FIREEYE™

CUSTOMER STORY

Specialty Chemicals Manufacturer Architects Security Continuity Across IT/OT Infrastructure

FireEye Solutions Revitalize People, Process and Technology

FACTS AT A GLANCE

INDUSTRY

Manufacturing

SOLUTIONS

- FireEye Network Security
- FireEye Endpoint Security
- FireEye Helix
- FireEye Managed Defense
- FireEye Threat Intelligence
- FireEye Malware Analysis
- FireEye Security Orchestrator
- FireEye Mandiant Incident Response Retainer
- FireEye Mandiant Compromise Assessment

BENEFITS

- Deployment of security solutions from one provider delivers cohesive protection across hybrid environment
- Unified monitoring of consolidated IT/OT traffic using a single dashboard
- FireEye-provided environmental data enables risk assessment and cost analysis of security investment
- Intuitive solution design expedites learning curve of new hires and optimizes resource efficiencies

CUSTOMER PROFILE

This manufacturer produces materials that are foundational to a variety of products used in most major industries and consumer applications. Headquartered in the US, the company's production network and manufacturing facilities span the globe. The company is a member of the Fortune 500.

In a manufacturing vertical where mistakes can cause catastrophic harm, the commitment to be a diligent steward of the safety of employees, local communities, and the environment is paramount the manufacturer. Maintaining safe operations while mass-producing specialty chemical materials requires an exceptionally heterogeneous global infrastructure comprised of both traditional back-office information technology (IT), and operational technology (OT): including a plethora of industrial control systems (ICS) vital to plant operations such as control valves, programmable logic controllers and SCADA systems.

The manufacturer is an attractive cyber attack target not only because of its IT domains, but because of what lies beyond the infrastructure of its OT environment. The company's chief information security officer (CISO), explained, "We're frequently moving highly unstable materials through our plants, so compromising any part of the control systems responsible for monitoring and managing the temperatures, volumes or pressures of these substances has potential to cause significant damage, and could ultimately prove devastating to human life."

The CISO observed that embracing a holistic approach to the cyber security of a hybrid IT/OT environment requires building awareness about the evolution of OT and its increasing interconnectedness with IT. Historically, IT security has been a CSO or CISO's predominant focus, with organizations relying on the best efforts of process control engineers and operational equipment manufacturers to take responsibility for securing OT devices. With the increasing convergence of infrastructures and the advent of cloud- and internet-connected technologies organizations must think differently about cyber security.

> "FireEye won me over early on just because we had the most amazing team assigned to us. I've been in cyber security for 25 years and the FireEye account team is probably the best I've ever had."
>
> — Chief Information Security Officer, specialty chemicals manufacturer

To architect elevated defenses for the manufacturer's complex and multifaceted environment, the CISO focused on improving asset management, which yielded the opportunity to implement additional standards and increase consistency in the company's technology stack.

The CISO also highlighted the importance of addressing vulnerabilities resulting from the shared pathway between IT and OT domains, "One of our biggest issues in the OT space was third-party access. We may have 15-20 vendors working on a plant at any given time and their physical access to our infrastructure, their ability to plug hardware into our systems and the opportunities they had to connect to our network presented a host of challenges that a traditional security strategy didn't account for."

A Best-of-Breed Package

Every security executive must choose whether to pick individual products to populate his or her security stack from a number of disparate vendors, or to take a more integrated approach by selecting a primary security solutions supplier to deliver protection across multiple threat vectors. The CISO opted for the latter strategy and tasked his team with identifying the optimal provider.

"Our market research quickly led us to the FireEye portfolio," recalled the CISO. "In addition to the quality of solutions, FireEye won me over early on just because we had the most amazing team assigned to us. I've been in cyber security for 25 years and the FireEye account team is probably the best I've ever had."

