CLIENT STORY

# MicroAge and Armis Transform Operational Visibility for Specialty Food Manufacturer

## THE CHALLENGE

A midsized specialty food manufacturing company, boasting a workforce of 1200 individuals spread across four physical locations, encountered mounting difficulties in overseeing its OT network infrastructure. The lack of necessary visibility presented substantial risks, such as potential security vulnerabilities, uncharted system interactions between internal and third-party systems, and complications in device tracking, configurations, and troubleshooting. Additionally, network maintenance grew progressively challenging due to frequent software updates by both the internal team and manufacturing operational partners.

"We didn't know what we didn't know, and for an IT team in manufacturing, that will keep you up at night," stated the company's IT Operations Manager. "We might get an alert saying something is wrong, but the alerts were often vague, so troubleshooting through to a resolution could take hours or longer. We really didn't have a clear sense of what 'normal' was supposed to look like with respect to all the various systems communicating with each other on the network. That meant it was just impossible to know if the network chatter was supposed to be there or not, and that's a really uncomfortable place."

## TECHNICAL ENVIRONMENT

The Specialty Manufacturing Company operates a fairly traditional technology infrastructure that relies heavily on Microsoft, VMware, and Cisco. For its manufacturing operations, it utilizes an industry-standard manufacturing execution system (MES) and a supervisory control and data acquisition system (SCADA) composed of software and hardware.

While the technology environment was designed to streamline operational processes on the plant floor by gathering data from all systems and controllers, it had become so complex that it began hindering end-to-end visibility.

## THE SOLUTION

The MicroAge team collaborated with IT leadership to effectively assess the challenges and better understand the OT network's blind spots across hardware, software, endpoints, and controls. After the discovery process, MicroAge reviewed potential solutions to determine an ideal fit with Armis, a MicroAge partner and proven solutions provider offering operational network security systems.

Specifically, the Armis Centrix™ for OT/IoT Security solution was chosen due to its proven ability to extend network visibility and security across a wide range of systems and devices. It creates a 360-degree, 24/7 view of all network activity while seamlessly integrating with existing operational systems.

With MicroAge, you can innovate faster with one end-to-end technology services and solution partner. Call us at 800-544-8877 or visit microage.com

MicroAge®

CLIENT STORY

> From a monitoring network traffic perspective, the Armis system does wonders in terms of being able to now see our ‘east/west’ traffic, which was murky at best before. We had decent ‘north-south’ visibility due to the firewall, but now we truly have 360-degree network visibility. And yes, I can honestly say… it helps me sleep better at night.
>
> — IT Operations Manager, Specialty Food Manufacturing Company

## THE SOLUTION (cont.)

Now, the company dashboard integrates data from all operational devices and systems, providing a clear view of device interactions, configurations, potential security threats, and all users interacting anywhere on the network. This occurs without any downtime or network congestion— all critical to maintaining production levels for daily operations.

MicroAge solution architects completed the initial discovery and assessment process in just one week. Once the team identified the Armis solution as a fit, the implementation process was completed within hours, including integrations with various systems like Azure/Microsoft 365, InTune, VMware, and Active Directory, as well as physical appliance setup. This provided quick visibility into the company’s entire infrastructure and recognized ROI almost immediately.

Now, the company has a specific and detailed line of sight into all the manufacturing devices and network communications, including programmable logic controllers (PLCs), enabling them to monitor for any changes made to these critical systems in near real-time. Beyond network traffic visibility, the Armis system helps identify and log users who make changes anywhere in the system, including internal staff and 3rd party contractors. This reduces troubleshooting time to a fraction of what it was previously.

MicroAge and Armis delivered a comprehensive solution, including a discovery assessment and implementation, to enhance network visibility and control, reducing exposure to cyber threats. Armis' passive data collection approach minimized disruption to existing systems and traffic.

## THE BENEFITS

The fast implementation of the Armis solution provided real-time visibility into every device and system as well as ‘east/west’ traffic. Now, the company can easily monitor for any unauthorized changes and potential security risks and access a change log history down to the minute and user.

Such enhanced visibility dramatically improves security and streamlines troubleshooting, reducing downtime and operational inefficiencies.

As their IT Operations Manager noted, "**Our alert investigation troubleshooting time went from around 30 minutes down to 1 to 2 minutes. That’s about a 93% reduction**, which not only means less manufacturing downtime and potentially missed production goals but also means our IT team is freed up from alerts and can spend more time running the business. It is truly life-changing.”

You don't have to go it alone. Find out how MicroAge can take the pain out of researching the best fit for your unique cybersecurity needs. Call us at 800-544-8877 or visit microage.com

MicroAge®