CLAROTY

Case Study

ELECTRIC UTILITIES

National Electric Generation & Transmission Company Secures Operations with Claroty

Power generation and transmission companies have considerable redundancy built into their operational technology (OT) environments. This redundancy helps power plants withstand sudden component failures, but it can exacerbate certain risks when combined with the complexity of a plant's OT network. This particular company, which serves millions of customers over a nationwide transmission network, looked to Claroty for help evaluating and minimizing these risks to ultimately preserve OT availability, reliability, and safety.

Challenges

Effectively securing its generation and transmission operations required the company to confront and overcome the following challenges:

1. **Inherently insecure OT networks:** Complex and widely distributed architecture, limited OT visibility, and inadequate security controls gave attackers hundreds of possible entry points into the company's OT networks.
2. **OT redundancy:** The redundancy of the company's OT environment meant that attacks were typically only detected if they caused immediate, easily noticeable damage. As a result, small-scale attacks usually went unnoticed despite aggregating substantial damage—and posing substantial risks to OT availability, safety, and reliability—over time.
3. **Heavy reliance on OT remote access:** The company's power plants utilize a large number of unmanned power generation units and also rely on multiple vendors to maintain and service their heat recovery generation systems (HRGS). Remote access to each plant's OT environment is frequent among both plant staff and third-parties as a result. Such remote connections, however, presented serious risks because the company lacked the ability to properly secure, authorize, and monitor them.

Customer Quote

> *"We were looking for a technology partner who could help us get a highly detailed visibility into our OT network. We needed information on all of our operational assets at a granular level: from the vendor, firmware, model, serial number and card slot information, down to the code information running on the power line communications. We evaluated several vendors, and only Claroty was able to give us the deep visibility feature set we required. What's more, they were able to identify each and every asset in our environment literally within minutes, without any impact to our infrastructure."*

The Solution

The company deployed The Claroty Platform on top of its existing infrastructure and utilized 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 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 EMC with IT infrastructure.

Outcomes

The Claroty Platform enabled the company to achieve the following:

Full visibility and immediate profiling of all assets across the OT networks at each of its power plants.

Continuous, real-time assessment and reporting of the company's overall OT risk profile automating and expediting what was once a tedious manual process.

Comprehensive alerting and root-cause analysis mechanisms that enable the company's security operations center (SOC) to know precisely when and why any anomalous or malicious activity occurs anywhere in any of its power plants' OT networks.

The ability for its plant staff and third-party vendors to remotely access its OT environments securely and only as needed, when fully authorized, and while being monitored in real-time.

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