SOLUTION BRIEF

Armis Centrix™ for OT/IoT Security

Protect and manage your Operational Technology (OT) and Internet of Things (IoT) environments with full asset visibility and control across the entire infrastructure

The Challenge

Operational Technology (OT) systems are often a combination of IT, IoT and OT assets. These environments host an enterprise's most critical assets and are a primary target for cybercriminals. At Armis we're addressing the critical issues facing OT/IoT environments, namely OT attack surface expansion, unmanaged and specialized OT assets, OT/IT convergence and the rise in extortion attacks.

At a glance

See, protect, contextualize, enrich, and manage every asset in your OT/IoT networks

Take measures and prioritize efforts against all exposures. Build effective and comprehensive security strategies through integration with your existing tools and workflows

Maximize productivity with process integrity streamlining your journey to Return on Investment (ROI) without compromising on security

41.2B

The number of connected assets (IT/OT/IOT/IMOT) is expected to grow from 23,8 to **41,2B by 2025**

OT Attack Surface Expansion means organisations are unable to keep up with regulatory security and compliance.

80%

of these assets will be **unseen, unmanaged and not secured by 2025**

Unmanaged and Specialized OT Assets create blind spots and security risks.

90%

IT professionals say rapidly-changing environments make asset management more difficult

Shift from air-gapped environments and the convergence of IT/OT due to the prioritization of efficiency.

60%

Of data breaches involved unpatched OT asset vulnerabilities

OT and ICS are now the primary target of Ransomware attacks-OT/ICS environments host the enterprise's most critical assets.

With OT attack surface expansion, organizations are unable to maintain regulatory standards, and business leaders are caught in a reactive cycle of cybersecurity risks and unplanned action. Organizations in the OT space are looking to proactively control, monitor, and protect their critical assets. Armis Centrix™, the industry's most advanced cyber exposure platform helps them achieve that goal.

In OT/IoT environments, ransomware and extortion attacks are the single biggest factor impacting critical infrastructure. Attackers are becoming more sophisticated, and they specifically target vulnerable OT/IoT systems due to their high-value nature. These systems often control crucial infrastructure sectors, such as energy, water, transportation, and manufacturing. Successful attacks can lead to operational disruptions, financial losses, and potential safety risks.

37%

increase in ransomware attacks between April 2022 and April 2023

$5.3m

The cost of the average demand in a ransomware attack. The average enterprise payout exceeds $100,000

21 days

The average downtime in OT environments after an attack

The OT/IoT Landscape:

Historically, the common security program placed OT/IoT networks in an air-gapped environment but in today's reality, air gaps are no longer a relevant strategy for most operations.

The convergence of technologies has been coupled with a convergence of responsibilities; CISOs are increasingly being tasked with maintaining cyber resiliency across the once separate OT, IT and facilities teams.

OT/IoT environments must secure their cyber-physical assets by achieving full visibility across OT/IoT, ICS and BMS assets. Achieving this means understanding and managing the risks associated with the interconnectivity of OT and IT environments.

Unlike IT environments, mitigation is typically the more appropriate option when compared to remediation in an OT environment.

As OT equipment can rarely incorporate security agents, a new approach requires enhanced behavioral visibility, traffic monitoring and vulnerability management with deep asset context and threat intelligence to highlight potential attack or compromise. All of this is needed without the need for disruptive agents.

A Holistic Approach with Armis Centrix™

Our unparalleled view of OT environments is achieved through three distinct data sources:

> Integrations with the solutions you already have- we provide you with hundreds of pre-built API-based integrations
>
> Telemetry data that adds traffic inspection and assesses behavior
>
> The AI-driven Asset Intelligence Engine, employing contextual knowledge from other Armis customers around the world

Armis Centrix™ for OT/IoT Platform How do we do it?

