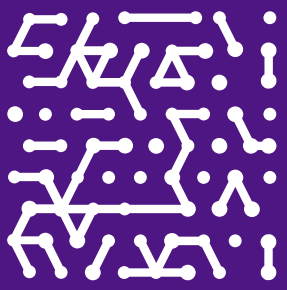
ARMIS®

SOLUTION BRIEF

Guide to Securing Manufacturing & Maintaining Operational Resilience in Cyber Physical Environments

Securing manufacturing environments is more critical than ever before—they are now the single most targeted Operational Technology (OT) industry globally according to CISA. In today's complex ecosystems, manufacturing facilities are composed of interconnected OT and IT devices. OT systems drive the automation of production processes, while IT systems manage these OT networks. This guide aims to show that a security solution offering bespoke OT capabilities while acknowledging the interconnectedness with IT infrastructure is best placed to deliver attack prevention and process protection.

Understanding security in OT requires a holistic approach—prevention is always better than reaction. A thorough understanding of your entire factory's asset makeup is crucial to ensuring robust security across both IT and OT landscapes.



The Attack Landscape in Manufacturing

The primary impact of ransomware attacks has shifted from only IT environments in 2021 to **both IT and OT environments** in 2023.

The attack landscape in the manufacturing industry is a growing problem, with the FBI estimating that malicious OT cyber activity has cost the U.S. economy **$18.7 billion** over the past five years.

In 2023, the global average cost of a data breach in manufacturing was **4.73 million U.S. dollars**.

In February 2023, Applied Materials, a multi-billion-dollar semiconductor technology supplier, suffered a ransomware attack that disrupted shipments and resulted in an estimated **$250 million in lost sales** in Q2 2023, highlighting the growing supply chain risks as organizations, especially in manufacturing, become more interconnected.

In 2021, JBS USA, one of the world's largest meat processing companies, was targeted by a ransomware attack attributed to the REvil group, which **temporarily shut down operations** in North America and Australia, raising concerns about supply chain disruptions and potential price increases.

That same year, Daimler AG, the parent company of Mercedes-Benz, faced a cyberattack **compromising sensitive internal documents**, including financial and personal data, highlighting vulnerabilities in protecting intellectual property and sensitive information.

Typical Components that Comprise Cyber Physical Environments protect industrial networks and control systems.

OT in the manufacturing or cyber physical environments involves hardware and software that detects or causes changes through direct monitoring and control of physical devices, processes, and events in the enterprise. Keep in mind that all of these assets are often connected to, if not controlled by IT devices. Here are some examples of what we find in typical Cyber Physical Environments:

Sensing and Actuation

- Industrial Sensors: Collect data specific to manufacturing processes (e.g., temperature, pressure, vibration).
- Robotic Actuators: Used in robotic arms and automated machinery for precise tasks.
- Autonomous Mobile Robots (AMRs): Robots for material handling and logistics.

Control and Automation

- Programmable Logic Controllers (PLCs): Control manufacturing processes and machinery.
- Supervisory Control and Data Acquisition (SCADA) Systems: Monitor and control industrial processes remotely.
- Manufacturing Execution Systems (MES): Manage and monitor production processes.

Data Management and Analytics

- Industrial Data Storage and Management: Store large volumes of manufacturing data.
- Predictive Maintenance, Lifecycle Management and Analytics: Analyze machine data to predict failures, flag EOL hardware and optimize maintenance.

Networks and Integration

- Industrial Communication Networks: Ethernet/IP, PROFINET, Modbus, and wireless protocols for industrial environments.
- Middleware for Industrial IoT: Connect various industrial systems for data exchange and interoperability.
- Supply Chain Integration Platforms: Integrate manufacturing operations with the supply chain for visibility and coordination.

Human Interaction and Security

- Human-Machine Interfaces (HMIs): Interfaces for operators to interact with manufacturing systems.
- Industrial Cybersecurity: Security measures to protect industrial networks and control systems.
- Energy Management Systems: Monitor and optimize energy usage within manufacturing plants.
- Environmental Monitoring Systems: Monitor environmental conditions for safety and compliance.

Cybersecurity Challenges in Manufacturing

Expanding Attack Surface: As more devices connect to OT environments, the points of entry for malicious actors multiply, creating a larger, more complex and dynamic attack surface. This trend is exacerbated by the Internet of Things (IoT), where everyday objects are linked to networks, often with insufficient security measures. Consequently, organizations must adopt comprehensive strategies to monitor and protect every node within these interconnected environments.

