corero

ISP, OPENCAPE, ENSURES UPTIME WITH CORERO'S

AUTOMATED DDoS PROTECTION __

>summary

TYPE OF SERVICE PROVIDER
Fiber optic network and Internet service provider

SCALE
>40Gbps of transit; 2 PoP locations with currently 2 x 10G transit circuits at each PoP

SOLUTION
Corero SmartWall® NTD280-40

DEPLOYMENT MODEL
Inline, at the network edge, with Zero Power Optical Bypass

COMMERCIAL MODEL
Customer Subscription

OpenCape

Headquartered in Barnstable, Massachusetts, OpenCape Corporation is a 501c3 non-profit Fiber Network and Internet Service Provider that owns and operates a state-of-the-art fiber optic network built to serve local governments, businesses, and residents of Southeastern Massachusetts, the Cape & Islands.

Its fiber network is on par with the most sophisticated and technically proficient fiber networks in the world, and the company sells a variety of Internet services to several hundred institutions, including libraries, government buildings, school systems, colleges, hospitals, public safety agencies, research institutions, businesses, and residences.

>the challenge

"Always on" service is essential to OpenCape, so DDoS attacks represent a significant threat to its business. The organization experiences DDoS attacks that varied greatly in size and frequency, creating occasional network congestion and latency. Prior to deployingCorero's SmartWall® in 2021, they noticed a significant increase in DDoS attacks that impacted schools and municipal agencies.

OpenCape could only manually blackhole the DDoS traffic, which not only consumed significant staff time and resources, but resulted in several minutes of downtime for OpenCape clients because that approach blocked legitimate traffic, along withthe DDoS traffic.

>the solution

OpenCape purchased Corero's SmartWall® Threat Defense System, deploying two appliances to protect their 10Gbps Internet connections inline at the network perimeter, one in Providence, RI and the other in Boston, MA where they are connected with multiple tier one providers. Both appliances have built-in zero-power bypass functionality that allows for them to be deployed safely and effectively inline, without data continuity risks in the event of system maintenance or a hardware failure. Wherever the network touches the Internet, Corero protects OpenCape and their customers by automatically blocking DDoS attacks at the peering edge to ensure only clean traffic enters their network. The real-time mitigation blocks over 98% of DDoS attacks automatically, ensuring high levels of network resilience and business continuity.

> *OpenCape considered other DDoS mitigation providers but, ultimately, chose Corero for several reasons. "First of all, Corero has a proven reputation of working successfully with Internet service providers. Second, we prefer Corero's inline model rather than a cloud-scrubbing solution because it provides greater protection from latency. Third, the Corero solution is automated, which ensures faster time to mitigation," said Steven Johnston, CEO, OpenCape Corporation.*

Last, but not least, Corero's ability to provide deep packet inspection was a crucial differentiator. *"Unlike other DDoS protection solutions, which rely on header-based 5-tuple flow information, SmartWall's Deep Packet Inspection looks into every bit of the packet header, before it enters our network, plus the first 128-bytes of the payload at line rate, to deliver the most advanced DDoS attack detection, with surgical mitigation, to ensure legitimate traffic is not impacted by damaging false positives, or an increase in latency,"* said Johnston. *"Corero's SmartWall provides OpenCape with the resources, expertise, and service that we could never provide on our own,"* added Johnston.

>the results

The DDoS protection is seamless, invisible and, most importantly, effective.

Because SmartWall works in real-time and is always operating 24/7, it identifies any attacks and protects the network against these before any damage is done.

Peace of Mind

"We are now able to offer an elegant, effective, and affordable DDoS protection service for all our customers, from the smallest to the largest, and we are already seeing strong adoption rates among our customers," said Johnston

For our customers, the biggest benefit is they don't have to do anything, except pay for the peace of mind that we are protecting them from DDoS attacks. As a not-for-profit technology company, OpenCape gets a return on its investment in the SmartWall appliances by selling DDoS protection as a subscription service to their customers.

"It is deeply subsidized by OpenCape and priced on one factor: the amount of bandwidth a client utilizes. That was the only way to make it fair, fully transparent and accessible for everyone," said Johnston.

Always On, Real-Time Protection

This protection is built around the mantra of "do no harm" to ensure that legitimate traffic is not impacted by the false positives that are common with other solutions. The SmartWall delivers comprehensive DDoS protection and visibility by inspecting every inbound packet header and payload data, and surgically removing the DDoS packets, without disrupting the delivery of legitimate network traffic. Corero's patented Smart-Rules leverage heuristics and closed-loop policy, allowing them to dynamically adapt, on-the-fly, thereby responding rapidly to evolving, sophisticated, DDoS attacks. This process of detection and mitigation typically occurs in less than a second, rather than the minutes or tens of minutes experienced with traditional DDoS protection solutions and on-demand cloud services

Automation Eliminates Manual Intervention

Because the SmartWall solution protects from over 98% of attacks automatically, OpenCape's IT security analysts rarely have to manually intervene, which increases their productivity and efficiency, and gives them more time to tackle other critical tasks.

Affordable OPEX Purchase Enabled Growth

The ability to acquire the Corero solution as a service (OPEX vs CAPEX) allowed OpenCape to invest in the technology they needed. In turn their ability to offer DDoS protection as a subscription service enabled them to increase customer acquisition and drive additional revenues.

Responsive Customer Support

"Another advantage is that the Corero solution comes with excellent customer support. Corero's Security Operations Center team is responsive, with deep knowledge and expertise in DDoS mitigation to quickly identify and protect against emerging threats," said Johnston. "That's an important factor because, even with automated mitigation, new attack vectors will emerge."

> Corero Smartwall at a glance

» Surgically removes DDoS attack traffic automatically, before it reaches critical systems, ensuring optimal performance and maximum availability.

» Delivers line-rate, in-line distributed denial of service attack protection, from 1Gbps to 100Gbps per rack unit, in a solution that scales to Terabits per second of protected throughput.

» Prevents the impact of attacks ranging from simple volumetric floods, to sophisticated state exhaustion attacks, at layers 3 to 7.

» Delivers comprehensive visibility for analysis and forensics, before, during and after attacks.

Single-pane Visibility into Attacks

"The mitigation appliances provide excellent visibility into our network even for attacks that may only last seconds. Having that level of insight is very valuable," said Johnston. "I can easily say it has made us more secure, productive, and better informed."

Standing Out from the Competition

"The fact that we are offering DDoS mitigation as a service to our clients is a huge differentiator in our marketplace," said Johnston. "We offer DDoS protection for both large and small clients, plus our larger customers have the option of live-stream access to a portal view of DDoS events in real-time."