A modular approach to address key security challenges

Managed Services

Asset Management and Security

Complete asset inventory of all asset types allowing any organization to see and secure their attack surface

Vulnerability Prioritization and Remediation

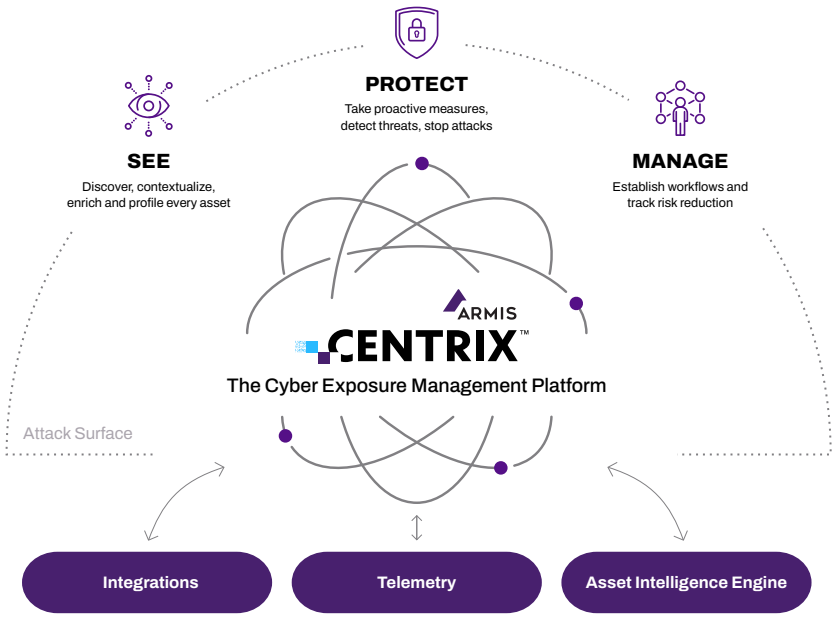
See, consolidate, prioritize and remediate all vulnerabilities; improve MTTR with automatic remediation and ticketing workflows

OT/IOT Security

Protect and manage OT/IOT networks and physical assets, ensure uptime and build an effective & comprehensive security strategy

Medical Device Security

Complete visibility and security for all medical devices, clinical assets and the entire healthcare ecosystem - with zero disruption to patient care



Armis for OT/IoT Use Cases

Deep Visibility Into All OT Assets

Armis Centrix™ provides complete asset visibility across all asset types in your OT environment, whether managed or unmanaged

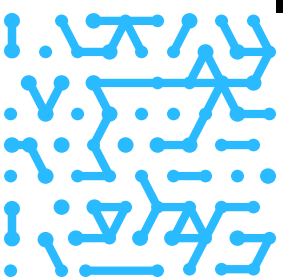
You can't protect what you can't see. Creating complete visibility with insights to reduce risk exposure and empower intelligent actions to mitigate risk is absolutely essential in OT environments. Deep asset visibility goes beyond basic asset discovery. It involves collecting extensive and accurate information about each asset, its characteristics, configurations, behavior, relationships, and vulnerabilities.

Incorporating visibility and alerting mechanisms for Programmable Logic Controller (PLC) changes aligns with the broader objectives of maintaining operational efficiency and cybersecurity resilience. By closely monitoring modifications occurring both within and outside planned maintenance windows, Armis Centrix™ helps you uphold the integrity of your critical processes and swiftly respond to any anomalies, ultimately ensuring the smooth functioning of industrial operations.

"We rolled out Industry 4.0 in all our facilities and needed a holistic view of the manufacturing floor as we know you can't protect what you can't see. Armis is critical for us to identify and protect all our assets as part of our Industry 4.0 efforts."

Friedrich Wetschnig

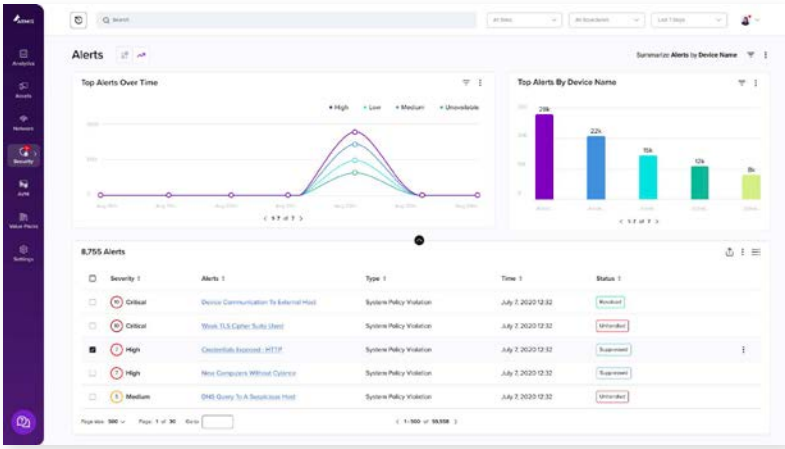
CISO & VP Enterprise Information Technology, FLEX