The manufacturer adopted an amalgam of the NIST cybersecurity framework and NIST's NICE cyber security workforce framework to determine how best to optimize its reference architecture. The CISO identified evolving his security operations center (SOC) and its three key pillars—people, process, and technology—as critical opportunities to enhance the company's security stance.

From a technology perspective, the manufacturer deployed an array of security components under the FireEye Helix security operations platform. FireEye Malware Analysis and FireEye Security Orchestrator were used to strengthen security processes. After a thorough FireEye Mandiant Compromise Assessment, FireEye Managed Defense and FireEye Mandiant Incident Response Retainer services were added to increase protection and further enhance the skills and effectiveness of people on the team.

FireEye solutions work together smoothly through the use of a single, integrated interface in FireEye Helix. The CISO noted, "FireEye solutions are intuitive to use: We can see everything from one vantage point. Also, the ramp-up time for a new hire is very short, which is great for our blended team of junior and senior professionals."

A Nation-State Attack Stopped in its Tracks

FireEye Managed Defense has become a critical asset in the company's security strategy. Around-the-clock coverage from Managed Defense analysts helps augment the manufacturer's SOC and enables the CISO to optimize his resources and ensure his team is focusing on the threats that matter, not chasing alerts. Since deployment, Managed Defense has stopped a sophisticated state-sponsored attack on the company's infrastructure and prevented the attack from evolving into a breach.

To further expand its capabilities for securing all aspects of the IT/OT continuum, FireEye has partnered with standout companies in the ICS sector. Through FireEye's relationship with Waterfall Security, the CISO has extended the protection of FireEye Managed Defense and FireEye Helix to the manufacturer's expansive OT environment. He elaborated, "With Waterfall's Unidirectional CloudConnect gateways, we can bring all the benefits of our FireEye portfolio over to our industrial control infrastructure and pull data out of that environment too. Our SIEM can then interrogate this OT traffic to identify and stop any suspicious activity, just like it does in our IT domain."

> "When I mention 'FireEye' to the board of directors during discussions about our defense strategy, the tension in the room visibly melts away and people are at ease. To me, that means everything."
>
> — Chief Information Security Officer, specialty chemicals manufacturer

What Gets Measured, Gets Improved

The analysis of data retrieved from the unified IT/OT environment has played an integral role in the manufacturer's ability to capture metrics that demonstrate the effectiveness of its cyber security posture. "We built a risk measurement mechanism specifically for our OT domain that assesses a piece of equipment's annual revenue generation against SOC data sourced from FireEye solutions that details its exposure and vulnerability to threats. The resulting risk score helps our C-suite understand the returns we are achieving from the investments in our security infrastructure.

"We also have a FireEye team onsite helping us formalize a vulnerability management program by rolling in FireEye Threat Intelligence feeds and vulnerability data—along with select KPIs, such as mean time to restore and mean time to triage—into the overall risk score," shared the CISO. "FireEye data is everything for us. We are great believers in the adage 'What gets measured, gets improved,' and 95% of the data we use comes from our FireEye solutions."

Despite the dynamic nature of the company's IT/OT infrastructure, FireEye is helping build confidence throughout the organization that the manufacturer is well positioned to stay ahead of cyber criminals. "When I mention 'FireEye' to the board of directors during discussions about our defense strategy, the tension in the room visibly melts away and people are at ease. To me, that means everything," said the CISO.

Cyber Security as Part of the Company DNA

As a specialty chemicals manufacturer, stewardship and safety are core tenets of the business. The company's overarching goal is to cause no harm to employees, contractors, the environment and the communities in which it operates, while achieving 100 percent quality and reliability.

As part of this commitment, the manufacturer has an initiative that reinforces the connection between business success and stewardship performance. "We're integrating cyber security into the DNA of our organization and aligning to business priorities by incorporating training, metrics and stewardship for our cyber safety approach across the entire company," enthused the CISO.

He concluded, "FireEye is an invaluable partner and has been instrumental in improving our security posture, helping us secure our IT domains and collaborating with us to expand defenses into OT."

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™