Retailer Safeguards Network with Advanced Security Solution

ABOUT THE COMPANY

This large scale retail leader has a huge national presence with physical locations all over the country, and a competitive online retail presence as well. Their success relies on a High Performance website enterprise, protecting customer information, and secure credit card transactions. With the large scale scope of the business, and high traffic both physically and virtually, a breach would result in exposure of personal data stored on the network, and a major financial blow due to a decline in customer satisfaction. Not having a secure network is a significant risk this retail company cannot afford.

THE CHALLENGE

The organization previously had an inadequate security system in place that still allowed threats into their network, and did not meet the speed and safety requirements essential for the scale of protection needed.

Retail institutions are consistently a target for hackers due to their large scale and constant influx of credit and debit card transactions. There are about 50 million attacks against retail networks every year, but basic firewalls lack the shielding technology needed to individually block and analyze every event. Retailers are susceptible to "card not present" fraud transactions that result in huge losses of revenue and customer trust. Hackers that are able to get into the network can also gain access to files containing profiles and information on every customer and employee. All of these threats are very dangerous and threatening to an organization, and would ultimately be very compromising to personal data and customer loyalty, which is damaging to the financial stability of the company.

The retailer had tried to implement the best network protection, but unfortunately, the firewall systems that had previously been used could not handle the volume of incoming threats. The retailer could have turned to a secondary cloud security system, but such solutions are also unequipped for the large influx of data, and cannot offer adequate coverage.

The organization's security team needed an advanced solution that provided:

• Enhanced active threat blocking protection against potential harmful breaches

• Shielding against all know vulnerabilities with real-time threat intelligence

• Protection against cybercriminals that are looking to steal sensitive customer data

• The ability to identify data exfiltration (unauthorized data transfer or theft) from an inside source

Centripetal

THE SOLUTION

The implementation and use of Centripetal's threat intelligence network security solution allowed the organization to filter, monitor, and alleviate cyber threats in real-time. This was achieved at scale without causing any disruption to the network. With applied threat intelligence, enforcement, and analytics, Centripetal was able to deliver the best solution possible for this retailer's network.

Applied Threat Intelligence: Centripetal's CleanINTERNET service is embedded with the AI-Analyst tool which helps expand the cyber analysis coverage within the threat intelligence feeds. This AI tool significantly reduces the time and workload needed to limit and prevent damage to the network by quickly and accurately resolving threats.

Enforcement: Once Centripetal's security solution was deployed on the organization's network, analysts were able to pinpoint exact locations of malicious hosts and block them from sending packets out on their network. The increase in their security posture was well received within the organization due to the highly advanced capabilities in both speed and scale that Centripetal's solution offered.

Centripetal's solution enabled the organization to monitor and mitigate cyber threats in real-time at scale without disrupting the network. Through Centripetal's partnerships with industry leading threat intelligence providers, Centripetal's solution allows the organization to operationalize more threat intelligence than ever before, over 5 million-rule unique indicators to every packet entering or existing the network.

Analytics: The analytics arsenal provided by Centripetal's service gives decision makers analysis that addresses both identified and credible threats.

Centripetal's ultra-high performance at scale security system has been developed and patented to filter high volume traffic against dynamic network threats. By using a comprehensive list of threat intelligence from multiple sources, including Visa, malicious activity and threats are stopped and blocked immediately. All traffic is filtered so that non-malicious ecommerce activity is allowed onto the network at fast speeds. This system becomes increasingly more efficient as time goes on after installation as more threat intelligence is continuously being compiled and applied. The network was able to operate at its most efficient and safest capacity.

THE RESULTS

The implementation of Centripetal's high performance network security solution allowed this retailer to filter through the benign activity, while blocking all known threats, enabling them to regain full control of their network.

This organization was able to keep security a priority, without compromising ecommerce network speeds. Malicious hosts were immediately identified and blocked so that all of the sensitive data stored on the network could remain secure.

Centripetal's threat intelligence network security solution brought confidence and control to the retailer by offering the best network protection possible.

Centripetal   www.centripetalnetworks.com