ARMIS®

SOLUTION BRIEF

Armis Centrix™ for OT/IoT Security | Pharmaceutical Manufacturing

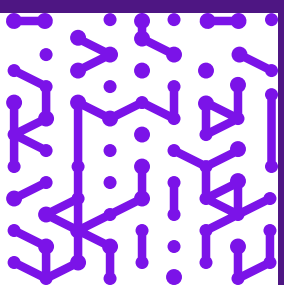
See, Protect, and Manage the Entire Pharmaceutical Manufacturing Process

The pharmaceutical manufacturing industry is responsible for some of the most sensitive data and essential technology that directly impacts the successful treatment of patients to achieve positive patient outcomes. Every step of the manufacturing process is essential for ensuring medical devices and medications are effective and are manufactured to exacting standards. Any deviation from these standards can put patient care and lives at risk. Securing devices and technology used in the pharmaceutical manufacturing environment is an all-important charge with no room for error.

Devices in the pharmaceutical and life sciences industry are extremely sensitive and require significant change management processes. Due to an influx of recent attacks such as the 2017 ransomware attack on a multinational pharmaceutical company causing worldwide disruptions or the 2020 attacks aiming to access vaccine production, pharmaceutical manufacturers must prioritize the need for better security. These efforts are complicated by the combination of legacy devices, third-party vendors, and new automation tools.

Securing Essential Manufacturing Operations – How Armis Helps

- Safeguard the manufacturing of essential medical and pharmaceutical materials by protecting against disruptions caused by attacks
- Deep visibility and situational awareness of all assets in the pharmaceutical manufacturing process
- Detect and classify every device within minutes, including robotic arms, building automation systems, HMIs and more
- Maintain the integrity and security of manufacturing processes by integrating with your existing tools and workflows
- Maximize operational efficiency by avoiding interruptions and outages with proactive risk management and prioritization.



Protect Vital Pharmaceutical Manufacturing Process Standards

Ransomware and extortion attacks are the single biggest threat to upholding the exacting standards in pharmaceutical manufacturing environments, from factories to research labs and corporate offices. Attackers are becoming more sophisticated and they specifically target vulnerable IoMT and OT/ICS systems due to their high-value nature. Successful attacks can lead to massive safety risks to patients who rely on essential medical and pharmaceutical materials, not to mention operational disruptions, brand reputation risks, and financial losses. Any minor deviation in the manufacturing process can ultimately be fatal.

37%

Increase in ransomware attacks between April 2022 and April 2023

$4.8M

The cost of the average pharma breach in 2023

189 days

Average time it takes to contain a cyber attack in pharma environments

21 days

The average downtime in OT environments after an attack

Armis Centrix™ allows security teams in the pharmaceutical and life sciences industries to properly secure all connected devices–manufacturing or research–without any disruption to the business. Our platform and suite of products deliver the ability to manage the lifecycle of all production assets and their users across dispersed manufacturing environments.

- Protect against tampering with lifesaving prescription formulas
- Protect sensitive patient data, patents, clinical trial information and IP
- Prevent potential outages, downtime, and disruption to the pharmaceutical supply chain
- Maintain continuous service to healthcare providers and patients
- Power effective security controls, predict and protect against emerging threats
- Demonstrate security for regulatory compliance reporting
- Gain comprehensive visibility of all devices, on or off your network