Evolving Threat Landscape: As manufacturers adopt digital technologies, they become targets for a broad range of cyber threats, including ransomware, phishing, industrial espionage, and nation-state attacks. The digital transformation in manufacturing introduces new convergence of systems and dependencies on technology, making these industries attractive targets for cybercriminals.

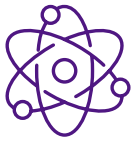
Remote access: Manufacturers increasingly depend on remote access to allow internal and third-party personnel to maintain the cyber-physical components of their OT environments. Traditionally, OT engineers and maintenance staff have shared admin access to ensure immediate resolutions during emergencies, often outweighing the risks associated with third-party access. However, this all-or-nothing approach is becoming increasingly perilous with the rise of remote work and the growing necessity for remote access.

Vulnerabilities in Legacy and Cyber-Physical Systems: Many manufacturing facilities still rely on outdated systems that lack modern security measures. Integrating these with newer digital technologies can cause compatibility issues and expose vulnerabilities exploitable by cyber attackers. Many have not integrated the technologies necessary to safely operate making the situation worse. Because manufacturers' profits are tightly linked to uptime, software patches for older systems are seldom applied. Patching necessitates downtime, which hampers productivity, and productivity drives profits. To exacerbate the situation, manufacturers rarely have the means to accurately prioritize these vulnerabilities. Too often, we hear stories of the top 20 issues being selected from a spreadsheet, leaving the rest to chance.

In some cases such as auto manufacturing, downtime is only scheduled when the production line stops to set up for the next model year, thus vulnerabilities can last for several months or even years without being handled.

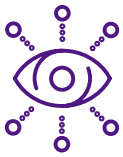
OT Protocols and Communicating with Delicate Assets: Both legacy OT assets and modern interconnected systems often rely on proprietary protocols, rendering them incompatible with traditional IT security tools. Active scanning techniques, for instance, are frequently deemed too risky for uptime, leaving manufacturers in the dark about their assets' behavior. These compatibility issues essentially affect everything from standard inventory to asset management. As a result, merely discovering—let alone protecting—the OT environment remains a significant cybersecurity challenge for

The Cornerstones of a Secure Production Floor



1. Asset Awareness: Achieving comprehensive visibility of not only OT devices but also IT, IoT, and IoMT is crucial in manufacturing environments. Not only should you achieve detailed information such as model, type, firmware version, and serial number etc, you must also understand how this information relates to your industry peers, how your baselines stack up against global trends and how your varied assets are being exploited differently. Such data is essential for maintaining an accurate inventory of the ever-expanding attack surface within the manufacturing environment.

2. Bespoke OT Capabilities: OT and cyber-physical environments require specialized capabilities to address their inherent complexities. These settings demand everything from active querying that ensures safe data collection and Purdue modeling to secure remote access, and alignment with robust compliance and security frameworks. Manufacturing environments, in particular, need a platform specifically designed to meet their unique needs.



3. Vulnerability Management: A strong cybersecurity program requires proactive measures such as vulnerability management. This capability must go beyond simple vulnerability and discover all security findings right down to code. Deduping, prioritization and mitigation is key if you're going to successfully address these findings. This strategy is crucial for identifying weaknesses in both contemporary cyber-physical systems and legacy assets in manufacturing environments. Prioritizing vulnerabilities should be guided by precise contextual data about your assets, their impact on organizational uptime, and how they are being exploited in real-world scenarios.

4. Threat Detection and Prevention: In a manufacturing environment, advanced threat intelligence is vital for early risk identification and prioritizing vulnerabilities, enabling you to tackle the most pressing issues first. It is essential to account for insider threats, alongside global intelligence on attacks affecting similar settings. Utilizing a multi-detection engine further enhances this process, offering varied insights into potential threats and ensuring a comprehensive layered view of your estate. Actionable threat intelligence derived from a combination of Human Intelligence and AI techniques, such as honeypots, provides invaluable insights into how your environment may be targeted. These capabilities are crucial if you're going to achieve a proactive strategy.

Manufacturing By Numbers

USD 4.88M

The global average cost of a data breach in 2024—a 10% increase over last year and the highest total ever.

IBM, Threat Report 2024

USD 2.22M

The average cost savings in million for manufacturing organizations that used security AI and automation extensively in prevention versus those that didn't.

