ARMIS

Enhancing Full Situational Awareness in OT Assets

At a Glance

- **71% of breaches** in OT Environments came from known vulnerabilities, things that have known weaknesses inherently in them.*
- Armis provides full situational OT asset awareness in **165+ countries** across the globe.
- Armis understands that OT systems pose **unique security challenges** due to legacy equipment, long life cycles, and convergence with IT networks.
- Armis delivers unparalleled asset knowledge to **35+ of the Fortune top 100** organizations globally.

Full Situational Awareness in OT Assets is No Longer a Luxury

Operational Technology (OT) systems are crucial for the functionality of critical infrastructures across various sectors. However, these systems face unique challenges due to their integration with IT networks, legacy equipment, and extended life cycles, making them prime targets for cyber threats. Achieving full situational awareness is essential for the security, reliability, and resilience of OT environments.

Designed To Address OT Visibility Challenges

Legacy Equipment Vulnerabilities: Many OT systems rely on outdated technologies that lack modern security features, making them susceptible to cyberattacks.

Convergence with IT Networks: The blending of OT and IT systems introduces new cybersecurity risks, exposing OT assets to potential threats from the broader network.

Sophisticated Cyber Threats: The rise of AI-powered attacks and the involvement of nation-state actors have increased the complexity and severity of potential cyber incidents.

See
Discover, contextualize, enrich and profile every asset

Protect
Take measures and prioritize efforts against all exposures

Manage
Establish workflows and track risk reduction

Christopher Fielder | Arctic Wolf

Supercharge your Asset Knowledge with Armis Centrix™

Unparalleled Visibility

Comprehensive monitoring of all OT devices across the network, including IoT and industrial control systems, to detect vulnerabilities and threats.

Powerful Global Contextual Intel

With the Armis Asset Intelligence Engine, understand your assets against the backdrop of 4+ billion other assets operating globally.

Lifecycle Management

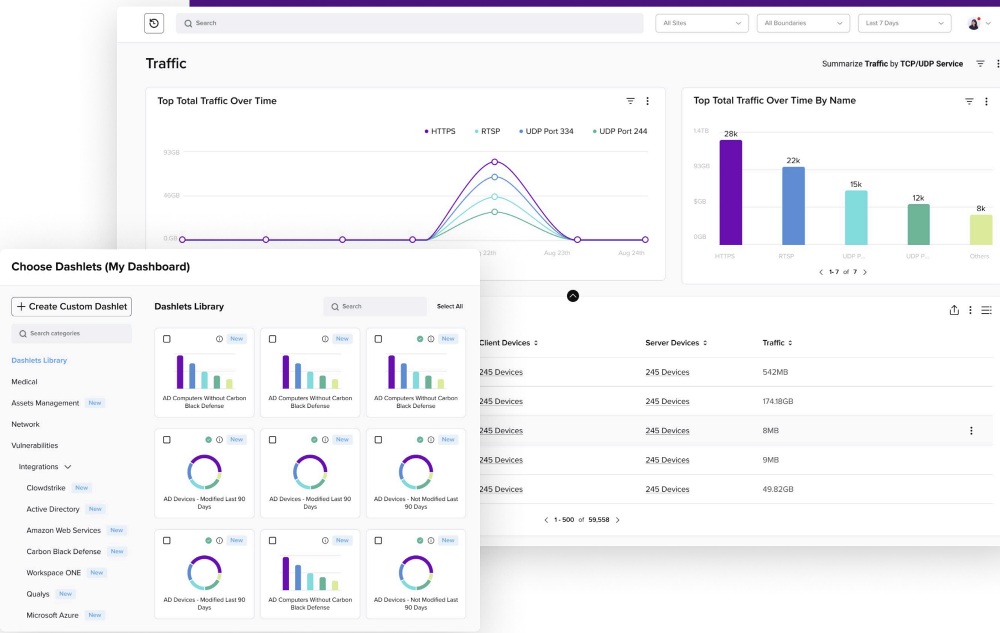
Proactive end-of-life (EOL) management of OT assets to mitigate risks associated with outdated and unsupported technologies.

Network Segmentation & Patch Management

Effective isolation and protection of critical systems, along with prioritization and automation of patch deployment to address known vulnerabilities.

Stakeholder Engagement

Encourages collaboration between IT and OT teams to enhance security postures and response to OT security challenges.



Client Devices	Server Devices	Traffic
245 Devices	245 Devices	542MB
245 Devices	245 Devices	174.18GB
245 Devices	245 Devices	8MB
245 Devices	245 Devices	9MB
245 Devices	245 Devices	49.82GB

1 - 500 of 59,558

See, protect, and manage your attack surface with Armis Centrix^{TM} for OT/ IoT Security

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

Built to Deliver Powerful Asset Context:

- **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.
- **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.
- **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.
- **An Early Warning System** that leverages AI to provide actionable insights to detect and thwart attacks before they are launched.

OT Customers are Seeing the Benefits of Prioritizing OT Security

1 **Reduced Risk of Cyberattacks:** Enhances the safety and reliability of critical infrastructures by mitigating potential cyber threats.

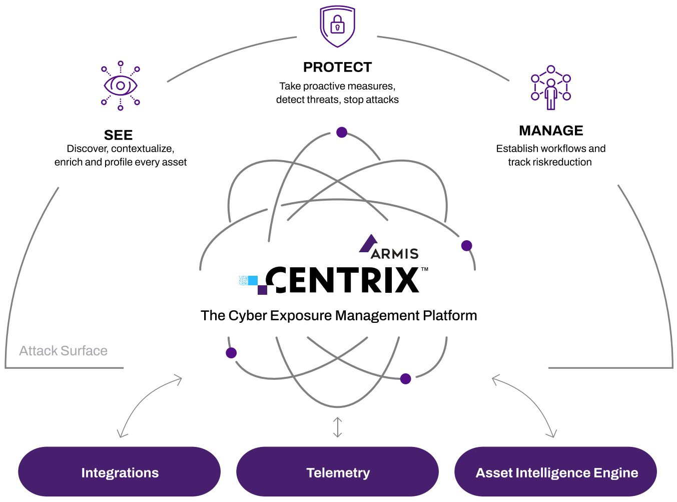
2 **Operational Continuity:** Ensures the uninterrupted operation of essential services by safeguarding OT systems against disruptions.

3 **Regulatory Compliance:** Helps meet stringent compliance requirements related to cybersecurity in critical infrastructure sectors.

The Importance of Prioritizing the Situational Awareness of your OT Asset

The past 12 months has demonstrated that the rate and complexity of attacks on OT Environments is increasing:

- ⚠ **Nov 2023:** Denmark hit by record cyberattack; Russian hackers target 22 power companies, exploiting command flaw since May to access decentralized grid.
- ⚠ **Sept 2023:** Iranian hackers strike Israel's railroad via phishing; target electrical infrastructure. Similar attack reported on Brazilian and UAE firms.
- ⚠ **Sept 2023:** Suspected Chinese hackers attack Asian country's grid with Chinese malware; exploit Windows app for lateral movement.


PROTECT
Take proactive measures, detect threats, stop attacks
SEE
Discover, contextualize, enrich and profile every asset
MANAGE
Establish workflows and track riskreduction
ARMIS
CENTRIX™
The Cyber Exposure Management Platform
Attack Surface
Integrations
Telemetry
Asset Intelligence Engine

See, protect, and manage your attack surface with Armis Centrix^{TM} for OT/ IoT Security

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