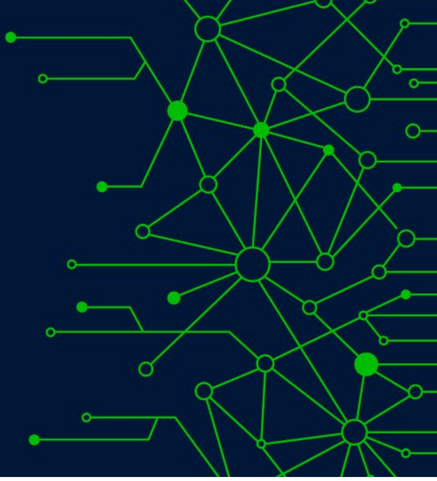
corero [THE DDoS PROTECTION SPECIALISTS]



CASE STUDY _

Regional Internet Service Provider Selects Corero Network Security for DDoS Protection

This regional internet service provider (ISP) offers residential customers and businesses in the southeastern U.S. a range of services including high-speed fiber internet, streaming video, hosted VoIP, managed and cloud services, network security, data protection, and disaster recovery.

The Challenge

When the ISP's Senior Director of Network Planning and Operations joined the company, he noticed unusual fluctuations in bandwidth consumption as he was reviewing network analytics. "I remember watching the utilization go up on a Tuesday and thinking, it's not the SuperBowl or March Madness, and I'm not aware of any new TV shows or movies that could cause this," he said.

With no obvious indicators that could be causing these spikes, he immediately had three concerns: slower internet speeds to customers, increasing cost of bandwidth utilization to the company, and cybersecurity threats that could impact everyone. He knew they needed to seek out a DDoS protection solution quickly.

"As a company, we want to prevent and mitigate problems before they impact our customers, not deal with collateral damage after the fact," he said. "I was having real heartburn over the availability of hardware appliances due to chip shortages, as well as pricing and ease of implementation because we aren't blessed with unlimited resources like the Tier-1 providers."

Why they chose Corero

Working with his team, they evaluated solutions from three different vendors, including Corero, which he personally had experience with for DDoS mitigation at a prior company. Given the urgency, they requested a loaner demo device from each vendor so they could become familiar with the different solutions and, in the process, start to get some immediate visibility into the cause of the bandwidth fluctuations and how to address them. One of the vendors couldn't offer a loaner so was immediately limited from contention.

The key criteria the ISP used to evaluate the two remaining vendors included: ease of implementation with no impact on performance, ease of use, and relationship with the vendor.

> “ The success of the demo ultimately compelled us to choose Corero and order a second appliance.”
>
> – Senior Director of Network Planning and Operations, Regional ISP

Implementation

The ISP was naturally concerned about any impact on performance to their clients as a result of introducing an appliance in-line. They soon realized that with Corero there was no need to worry. “We were able to apply the Corero demo unit into normal business operations without it causing an issue to our subscriber base,” said the customer.

Ease of use

The demo experience with Corero showed how easy mitigation is. The Corero SmartWall ONE™ platform offers comprehensive visibility into DDoS attack activity, rapid detection of DDoS attacks of all sizes, and automated blocking of bad traffic while allowing good traffic to flow uninterrupted. According to the customer, “One of Corero’s strong suits is that essentially you set that box up one time with the support of their engineering team, and then it’s almost a ‘set and forget,’ meaning that it’s doing the mitigation practices on its own without a lot of handholding and through the dashboard we monitor everything that’s going on.”

Partnership

The customer also credits the quality of the sales support they received for their selection of Corero. “We shared our philosophy towards supporting our customer base with the team at Corero and it was through that conversation and partnership that it became really clear as to where to put the appliance and what would work best for us as a company,” said the customer.

> **“ The folks at Corero that we worked with were really stand up people. They rolled up their sleeves, they dove in to help us solve the problems we were seeing in our network, and they continue to support us today.”**
>
> **– Senior Director of Network Planning and Operations, Regional ISP**

The Benefits

Today, the customer has three Corero appliances deployed and is realizing the following benefits:

> **“ We’re getting exactly what we expected in regard to return on investment which we measure in two ways: mitigated attacks and reduced bandwidth costs.”**
>
> **– Senior Director of Network Planning and Operations, Regional ISP**

- **DDoS Protection –** With always-on DDoS protection, the ISP can see that DDoS attacks are being stopped before they reach the network, eliminating unexpected bandwidth fluctuations and protecting their subscribers’ online experience with no impact on their day-to-day services.

- **Cost Savings –** Based on the bandwidth saved or consumption not being used by eliminating bandwidth spikes, the ISP is also realizing cost savings. “We pay for bandwidth through a third party,” the customer explained. “Every time we would see a spike, we were paying for that additional bandwidth that wasn’t really being used by our subscribers.”

- **Support –** When the ISP needs support, the Corero support team is always available in a timely manner. “The real advantage to Corero’s customer service is that if I need some help, they always pick up the phone and help us navigate that issue,” the customer explained. “Recently, we had a DNS DDoS anomaly and they helped us well into the wee hours of the morning, so we can’t thank them enough.”

- **Future Revenue Stream –** The ISP currently offers DDoS protection at no additional fee. However, they are considering moving to a DDoS-protection-as-a-service model and working with Corero for guidance on establishing pricing and service models.

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.