National Supermarket Chain

Industry
Retail and E-Commerce

Region
Asia-Pacific

Business Outcomes
Fewer security incidents, improved stability, faster installation of security patches and updates, reduced downtime

Product
Forcepoint NGFW

Overview

Retailers continue to be a major target for cybercriminals due to the sheer volume of transactions processed around the clock and the type of data they collect. The challenge is even greater for retailers with both a physical and online presence, since these channels expose the business to unique vectors of attack. Highly distributed networks, such as those in retail, can be difficult to manage since it's not feasible to have security technicians at each location.

The data retailers collect is largely dependent on where the transaction takes place. Brick and mortar locations use point-of-sale systems to collect customer payment details, including credit card numbers and personal identification numbers (PINs). Ecommerce websites first capture login credentials, and then log personally identifiable information (PII) (e.g., customer name, phone number, email address), credit card numbers (which are often stored), and track order histories. Many retailers have loyalty programs that collect purchasing trends.

High profile breaches with American retailers such as Target, Home Depot, and TJ Maxx have been a wake-up call for others across the globe, serving as a warning to improve cybersecurity programs and protocols or risk becoming the next headline.

Challenge

A national supermarket chain was up for renewal with their existing NGFW vendor. Since the initial deployment, the incumbent vendor had divested in the security industry, instead placing their efforts and investments into networking technology. This lack of focus created issues for many on the network security team, who describe the NGFW management system as unstable.

Get in touch with us.

Learn how Forcepoint can protect you. Contact us at **forcepoint.com/contact**.

Securing transactions for 1,500 stores, a highly utilized e-commerce site, and their supporting warehouses is a Herculean task. With a fierce commitment to customer privacy, the retailer had no room for unpredictability in regards to their network security. They needed an NGFW solution that offered reliable and centralized management for all existing locations, as well as the scalability to support future growth. To avoid unnecessary costs and complexity, it was important that the chosen solution was interoperable with their existing intrusion prevention, endpoint, and sandboxing products. Above all, the NGFW that they selected would need to offer the very highest level of protection against known and unknown exploits and evasions.

Solution

After evaluating multiple vendors, the customer concluded that Forcepoint NGFW offered the best solution for their complex requirements. Several factors contributed to the decision, including Forcepoint's straightforward pricing model—one price inclusive of all features required from the appliance.

With Forcepoint NGFW, policies are now managed across all Forcepoint deployments using a single interface. The Security Management Center (SMC) dashboards allow the network security team to quickly and easily identify potential threats on the network, enabling timely responses and mitigation. The team also has a clear path to integrate Forcepoint NGFW with other solutions, fulfilling the company's interoperability needs, and can easily scale as the network expands.

Understanding the costs associated with any amount of network downtime, the customer opted to upgrade to enterprise level support for help with the initial installations. Forcepoint's Professional Services streamlined the process and ensured a similar experience for future installations. Forcepoint NGFW appliances have since replaced aging models in the company's data centers, deployed in two node clusters for redundancy and load-balancing and configured to the highest security level settings to facilitate maximum protection.

Results

With Forcepoint NGFW's industry-best security efficacy, the team now experiences fewer incidents requiring investigation. Forcepoint's SMC has been stable and reliable, offering the network security team a trustworthy source of intelligence about their network traffic, as well as assurance that security policies will be enforced as intended.

One of the features most appreciated by the customer are zero-downtime upgrades. By deploying the NGFWs in two-node clusters, traffic can continue to be routed through one node while the other gets updated, eliminating the wait for a maintenance window as well as the possibility of lost revenue due to an outage. Clustering also improves the network's throughput levels over the previous solutions, even with configurations at the highest security level.