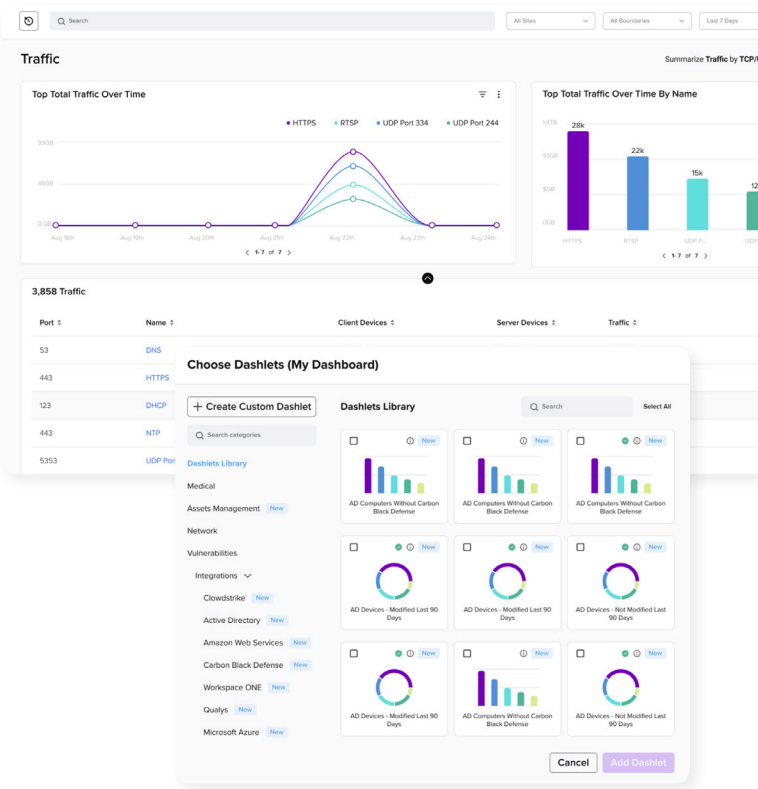
Armis Centrix™ for OT/IoT

Protect and Manage OT/ IoT networks and physical assets, ensure uptime. Build effective & comprehensive security strategies that earn trust and supercharge ROI

Take charge of your OT Environments with **Full Asset Visibility & Control Across** the Entire Infrastructure

Secure cyber-physical assets by achieving full visibility across OT/IoT, ICS and BMS assets. Control, monitor and protect critical OT assets such as industrial controls, BMS and critical infrastructure using the industry's most advanced cyber exposure platform.



The OT/IoT Platform

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 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 & track risk reduction

Armis for OT/IoT Critical Use Cases:

Deep Visibility into all OT Assets - You can't protect what you can't see, creating complete visibility with insights to reduce risk exposure and empower intelligent actions to mitigate risk is absolutely essential in OT environments.

Promote OT Environment Hygiene - Create an inventory of installed and active applications, agents, operating systems and their versions.

Manage IT/OT Convergence - Air gapping is no longer a valid means of securing your environment. It is essential to continuously monitor your entire ecosystem and take an asset first approach. ICS and manufacturing environments need an agentless solution like Armis, which works with all devices.

Protect OT networks and monitor behavior - Protecting OT environments starts with mitigation-creating manageable network segmentation that is continuously monitored.

Maximise Productivity - With Process integrity Streamline your journey to ROI without compromising on security.

Secure Remote Access - Armis's SRA enhances comprehensive OT security by enabling the creation and enforcement of granular, identity-driven access policies between operational assets and remote users and applications. This capability ensures that digital interactions are securely managed without the need for disruptive changes to existing infrastructure.

See, protect, and manage your attack surface with Armis for OT/IoT Security.

Visit **Armis.com** to find out more

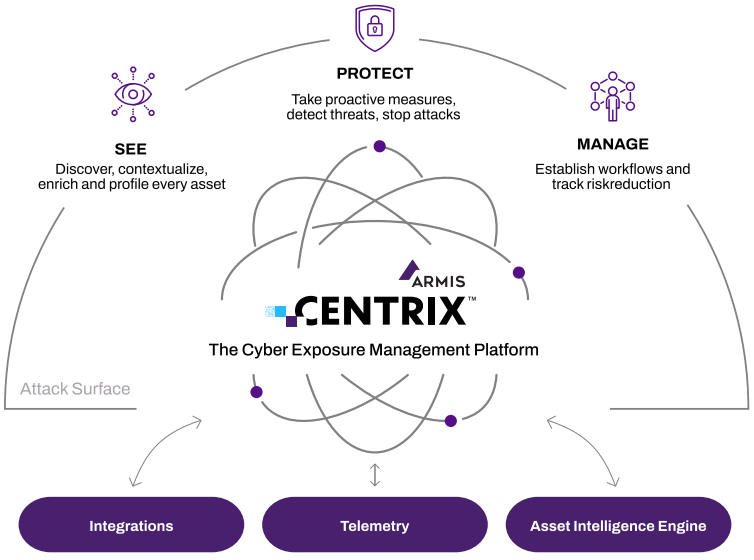
ARMIS

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.
- **Early Warnings.** Take advantage of our threat intelligence feed to understand your attack landscape better.

Why more businesses **are 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 organisation.
3. **Future-Proofed Cybersecurity with Armis,** organisations are ready for future digitalisation.
4. **Operational Resilience** with Armis organisations 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** Organisations using Armis for OT are industry leaders upholding best cybersecurity practices



COLGATE-PALMOLIVE · Mondelēz International · flex · FORTIVE · reckitt · Takeda

See, protect, and manage your attack surface with Armis for OT/IoT Security.

Visit **Armis.com** to find out more