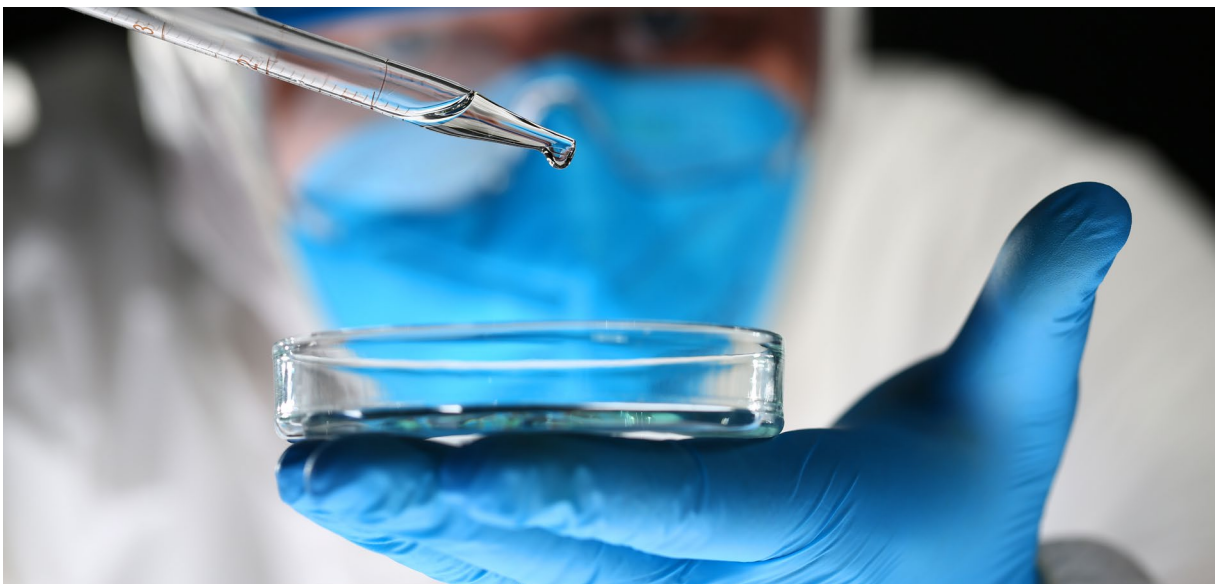# Trellix

Architecting security continuity across IT/OT infrastructure with Trellix solutions

Specialty chemicals manufacturer revitalizes people, process, and technology

Manufacturer protects its environment with a single vendor

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 to 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).

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

The manufacturer is an attractive cyberattack target not only because of its IT domains, but because of what lies beyond the infrastructure of its OT environment.

The CISO 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 their security stack from a number of disparate vendors, or 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 Trellix portfolio," recalled the CISO. "In addition to the quality of solutions, Trellix won me over early on just because we had the most amazing team assigned to us. I've been in cybersecurity for 25 years and the Trellix account team is probably the best I've ever had."

The manufacturer adopted a combination of the NIST cybersecurity framework and NIST's NICE cybersecurity workforce framework to determine how best to optimize its reference architecture. The CISO identified that evolving his security operations center (SOC) and its three key pillars—people, process, and technology—provided critical opportunities to enhance the company's security stance. The manufacturer also deployed Trellix Malware Analysis and Trellix Security Orchestrator to further strengthen security processes.

Trellix solutions work together smoothly through the use of a single, integrated interface in Trellix Helix. The CISO noted, "Trellix 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."

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 cybersecurity 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 Trellix 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."

// When I mention 'Trellix' 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

"We also have a Trellix team onsite helping us formalize a vulnerability management program by rolling in Trellix 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. "Trellix 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 Trellix solutions."

Despite the dynamic nature of the company's IT/OT infrastructure, Trellix is helping build confidence throughout the organization that the manufacturer is well positioned to stay ahead of cybercriminals. "When I mention 'Trellix' 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.

Cybersecurity as part of the company DNA

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% 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 cybersecurity into the DNA of our organization and aligning to business priorities by incorporating training, metrics, and stewardship for our cybersafety approach across the entire company," enthused the CISO.

He concluded, "Trellix 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 Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Trellix

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.