CLAROTY

Case Study

MINING

Global Mining Company Unearths Industrial Cybersecurity Simplicity with Claroty

A large and growing mining company with operations around the world, this company struggled to achieve a comprehensive view of its entire operational security risk profile. The integration of multiple remote sites, coupled with a wide range of legacy equipment in common use made this company, like many in the industry, eager to find a solution to simplify their industrial cybersecurity profile.

Challenges

As with most large mining companies, this multinational faced a challenge of securing overall operations from a central SOC all the way down to the site and process level. In this case, that meant finding a solution that would apply to a large and spread out series of operational control systems, while addressing the following concerns:

1. **Operational complexity:** Most mining companies operate in complex environments, involving multiple units from several operational technology (OT) vendors, across broad and often remote geographical areas. This company is no exception.

2. **Prevalence of legacy technology:** The company had been relying on fairly traditional, IT-centric security tools and legacy equipment. This fact, coupled with insufficient documentation of system and network resources, and compounded by the remote geographies of many sites, made the task of interrogating the system a particularly daunting one.

3. **Requirements for zero downtime:** Because of the company's size and complexity, their operations need to operate continually in order to function optimally. When systems go down even temporarily, losses can be difficult to recover, so installation of a security platform needs to be done without interrupting production.

Customer Quote

> *"We needed a very deep level of visibility into our industrial networks, and once we started our evaluation process, it quickly became clear that Claroty was the best choice. Not only were they the preferred vendor for all of our OT partners, but their technology really stood up to our rigorous demands. Their platform gave us visibility into things we didn't expect to see, and did so without compromising our production. No other platform we evaluated could offer us what Claroty did."*

The Solution

The Claroty Platform, which is backed and adopted by most of the leading industrial automation vendors, was deployed to protect the company's industrial networks from cyber-attacks, from a central SOC and down to 50 different production sites across three separate geographies. Platform components utilized include:

- **Continuous Threat Detection (CTD)** for full spectrum visibility, continuous security monitoring, and real-time risk insights with zero impact to operational processes and underlying devices. CTD's deep packet inspection technology extracts precise details about each asset on the industrial network, regardless of the device's underlying technology.
- **Secure Remote Access (SRA)** to safeguard the industrial networks from threats introduced via unmanaged and/or unmonitored access by remote users, including third-party vendors, contractors and technicians.
- **Enterprise Management Console (EMC)** to simplify the management of, and consolidate the data from all points in the OT network. The EMC provides a unified view of all assets, activities, and alerts across multiple sites. The Claroty platform also integrates seamlessly via the EMC with IT security infrastructure.

Outcomes

The Claroty Platform enabled the company to achieve the following:

CTD discovered and profiled all OT assets, asset details, and communication patterns and baselines at 50 production sites across three separate geographies within two weeks of deployment.

While CTD was established with zero downtime or interruption in production, its installation allows the company to scale up as necessary when new sites are brought online. The EMC gives the SOC teams the tools to filter, correlate and analyze data about the entire network, while augmenting their IT security knowledge with valuable and actionable insights about the industrial networks' security and risk posture as well.

SRA provides the company's contractors and remote users with a user-friendly, OT purpose-built interface through which they can connect remotely — and securely — to service OT assets. Meanwhile, the company's IT security team relies on SRA's customizable user access controls, permissions and auditing features to monitor, manage and minimize the risks inherent in remote access.

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.

CLAROTY

CONTACT US

contact@claroty.com