Promote OT Environment Hygiene

Lacking a complete, continuous and enriched asset inventory makes maintaining good OT environment hygiene challenging

Gap analysis plays a crucial role in cybersecurity by identifying vulnerabilities, weaknesses, and discrepancies within an organization's security measures. Armis Centrix™ enables you to compare an organization's current cybersecurity posture to industry best practices, regulatory requirements, and internal security standards. Gap analysis with Armis Centrix™ also indicates compromise and attacks including unusual communications between OT devices, communications between the IT and OT networks, and communications to and from external networks.



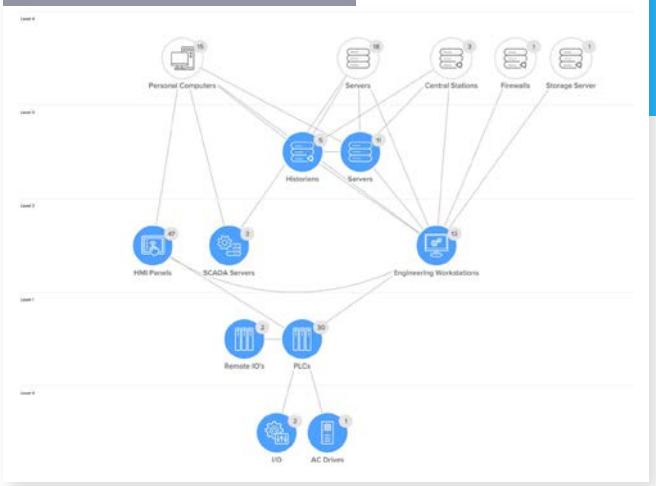
The rise in unmanaged assets has led to a serious increase in security risk and breaches. A real-time overview of your critical infrastructure and identification of gaps is a great way to mitigate these risks. With a complete and reliable asset inventory, you can meet the zero trust challenge with a single, authoritative source of truth for all organizational assets.

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.

Converged environments create a larger and more complex attack surface, where vulnerabilities in one domain can impact the other. Armis enables organizations to implement best practices that can help to address some of the issues facing converged environments. These include segmenting networks to limit lateral movement of threats between IT and OT systems, and employ access controls to ensure authorized communication. Armis Centrix™ also uses continuous monitoring to detect anomalous activities or behaviors and potential breaches in real time.

Visualization of the entire Purdue model



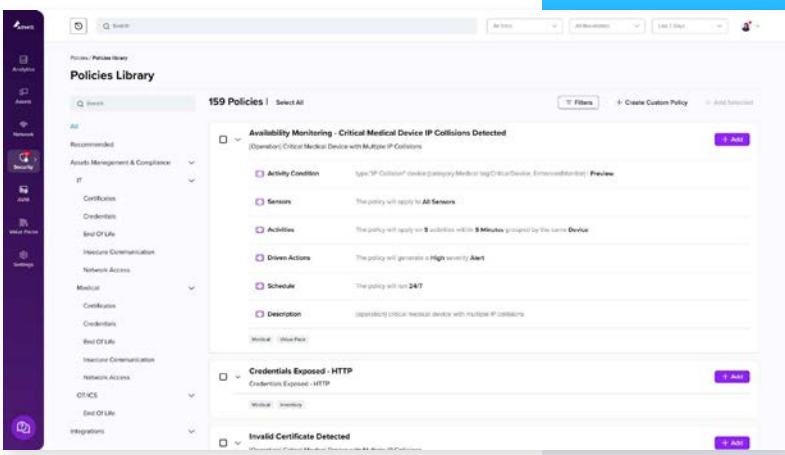
With Armis Centrix™, customizable dashlets map to evidence requirements outlined in security frameworks and customizable reports enable cross-team collaboration and board-level reporting. Role-based access enables teams to focus only on the devices in their scope of responsibility and perhaps most importantly common OT frameworks such as MITRE ATT&CK for ICS framework, ISA/IEC 62443 and NIS2 can be adhered to.

Protect OT Networks and Monitor Behavior

Protecting OT environments starts with mitigation, creating manageable network segmentation that is continuously monitored.

Commencing a segmentation initiative within your industrial setting involves addressing the complexities of deciding the specific policies to establish, and the methods to implement them. Whether it's employing firewalls, Network Access Control (NACs), or other technologies, the choice of tools to enforce these policies is crucial.

Assessing your compliance standing involves grasping the rules governing the interaction between assets and users in your environment during regular operations. Armis Centrix™ has devised a network policy management capability precisely for this purpose.



Maximize Productivity

Streamline your journey to ROI without compromising on security with Armis Centrix™- a proactive way to protect OT environments.

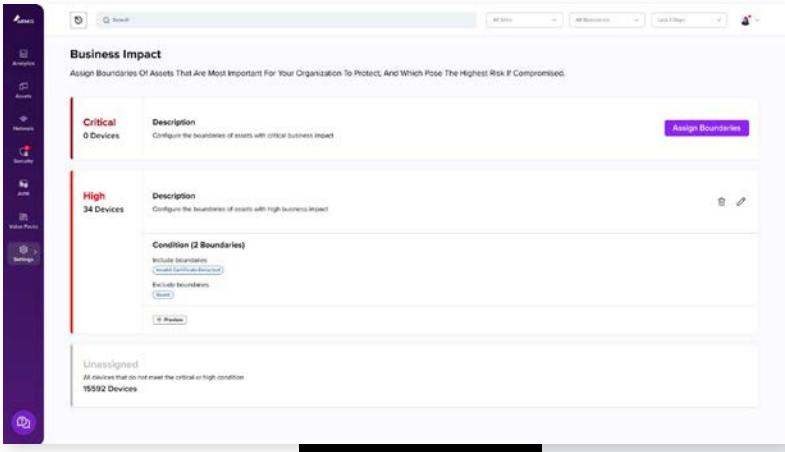
"Of all the vendors we looked at, Armis provided the fastest time to value and the widest coverage. Because it's cloud-based, Armis is also simple to manage. All these factors made it easy to choose Armis, frankly."

Mike Towers

Chief Security and Trust Officer, Takeda Pharmaceuticals

Incorporating Armis Centrix™ into your organization's cybersecurity strategy delivers more than just protection. It enhances the overall operational efficiency and production agility. By securing the convergence of IT and OT systems, security resources can be allocated more effectively. The streamlined communication and data sharing enabled by IT/OT convergence results in smoother operations and quicker decision making. This agility leads to increased productivity, reduced downtime, and ultimately, a positive impact on the ROI.

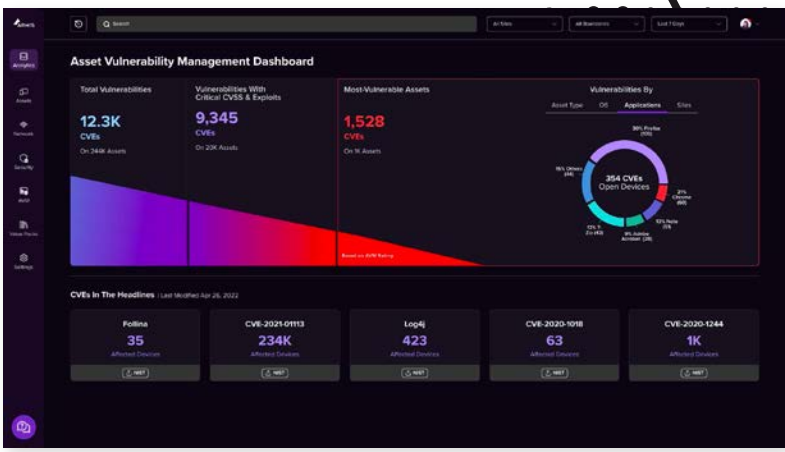
The ability to track and report errors stemming from ICS assets or misconfigurations is pivotal for maintaining operational stability and preventing potential disruptions. Monitoring the performance of ICS assets allows organizations to identify anomalies, diagnose underlying issues, and take corrective actions to prevent downtime or safety risks.



Achieve Vulnerability Prioritization

Tightly managed OT environments have the ability to enhance your vulnerability prioritization efforts.

OT assets are an essential data source for accurate and continuous vulnerability assessment. Through processes such as: Risks and exposures to assets, risk scoring and prioritization, your teams can focus on critical exposures, and matching CVEs. You can also integrate with your organizational playbooks to take action with SIEM, SOAR and SOC processes.



It's time to prioritize remediation efforts based on real risks to your operations and enable continuous security posture management and compliance.

Business Outcomes and Benefits

ROI with Production Agility and Efficiency:

Incorporating Armis into your organization's cybersecurity strategy delivers more than just protection- it enhances the overall operational efficiency and production agility. By securing the convergence of IT and OT systems, resources can be allocated more effectively.

Future-Proofed Cybersecurity:

Armis Centrix™ equips organizations with the tools needed to address evolving cyber threats and the demands of digital transformation. Our AI-powered Asset Intelligence Engine is constantly learning from the assets that we track, improving our ability to contextualize behavior in your environment, no matter the industry.

Compliance and Safety Across the Entire Production Process:

Sectors relying on Operational Technology (OT/IoT) and Industrial Control Systems (ICS) are bound by rigorous compliance standards. Armis Centrix™ offers a comprehensive solution that not only safeguards these industries from cyber threats but also ensures compliance and safety across the entire production process.

Cyber Resilience with Complete Asset Discovery:

Complete visibility over all assets connected to an organization is one cornerstone of cyber resilience. By identifying and managing every asset within the network, from IoT devices to critical machinery, organizations can bolster their cyber resilience. Armis Centrix™ enables precisely this through comprehensive asset discovery and empowers organizations to swiftly detect, respond to, and mitigate potential threats.

Operational Resilience with Armis:

Ransomware attacks on critical infrastructure are escalating. Armis Centrix™ plays a pivotal role in enhancing operational resilience by significantly reducing the risk of ransomware attacks. Armis' robust defenses and real-time monitoring capabilities fortify an organization's infrastructure against such threats, translating into fewer disruptions and minimized downtime.

Reputation and Trust:

Organizations that implement Armis for OT security distinguish themselves as industry leaders committed to upholding best cybersecurity practices. This commitment not only safeguards their operations, but also fosters trust among customers, partners, and stakeholders.

"The number of alerts we get are easy enough to take a look at. Recently, I got an email alert about a phishing campaign. I went to the Armis console, and I started drilling down into the assets. It was easy to make a decision as to whether it was something that needed to be addressed or not. Armis saves a lot of time in investigation."

Director of IT, Global Food Manufacturer

The Armis Asset Intelligence Engine

Armis AI-Driven Asset Intelligence Engine

At the core of Armis Centrix™ is our Asset Intelligence Engine. It is a giant, crowdsourced, cloud-based asset behavior knowledge base- the largest in the world, tracking over three billion assets.

Each profile includes unique device information such as how often each asset communicates with other devices, over what protocols, how much data is typically transmitted, whether the asset is usually stationary, what software runs on each asset, etc. And we record and keep a history of everything each asset does.

These asset insights enable Armis to classify assets and detect threats with a high degree of accuracy. Armis compares real-time asset state and behavior to “known-good” baselines for similar assets we have seen in other environments. When an asset operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine an asset.

Our Asset Intelligence Engine tracks all managed, unmanaged, and IoT assets Armis has seen across all our customers.

The Armis Difference

Comprehensive

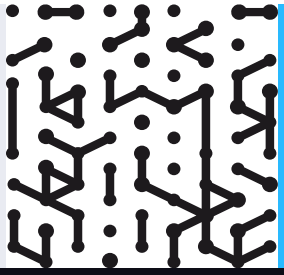
Leverage a complete, unified inventory of every asset in the environment, including those that are outside your corporate network such as OT and IoMT devices, to ensure awareness across the full asset attack surface.

Contextualized

Only Armis has a global Asset Intelligence Engine of over 3 billion devices and growing. The behavior of this unparalleled data set allows us to accurately define normal baseline behavior for assets in your ecosystem.

Complete

Only Armis knows the risk of every asset in your OT environment, allowing you to prioritize your mitigation efforts and focus on high stakes remediation tasks.



ARMIS.

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.

1.888.452.4011