CASE STUDY

FOOD & BEVERAGE

Global Food & Beverage Company Achieves Secure Digital Transformation with Claroty

A global food and beverage company was proud of how its digital transformation initiatives were increasing productivity and efficiency. The company knew it could multiply these benefits by extending digital innovation and connectivity to its plants and bottling partners worldwide to see production anytime, anywhere. However, the company also knew it had to do this securely, which meant gaining visibility into its operational technology (OT) networks so its security teams could see threats anytime, anywhere as well.technology (IT) and operational technology (OT) environments.

Challenges

The company had prioritized its use cases to address the top three areas of risk that threatened the continuous operational availability, safety, and reliability of its production environment:

1. **Malware infection:** While the convergence of IT and OT networks unlocks business value, it also can give rise to new risks. Without proper controls in place, both targeted and non-targeted threats can maneuver from IT to OT environments. The potential spillover from a malware attack to OT networks can be costly — disrupting or halting production while creating safety and compliance issues.
2. **Threat from third-party remote access:** External vendors remotely access plants' OT networks to service machinery. This exposes the systems and controllers on the shop floor to potential compro mise if the authorized party's systems are infected with malware, their access credentials are stolen, or they otherwise don't uphold adequate security hygiene. The company also needed visibility into unauthorized as well as inappropriate use of access.

3. **Change in controller operation at remote facility:** The company's water treatment facility is physically isolated from the plant. The systems that run the facility operate the same way every day. Any change could indicate a threat of contamination to the water, but the company lacked granular visibility into these systems to understand and explain changes.

The Solution

After a rigorous evaluation, the company selected Claroty as its partner for converged IT/OT security. The Claroty Platform was deployed on top of the existing infrastructure at each plant and bottling facility and then integrated with the security information and event management (SIEM) technology used by the company's security operations center (SOC). As part of The Claroty Platform, the company deployed:

- **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 an 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 company now has end-to-end (IT/OT) playbooks for each use case. Using an integrated SOC, IT and OT teams can collaborate to detect threats, mitigate risk, and remediate to bring devices back into compliance with security policy while limiting operational disruption.

Malware infection: CTD identifies a potential threat and issues a ticket to the SOC for investigation. Gathering data from the OT network using CTD, the IT and OT teams work together to confirm infection. Playbooks vary depending on the device and impact. For example, an infected engineering workstation is isolated to prevent the spread of malware while teams continue investigation. If controllers are infected, IT works with OT policies and procedures to remediate while mitigating disruption.

Threat from external access: SRA limits authorized user activity to specific OT assets while remaining segregated from the IT network. SRA also blocks unauthorized parties accessing the shop floor. Concurrently, CTD monitors privileged users for unusual activity and, when it detects baseline deviations, sends alerts to the SOC. User sessions are stored for forensics if suspicious activity emerges later.

Change in controller operation at remote facility: CTD generates a behavioral pattern that characterizes legitimate traffic and monitors for configuration changes. Deviations trigger alerts to the SOC which are escalated for investigation and response. Shutdown is up to individual control room internal policies and procedures. By protecting OT environments, the food and beverage leader is extending the value of its digital transformation initiatives across the global enterprise. With playbooks in place to address its top risks, the company is looking at also using The Claroty Platform to support vulnerability management and reporting requirements.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.