Case Study

CONSUMER GOODS

Consumer Goods Company Secures Global Industrial Networks with Claroty

This company, the consumer goods arm of a global conglomerate, manufactures everything from dishwashers to jigsaws, espresso machines to hedge trimmers. Its manufacturing sites are spread around the world; some have been in operation for decades, while others are relatively new. Juggling hordes of devices and multiple systems that scale up and down regularly, while managing remote access for a multitude of third-party contractors adds to the complexity of the company's industrial cybersecurity posture.

Challenges

This company faced a challenge of securing the entirety of its operational technology (OT) environment — from its global security operations center (SOC), to its regional SOCs, all the way down to the factory floor level. The company sought a solution that would apply to its large and dispersed manufacturing operations comprising a dizzying array of OT assets. The solution needed to address the following concerns:

1. **Prevalence of incompatible security tools and legacy technology:** The company had been relying on fairly traditional, IT-centric security tools that were not compatible with, and thus not did not effectively secure, its OT environment. This fact, along with the prevalence of legacy systems, inconsistent documentation of OT assets, and diverse geographies and local practices of many sites, made the task of gaining full visibility into its OT environment — including attaining and maintaining an accurate inventory of all OT assets — a particularly daunting one.
2. **Unmonitored remote access and misconfigurations:** Operational complexity historically had led to the company being unable to effectively monitor and manage remote access to its OT environment. Furthermore, the company struggled to prevent both undocumented and unauthorized changes to OT assets, which had previously led to misconfigurations that resulted in downtime.
3. **Patchwork of systems due to acquisitions:** Like other large manufacturers, this company has grown in part by acquisition of smaller companies, requiring it to manage multiple vendors and a range of approaches to IT and OT security. Outsourcing practices prevalent in the industry further complicated this issue.
4. **Lack of OT anomaly detection capabilities:** Operational disruptions are often difficult to detect until after they have already begun to impact production, which has a cascading effect on operations. Precise and automated alerts are necessary to allow staff to respond quickly and keep each factory operational, but the company had no adequate tools or processes in place to enable such alerts.

Customer Quote

> *"Our production sites manufacture a wide range of products, and our industrial network has been developed over a period of many years. It can sometimes feel like a patchwork of old and newer devices, and our biggest challenge was integrating this diverse group of endpoints into a single unified view. Until we found Claroty, we didn't have that capability. They got up and running immediately and gave us an unprecedented amount of information and security capability across our entire industrial network. No other provider we evaluated approached this level of functionality."*

The Solution

After a thorough evaluation and demonstration process, The Claroty Platform was chosen and deployed across the company's manufacturing operations comprising more than 75 factories in eight countries. Platform components utilized include:

- **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 industrial 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 EMC with IT security infrastructure.

Outcomes

CTD discovered and profiled all OT assets, many of which had been previously unknown to the company, rapidly and with unprecedented detail, resulting in comprehensive and unified visibility across the company's entire OT environment. This process was achieved without any downtime or operational disruption.

After achieving full visibility and baselining the company's OT environment, CTD enabled real-time anomaly and threat detection, vulnerability monitoring, and ongoing risk assessments. CTD's Root Cause Analysis and Risk Scoring features also enabled each of the company's SOCs to easily and effectively prioritize and triage the resulting alerts.

SRA eliminated direct interactions between remote users and network assets by enforcing a secure, single-access pathway for remote diagnostics and maintenance operations. This led to a dramatic increase in third-party risk, as well as security best practices across the entire OT environment. Meanwhile, SRA's auditing capabilities helped the company to improve change management by preventing undocumented and unauthorized changes within the 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**.

CONTACT US

contact@claroty.com