CASE STUDY

Armis Centrix™ Enhances IT and OT Asset Visibility and Security for Leading Poultry Processor

The Challenge

- Limited visibility into the plant's Operational Technology (OT) network
- Fragmented and siloed asset data from multiple vendors
- Lack of comprehensive monitoring of network traffic and device activities
- Inefficient manual processes for identifying and managing assets

The Solution

- Deployed Armis Centrix™ across the entire OT and IT infrastructure
- Integrated Armis Centrix™ with Microsoft Azure, VMware, and other existing tools
- Implemented real-time monitoring and alerting for all network-connected devices
- Created tailored dashboards and automated reporting for better management

The Results

- Identified and tracked 4,500 assets, over four times more than the estimated 1,000
- Improved response time for network investigations, reducing from 1 hour to 5 minutes
- Enhanced visibility and control over OT devices, reducing risks of unmonitored changes
- Streamlined audit preparation and compliance reporting with accurate real-time data

Industry Manufacturing

Location Nebraska

Number of employees 1100

Armis Centrix™ for OT/IoT Security

Background

A large poultry manufacturer, established in 2016 in collaboration with a major warehouse retailer, operates a vertically integrated chicken processing facility in Nebraska. With 1,100 employees spread across four buildings and a daily processing capacity of 400,000 chickens, the facility includes a hatchery, feed mill, and processing plant, all crucial to supplying quality products to customers. The IT Network and Systems team, led by their Operations Manager, faced significant challenges in gaining visibility and control over the company's extensive and diverse asset landscape, particularly within the OT environment.

The Challenge

Despite having a solid grasp of the IT assets within their office environment, the poultry manufacturer struggled with limited visibility into their OT network. The OT environment was a "black box," primarily managed by various vendors who operated independently, leaving the IT team with little knowledge of the connected devices, their functions, or the traffic they generated. OT equipment consisted of workstations, conveyors, chain controllers, transfer stations, marination machines, case sealers, case labelers, and a variety of sensors, PLCs, and controllers.

"Our plant's OT network was a big unknown," the IT Operations Manager explained. "We had a very limited idea of what devices were connected, what

"Armis Centrix™ has transformed our approach to managing our IT and OT environments. The visibility it provides is unparalleled, and it's now a critical tool for ensuring the security and efficiency of our operations."

IT Operations Manager
Large Poultry Processor

they were doing, and how they were interacting with each other. It was a serious vulnerability that we needed to address."

This lack of visibility presented significant risks. The IT team couldn't efficiently monitor or manage OT devices, leading to concerns about potential vulnerabilities and the inability to quickly address issues. There was also the added concern of any process to effectively prioritize security findings according to genuine risk. The company's initial attempts to manually track assets and monitor network activities were cumbersome and time-consuming, with investigations often taking hours to complete.

The Solution

To overcome these challenges, the company deployed Armis Centrix™ for OT/IoT Security. The solution was recommended by their major retail partner, who had implemented it across their facilities. The deployment was swift, with the IT team setting up Armis Centrix™ across the entire plant and office network.

Within the first few weeks, they added multiple network test access points (TAPs) and integrated Armis Centrix™ with existing tools such as Microsoft Azure, Microsoft Intune, VMware, Microsoft Active Directory and Entra ID, Cisco network infrastructure, and their network access control system.

These integrations allowed the IT team to unify and correlate asset data across different platforms at the outset, enhancing their ability to monitor and manage both IT and OT environments efficiently from a single, centralized platform. An immediate benefit was enrichment of programmable logic controller (PLC) data gathered from Rockwell engineering workstations connected to the OT network. The seamless integration also ensured that existing security policies and compliance standards could be monitored across all systems.

"The deployment of Armis Centrix™ significantly improved our operations," the IT Operations Manager noted. "We were able to quickly integrate it with our existing tools, and the platform's ability to automatically identify and classify every connected device in real time, including OT devices, provided immediate value."

One of the major advantages of Armis Centrix™ was its ability to provide real-time monitoring and alerting for network-connected devices. This feature allowed the IT team to proactively monitor the network for unusual activities, such as unauthorized device connections, unexpected changes in device behavior, and new devices—especially in the OT environment. The platform's design utilizes multiple discovery methods including Smart Active Querying to ensure that there is no risk of downtime during deployment and beyond, a critical factor for ensuring uninterrupted operations.

The Results

The deployment of Armis Centrix™ brought immediate and significant improvements to the company's IT and OT operations. The platform identified and tracked 4,500 assets—more than quadrupling the original estimate of 1,000. This comprehensive visibility into the network allowed the IT team to reduce the time required for network investigations from an hour to 5 minutes, enhancing overall efficiency.

"Before Armis, finding a specific device on our network could take up to an hour," the IT Operations Manager recalled. "Now, with all the data centralized in one place, it only takes a few minutes. It's made a huge difference in how we operate and has made network investigations more efficient."

Armis Centrix™ also played a critical role in improving the company's security posture. The IT team now receives real-time alerts about unauthorized changes to OT devices, helping them quickly address potential issues before they escalate. This capability is particularly valuable during audits, enabling the team to easily demonstrate compliance and provide detailed reports on the state of their assets, especially end-of-life (EOL) devices. Additionally, Armis

Centrix™ supports business and operational continuity by curtailing outages.

“We had an instance where a few misconfigured phones ended up on the wrong side of the firewall,” the IT Operations Manager shared. “Armis Centrix™ picked them up right away, and we were able to resolve the issue before it became a bigger problem.”

In addition to these operational benefits, Armis Centrix™ has also laid the groundwork for future security enhancements. The IT team plans to collaborate with the automation team to standardize firmware versions across OT devices, further reducing vulnerabilities and ensuring the continued safety and reliability of the manufacturing process.

4,500 assets identified and monitored, more than 4 times the original estimate

91% Network investigation time reduced from 1 hour to 5 minutes

Real-time alerts for unauthorized OT device changes

4+ audit reports generated effortlessly

ARMIS®

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011
www.armis.com