Case Study

CHEMICAL MANUFACTURING

Chemical Manufacturer Secures Global Operations with Claroty

For this chemical company, achieving a comprehensive view of cybersecurity across its network of more than 60 chemical production facilities around the world was a major goal. The company's unflinching commitment to quality meant that few things were more important than the integrity of its production process. The highly competitive nature of the industry and near-zero tolerance for downtime were key factors as well.

Challenges

The company faced several significant challenges, typical of larger chemical companies with manufacturing sites scattered across the globe, that made it difficult to achieve a high degree of security integrity and unified visibility throughout its OT environment.

1. **Differences in network topology:** Due to the varied nature of its product portfolio, many of the company's sites have different OT network topologies, and some even have a mismatch between the topology of the individual site and its production logic. This means there are usually multiple redundant, unmonitored connections at each site, which provides threat actors with numerous opportunities to penetrate the OT network and, once inside, to move laterally within it.
2. **Insecure remote connections:** Both the central control and individual site OT networks involve periodic remote connections from third parties including technicians, contractors and vendors. Both the lack of constant monitoring and widely varying security practices of these players contribute to a fundamental need for consistent, vigilant remote access security.
3. **High stakes:** In the chemical production business, security isn't just an abstract concept — it's about safety as well. There are often a wide range of approaches to OT and IT in the various production sites, and frequently inconsistent visibility into the individual networks' levels of vulnerability to threats and attacks. Combined, these factors significantly increase exposure to risks to OT availability, reliability, and safety.

Customer Quote

> *"We looked at several OT security vendors, and none but Claroty made it past the demo stage. Our team was wowed by Claroty's performance and capabilities right from the start. Very shortly after installation, Claroty was able to identify — with uncanny accuracy — every asset in our environment. The impressive performance of The Claroty Platform, coupled with the outstanding referrals from trusted partners made this a very straightforward decision for us."*

The Solution

Once deployed, The Claroty Platform was able to quickly gain visibility into detailed information about every asset in the company's entire network, manage them, and secure them using the following components:

- **Continuous Threat Detection (CTD)** for full-spectrum OT asset visibility, continuous security monitoring, and real-time risk insights with zero impact to operational processes and underlying devices.
- **Secure Remote Access (SRA)** to safeguard OT networks from threats introduced via unmanaged and unmonitored access by remote users, including employees and third-party vendors.
- **Enterprise Management Console (EMC)** to simplify management overall, consolidating data from across The Claroty Platform and providing a unified view of assets, activities, and alerts across multiple sites. The platform also integrates seamlessly via the EMC for IT security infrastructure.

Outcomes

CTD rapidly achieved complete asset visibility across the company's OT environment spanning more than 60 production facilities around the world. Its passive scanning was found to be both outstanding quality and highly accurate in terms of breadth and depth.

Integrating The Claroty Platform with existing IT security infrastructure allowed the company to enhance the overall capabilities of its security operations center (SOC), greatly improving alignment and collaboration between and across IT and OT security, as well as with a range of third-party vendors, technicians, and contractors.

Speaking of third parties, SRA provides them with a user-friendly interface they use to connect remotely (and securely) to the OT assets relevant to their engagement. Meanwhile, the company's security team leverages SRA's user-access controls, permissions policies and auditing features to monitor, manage and minimize risks introduced by remote access.

The company now has comprehensive OT visibility, in addition to real-time threat detection, vulnerability monitoring, and secure remote access capabilities. As a result, the company is able to proactively protect against security incidents, improving its overall risk exposure and enhancing the availability, reliability, and safety of its OT environment.

About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America, and deployments on all seven continents.

To learn more, visit **www.claroty.com**.

CLAROTY

CONTACT US

contact@claroty.com