Case Study

PHARMACEUTICAL

Multinational Pharmaceutical Company Inoculates Its OT Environment with Claroty

A global pharmaceutical company with ample intellectual property (IP) understood the importance of protecting its production operations. Since these operations rely on critical processes and machinery connected to operational technology (OT) environments at its various manufacturing plants, the company recognized that securing its production required securing its OT environment. After evaluating several vendors, the company selected Claroty due the unmatched OT visibility and comprehensive industrial cybersecurity controls The Claroty Platform provides.

Challenges

This company, like many in its highly-regulated industry, faced a complex array of challenges when addressing its industrial cybersecurity.

1. **Inconsistent security due to acquisitions:** As is common in the pharmaceutical industry, this company had previously acquired several other companies and thus inherited not only their range of approaches to security, but also the patchwork of different vendors they utilized to service and maintain their patchwork of different OT, IoT, and IIoT assets.
2. **Ransomware risk:** Due to their size, scope and profile, major pharmaceutical companies, including this one, tend to be frequent targets of ransomware attacks. These attacks commonly enter through a VPN connection and then spread from the IT to the industrial network where they can lead to significant downtime and operational disruption.
3. **Lack of OT anomaly detection capabilities:** Despite having limited OT expertise, the company's IT security team had recently been assigned to manage its industrial cybersecurity. Since the industrial networks at each of the company's manufacturing plants had no anomaly detection systems in place, the team attempted to implement the same systems used by the corporate IT network. The team quickly realized, however, that such systems were incompatible with OT environments. As a result, the team could not identify—much less evaluate or mitigate— potentially malicious activity within the company's industrial networks.

Customer Quote

> *"We have existing relationships with Rockwell, Siemens and Schneider Electric, all three of whom endorsed Claroty for our industrial cybersecurity challenge. Those endorsements were a huge factor in our decision, as was the fact that Claroty was able to give us the best view into our asset inventory we've ever had. Their platform truly exceeded our expectations. When we asked ourselves 'Which company will be there for the long term, and who has the partnerships that matter to us?' Claroty was the only answer."*

The Solution

After exceeding expectations during a brief testing period, The Claroty Platform was deployed across each of the company's manufacturing sites. Platform components utilized include:

- **Continuous Threat Detection (CTD)** for full-spectrum OT, IoT, and IIoT 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 industrial 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

Utilizing The Claroty Platform, the company was able to:

Achieve full OT visibility: CTD discovered and profiled all OT, IoT, and IIoT assets rapidly and with unprecedented detail. In one test site, for example, the company was aware of 65 assets, but Claroty identified 95.

Secure OT remote access connections: SRA provides plant staff and third-party vendors with a user-friendly interface through which they can access and service OT, IoT, and IIoT assets remotely, easily, and securely. It also enforces privileged access controls and proactive monitoring, among other best practices, thereby minimizing risks posed by remote users.

Leverage IT security tools to strengthen OT security: The Claroty Platform integrates fully and seamlessly with IT security infrastructure. Integrating the platform with a SIEM solution enabled the company's IT security team to utilize an existing and familiar tool to achieve comprehensive security across the entire 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