CUSTOMER STORY

International Railway Operator Defends IT and OT Systems

Diverse FireEye Portfolio Helps Secure Public Transport Network

FACTS AT A GLANCE

INDUSTRY

Transportation

SOLUTIONS

- FireEye Network Security with SmartVision
- FireEye Endpoint Security
- FireEye Email Security
- FireEye ICS HealthCheck
- FireEye Managed Defense
- FireEye Mandiant Incident Response Retainer
- FireEye Mandiant Consulting Services

BENEFITS

- Impact and efficiency of cyber security team amplified by world-class solutions and services
- Simplified compliance with local data security regulations, such as GDPR and PDPO
- Deep visibility across entire global infrastructure
- Neutral, unbiased advice enhances overall security posture

CUSTOMER PROFILE

For nearly half a century, this railway operator has provided impeccable public transportation services. The company's tens of thousands of staff members manage railway operations in multiple countries, overseeing millions of passenger trips worldwide every day.

Lauded for its safety, efficiency and high reliability, one public transport network serves as a model for modern railway operations in many cities worldwide.

Every day, millions of commuters depend on the company's trains to transport them safely to their destinations. The railway operator's popularity stems largely from the unwavering timeliness of its trains and technology-enhanced accommodations, which provide a seamless commuter experience through amenities such as mobile phone apps and an electronic fare payment system.

The railway's chief information officer (CIO) is responsible for ensuring that the organization's business operations run smoothly and without service disruptions caused by any form of malicious cyber activity. The CIO's charter revolves heavily around maintaining the confidentiality, integrity and availability (CIA) of sensitive company information.

As a high-profile target, any exploits may tarnish the railway operator's brand and customer trust, and at worst, jeopardize the safe operation of hundreds of kilometers of railway track. The CIO shared, "Safety is critically important to us. In the most extreme cases, disruption to our systems could impact the wellbeing of our customers."

In addition to the responsibility of maintaining a rigorous cyber security posture to defend IT and industrial control systems (ICS), the transport network is accountable for the personal information of more than 10 million customers and employees. The organization is also required to comply with multiple data security-related mandates—including the European Union's GDPR.

"FireEye has become a trusted partner to a lot of organizations, in particular to our railway, and on a personal level, to me."

— Chief Information Officer, international railway operator

Robust Defenses for Today, Tomorrow and the Distant Future

To decide on their technology stack components, the security team assessed many products against global benchmarking standards for cyber security. The CIO was particularly interested in understanding each tool's roadmap: The potential of a solution to evolve and address the new vulnerabilities and forms of cyber attack emerging as a result of the world's digital transformation. The organization was also concerned with the quality and accessibility of a security supplier's local and global support teams.

After a stringent selection process, the security team chose to go with FireEye. FireEye Mandiant consultants were engaged to assess the company's overall network infrastructure and industrial control systems. Based on their results and security improvement recommendation, the CIO integrated FireEye Network Security, FireEye Email Security and FireEye Endpoint Security into the company's defenses.

To deepen visibility into lateral network traffic and ensure timely detection of any malicious activity post-network infiltration, the security team also implemented FireEye SmartVision—a component of FireEye Network Security—into the environment.

All these FireEye technologies work together to protect the entire infrastructure from core to perimeter and helps the railway operator remain a responsible data steward. The security stack can automate breach detection and simplify incident response, leaving the railway better equipped to comply with data breach notification mandates and requirements to safeguard personal data from unauthorized use. After the first successful implementation, the security team replicated the strategy for the company's subsidiaries in another region.

Leveraging Intelligence from the Frontlines

FireEye consultants openly shared threat intelligence derived from frontline experience of the world's largest and most impactful breaches. Their expertise was a compelling factor in selecting FireEye. "Cyber security is always changing; recruiting the talent needed to take on the challenge is difficult for any company, no matter how attractive or prestigious the organization," explained the CIO.

He continued, "I really value the professional guidance I get from the FireEye Mandiant team. Even when I have questions that aren't directly related to FireEye solutions, the consultants still provide neutral, unbiased advice."

The railway operator also invested in a FireEye ICS HealthCheck, to pursue security equally rigorously across both its IT and ICS environments. Mandiant consultants conducted a workshop-based ICS architecture review, coupled with a detailed technical analysis.

A FireEye Mandiant Incident Response Retainer (IRR) was added to provide the railway with the ability to rapidly identify malicious activity and receive contextual intelligence on attacks, facilitating an even faster and more effective response to cyber incidents.

Finding a Trusted Cyber Security Technology Partner

Having operationalized their FireEye solutions, the CIO reported feeling better equipped to safeguard the organization from a cyber security attack. "We always want to be confident in our ability to protect our most important 'crown jewel'—the safety of our systems. I know that I can rely on FireEye, especially the company's incident response capability, and that makes me feel more comfortable than before," he admitted.

Reflecting on the overall impact of the FireEye solutions on the company's security stance, the CIO concluded, "FireEye offers a great range of solutions, which are further complemented by the expertise of the Mandiant consultants. FireEye has become a trusted partner to a lot of organizations, in particular to our railway, and on a personal level, to me."

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™