense. And if we're being candid with ourselves, it can be cheaper to have some form of detection and let the humans respond.

Mitigation

"Mitigation" is the most common form of DDoS defense used in the industry. Mitigation, by definition, is a lessening of the impact of an attack versus completely block it. Of course, there are many shades of gray here with the differences coming down to the time it takes to *detect* the attack, the time it takes to *block* the attack, and the *method* used to block it.

Our research shows that the majority of attacks have a duration of less than 10 minutes and are under 10 Gbps in size. In other words, time is of the essence. But also consider that responding immediately by black holing traffic is still quite impactful. That's why fast detection, fast response, and the most appropriate response is so important.

Protection

Protection is about completely defeating a DDoS attack with the fastest detection and response possible – without impacting legitimate traffic. Many organizations are fine with mitigation and may not move to a protection-based model. The decision has to do with risk tolerance and business priorities. For those who have an extremely low risk tolerance and/or want to offer DDoS protection-as-a-service, then it's pretty clear that DDoS protection is the way to go.

DDoS Protection-as-a-Service

How many of your security investments can actually pay you back? Offering DDoS protection-as-a-service (DDPaaS) has given many of our service and hosting providers the ability to deliver a revenue-generating, value-add service to their subscribers, improve the customer experience, and set themselves apart from their competitors. We also help our customers with brandable marketing and sales content along with guidance in establishing pricing and service models.

Please see our DDoS Protection-as-a-Service solution brief for more details.

SmartWall ONE Modules

All SmartWall ONE modules can be deployed on physical appliances or as virtual instances. This flexibility lets you choose the deployment model that best suits your infrastructure needs.

Once implemented, all modules can be seamlessly upgraded via license updates. No need to rip and replace hardware or software to gain new capabilities. In-place upgrades save you time, effort, and potential disruption to operations as your protection needs scale.

SmartWall ONE Core Detect

SmartWall ONE Core Detect is the foundation of all architectures. It includes:

- **SmartWall ONE Management**
  This is essentially the brain of the platform. It is the interface through which all associated components are configured and which pushes policies to our sensors, known as NTDs, and orchestrates which component(s) of our system respond to an attack.
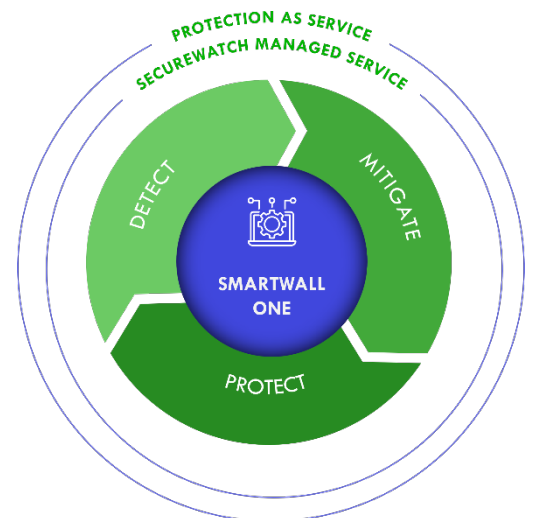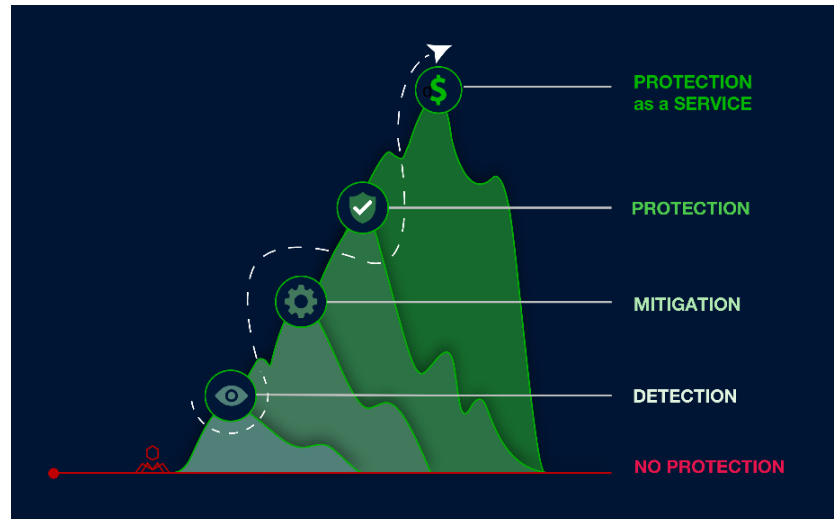
- **SmartWall ONE Analytics**
  This is the interface for all reporting and real-time dashboards. The analytics engine both pulls information from and pushes information to the management engine.

