FireEye

Case Study

National Grocery Retailer Combats Advanced Threats with FireEye

Key Components

- FireEye Threat Prevention Platform
- FireEye Web Security (NX series) platform

As one of the nation's largest retailers, this grocery chain supplies hundreds of communities, serving as a local hub to buy food, fill prescriptions, fuel up vehicles, and more. In the process, it amasses a trove of sensitive data: everything from credit card numbers to health care records.

Given the sheer volume of data the grocery chain is entrusted to protect, deterring attacks is critical. For the company, that mission includes safeguarding more than 10,000 servers and 120,000 endpoints and devices.

The job is getting tougher. Today's cybercriminals can easily bypass traditional defenses. A wave of attacks has hit retailers' balance sheets—and tarnished carefully honed reputations and brands.

When it comes to defending the IT assets, anti-virus (AV) software "just doesn't get it done, and IPS (intrusion prevention systems) aren't reliable" said the grocery chain's cyber security chief. "We were looking for something to fill that gap."

Company	National Grocery Retailer
Industry	Retail
Description	With a continued focus on delivering customer value, a North American grocery chain had grown to encompass thousands of stores, tens of thousands of employees, and more than a hundred thousand network-connected devices.
Challenges	• Safeguarding transactions and customer data against advanced cyber attacks • Visibility to detect threats missed by existing anti-virus, IPS, and firewall technologies • Spotting advanced malware, and acting fast to mitigate potential damage
Solution	• FireEye Threat Prevention Platform • FireEye Web Security (NX series) platform
Benefits	• Spotted advanced malware that other defenses were missing • Minimized false positives and negatives • Gained timely, accurate insights into threats so staff could quickly address them

FireEye

Case Study

"[With FireEye], we're not spending time filtering through the noise of false positives, which means we can respond much more quickly when a real issue arises."

— Senior Manager of Threat and Vulnerability Management, National Grocery Retailer

Easy to deploy

The grocery chain wanted to avoid becoming the next high-profile example.

Knowing that traditional security tools were designed for an older generation of attacks, security leaders began looking beyond legacy defenses. It needed something built from the ground up to combat today's fast-moving, ever-morphing threats.

The security team researched and tested several products, including the FireEye platform. FireEye first stood out for its easy, low-cost deployment. In a FireEye proof-of-value trial, initial setup took about 15 minutes.

The FireEye platform "was the only product—out of the dozens and dozens that I've deployed—that truly worked out of the box," the security manager said.

And the FireEye platform quickly proved its ability to detect attacks without drowning the security team in a flood of false-positive alerts.

"We have a small team with limited resources," the security manager said. "We were looking for something that was easy to set up and administer. That's exactly what the FireEye platform delivered."

The FireEye platform immediately began identifying threats that had bypassed the grocery chain's existing defenses.

To make sure the results were not just a fluke, the security team tried to retune its existing security tools to see whether they could spot detect the attacks FireEye had found. They didn't.

Accurate, actionable alerts

Today, the FireEye platform plays a pivotal role stopping cyber attacks before they become big, costly problems for the retailer.

The company uses the FireEye Web security product, which now goes by the NX Series name. In addition to using the FireEye appliance to analyze Web objects and files directly, the security team also sends alerts into the grocer's log-management appliance for further research.

Thanks to a tightly managed IT environment, the retailer sees few alerts, "maybe a couple a week," the security manager said.

"But the couple a week we get aren't caught by anything else," he added. "That's the key."

Working with the grocery chain's legacy security tools, FireEye cuts through the clutter of false positives, event data, and vague alerts.

"That's where FireEye shines," said the security manager. "When we get a critical or high-risk alert, there's a 99 percent chance it's actionable."

The FireEye platform also allows the grocery chain to stretch its limited IT budget, because it does not require a large staff or an inordinate level of technical expertise to manage. The FireEye platform requires little ongoing administration, tuning, or troubleshooting, the manager said.

"It fills the gap we knew we had," he said.