corero [ THE DDoS PROTECTION SPECIALISTS ]

CASE STUDY _

# Service Provider Selects Corero Network Security for Cutting-Edge Approach to DDoS Protection

This US-based, regional service provider offers fiber, telephone, and data center services to both businesses and government agencies. The internet service provider (ISP) primarily focuses on the Washington, D.C. metropolitan area, with capabilities to service other regions, as well.

## The Challenge

ISPs face a rising tide of DDoS attacks, which pose a security and availability issue, and this ISP is no exception. Although they have experienced DDoS attacks in previous years, they began to rethink their approach to addressing these attacks after suffering a "volumetric" DDoS attack that proved particularly challenging to deal with manually. This attack occurred in the evening and directly impacted customers who work 24 hours a day. Eager to reduce the manpower load from their current manual process and improve uptime and security for customers, the service provider decided to initiate a search for a DDoS protection solution.

Segmenting their evaluation into two categories – cloud service providers and on-premises providers – they soon realized that an inline, on-premises solution would better meet their needs. The customer portals within the cloud-based solutions they evaluated seemed to be enterprise-focused, not focused on service providers and their customers. Their approach to protecting users from DDoS attacks was also more reactive in nature, redirecting traffic to the cloud while they investigated what was happening, which would also be more costly for the ISP.

> The average DDoS attack is short, so real-time detection and mitigation are essential requirements for comprehensive protection.

## Why they chose Corero

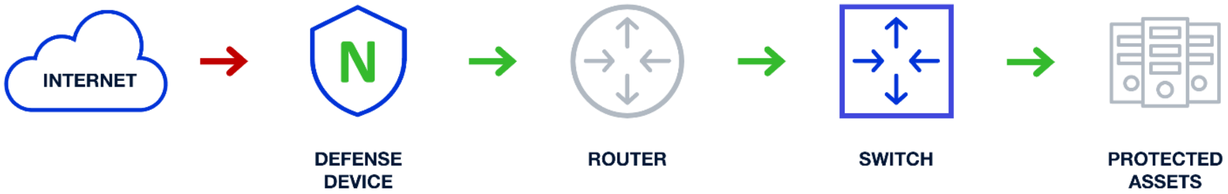
The service provider conducted an extensive search of hardware-based solutions before narrowing the field to Corero and one other provider. “Corero’s sales team was far superior to the other vendor’s team and very responsive,” said the customer’s CEO. “After a very thorough analysis that included a strong demo, product material that spoke to me and the challenges unique to ISPs, and one of the better RFPs we’ve ever done, we decided Corero was the solution we would deploy to our customers.”.

> “I remember thinking this sounds too good to be true, but seeing is believing.”

The CEO went on to explain, “In comparison to the main competing vendor, the methodology that Corero adopts in its product is more cutting edge and the functionality works in a more automated fashion.”

Corero takes the approach that protection is about completely defeating a DDoS attack with the fastest detection and response possible – without impacting legitimate traffic. The solution automatically detects and eliminates DDoS traffic before it reaches the network which allows this ISP to reduce the manual workload of their current processes and scale their service to provide revenue-generating, value-add DDoS protection to customers.

### Inline deployments



Corero offers flexible deployment models. The ISP selected an inline deployment architecture in which a Corero appliance is physically situated between the internet link and edge router. All traffic goes through the appliance before reaching the router.

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

## The Results

The onboarding and implementation of the Corero SmartWall ONE™ on-premises DDoS protection solution went smoothly. “There were no outages or customer-affecting issues when we deployed the solution. It was a very positive experience and Corero should be proud of the successful implementation,” said the customer.

ISPs are able to protect their customers without “blackholing” or disrupting legitimate traffic.

The Corero SmartWall ONE platform offers high throughput with virtually no latency to meet the ISP’s service requirements to customers. With always-on protection, the service provider is able to stop DDoS attacks within seconds or less and keep customers apprised of the status live via the service portal. Their customers don’t have to worry about DDoS attacks and the IPS’s own engineers can focus on more strategic projects.

## Corero SmartWall ONE Highlights

- Surgically and automatically removes DDoS attack traffic before it reaches critical systems, eliminating downtime and ensuring optimal performance and maximum availability.
- Mitigates the impact of a wide range of DDoS attacks, from simple volumetric floods to sophisticated state exhaustion attacks, at Layers 3 through 7.
- Delivers line-rate, in-line DDoS attack protection from 1 Gbps to 100 Gbps per rack unit in a solution that scales to terabits per second of protected throughput.
- Provides comprehensive forensic-level analysis before, during, and after attacks.
- Ensures that legitimate traffic is not impacted by false positives.
- Inspects every inbound packet header and payload data, surgically removing DDoS packets without disrupting the delivery of legitimate network traffic.
- Uses Smart-Rules to leverage heuristic and closed-loop policy so that rules can be reconfigured and deployed on the fly, thereby responding rapidly to evolving, sophisticated DDoS attacks.
- Detects and mitigates attack traffic in less than a second instead of the minutes or tens of minutes required by traditional DDoS protection solutions.