IBM, Threat Report 2024

37%

increase in ransomware attacks between April 2022 and April 2023,

Armis Labs

80%

of industrial organizations have cyber insurance policies, half of which are $500K or more.

IBM, Threat Report 2024

Manufacturing trumps all OT industries with the highest number of Critical CVEs, totaling

18,382

Armis Labs 2024

Manufacturing tops the Armis Centrix™ for Actionable Threat Intelligence early warning list with

936 alerts

in 2024.

Armis Labs 2024

According to NIST, 85 percent of ICS devices currently deployed in the field are between

85 percent

of ICS devices currently deployed in the field are between

10-15 years old

Many, such as Programmable Logic Controllers (PLCS), process sensors, gateways, and workstations are no longer patchable and can't be upgraded due to technical or operational constraints.

NIST, 2024

Manufacturing is the industry most-affected by cyberattacks, accounting for

19%

of all reported victims and experiencing a

46% increase

in victim volume from

46 to 67

between March and April."

GRIT Ransomware Report, 2023

OT Organizations that used these [AI and automation security] capabilities extensively within their approach experienced, on average, a

108-day

shorter time to identify and contain the breach.

IBM / Cost of a Data Breach Report, 2023

What should Manufacturing Plant Managers Ask Themselves?

When choosing an OT Solution, decision makers should be mindful that OT no longer works in isolation. A complete end to end platform play will help address the complex nature of OT networks that are invariably connected to IT, IoT and IoMT assets.

Does it provide deep situational awareness of all assets?

In today's threat landscape, where many attacks target OT infrastructure after moving laterally through IT environments, having a unified view of IT and OT systems has become an invaluable tool for detecting and neutralizing threats before the damage is done. Similarly, OT security professionals should consider a security solution that provides both active and passive options for keeping track of every asset connected to their network.

- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

Does it offer proactive threat detection?

Mitigation is a priority in OT, as proactive threat detection is critical in stopping potential attacks before they occur. By identifying and addressing vulnerabilities and risk early, organizations can prevent security breaches, maintain system integrity, and ensure continuous operational efficiency. This proactive approach not only safeguards manufacturing but also saves time and resources that would otherwise be spent on damage control and recovery. Investing in robust threat detection mechanisms is an essential strategy for any organization committed to protecting its assets and maintaining a secure operational technology environment.

- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

Does it allow you to control how you see your environment?

Gathering data passively is no longer enough because many assets are dormant and do not communicate over the network; the capacity for 'safe active scanning' without disruption needs to be available as an option that gives the user control over how they gather asset information. This ensures that threats can be identified and mitigated in real-time, enhancing overall security and responsiveness.

- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

Does it help meet required compliance and security frameworks?

Many OT operators are employed in critical infrastructure sectors like government/defense, water supply, electric cooperatives, manufacturing and transportation. Consequently, they must adhere to government-mandated security standards and best practice security frameworks. It is wise to seek an OT security solution that demonstrates how its features and functionalities can help your organization meet compliance and security requirements such as NIST, ISO 27001, ISA 62443, CIS Controls, MITRE ATT&CK for ICS and others.

- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

Does it have the availability to scale?

As new devices are integrated and OT environments expand or evolve, static security solutions often need continuous adjustments, updates, and sometimes complete overhauls. To meet the demands of digitization and business growth, OT security buyers should look for solutions that can scale alongside their business

including new business initiatives and collaboration with the existing security stack.

- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

Does it offer a multi detection engine as means of vulnerability hunting? Does this include anomaly-based and policy-based detection processes?

Anomaly and policy based detection enhances an organization's cyber security posture by staying ahead of evolving threats, proactively defending against potential attacks, and maintaining a comprehensive view of their attack surface. A collective data lake such as the **Armis Asset Intelligence Engine** that creates living baselines of expected behavior is a powerful way of performing anomaly detection. Static baselines cannot keep pace with changes and siloed security solutions also fail to detect attacks that span the entire organization - ie. lateral creep from IT to OT.

- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

Does it offer Secure Remote Access?

Modern manufacturing environments require secure remote access to ensure operational efficiency without compromising security. A robust OT security solution should provide secure, granular remote access that allows OT engineers and third-party service providers to perform their tasks efficiently. It is essential for the solution to offer multi-factor authentication (MFA), single sign on (SSO), avoid 'all or nothing' access in favor of 'just in time' and provide encrypted communications to prevent unauthorized access. By incorporating these security features, manufacturers can significantly reduce the risk of cyber threats while maintaining the necessary flexibility for remote maintenance and support.

- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

Can it secure both IT and OT environments on one platform?

Given that most OT cyber-attacks actually start in IT networks before pivoting into OT, investing in an IT security solution rather than an OT-specific solution may at first seem like a better business decision. However, IT solutions fall short if an attacker successfully pivots into the OT network, or if the attacker is a rogue insider who already has direct access to the OT network.

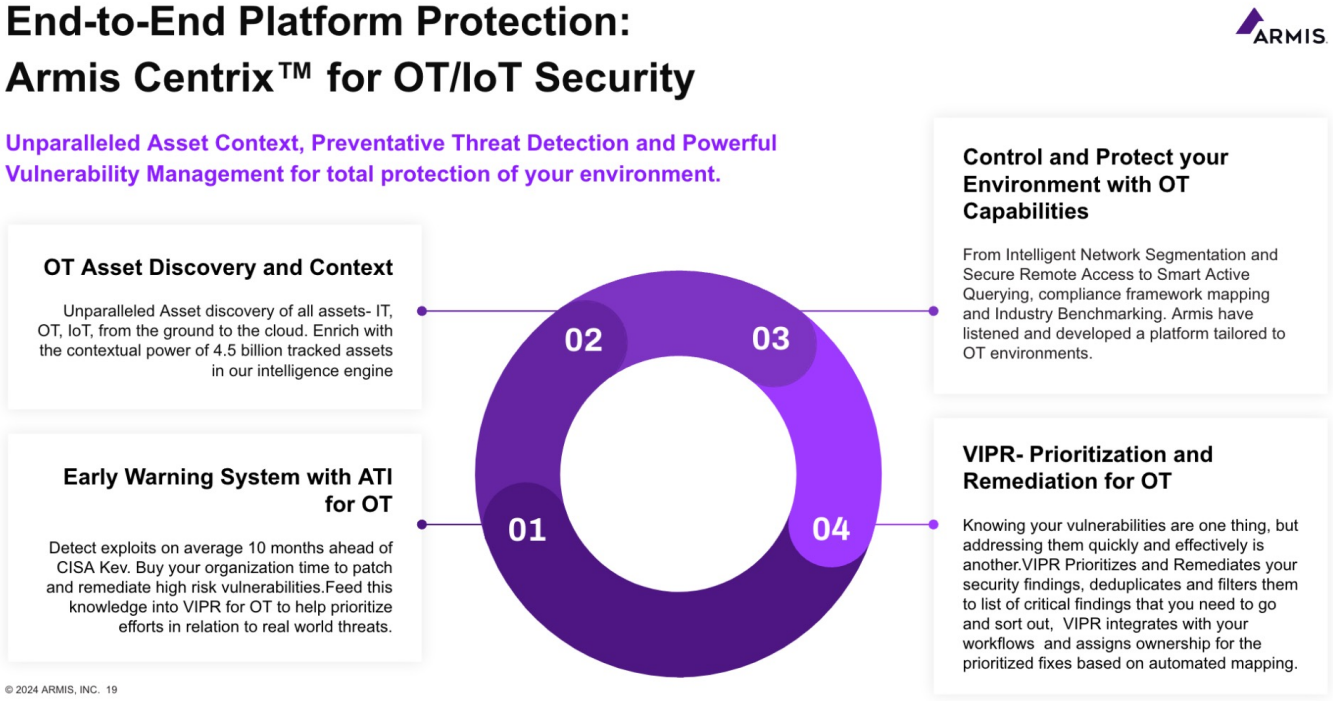
- [x] **Does Armis deliver?**
- [ ] **Does my organization currently have this?**

