CLAROTY

Case Study

AUTOMOTIVE MANUFACTURING

Automaker Drives Towards Comprehensive Industrial Cybersecurity with Claroty

As the scope of an auto manufacturer's operation grows, the complexity of its security requirements often increases exponentially. Struggling to gain a unified view into its industrial cybersecurity posture, this large automaker initially tapped Claroty for its comprehensive OT, IoT, and IIoT asset visibility offering. This discovery led to a host of other benefits that ultimately helped the company improve availability, reliability, and safety across its entire OT environment.

Challenges

The company — like many others in its industry — sought a way to view, monitor and manage the security of its numerous production sites, each consisting of hundreds of assets, in order to proactively strengthen its industrial cybersecurity and more effectively manage the inherent risks.

1. **Complex and diverse attack surface:** Automakers typically have numerous factories, usually spread across a large geographic area, each comprising a wide range of networked devices. This poses a particular challenge in finding a scalable but consistent approach to industrial cybersecurity because the technical requirements for OT, IoT, and IIoT devices differ considerably across use cases and vendors.
2. **Unauthorized users and misconfigurations:** Operational complexity causes many automakers to struggle to effectively monitor and manage unauthorized remote access to OT environments. Furthermore, many also struggle to prevent unauthorized changes to OT, IoT, and IIoT assets, leading to misconfigurations and operational downtime.
3. **Lack of production-related alerting:** Industrial cybersecurity incidents are often difficult to detect until after they have already begun to impact production, which has a cascading effect on operations. Precise and automated alerting are necessary to allow staff to respond quickly and keep the plant operational.

Customer Quote

> *"We have a few dozen factory sites across two continents. That translates thousands of assets in our entire manufacturing operation, so you can imagine the challenge of establishing a confident industrial cybersecurity posture. Even just getting simple visibility of everything in our ecosystem is a huge challenge, and most solutions can't even do that basic thing very well. Of all the platforms we evaluated, only Claroty's was capable of giving us the unified view and total control we were looking for, and they did it with zero downtime. There honestly wasn't even a close second."*

The Solution

After a comprehensive evaluation process, The Claroty Platform was chosen and deployed across an automobile manufacturing operation spanning more than 40 factories across two continents. 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 potential misconfigurations and unauthorized users, including third-party contractors.
- **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, wherever appropriate.

Outcomes

CTD immediately profiled all assets in the company's network and provided a depth and volume of detail on each asset that was unmatched by any other vendor evaluated. This process was achieved without disruption to operational processes.

SRA eliminated direct interactions between remote users and network assets by enforcing a secure, single-access pathway for remote diagnostics and maintenance operations. This elimination of direct interaction led to a dramatic increase in security best practices across the entire OT surface.

By giving the company a unified view of all devices in the ecosystem, even legacy devices in use since before modern cybersecurity was a primary design consideration are identified, monitored and secured. This comprehensive OT, IoT, and IIoT visibility and real-time threat detection empowered the company to be proactive about protection against a much wider range of threats.

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