- **SmartWall ONE Network Threat Defense (NTD)**
  SmartWall ONE NTDs are hardware or software appliances that can act as "detectors" or "protectors." Again, as the names imply, a detector detects DDoS activity, but takes no action. A protector both detects DDoS activity and will filter traffic as directed by the SmartWall ONE core.

  When SmartWall ONE Core Detect is deployed, at least one virtual detector NTD is required. Detector NTDs may be deployed as physical appliances, though due to our throughput capabilities, physical appliances are often overkill for the task at hand.

SmartWall ONE Core Detect

SmartWall ONE Protection Appliances are available as hardware or virtual protector NTDs. Both are capable of high throughput with virtually no latency, so selection of hardware of virtual protection applications will most likely be based upon customer requirements unrelated to throughput. (Please see the SmartWall ONE Protection Appliances datasheet for technical specifications.)

From an architectural perspective, these appliances are best suited for what are known as inline, data path, and/or scrubbing deployments, which are described below.

Inline deployments

In this straightforward architecture, a protector NTD is physically situated between your internet link and edge router. All traffic gets filtered through the NTD before reaching the router.

By analyzing traffic first, the NTD can detect and stop DDoS attacks in milliseconds. The inline position also grants full visibility into all inbound and outbound flows. With the NTD in the direct path, mitigation occurs at line rate.
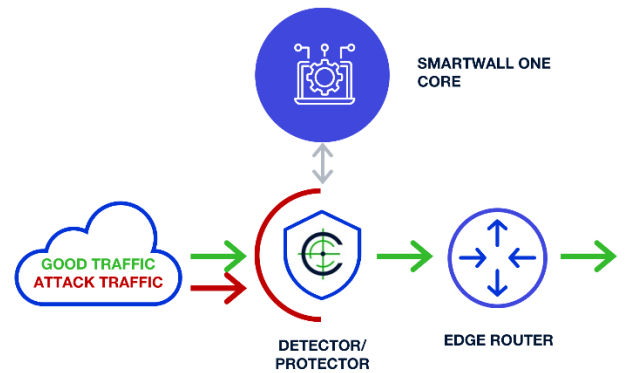

Data path deployments

Also known as "virtual inline," this architecture is very similar to that of a pure inline design. The key difference: Your internet link and edge router remain directly connected. But the router forwards all traffic to the protector NTD for analysis before sending it into your network.

Like an inline deployment, the NTD filters out bad traffic and returns only clean packets to the edge router. This happens instantly over a virtual link between the devices.

The data path approach retains the core benefits of an inline design:

- Full traffic visibility for granular threat detection
- Lightning-fast protection at line rate to stop DDoS in its tracks
- Seamless integration without changing existing network topology

This makes data path an ideal choice for adding robust DDoS protection with minimal disruption. The virtual inline configuration grants the same rapid response and other advantages as a pure inline deployment.
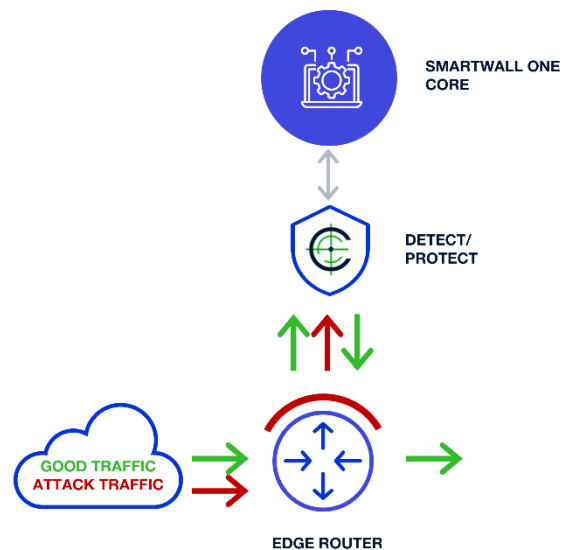
Scrubbing deployments

Also known as "detect and redirect," here's how it works:

A detector NTD analyzes samples of inbound traffic. When it detects an attack, SmartWall ONE instructs the router to redirect traffic to a protector NTD for inspection and scrubbing, filtering out bad packets and allowing only clean traffic to return to the router.

