



CASE STUDY

Medical Device Customer Enhances Asset Visibility, Risk Management, and M&A Integration with Armis Centrix™



The Challenge

- Incomplete visibility into IT, IoT, and OT assets
- Difficulty identifying unmanaged devices across regions and mergers and acquisitions (M&As)
- Limited automation for asset discovery and risk management
- High regulatory pressure and risk of operational disruptions in production

The Solution

- Deployed Armis Centrix™ for real-time asset management
- Integrated Armis across converged IT, IoT, and OT environments
- Automated risk analysis and reporting at production sites
- Streamlined integration of acquired companies

The Results

- Achieved full visibility into all assets, including unsanctioned OT connections
- Enhanced production site security through real-time risk assessments
- Simplified integration of M&As with full asset visibility
- Improved operational efficiency and continuity through automated monthly key performance indicators (KPIs)

Industry **Medical Devices**

Location **Sweden**

Number of employees **1900**



Armis Centrix™ for Asset Management and Security



Armis Centrix™ for OT/IoT Security

Background

This medical device company is a global leader in manufacturing customized electric wheelchairs and other advanced medical assistive devices for individuals with disabilities. The company is driven by a mission to empower independence through innovative, personalized mobility solutions. With approximately 1,900 employees worldwide, the company faces the challenge of managing assets across various regions and integrating newly acquired companies. The need for complete visibility into both managed and unmanaged devices, including IT, IoT, and OT, is critical for ensuring continuity and availability for production sites, minimizing interruptions, protecting against various forms of intrusions, and maintaining regulatory compliance.

The Challenge

The CISO faces the daily challenge of balancing strategic and operational responsibilities with a relatively small IT team. Like many companies today, it is increasingly focused on digitizing its operations, which means security is essential to its core business. One of the CISO's key concerns was the lack of visibility into the company's technology assets, particularly unmanaged devices such as IoT and OT, across its production sites. Without a full inventory of these assets, the IT team struggled to prioritize security efforts, leaving potential vulnerabilities unaddressed.

The company also regularly acquires new companies, adding complexity to its asset management. Integrating these new companies into their current

“Armis provides us with real-time visibility and control over our assets, allowing us to proactively manage security risks and improve our operational efficiency.”

CISO,
Medical Device Company

ecosystem was a resource-intensive process, further complicated by the lack of automated tools to identify assets and monitor risks across diverse environments.

“Before using Armis, we didn’t have full visibility into our assets, making it hard to set priorities for security and manage risks effectively,” the CISO explained. Additionally, regulatory pressure has been increasing, making it crucial for the company to maintain operational continuity and minimize interruptions, especially at its production sites.

The Solution

To address these challenges, the company turned to Armis Centrix™ for Asset Management and Security and Armis Centrix™ for OT/IoT Security. The Armis AI-driven Asset Intelligence Engine automates real-time asset discovery across IT, IoT, and OT environments, providing a comprehensive and accurate view into all assets and reducing the risk of human error that comes with traditional approaches to asset management. The engine utilizes a data lake of over 5 billion assets globally to set highly accurate behavioral baselines and provide critical context for anomaly detection. By integrating Armis into its environment, the company has gained the ability to manage vulnerabilities and monitor network activity in real time. Beyond generating alerts, Armis also triggers automated actions to stop attacks in their tracks.

Unlike traditional cybersecurity scanning solutions, Armis Centrix™ for OT/IoT Security has eliminated blind spots in the company’s OT and IoT environments by collecting extensive, highly granular, and always up-to-date information about all these assets—managed and unmanaged devices—without disrupting the operations of the manufacturing environment.

The flexibility and ease of implementation of the Armis platform contributed to the success of the deployment. The company’s relatively small IT organization was initially concerned that it would not have the capacity to support the rollout of a new platform. However, Armis made the implementation process straightforward by working closely with the company’s internal network and communication specialists.

“Armis quickly became a key part of our daily work, helping us manage our assets in real-time across all regions,” the CISO stated. The platform’s automated risk analysis at production sites has enabled the identification of unsanctioned connections, significantly improving security. Moreover, the company now uses Armis to produce monthly KPIs for each region, providing valuable insight into the company’s overall security posture.

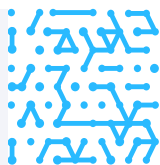
The Results

The company’s adoption of Armis Centrix™ has benefitted the organization in multiple ways. First, the platform provides real-time asset management across IT, IoT, and OT environments. This real-time visibility reduces the risk of missing assets or security gaps and ensures that all regions are continuously monitored.

Second, Armis has strengthened security at the company’s production sites by automatically identifying potential vulnerabilities and providing risk analysis. “Nothing escapes detection with Armis,” the CISO noted. “This proactive approach has minimized the risk of disruptions, helping the company maintain operational continuity.”

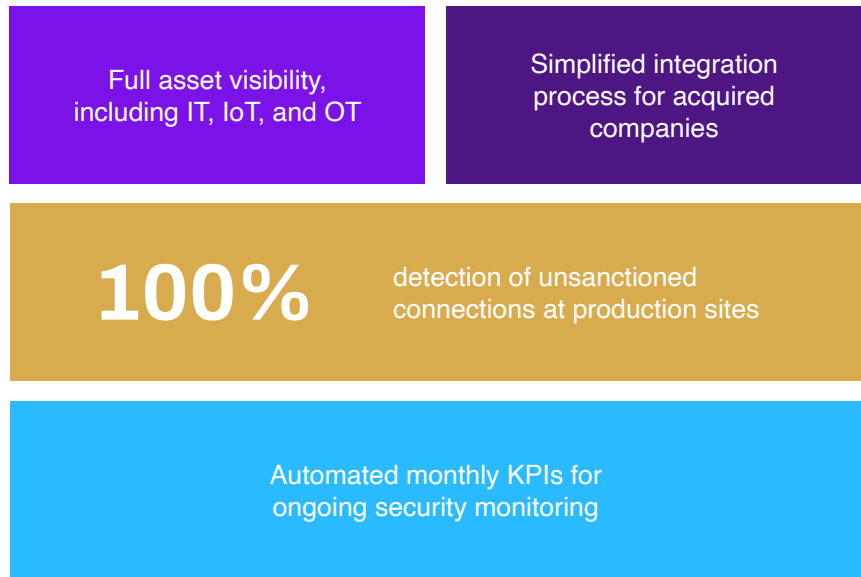
Armis has also greatly simplified the process of integrating newly acquired companies. The company now has full visibility of all assets from M&As on day one, ensuring that potential risks are identified and mitigated before full integration. This has significantly reduced the time and resources required to bring new companies into the company’s ecosystem.

Finally, the platform’s automated monthly KPIs have improved the company’s



operational efficiency across its regions. These KPIs are used to track and report vulnerabilities, risks, and asset statuses to management. "We regularly follow up and report the status to our management," the CISO explained. This system has enabled the manufacturer to prioritize its security efforts more effectively and respond faster to potential risks." For example, she pointed out that Armis has helped identify unsanctioned OT connections at production sites, allowing them to proactively address security gaps before they impact operations.

Thanks to Armis, the company now enjoys increased efficiency, enhanced security, and improved oversight across its global operations. "We feel much more in control of our current security situation, and Armis will continue to provide value as we expand and evolve," the CISO remarked.



1.888.452.4011
www.armis.com

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.

