SOLUTION BRIEF

Armis Centrix™ for for OT/IoT Security

Protect and manage your OT/IoT Environments with Full Asset Situational Awareness & Control Across the Entire Infrastructure

Challenge/Intro

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 and weaponized attacks.

At a glance

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

Take proactive measures and prioritize efforts against your entire attack surface. Build effective & comprehensive security strategies through integration with your existing tools and workflows.

Handle the convergence of complex and diverse OT/IT environments with ease.

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 organizations 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 see, secure and manage their critical assets. Armis Centrix™, the industry's most advanced cyber exposure platform helps them achieve that goal.

For OT/IoT environments ransomware and weaponized 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 and industrial sectors, such as energy, water, transportation, and manufacturing. Successful attacks can lead to operational disruptions, financial losses, and potential safety risks.

37%

The increase in attacks specifically on OT environments in 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

5 key OT Landscape features:

- 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, nor are they guaranteed for most operations.
- The convergence of technologies has been coupled with a convergence of responsibilities; security team 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 as well as vulnerability and security finding management with deep asset context and threat intelligence to highlight potential attack or compromise. All of this is needed without impacting process integrity or operations.

A Holistic Approach with Armis Centrix™

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

- Integrations with the solutions you already have - we provide you with hundreds of pre-built API-based integrations
- Actionable Threat Intelligence data adds awareness of potential risk relevant to your industry before they have a chance to take hold
- 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 AI-driven Asset Intelligence Engine

Core to the Armis Centrix™ platform is our Asset Intelligence Engine. It is a giant, crowd-sourced, cloud-based asset behavior knowledgebase—the largest in the world, tracking over three billion assets—and growing.

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 on everything each asset does.

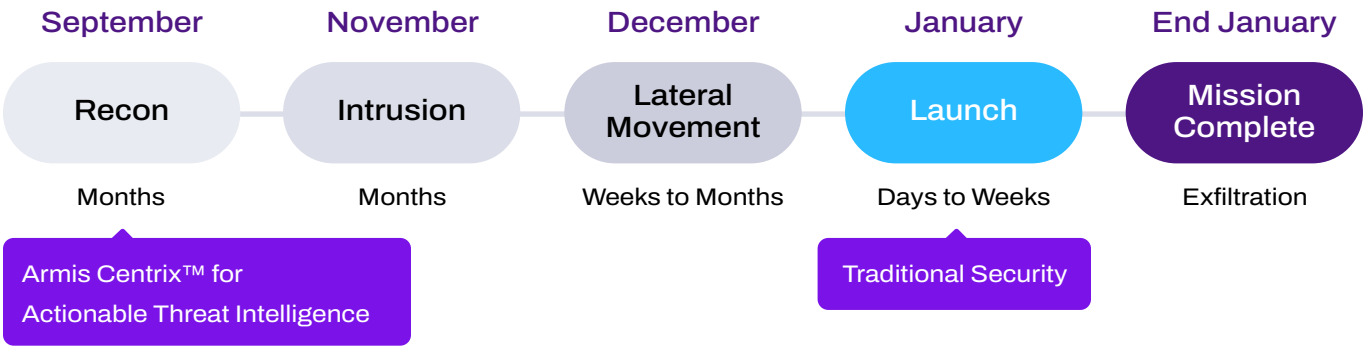
These asset insights enable Armis to classify assets and detect threats with a high degree of accuracy. Armis compares real-time asset state and behavior to “known-good” baselines for similar assets we have seen in other environments. When an asset operates outside of its baseline, Armis issues an alert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

Armis Centrix™ for Actionable Threat Intelligence in OT Environments

Armis Centrix™ for Actionable Threat Intelligence is an optional integration and introduces a paradigm shift. Whereas traditional security goes to work when an attack is launched, actionable threat intelligence enables organizations to find potential threats before they are ever launched and before their environment is ever impacted. In many cases, months earlier. In fact, Armis has hundreds of instances where customers were proactively alerted to a threat before a CVE was issued.

This is particularly crucial in OT environments where the stakes are high and the systems are often deeply integrated into critical infrastructure. With Armis Centrix™, industrial environments can gain a deep understanding of how they are being targeted, using this contextual information to fortify their defenses effectively. The platform's focus on preemptive threat identification allows for a strategic, informed response to potential vulnerabilities, ensuring that OT environments remain resilient in the face of evolving cyber threats.



Armis Centrix™ for Actionable Threat Intelligence offers a revolutionary AI technology that leverages dark web, dynamic honeypots and human intelligence to stop attacks before they impact your organization.

Why do organizations choose to add Armis Centrix™ for Actionable Threat Intelligence?

