



Armis Centrix™ for Manufacturing

Take charge of your critical infrastructure networks and manufacturing OT/IoT assets to ensure uptime. Build effective and comprehensive security strategies that keep you compliant, help you manage vulnerabilities and supercharge ROI.

Protect and Manage Complex IT/OT Manufacturing Environments With Armis Centrix™

Traditional cybersecurity is ineffective in industrial environments. This is particularly pertinent in Manufacturing, with a complex web of IT, OT, and IoT assets needing interconnectivity to remain functional. Armis Centrix™ delivers the ability to manage the lifecycle these assets and their users across sprawling environments.

Designed To Address Expanding Attack Surface

Powered by our AI-driven Asset Intelligence Engine, Armis sees your entire attack surface holistically. Through telemetry data and deep packet inspection, active querying, integrations with your existing solutions, active discovery and collective intelligence gathered from our extensive multibillion asset engine. Now you can:



See

Discover, contextualize, enrich and profile every asset



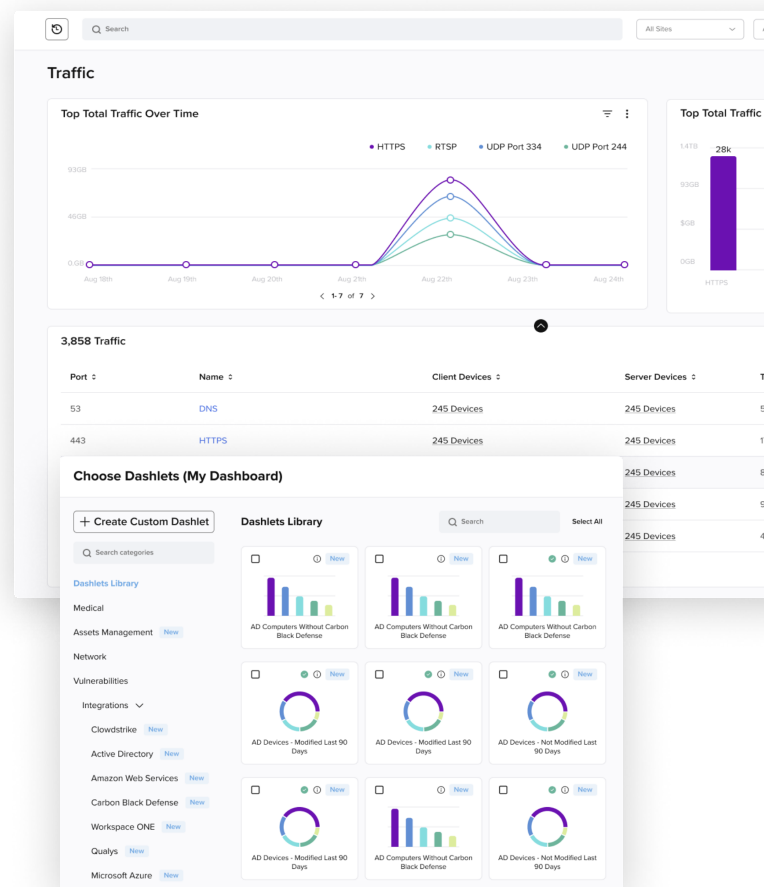
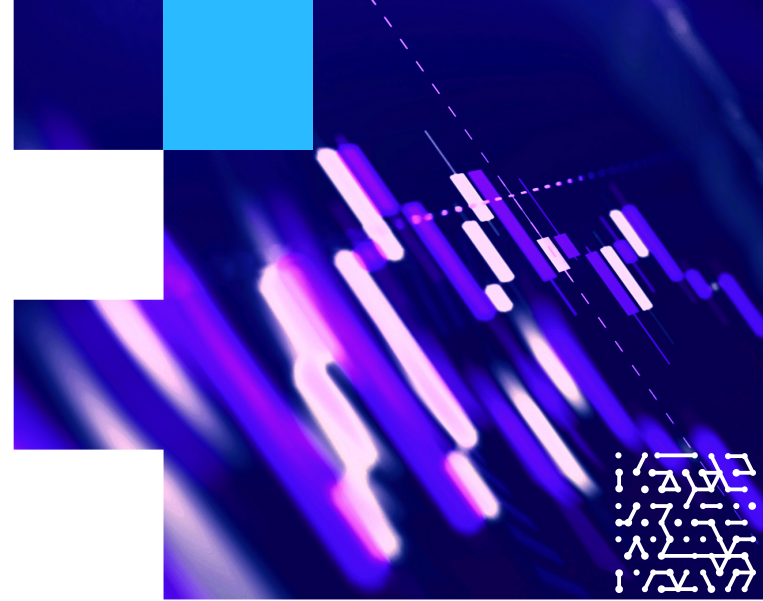
Protect

