Armis Centrix™ for Automotive (Auto Manufacturing)

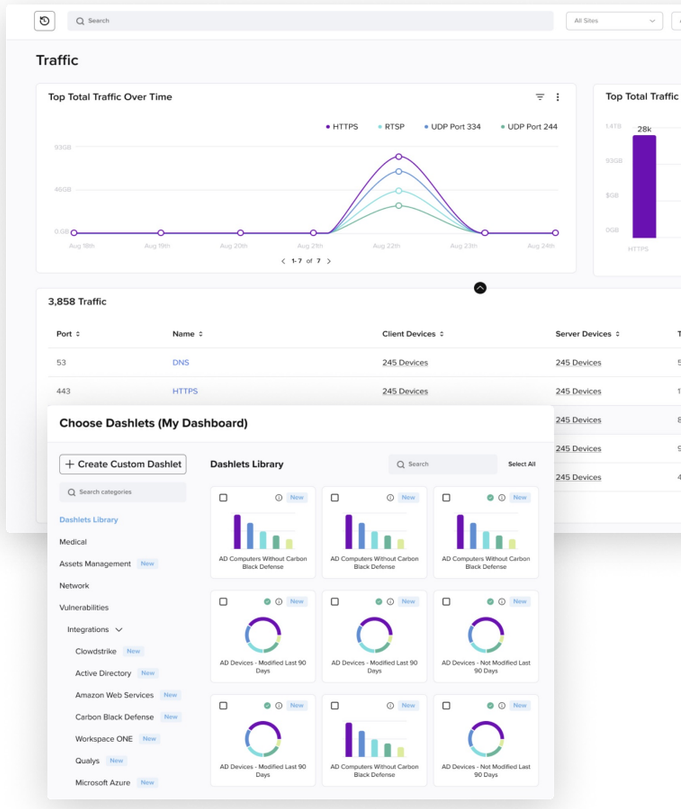
Take charge of your critical infrastructure networks and Auto Manufacturing assets to ensure uptime. Achieve improved sustainability and efficiency, whilst handling the new associated cyber security risks and managing vulnerabilities.

Preventing Supply Chain Down Time in the Auto Manufacturing Industry with Armis Centrix™

Traditional cybersecurity is ineffective in ICS environments. This is particularly pertinent in auto manufacturing with a complex web of IT, OT, and IoT assets needing interconnectivity to remain functional. Armis Centrix™ delivers the ability to protect, monitor and manage these assets and their users across critical environments.

Designed to Protect Critical Infrastructure and Manage Legacy Systems

Powered by our AI-driven Asset Intelligence Engine, Armis sees your entire attack surface holistically. Through integrations with your existing solutions, telemetry data to add deep packet inspection, active querying and asset behaviour and collective intelligence gathered from our extensive multibillion asset database. 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 Automotive Use Cases:

Complete, Real-Time Visibility Into Entire Estate
Automotive OT environments can contain a mix of IT, OT and IoT assets. Armis Centrix™ provides an automated real-time asset inventory of exactly what is in your network. Armis leverages its own proprietary asset intelligence engine that contains profiles of over 4 billion assets. It provides known profiles for each asset and can append data where appropriate to provide unparalleled intelligence on each and every asset

Efficiently Address Vulnerabilities
Armis Vulnerability Prioritization and Remediation (ViPR) offers risk based vulnerability management that enables security teams to quickly identify and remediate the vulnerabilities that are most likely to be exploited and negatively impact the business.

Achieving Adherence To Regulations and Security Frameworks
To comply with IATF, NIS2, ICA/IEC 62443, MITRE ATT&CK and ISO standards, maintaining a proper paper trail is essential. Armis Centrix ™ provides deep awareness of every device's state and characteristics, accurate matching with vulnerability knowledge bases, and real-time capture of deviations.

Maximize Productivity
With process integrity Streamline your journey to ROI without compromising on security.

Securing the Entire Supply Chain
and third party interconnections requires real-time control and precision. Implementing security measures without causing delays or disruptions in the production process is crucial for maintaining efficiency.

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 Automotive 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 Auto Manufacturing organizations are reducing ransomware attacks on their critical infrastructure.
5. Compliance and safety across the entire production process in manufacturing and other OT/ICS industries.
6. Reputation and trust. Organizations using Armis for Auto 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.