- Protect against weaponized threats.
- Preempt threat actors and stop them before they impact your organization.
- Address the vulnerabilities that are actually being exploited by threat actors.
- Gain a head start before a CVE gets published.

Armis Centrix™ for OT Platform- How do we do it?

A modular approach to address key security challenges

Managed Services

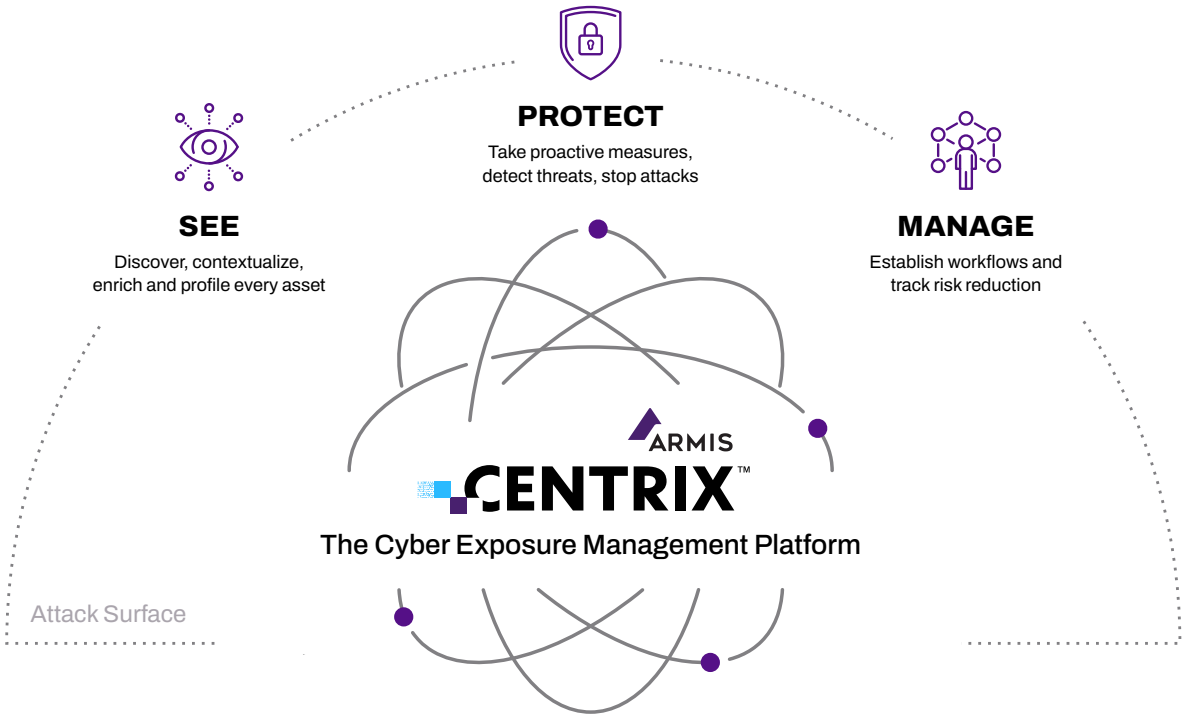
Asset Management and Security
Complete asset inventory of all asset types allowing any organization to see and secure their attack surface

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

OT/OT 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

Actionable Threat Intelligence
Early warning AI based system that leverages intelligence from the Dark Web, Dynamic Honeypots and HUMINT to stop attacks before they impact your organization



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

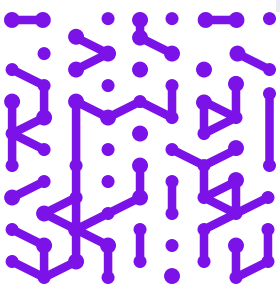
Creating complete visibility with insights to reduce risk exposure and empower intelligent actions to mitigate risk is absolutely essential in OT environments. Deep asset visibility goes beyond basic asset discovery. It involves collecting extensive and accurate information about each asset, its characteristics, configurations, behavior, relationships, and vulnerabilities.

Incorporating visibility and alerting mechanisms for 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 or other security findings, 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

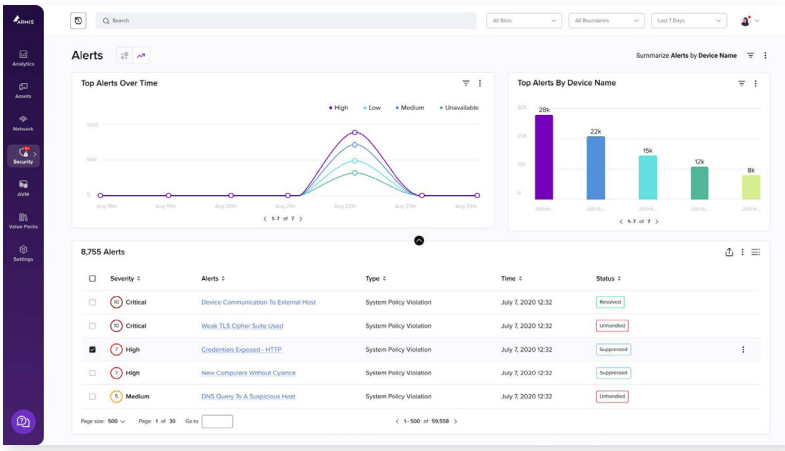
CISO & VP Enterprise Information Technology, FLEX



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.



