Forcepoint

Customer Story

National Supermarket Chain Turns to Forcepoint for Centralized Firewall Control, Better Protection Against High-Profile Data Breaches

After watching big US retailers get hacked, this nation-wide supermarket chain was determined not to let it happen.

Disastrous data hacks of US-based big box retailers like Target, Home Depot, and TJ Maxx put companies like this supermarket chain on notice. The company, which controls a large portion of the Australian market, wanted an easy-to-manage, centralized solution to safeguard a highly distributed network of more than 800 supermarkets, nearly 700 petrol station stores, warehouses, and an ecommerce site. It turned to Forcepoint Next Generation Firewall (NGFW) as a vital part of the integrated security system deployed to protect customer payment card data and other sensitive information.

CUSTOMER PROFILE:
Leading supermarket, retail, and consumer services chain with more than 100,000 employees and 1,500 locations.

INDUSTRY:
Retail

HQ COUNTRY:
Australia

PRODUCT:
Forcepoint NGFW

Large retail chains are some of the most attractive targets for cybercriminals due to the sheer volume of transactions they process around the clock and the type of sensitive financial data they collect from customers. The security challenge is even greater for chain retailers which have both a physical and online presence, exposing the business to multiple vectors of attack.

The data that 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 can log personally identifiable information (PII) such as customer names, phone numbers, and email addresses, credit card numbers (which may be stored for follow-on transactions), and order histories. Like many retailers, the company has a loyalty program that collects purchasing trends—more data that could be misused by malicious actors.

Highly distributed networks, such as those used by brick-and-mortar retail chains, can be difficult to manage since it's not feasible to have cybersecurity technicians stationed at each location.

A network security solution for Australia's geographic challenges

The challenge of servicing a highly distributed network is made even more difficult by the vast geography of Australia, where distances between some major population centers can be measured in the thousands of kilometers. The cost would be prohibitive to send cybersecurity technicians for regular in-person visits to more than 1,500 supermarkets and branded petrol station stores situated throughout Australia.

Still, the company knows it cannot afford to scrimp on IT security—a lesson that has hit home in recent years for Australian retailers in the wake of a string of high-profile data breaches involving American big box stores like Target, Home Depot, and TJ Maxx. Knowing that its competitors were busy shoring up their own cybersecurity, the pressure to avoid being the victim of a disastrous data breach was mounting.

Hacked American retailers were making headlines for all the wrong reasons and the company didn't want to become the Australian version of a data breach cautionary tale. Fortunately, Forcepoint was uniquely positioned to help the supermarket giant install better network security across an entire, sprawling continent.

The right firewall for a distributed network

The supermarket chain decided it wanted a firewall solution that offered reliable and centralized remote management capabilities 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, and endpoint products. Above all, the firewall the company selected would need to offer the very highest level of protection against known and unknown exploits and evasions.

Forcepoint Next Generation Firewall (NGFW) provided the best solution for the company's complex requirements. The ability to centrally manage NGFW appliances across the supermarket chain's highly distributed network was the primary driver for the decision to choose Forcepoint.

Challenges

Protect customer PII and PCI from massive data hacks like the ones experienced by US retailers.

Approach

Implement Forcepoint Next Generation Firewall to protect 1,500 supermarkets and petrol station spread across the country.

Forcepoint now helps safeguard transactions and communications for 1,500 brick-and-mortar retail locations, as well as for warehouses and distribution centers located throughout Australia, and finally, for its growing ecommerce site.

Managing security without racking up frequent flyer miles

With Forcepoint NGFW, the company now manages policies across all Forcepoint deployments from a single screen. 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 with less expenditure of resources than the previous firewall solution. 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 company 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.

Stable security leads to safer shopping

Since deploying Forcepoint NGFW, the company has experienced fewer network security incidents requiring investigation. The SMC gives the network security team a trustworthy source of intelligence about their network traffic and security policies are consistently enforced as intended. The networking team also reports that the two-node NGFW clusters have improved the network's throughput levels compared to previous solutions, even with configurations at the highest security level.

The company has also found upgrading easier thanks to the two-node clusters, which allow traffic to be routed through one NGFW node while the other is updated, resulting in zero-downtime upgrades. This process has eliminated the wait for a maintenance window to perform updates, while also reducing the possibility of lost revenue due to an outage.

Today, the supermarket giant is confident that better protection from Forcepoint will help keep it in the business of serving Australia's supermarket shoppers... and out of the headlines for an embarrassing, damaging data breach.

Results

Fewer network security incidents requiring investigation.

Improved network throughput levels compared to previous solutions.

Zero-downtime upgrades.