"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

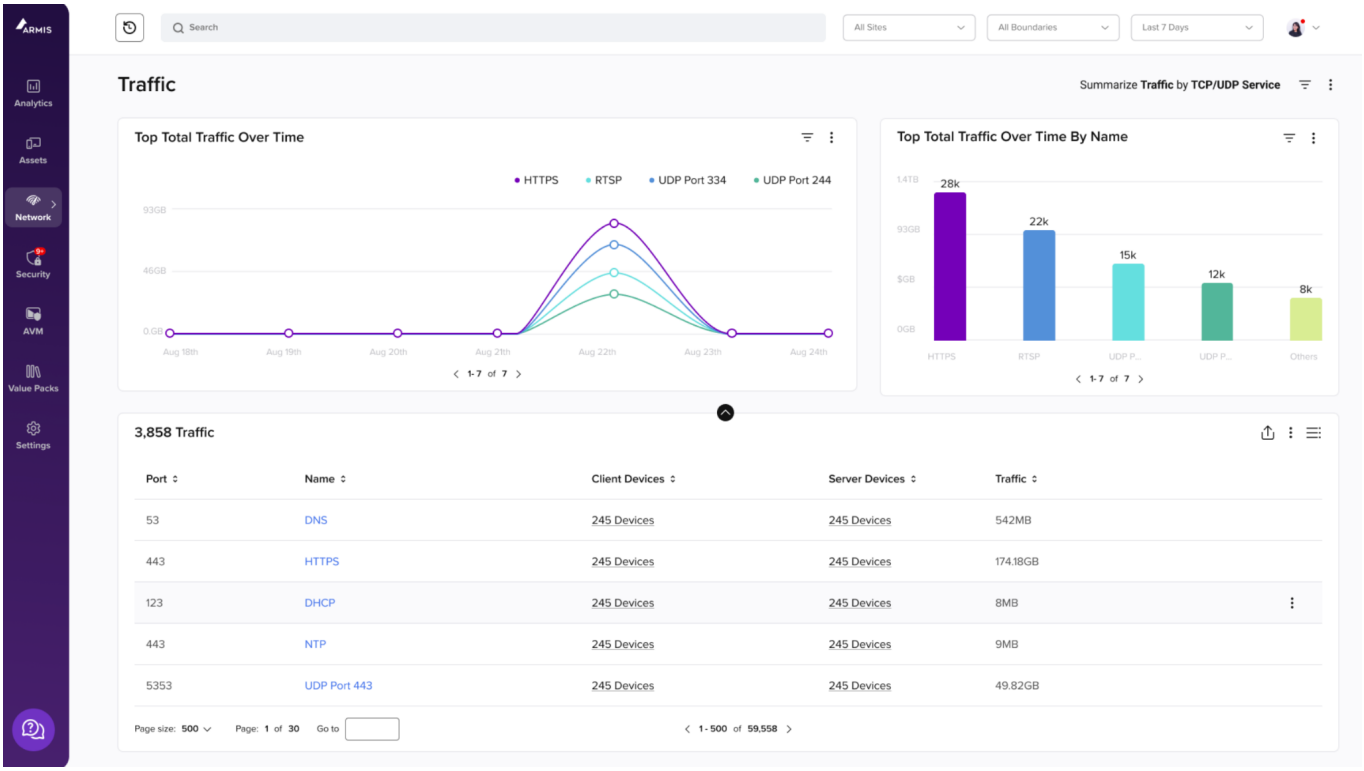
Protect your Manufacturing Processes with Armis Centrix™ for OT/IoT Security: An end-to-end Platform Solution

Organizations providing cyber-physical systems must now look to cyber security technologies that deliver real time insights based on rich contextual data, early warning of both indiscriminate and targeted compromises and vulnerability management that prioritizes findings with world class AI. Armis's proactive take on prevention, protection and management in manufacturing enables a fundamental shift from the traditional approach to security strategy.