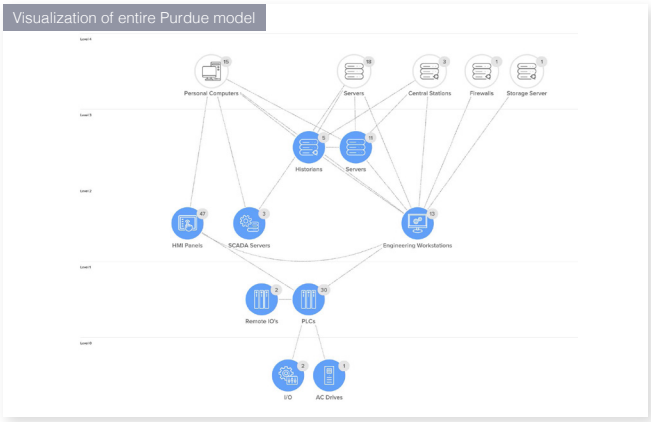
The rise in unmanaged assets has led to a serious increase in security risk and breaches. A real-time overview of your critical infrastructure and identification of gaps is a great way to mitigate these risks. With a complete and reliable asset inventory you can meet the Zero Trust challenge with a single, 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 and other security findings 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/ behaviors and potential breaches in real time.

Visualization of entire Purdue model



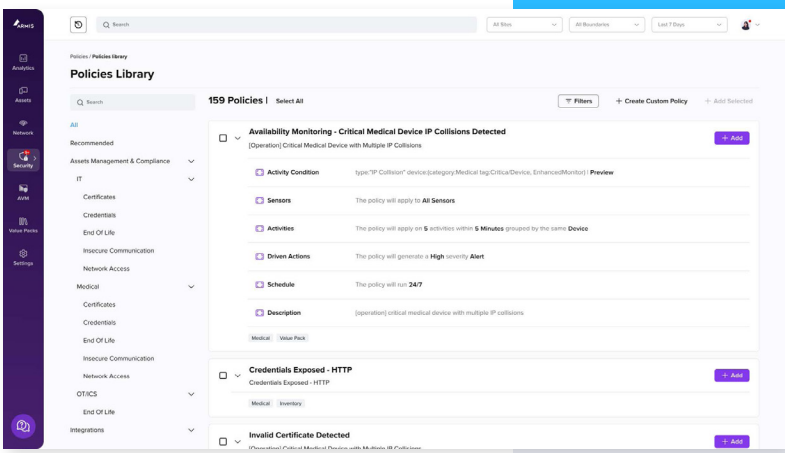
With Armis Centrix™, customizable dashlets map to evidence requirements outlined in security frameworks, customizable reports enable cross team collaboration and board-level reporting. Role-based access enables teams to focus only on the devices in their scope of responsibility and perhaps most importantly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

Protect OT networks with Intelligent Segmentation

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

Commencing a segmentation initiative within your industrial setting inevitably involves addressing the complexities of deciding the specific policies to establish and the methods to implement them. Whether it's employing firewalls, 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

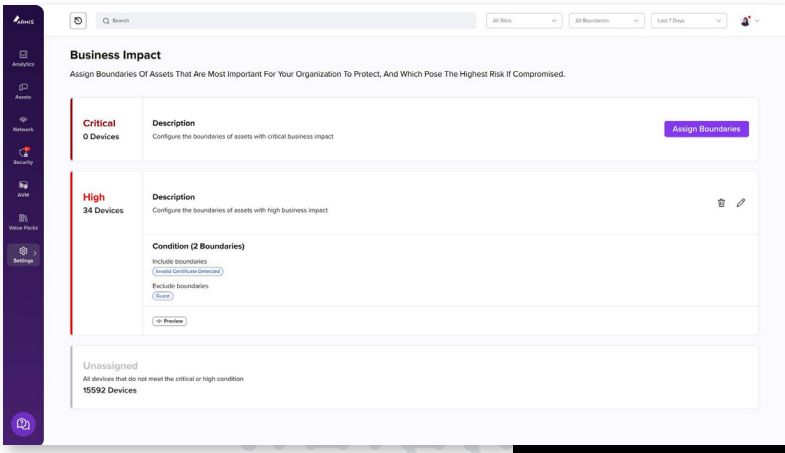
Streamline your journey to ROI without compromising on security with Armis Centrix™- a proactive way to protect OT environments

"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 result in smoother operations and quicker decision-making. This agility leads to increased productivity, reduced downtime, and ultimately, a positive impact on the return on investment (ROI).

