CLAROTY

CASE STUDY

AIR TRANSPORTATION

One of World's Busiest Airports Securely Connects OT Environment with Claroty

One of Europe's busiest airports transports more than 50 million passengers and more than 2.5 million tons of cargo a year, serving as a main hub for freight shipments as well as forwarding and courier companies. A vital link to getting goods to destinations in more than 100 countries, the airport needed greater visibility and control over its expansive operational technology (OT) environment. This includes miles of automated conveyor belts that enable the reliable movement of cargo, and critical internal infrastructure systems that help ensure the safety and productivity of thousands of employees.

Challenges

- **Digitization**. Increasingly, shipping companies expect real-time visibility into the status of their shipments within the airport – whether cargo has arrived, is being processed, or has been dispatched. Inputs from conveyor systems need to be connected to shipment management systems to provide accurate and timely status updates. Airport operators also need real-time visibility into automated conveyor systems to monitor operational uptime and performance. Additionally, connectivity across internal infrastructure – between security cameras, fire detection systems and tens of thousands of sensors, HVAC and power systems – allows operators to quickly detect and respond to emergencies and failures. But they needed a level of assurance that each of these connections was secure.
- **Aging systems**. Some critical airport OT systems still dated from the 1980s and 1990s when the airport was modernized initially. Never designed to be connected, these older, legacy systems were now being connected to newer, digitized, and sometimes cloud-connected systems. Having been in place for decades, they lacked even basic security controls. The risk of disruption and downtime to implement a new security control, a patch or a system upgrade (if even available and deemed to be effective) had to be carefully managed so as not to interfere with operations.
- **Third-party access.** Multiple vendors were responsible for maintenance of critical infrastructure – monitoring performance and servicing the control systems for conveyor belts and building operations assets. Vendors accessed these systems remotely via a VPN which secured the connection itself. But once third parties were inside the network, airport operators had no way to ensure that only authorized personnel were accessing appropriate systems, performing agreed upon activities, and were not inadvertently introducing malware or other risks due to inadequate security hygiene practices.

CUSTOMER QUOTE

"As we accelerated our digitization initiatives, our ad hoc approach of connecting systems was insufficient. We needed visibility into the risks associated with each connection – every device, user, and on-premise and cloud system – and a strategy for how to approach this safely. The planned addition of a new security camera system added to the urgency. We didn't have the luxury of a multi-year rollout. Of all the vendors we evaluated, only Claroty could provide us immediate asset visibility and continuous threat monitoring so we could identify risks and take action before any measurable impact to operations."

The Solution

After an extensive evaluation, the airport operator selected Claroty as its partner to secure both its critical, automated cargo movement operations and internal infrastructure, utilizing the following components of the Claroty Platform:

- **Continuous Threat Detection (CTD)** for full spectrum IoT and OT 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 unmanaged and unmonitored access by remote users, including third-party vendors and employees.
- **Enterprise Management Console (EMC)** to simplify management at scale, consolidating data from Claroty products and providing a unified view of assets, activities, and alerts across multiple gates and facilities. The Claroty Platform also integrates seamlessly via the EMC with IT security infrastructure.

Outcomes

Full transparency, visibility, and asset profiling across the airport's entire OT environment to manage risk. For example, airport operators quickly discovered devices connected to the Internet that didn't need to be and were able to cut those connections right away. They can better manage and prioritize system upgrades and patches based on connectivity levels and insights into vulnerabilities that are being exploited in the wild. And they can optimize shipping performance by monitoring conveyor belt systems and, based on age, know if one may be less reliable than another and take action as needed.

Managed and secure remote, third-party access. Vendors can seamlessly access systems remotely, while security teams have granular control over remote sessions, specifically the ability to manage the who, what, and when of access to devices and systems. Additional levels of security such as vaulting credentials to prevent password-sharing and alerts notifying the team to unusual network activity, further mitigate risk.

Integration with IT for holistic risk management and secure digitization. With a single interface, the control room has centralized visibility of different systems across different departments and gates throughout the airport. Data is aggregated so that operators can quickly see where issues are coming from – an internal or external connection – if they have spread, and how to mitigate them.

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.

CONTACT US

contact@claroty.com