Key benefits of this design:

- Early attack detection from the detector NTD observing traffic flows. This enables rapid response.

- Scalable scrubbing from the protector NTD to cleanse high volumes of traffic during large assaults.

- No need to disrupt the existing network topology. The detector NTD and redirect integration provide seamless visibility and protection.
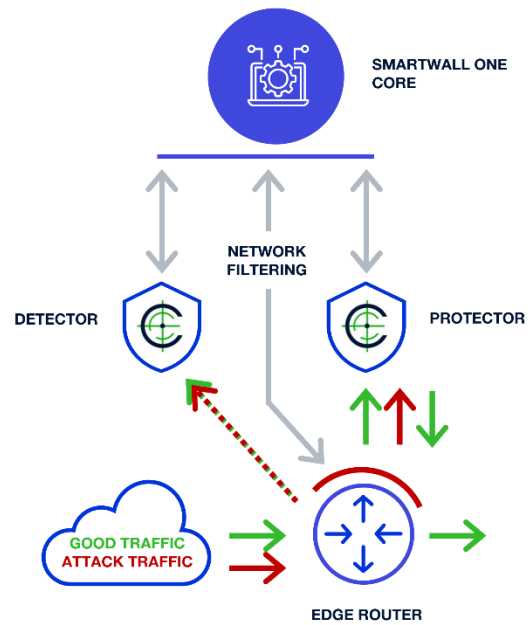
SmartWall ONE Edge Mitigation

SmartWall ONE seamlessly integrates with a wide variety of edge routers to deliver targeted DDoS protection.
This native integration ingests router traffic data to detect attacks. It also commands your routers to surgically block malicious packets while preserving good traffic.

The precision of our mitigation varies based on each router's capabilities. For example, our integration with Juniper MX and PTX routers enables exceptionally granular traffic filtering.

No matter your edge infrastructure, SmartWall ONE integrates natively for strong DDoS defenses with minimal disruption.

Please see our SmartWall ONE Edge Mitigation datasheet for technical details.
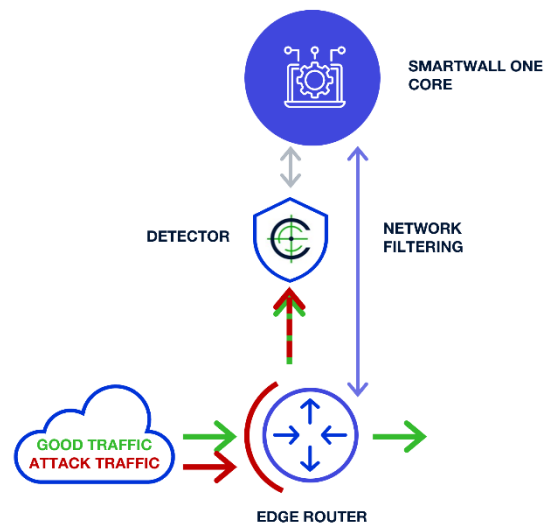
A note on deployment flexibility

These architectures offer tremendous flexibility. Mix and match options to suit your needs. NTDs can intake data from multiple routers in 1:many relationships. Deploy scrubbing centrally or distributed across multiple sites. Tailor configurations to your network, budget, and business needs. SmartWall ONE adapts seamlessly to your environment through customizable deployments.

SecureWatch Managed Services

We know many organizations are short on time, resources, and staff. Our SecureWatch Managed Services can relieve the burden. This suite of optional services lets you outsource SmartWall ONE administration, monitoring, and more. Lean on our experts to manage your defenses so you can focus on your core business.

Please see our SecureWatch Managed Services solution brief for more information.

corero
| THE DDoS PROTECTION SPECIALISTS |