Complete Visibility Across Complex Estates

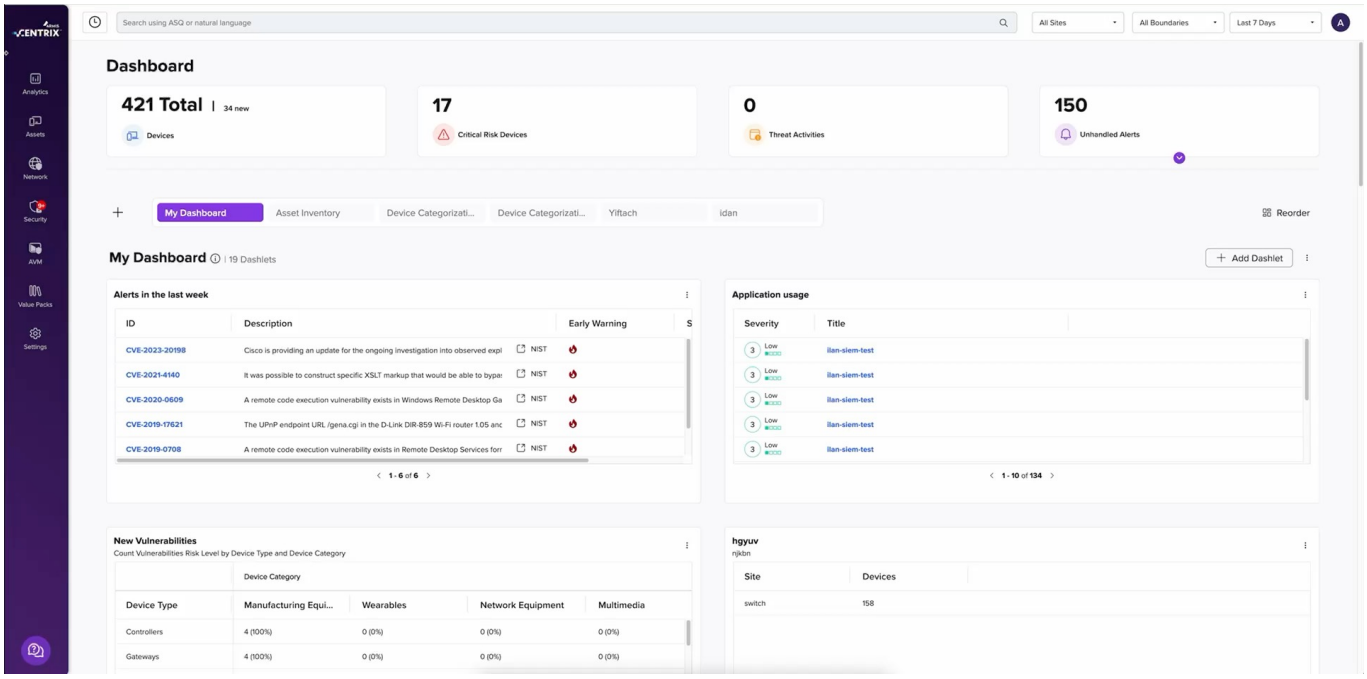
Armis provides comprehensive asset awareness across manufacturing estates by ensuring a seamless view of all OT, IT, IoT and IoMT assets that make up your cyber-physical systems. In manufacturing environments where production lines adhere to tight schedules, Armis facilitates smooth operations by enabling teams to manage tasks such as machine assignment, material handling, maintenance, and safety protocols efficiently. By offering 360-degree visibility across the entire infrastructure, Armis identifies security blind spots that could disrupt operations. It monitors assets and devices against threats, risk, vulnerabilities and other security issues, ensuring any threats are quickly identified and mitigated.

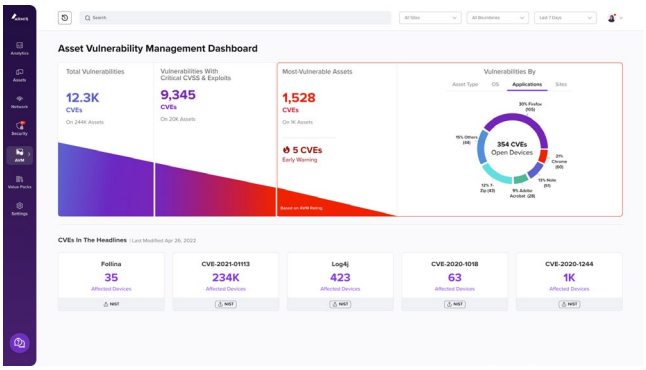


Proactive Threat Management

Leveraging AI technologies for proactive threat detection, Armis employs sophisticated algorithms and machine learning with its Asset Intelligence Engine to identify and respond to cybersecurity threats while still in the formulation stage. This advanced capability enables the preemptive recognition and mitigation of cyberattacks that traditional security tools miss.

Armis Centrix™ for Actionable Threat Intelligence is revolutionizing how manufacturing organizations proactively understand and mitigate risk. In an era where the manufacturing sector faces more breaches than all other OT Industries combined, Armis provides a comprehensive view of specific industry events, allowing manufacturers to stay ahead of potential risks. With human intelligence, smart honeypots, and state-of-the-art research, Armis Centrix™ ensures timeliness, unparalleled coverage, and accuracy, enabling organizations to stay ahead of evolving cyber threats, protecting their critical assets with confidence.





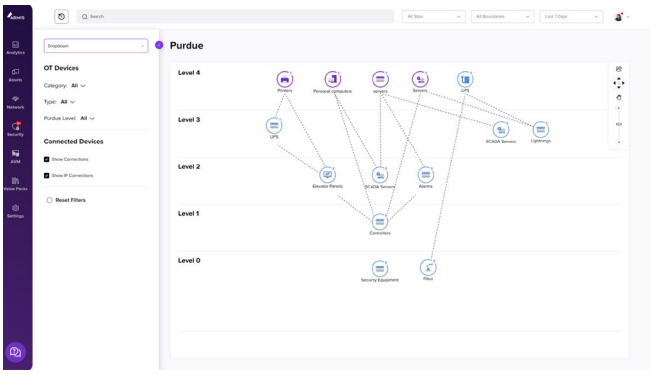
Secure Remote Access

Unlike conventional remote access solutions, Armis' Secure Remote Access powered by Xage (SRA) is specifically designed to address the unique operational, administrative, and security requirements of manufacturing and critical infrastructure. By simplifying remote access, it cuts costs, conserves resources, and boosts security, allowing staff to concentrate on core business tasks and improving total cost of ownership (TCO).

The solution addresses regulatory pressures by providing robust Zero Trust identity and access management for all devices, and all individuals whether internal or third party. It implements Multi-Factor Authentication (MFA) and Single Sign-On (SSO) for secure and seamless access, and sets 'just-in-time' access windows for essential maintenance. Moreover, it ensures that each individual gets the exact right access to resources, devices and assets in order to get their authorized activities or job done. SRA prevents unauthorized lateral movement within the network through machine-to-machine access control and simplifies privilege management, reducing the risk of unauthorized access and privilege abuse.

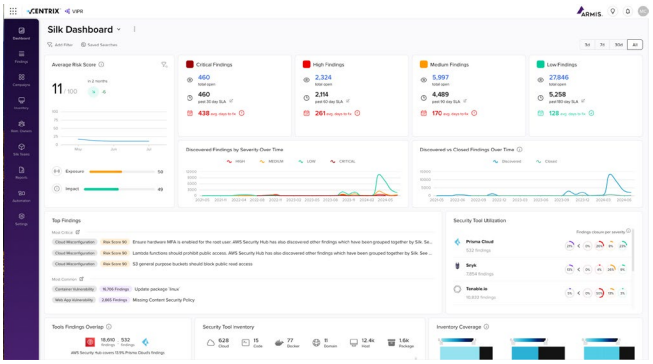
Network Segmentation and Policy Enforcement

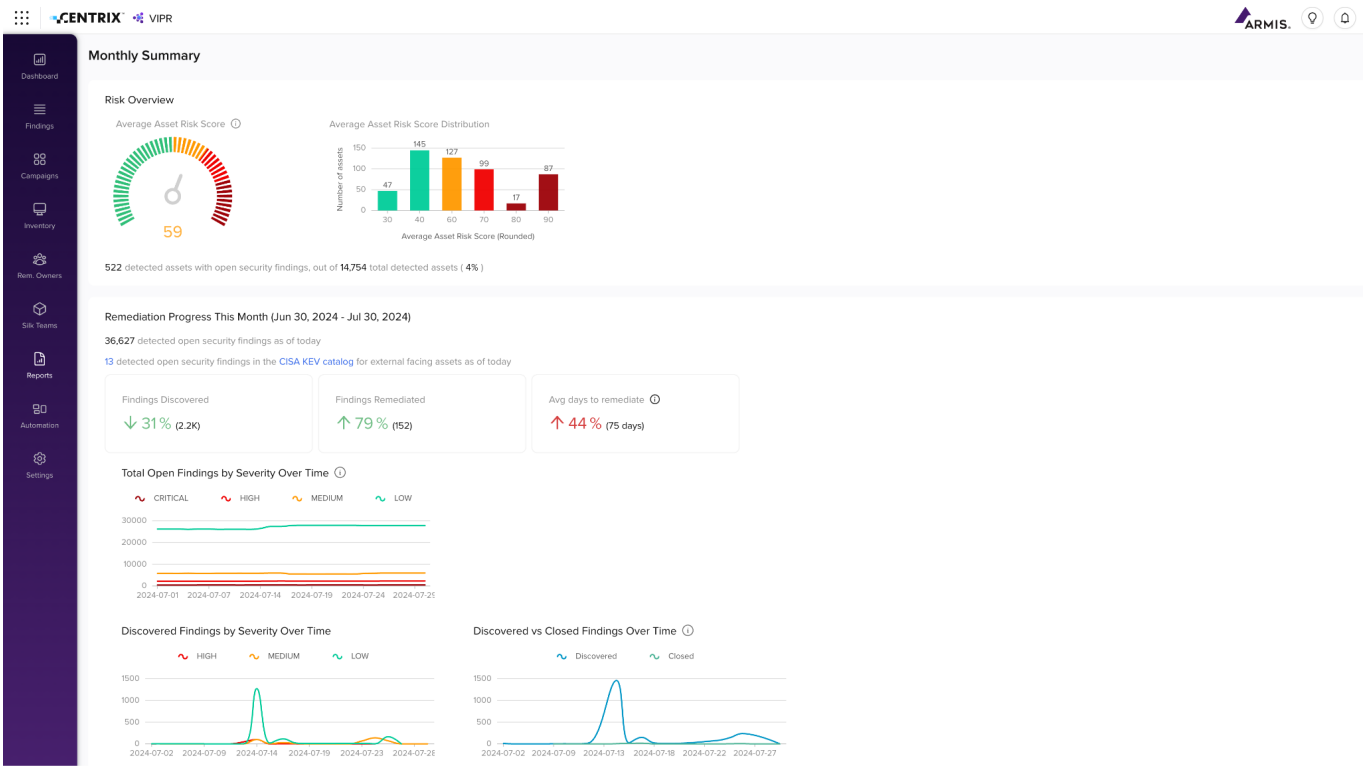
Armis helps manufacturing organizations create and enforce network segmentation policies that protect critical systems. By providing comprehensive visibility into connected assets and their communications, Armis can segment or recommend network segmentation policies that are automatically enforced via existing firewalls and network access control (NAC) solutions. This ensures critical systems are isolated from potential threats, enhancing overall cybersecurity resilience.



Addressing Vulnerabilities and Other Security Findings

Manufacturing organizations are faced with a deluge of security alerts, with no scalable and automated way to prioritize them and operationalize remediation. This results in long lag times between the “finding”, assigning of the “owner” and the “fix”. **Armis Centrix™ for VIPR Pro - Prioritization and Remediation** goes beyond vulnerability management to find and consolidate security findings across all sources to holistically understand risk and automate prioritization. Armis Centrix™ streamlines the entire remediation lifecycle, from identifying owners to operationalizing fixes, providing a unified platform for prioritization and efficient risk resolution management.





Anomaly Detection

Critical infrastructure organizations manage essential systems such as power grids, water treatment plants, transportation systems, and manufacturing facilities, where operational downtime can be detrimental to society and risk people's safety.

Real-time detection and response help identify early warning signs of a cyber-attack, significantly reducing operational downtime and enabling quick, effective mitigation.

Armis provides continuous detection, full visibility, and actionable insights by analyzing all traffic and activity on a granular level in a protocol and technology-agnostic manner

Leveraging advanced anomaly detection, Armis delivers autonomous response to diverse and complex OT ecosystems, continuously learning 'normal' behavior baselines to identify deviations indicative of emerging threats.

In an era marked by the convergence of IT and OT networks, secure and seamless operations are no longer a luxury but a necessity.

Manufacturing organizations face unprecedented cybersecurity challenges that require an integrated approach to address them effectively. Armis Centrix™ for OT/IoT Security provides the comprehensive solutions necessary to safeguard critical infrastructure, ensuring operations remain resilient against the ever-evolving landscape of cyber threats.

By delivering complete visibility, proactive threat management, secure access, robust network segmentation, vulnerability management and advanced anomaly detection, Armis empowers organizations to protect their assets and maintain uninterrupted production processes.

As manufacturers continue to adopt new technologies and expand their digital footprints, investing in a holistic, end-to-end OT security platform becomes paramount.

Trust Armis to be your partner in securing the future of manufacturing.

CASE STUDY

COLGATE-PALMOLIVE

Challenges:

- Limited asset awareness
- Lack of control over creating and enforcing policies.
- Lack of insight into gaps, and limited ability to fine-tune policy in alignment with current threats and risks.

Armis Results:

- Detailed insights into the new technologies that are continually introduced to the manufacturing environment.
- Easy-to-create security policies that map to the latest threats and risks.
- Modern, easy-to-navigate user interface.
- SaaS solution for easy deployment and maintenance.
- Automatic threat detection and response.
- Rich data sets available in a single dashboard thanks to integrations with existing tools.

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