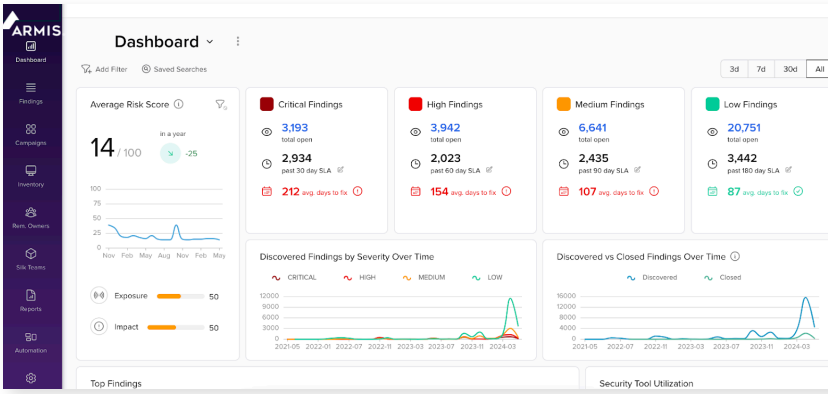
The ability to track and report errors stemming from ICS assets or misconfigurations is pivotal for maintaining operational stability and preventing potential disruptions. Monitoring the performance of ICS assets allows organizations to identify anomalies, diagnose underlying issues, and take corrective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



Handling Vulnerabilities and Other Security Findings

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

Assets in an OT environment must undergo accurate and continuous vulnerability and security findings assessment, deduplication, prioritization, assignment, and remediation efforts. Armis OT organizations with a unified platform for technology risk prioritization and resolution lifecycle management. Armis takes a data-centric, AI-driven approach to enable security stakeholders to better identify risks, communicate priorities, assign owners, and collaborate with developers and operations stakeholders to efficiently manage the entire lifecycle of the resolution management process.



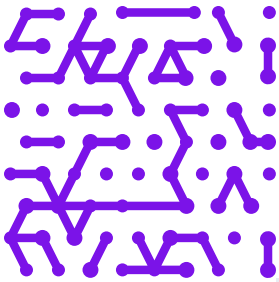
This approach extends across any security finding including infrastructure, code, cloud and application security tools, providing security teams with a consolidated view and clear understanding of how to prioritize and remediate along with how these activities impact overall risk posture that can impact the business.

Address the Complexity of Scale and Diversity with Lifecycle Management

Maintain process integrity in your OT network with continuous lifecycle management

Effective lifecycle management of OT assets is a foundational element in maintaining both the reliability and security of the entire network they enable. With Armis, systematically track each asset's lifecycle stages—from deployment through behavior monitoring, remediation, maintenance and eventually retirement—organizations can ensure that their assets are not only up to date and compliant with current regulations but also perfectly aligned with the evolving needs of the business. This prevents the utilization of outdated or unsupported assets where possible.

Incorporating lifecycle management practices into your Operational Technology (OT) asset management strategy is pivotal for enhancing operational resilience, significantly reducing risks, and fostering a proactive stance towards infrastructure maintenance.



Business benefits

Future-Proofed Cybersecurity:

Armis Centrix™ equips organizations with the tools needed to address evolving cyberthreats 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:

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.

Proven At Scale:

Organizations that implement Armis for OT security distinguish themselves as industry leaders committed to upholding best cybersecurity practices. Armis has a track record of working with some of the most critical and secured orgs at scale delivering peace of mind to even the most complex of OT environments.

This commitment not only safeguards their operations but also fosters trust among customers, partners, and stakeholders.

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. Whether it's automating asset discovery, finding risk, stopping attacks before they happen or prioritizing and managing the vulnerabilities & security findings that matter most, Armis delivers a true return on your investment.

"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 Difference

Comprehensive

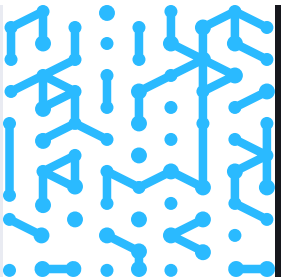
Leverage a complete, unified inventory of every asset in the environment, including those that are outside your corporate network such as OT and IoMT devices, to ensure awareness across the full asset attack surface.

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, 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

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial