corero [THE DDoS PROTECTION SPECIALISTS]

CASE STUDY _

Regional ISP Finds Corero Network Security is the Exact Fit for DDoS Protection

This US-based, regional internet service provider (ISP) offers wireless internet services in several states across the southwest. The ISP prides itself on delivering fast, reliable broadband service with fiber redundancy to businesses, government agencies, and residents.

The Challenge

The DDoS threat landscape continues to have ISPs concerned about outages and latency of their online services. This ISP was determined to mitigate the impact of attacks and preserve their reputation for fast and reliable internet service.

From attacks aimed at sabotaging professional gamers to digital mercenaries and hacktivists targeting businesses and city governments, the ISP often finds itself in the crosshairs of DDoS attacks and needing to protect its customers. While they lacked a specific DDoS protection solution, they had processes in place to isolate attacks.

"Being an ISP, we're constantly either the subject of an attack or we're transporting an attack in some way, and they can vary in scope, size, and intent," the service provider's CIO explained. "We used blackholing to basically route the traffic to a place where it doesn't go any further, try to identify the source, and then work with upstream providers to handle the problem."

Wanting a better way to protect their customers, they began a search for a DDoS protection solution that had to meet the following criteria.

- On-premises appliance
- Centralized management
- Ease of deployment
- Cost effective

The average DDoS attack lasts just a few minutes, so real-time detection and mitigation are essential requirements for comprehensive protection.

Why they chose Corero

After conducting their due diligence and doing proof of concepts with various SaaS-based and on-premises solutions, they selected the Corero SmartWall ONE™ platform. While the CIO joined the company after the decision to go with Corero had been made, he was very supportive of the choice. "I came from the value-added reseller world, and I know many organizations that use Corero," said the CIO. "I've been involved in use cases and networks that use the product – not just service providers but the gaming industry, defense-type applications, and others – so I knew Corero was a good product and a good fit for what we were trying to do."

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.

According to the customer, "Cloud solutions add latency to our network, and we don't really want that latency for our customers, so we had to have an on-prem appliance."

The Corero SmartWall ONE also checked the boxes in terms of ease of use and management. The solution delivers comprehensive visibility into DDoS attacks with easy-to-read dashboards that deliver actionable intelligence.

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 protect their customers without "blackholing" or disrupting legitimate traffic.

Finally, Corero SmartWall ONE delivers the capabilities required without forcing the customer to pay for extraneous features, making it extremely cost effective. "It's hard with certain products to eliminate feature sets that you don't need – so you have to buy those features, even though you don't need them," said the customer. "Corero is a point product that does exactly what we need it to do."

> "Corero SmartWall ONE does exactly what we needed it to do."
>
> – CIO at a Tier-2 ISP

The Results

> "The Corero solution is very easy to use, very easy to deploy, and you don't have to be a security expert to use it."
>
> – CIO at a Tier-2 ISP

The onboarding and implementation of the Corero SmartWall ONETM on-premises DDoS protection solution went well. "You just put the appliances inline and use them, so the implementation is really smooth and easy," said the customer.

From a protection standpoint, Corero SmartWall ONE has delivered as promised, helping the customer on a daily basis identify the source and destination of the attack and protect against it. "Corero's product is really good at getting in between these crafted attacks and helping us, number one, identify who the source of the attack is if we can, and then number two, stop the attack," said the customer.

The ISP has found that in the face of rapidly changing threats, Corero keeps pace. "Attacks are constantly evolving and the only thing you can ask for from a company like Corero is, 'Are they staying up with the times?' and they seem to be," said the customer. "They have anomaly detectors which are non-signature based and they have signatures that we update as they come out. So, I think Corero does the best they can for what we have to work with in this industry."

Service and support have also lived up to expectations. "Corero has a good team," said the customer. "We haven't had any issues and I think they support us in every way we could ask."

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.