CLAROTY

Case Study

WATER UTILITIES

Water Supplier to More than 2 Million People Secures Operations with Claroty

A U.S.-based water utility charged with delivering a safe, reliable supply of water to more than two million residents across several counties was upgrading its IT infrastructure and modernizing its IT security architecture. The time was right to assess and enhance security across its expansive and growing operational technology (OT) environment, which includes hundreds of miles of pipeline and more than 20 physically dispersed water facilities, including pumping stations, water treatment plants, and storage and distribution systems throughout the region.

Challenges

1 **Lack of asset visibility:** Water utilities are inherently geographically dispersed with facilities and devices located across the area they serve. The large physical footprint combined with the company's rapidly growing infrastructure to support population and business growth in the region, resulted in inconsistent documentation of OT, IoT, and IIoT assets and lack of full visibility into the OT environment to detect potential threats and vulnerabilities and mitigate risk.

2 **Remote, unmanned facilities:** Many of the company's pumping stations and other facilities are unmanned. Employees and third-party vendors access these systems to perform remote maintenance and gather operational data. Systems, switches and controllers may be compromised if the authorized parties' systems are infected with malware, their access credentials have been stolen or they otherwise don't uphold adequate security hygiene. Further exposing these systems to risk, the company had no way to ensure that only authorized parties were accessing appropriate systems and making agreed upon changes.

3 **Compliance with new regulations:** Under America's Water Infrastructure Act (AWIA), utilities that provide drinking water must conduct risk and resilience assessments and revise emergency response plans. These changes require a detailed understanding of their industrial network in order to meet the U.S. Environmental Protection Agency (EPA) deadline in 2020. The water provider needed additional visibility and data to comply with the new mandate.

Customer Quote

> "We're primarily a Rockwell shop and were really impressed with the continuous threat monitoring the Claroty Platform provides across our entire OT environment so we can remediate before it's too late and with minimal impact to our operations. We also have greater confidence that workers who are off-site but regularly need remote access to our systems to do their jobs can do so without introducing risk. We even gained an unanticipated benefit – during the pandemic we were able to pivot quickly to support the surge in staff needing to work from home. It's great to know we can flex again if necessary."

The Solution

The water supplier deployed the Claroty Platform on top of its existing infrastructure and utilized the following components:

- **Continuous Threat Detection (CTD)** for full spectrum OT, IoT, and IIoT visibility, continuous security monitoring, and real-time risk insights with zero impact to operational processes and underlying devices.
- **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 management at scale, consolidating data from Claroty products and provide a unified view of assets, activities, and alerts across multiple sites. The Claroty Platform also integrates seamlessly via the EMC with the company's newly deployed IT security infrastructure.

Outcomes

Full visibility and immediate profiling of all assets across the company's expansive OT environment. The IT security, network and OT teams now have granular details of all assets, sessions, processes, and corresponding risk levels, to identify threats and vulnerabilities in the industrial network to mitigate risk and assure continued operations of critical processes.

Secure OT remote access. Staff and third parties can access systems to do their jobs from wherever they are. While security teams have granular control, the ability to audit access, and additional levels of security, such as password vaulting, to enforce stringent security hygiene and mitigate risk. Unauthorized access is immediately blocked, and unusual network activity triggers an alert to the team.

Compliance with the AIWA mandate. The water utility was able to submit to the EPA by the deadline of March 31, 2020. The Claroty Platform gave them the tools necessary to conduct the appropriate risk and resilience assessment according to the new requirement.

Optimization of IT security, network, and OT teams. The Claroty Platform integrates with the company's ecosystem of OT and IT systems and workflows, so all teams can use the solution to strengthen security – lowering total cost of ownership (TCO) while maximizing return on investment (ROI).

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