CUSTOMER STORY

Top 10 global retailer builds world-class cyber defense capabilities with FireEye

FACTS AT A GLANCE

INDUSTRY

Retail

CUSTOMER PROFILE

In business for many decades, this company ranks in the 'Global Top 10' of worldwide retailers and is among the five largest retail organizations in the U.S. As a component of multiple financial market indexes and with many thousands of locations, this retail giant is a highly familiar household name.

Business challenge

The retail sector has experienced some very high-profile breaches that are symptomatic of the changing threat landscape: The vice president of information security for the retail giant expounded, "We're seeing a blending of cyber-criminal activity, nation-state sponsored attacks, hacktivism, geo-political activity, etc. Specific consumer information is more frequently being targeted and exploited for profit by organized crime."

> "As an overall package, the combination of products and services makes FireEye an absolute fundamental differentiator for my company."
>
> — **VP of information security**

He added, "The continually escalating sophistication, creativity, and expertize of today's threat actors means that there's a high likelihood that prevention will inevitably fail. Our approach is to implement best-in-class security measures but to assume that there is always the possibility of a worst-case scenario occurring; we strive to detect potential threats in as close to real-time as we can get and then mitigate the situation in as short amount of time as possible."

Bringing it all together

"An effective cyber security strategy is created by bringing people, process, and technology together. You can't place emphasis on just one of these three components. Obviously selecting the right technologies is imperative but it's equally important to understand that there's a responsibility to ensure that the appropriate measures are put in place to leverage what is implemented to the fullest extent."

A major milestone for the company has been the creation of a 24x7x365, fully integrated security operations center; accommodating focused teams for cyber threat intelligence, threat defense, computer security instant response, and vulnerability management, all co-located in a single, secure building. "The center gives us the ability to process data in real-time and to assess events around the clock," noted the VP. "The threats don't stop when the end of the day arrives!"

Speed is of the essence

The company has adopted a platform-based architecture to facilitate the deployment of best-in-class components throughout the organization. "The speed to detect known and unknown malicious activity is a critical part of what enables us to deliver a viable detection function. Knowing that there's something malicious in your environment weeks after it initially shows up doesn't do anybody any good. This is why we make extensive use of FireEye solutions and have deployed the FireEye Threat Analytics Platform, as well as the Network Threat Prevention and Email Threat Prevention platforms," noted the spokesperson. "The continuous updating of signatures based on data collected from around the globe is of very high value."

Professional services bring world-class results

He articulated, "Another compelling aspect of the partnership with FireEye is the caliber of the company's professional services team: Marrying very smart people to strong technology is absolutely the right solution.

"One of the many benefits we get from our professional services relationship is that the FireEye teams are delivering across many different domains: Being able to access that breadth of cross-industry expertise is absolutely critical for us. If we focused exclusively on threats relevant only to retailers, we'd be missing the mark dramatically. The FireEye professional services organization possesses a deep understanding of the motivations, the processes, and the subtleties behind a myriad of different threats. This first-hand knowledge equips us with a set of attributes that is just not available anywhere else."

Visibility and control

The FireEye Threat Analytics Platform (TAP) applies threat intelligence, expert rules, and advanced security data analytics to high-volume event streams. The VP commented, "The TAP has become a tremendous source of analysis for us. Not only does it provide us with the ability to proactively raise alerts, based on FireEye's intelligence, it also serves as a great analytics tool to be able to query our data when we need to look for a specific item or chain of events. It's the platform that we most frequently use to triage potential threat-related situations."

Every second the company experiences an average number of events measured in tens of thousands. To handle this volume of alerts, the company utilizes FireEye Central Management (CM Series). "Deploying FireEye Central Management has provided a lot of value as it enables us to centralize all the alert data, as well as to manage our widespread infrastructure. It allows for all the events that are detected — including those triggered by the network and email threat prevention platforms or by the TAP — to be centralized and aggregated in the CM Series console for us to take informed action," stated the VP.

"FireEye gives us that cross-industry view that is so critical; not only to my company and other retailers but for every industry."

— VP of information security

Summary

He concluded, "There are several core reasons why FireEye is compelling to us. One is the quality of security data analytics: With the Threat Analytics Platform, and the way we've architected our network sensors, we're able to get closer to a true security data analytics capability than I've seen anyone else get to.

"A second clear differentiator for FireEye is the caliber of professional services; the relationship gives us intelligence and fidelity of response. There's no other company out there that can claim to have the world's elite-most responders, period.

"Getting these two elements from one partner, plus all the other capabilities provided by the suite of FireEye threat prevention solutions is totally compelling and impossible for anyone else to replicate. The threats, the intelligence, and the actors being tracked and profiled by FireEye give us that cross-industry view that is so critical; not only to my company and other retailers but for every industry."

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye®