A Case Study Continued: Two Years After Implementation, Streamline Doubles Down on Corero for Inline, Instant DDoS Mitigation

A little more than two years ago, Streamline Servers, a market innovator that provides enterprise-grade game, dedicated, VPS and web servers to their clients, implemented Corero's SmartWall® Threat Defense System (TDS) DDoS protection to provide quality service and high uptime to their customers. The company first rolled out the Corero solution in its Sydney, Australia headquarters, and a few short weeks later followed with a second Corero solution in its Singapore office to protect the Singapore network from malicious attacks. Because those implementations are so successful, Streamline Servers has decided to double down on its SmartWall implementation, and recently implemented SmartWall appliances in its Melbourne, Australia, Auckland, New Zealand, and Los Angeles, California offices.

The Solution

The Corero SmartWall TDS solution utilizes a modern DDoS mitigation architecture to automatically and surgically remove volumetric single and multi-vector DDoS attacks, and it incorporates custom defined filters for more sophisticated attack vectors, while still allowing good user traffic to flow uninterrupted. In addition, the built-in SmartWall Analytics enables fast and deep traffic analyses, identifying patterns and anomalies in real-time, facilitating the creation of highly granular filters, to detect, test, and mitigate new attack vectors in real-time.

"The product just works so well our security analysts can simply monitor it without having to make frequent adjustments," said Nathan Harding, Chief Executive Officer, Streamline Servers. The Streamline Servers security team adjusts the SmartWall appliances network-wide only once every three to six months. However, they access the appliances fairly frequently when clients request the addition of custom flex rules.

The SmartWall Dashboard allows Streamline Servers to monitor its network traffic and patterns in real-time, which allows them to create custom flex rules for new DDoS attack types so they can be detected and mitigated in real-time, before they reach their clients and cause disruption to gaming sessions or enterprise application use.

As an example, Corero's Flex Rules capability enabled Streamline Servers security team to create a new attack rule to mitigate botnet TCP URG Flag attacks, an attack type that is currently prevalent but had not been used for DDoS attacks in the past 10 years. "SmartWall has undergone several updates since our initial deployment, which allows us to create significantly more flex rules, with greater level of sophistication and fine tuning," said Harding.

Single Pane Views of Every Packet

"The main difference between Corero SmartWall and other products is the level of insight that Corero provides," said Harding. The SmartWall offers comprehensive visibility into attempted DDoS attacks. "We can now see attacks that in the past would have gone unnoticed," said Harding. For example, Streamline recently observed a 14 Gbps attack spread between Los Angeles, California, New Zealand, and Australia to target one of Streamline's customers.

"We have a bird's eye view of the whole network, whereby we can see every single packet reaching our network, and we can drill down into every new attack vector and provide a solution for it. Corero gives us a single pane of glass view for every packet across all of our network locations, allowing us to have a sophisticated overview of our network rather than guessing where packets are going. Other solutions on the market only work for net flow data," says Harding. "The engineering behind Corero is beyond anything on the market; other solutions don't compare," he added.

Streamline Servers also finds great advantage in the SmartWall Service Portal, which allows Streamline's customers access to a dashboard view of attempted DDoS attacks. Harding says, "Our customers love the fact they can see clean traffic as well as DDoS traffic, and that we send them automatic emails which includes details of an attempted DDoS attack. It shows our DDoS protection service works very effectively and pre-emptively to mitigate attacks, so customers can see they are getting great value from it."

Outstanding Support

"The Corero support team is second to none," according to Harding. "The support team is extremely responsive and intelligent when handling the occasional support requests we submit," he said. "They respond within minutes, even at odd hours. One time when we had a question about a particularly complex attack, the support team resolved the problem for us within a few hours," added Harding. Corero support also assisted Streamline Servers by adding new attack vector rules even before the vectors showed up on their network, which enabled preemptive blocking of new attack vectors.

Streamline Servers benefits from its Corero implementation in a couple of ways. First of all, it increases revenue because its DDoS service is a competitive differentiator in a crowded server, gaming and hosting marketplace. Second, it keeps current Streamline customers happy because they have access to the SmartWall Service Portal that shows proof of attempted and thwarted DDoS attacks that would have otherwise negatively impacted the customers' networks.

Competitive Advantage

In the crowded servers and hosting market, Streamline Servers stands out for its uniquely effective DDoS protection service. The company offers DDoS protection as a value-added service free of charge to all of its customers, and it offers higher levels of support for those who need greater protection. Streamline Servers built the solution into its billing infrastructure so that the protection is instantly and automatically deployed for their clients. It has proven to be a competitive differentiator for the company, as it protects current customers from DDoS and helps win new customers. Streamline Servers linked all of its sites to the Corero DDoS protection appliances, so each site scrubs traffic closer to the source of the attack. This adds an umbrella of protection for the New Zealand customers, which is a first in the New Zealand market, where DDoS protection is relatively rare.

Corero SmartWall At a Glance

» Removes attack traffic surgically and automatically, before attacks compromise performance and availability of critical systems

» Offers line-rate, in-line, denial of service protection from 20Gbps to 100Gbps per rack unit, in a solution that scales to Terabits per second of performance

» Prevents extremely sophisticated layer 7 attacks, as well as state exhaustion and volumetric attacks at layers 4 and 3

» Utilizes a high-performance scalable architecture

» Delivers comprehensive visibility for attack analysis and forensics

The Results

» Maintains maximum levels of reliability for applications and mission-critical systems, even in the face of a DDoS event

» Enables Streamline Servers to mitigate DDoS attacks locally, at each of their multiple locations around the world

» Allows flexible deployment configurations to best meet the needs of Streamline Servers' individual customers

corero

As the DDoS threat landscape continues to evolve, enterprise, hosting and service provider customers around the world rely on Corero for industry-leading defense systems to provide 24/7, automatic attack mitigation services, with threat visibility, sophisticated reporting and analytics. For over a decade, Corero has been providing state-of-the-art, highly-effective, automatic DDoS protection solutions.

For more information, visit www.corero.com