CUSTOMER STORY

Leading Railroad Network Adopts Proactive Approach to Cyber Security

Transport Operator Defends Critical Infrastructure with FireEye Solutions

FACTS AT A GLANCE

INDUSTRY

Transportation

SOLUTIONS

- FireEye Network Security
- FireEye Endpoint Security
- FireEye Managed Defense
- FireEye Network Forensics
- FireEye Verodin Security Instrumentation Platform

BENEFITS

- Enhanced visibility and actionable threat intelligence enable proactive security approach
- Alert accuracy and high-quality reporting reduce SOC alert fatigue
- 24 x 7 real-time monitoring ensures expedited implementation of tailored security measures
- Unique blend of FireEye technology, intelligence and expertise elevate overall security posture

CUSTOMER PROFILE

This leading railroad operator transports agricultural, consumer and industrial products, as well as coal over tens of thousands of route miles across the United States.

With its charter to supply food, power and other essential goods, the company is federally designated as being part of the critical infrastructure of the country. With many millions of shipments made each year, the railroad makes a significant contribution to alleviating highway traffic congestion and lowering carbon emissions from road vehicles.

As a critical component within multiple global supply chains, a vital enabler of the economy and a daily influence in the lives of millions of Americans, the company's infrastructure requires effective protections against cyber attack. The railroad's security operations center (SOC) manager emphasized, "We move an immense amount of goods across the country and that trade is paramount to our success in America. We place a great deal of importance on staying vigilant for geopolitical events that could make us a target."

The SOC manages all cyber threats the company may intercept, whether they are targeted toward the enterprise's IT operations or its rail infrastructure. The SOC manager and his team act as alert analysts, threat managers and incident responders 24 hours a day, 365 days a year. The SOC's diligence prevents misuse of thousands of customer accounts, defends the large number of email accounts from exploitation and protects the company's extensive endpoint deployment from cyber attack.

> “We’re supported by a team that is on the frontlines of the latest threats and invested in protecting our environment. FireEye sees us as we do: Critically important to America.”
>
> — SOC Manager, Major US Railroad Operator

Though it has always had a rigorous security posture, the railroad wanted to implement a more efficient, proactive approach to cyber defense. The SOC manager explained, “We were a very reactionary force. All our security data came to us through someone else. If a phishing attack happened, we would potentially only find out about it at some indeterminant point in the future. We wanted to transition from this mode of operating and position ourselves to identify a threat before it had the opportunity to cause harm.”

More is Not Necessarily Better

The company also sought to reduce alert fatigue in its SOC, where numerous false positives and the sheer volume of information were beginning to compromise accuracy and efficiency. The proliferation of multiple agents across their environment and the ensuing generation of massive amounts of disparate, inconsistent data further compounded the untenable situation.

The manager particularly focused on validating the effectiveness of the railway’s security tools and reporting capabilities. He wanted to determine if the services used by the company were doing their job correctly, and if the SOC could capture threats procedurally and accurately identify an attack’s trajectory.

Real-Time Threat Investigation and Security Infrastructure Evaluation

The company initially deployed FireEye Network Security and implemented FireEye Endpoint Security on a specific group of devices along the perimeter of its environment. The railway also added FireEye Network Forensics and FireEye Managed Defense services to further enhance the SOC’s capabilities.

The FireEye solutions demonstrated their value when the SOC team uncovered an intrusion that occurred on the railway’s edge infrastructure. Using the web shell detection capabilities of FireEye Network Security, the team discovered attempts to upload a malicious script to the company’s servers.

A subsequent investigation used FireEye Endpoint Security to address the threat on the affected servers. Intelligence from the integrated FireEye solutions supported the team as they mapped out and responded to the attack,” The manager recounted. “Our FireEye stack identified the targeted servers: We quickly determined that malware had actually been introduced but we were able to halt the attack before the web shell was able to validate its install.”

He leveraged the successful analysis and response to communicate the benefits of elevating the SOC’s ability to monitor and mitigate threats across the entire environment. As a result, the railway company expanded its deployment of FireEye Endpoint Security and, consequently, the vigilance provided by its suite of FireEye solutions.

The manager also brought the FireEye Verodin Security Instrumentation Platform into the SOC to optimize his team’s ability to measure and improve the effectiveness of defenses. He elaborated, “By the time you take action on the results of a penetration test, conditions have changed and the adjustments are less impactful. Adopting the FireEye Verodin platform enables us to identify potential security vulnerabilities and to validate the quality of our protection in almost real time.”

The railroad operator combines data from FireEye Verodin with intelligence from the other FireEye solutions to monitor for indications of specific APT groups and threat actors to ensure the railway is prepared to safeguard against them. “FireEye Verodin fills a void that we’ve been asking the security industry to address for a long time,” noted the manager.

A Proactive Approach to Threat Mitigation

The transport company uses a wealth of different solutions, tools and services in its SOC to secure the railway’s massive infrastructure. The manager disclosed, “We view our suite of FireEye capabilities as well-trusted resources and our primary threat hunter relies on FireEye as his provider of choice.”

> FireEye Verodin fills a void that we've been asking the security industry to address for a long time."
>
> — SOC Manager, Major US Railroad Operator

Despite its complex infrastructure and elaborate SOC, the quality of alerting and support from FireEye has helped simplify the railway's overall security operations. "The accuracy of FireEye notifications has enabled us to really minimize alert fatigue. When an alert does come in, we not only have our own analysts to investigate the potential issue but we also have immediate assistance from the FireEye Managed Defense team as well if we need it," enthused the security professional.

With high-quality alerting, threat visibility from core to perimeter, reliable feeds of actionable intelligence and enhanced forensic analysis abilities, the company has been able to dramatically elevate their cyber security stance. The manager shared, "Whenever we detect unusual behavior or observe an uptick in suspicious activity, we are able to immediately investigate the situation and ensure that we have the right strategy in place to mitigate any potential impact from the threat."

Ease of access to FireEye team members, their expertise in cyber security and understanding of the railroad's unique security posture offers additional returns from the railway's investment in FireEye solutions and services. "The relationships we have with the people we work with at FireEye are key to us. Not only are they very approachable, they also are extremely knowledgeable," remarked the manager. "We're supported by a team that is on the frontlines of the latest threats and invested in protecting our environment. FireEye sees us as we do: Critically important to America."

The Importance of Partnership

Commenting on the partnership between the railroad operator and FireEye, the SOC manager concluded, "In the cyber security field, one thing that I've learned is that you can drown yourself in too much intelligence. Many vendors offer intelligence but not a lot have a depth of understanding around what is happening in the world. FireEye has analysts that speak the language and understand the geopolitical context of where malware is being created. As these details become more significant and the threat landscape continues to rapidly evolve, our relationship with FireEye becomes even more important."

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

©2020 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. F-EXT-CS-US-EN-000239-01

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.