Take measures and prioritize efforts against all exposures



Manage

Establish workflows and track risk reduction



Supercharge your Critical Infrastructure with Armis for Manufacturing Use Cases:

Complete IT and OT Device Visibility in Industrial Environments

Employing agent-based or scanning-based tools for perpetual asset discovery poses potential disruptions to these devices. Armis Centrix™ uses a holistic asset discovery approach to gather deep knowledge and context of all assets without risk to uptime.

Protect Critical Data with Proactive OT/IoT Environment Hygiene

Use industry best practices and take a proactive stance against data loss. See all the known – and unknown – relationships between your devices and segments, including connections to unmanaged assets, rogue networks, and unauthorized communication channels.

Prioritize Risks and Accelerate Incident Response Remediation

For manufacturers, data breach incidents can be extremely costly. It is critical to identify compromised devices that are connected to the network to prevent spreading or exploitation.

Protect against IP Theft

For manufacturers, data breach incidents can be extremely costly. It is critical to identify compromised devices that are connected to the network to prevent spreading or exploitation.

Adhere to Manufacturing Compliance Standards

With comprehensive visibility into asset security, Armis Centrix™ evaluates compliance with security policies, regulations, and guidelines such as the IEC 62443 framework.



Key features that make Armis the go-to platform for total exposure management.

- Full representation of Purdue Model including assets, communications and potential violations.
- Complete non-intrusive discovery exposing legacy software that current tooling is unable to detect.
- Create an up-to-date inventory of which applications are deployed on which assets.
- Bridge the IT/OT gap. Air gapping is no longer a valid means of securing your environment.
- Create policies and queries that highlight boundary violations, then automate your segmentation processes with intelligent recommendations.
- Agentless solution which works with all devices, managed and unmanaged, IT or OT/ICS.
- Assist your zero trust validation. This framework ensures that all devices and users are continuously verified.
- Define segments for IT/OT areas of your organization and ensure you're communicating across segments.
- Identify any abnormal or risky activity with network baseline rules.
- Monitor connectivity and track asset behavior. Create a real-time network baseline.
- Monitor and audit changes of ICS assets.
- Track and report on errors produced by ICS assets and misconfigured ICS assets.
- Smart Active Querying to safely deep dive into asset visibility through smart querying.
- Actionable Threat Intelligence Feed included with Armis Centrix for OT/IoT Security allows you to leverage our dark web insights.



Why the Manufacturing Industry is Trusting Armis to Deliver Better Outcomes

- 1 ROI with production agility and efficiency, resources can be used more effectively.
- 2 Cyber resilience with complete asset discovery ensures visibility of all assets connected into your organization.
- 3 Future-Proofed cybersecurity with Armis, organizations are ready for future digitalization.
- 4 Operational resilience with Armis for Manufacturing, organizations are reducing ransomware attacks on their networks.
- 5 Compliance and safety across the entire production process in manufacturing and critical Infrastructure.
- 6 Reputation and trust. Organizations using Armis for Manufacturing are industry leaders upholding best cybersecurity practices.
- 7 Speed of Deployment is critical in manufacturing where quick resolution and reduction of risk is a high priority.