Ensure Secured Pharma Manufacturing Operations with Armis Centrix™

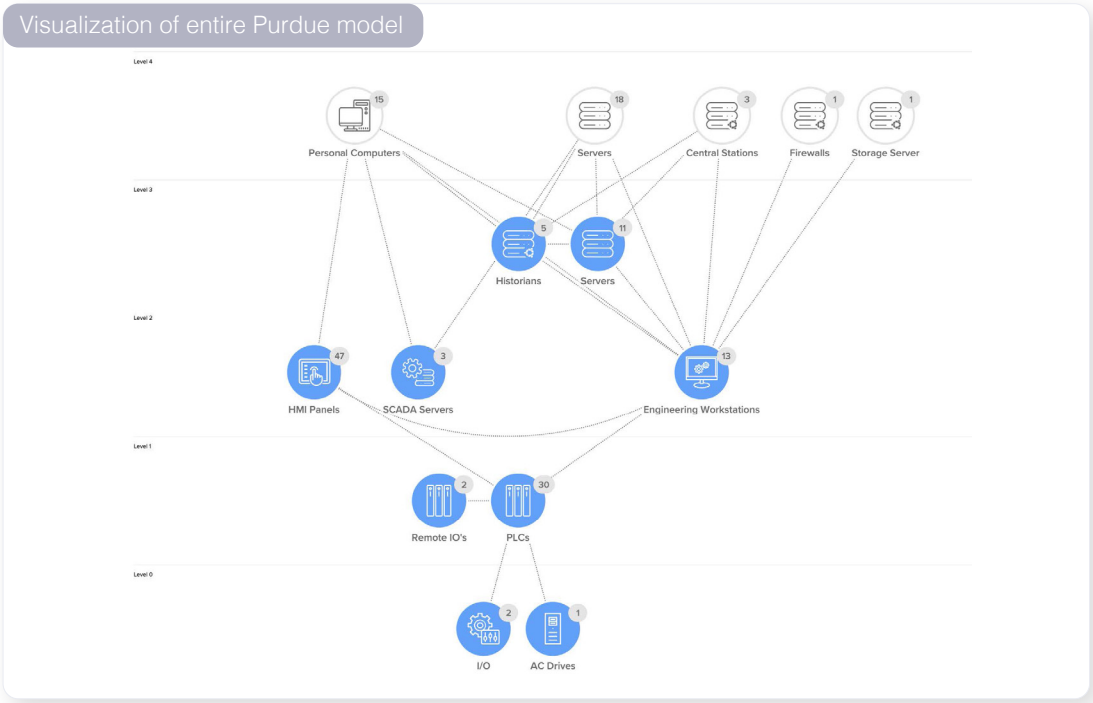
Deep visibility into all Assets

Gain complete asset visibility across all asset types in your manufacturing 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 pharmaceutical manufacturing. Deep asset visibility goes beyond basic asset discovery. It involves collecting extensive and accurate information about each asset, its characteristics, configurations, behavior, and relationships.

Armis Centrix™ utilizes a multi-discipline detection engine which not only discovers each asset in your organization, but also delivers deep context and insights so that you always know the condition of your environment. Comprehensive non-intrusive discovery via Armis Smart Active Querying exposes legacy assets that current tooling is unable to detect and ensures zero disruptions to your essential devices. 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 and precise functioning of industrial operations and cybersecurity resilience.

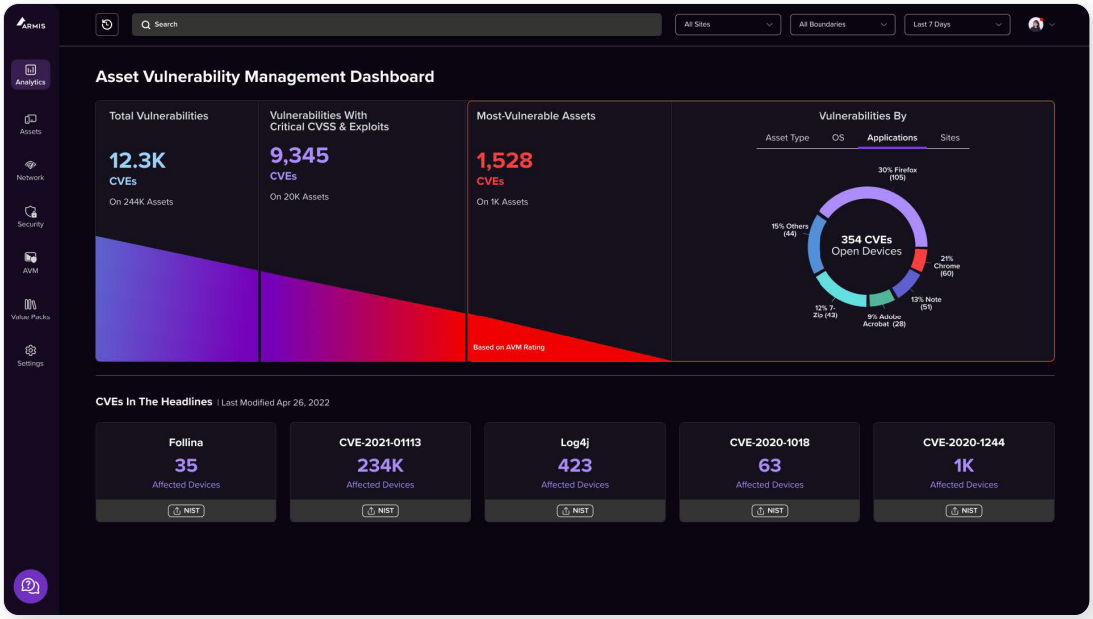
Visualization of entire Purdue model



Efficiently Address Vulnerabilities

Enhance your vulnerability prioritization efforts and efficiently manage remediation to save hours of effort

Pharmaceutical Manufacturing operations require accurate and continuous vulnerability assessment. Through processes such as risks and exposures to assets, risk scoring, and prioritization, your teams can focus on CVEs that are identified and triaged based on the criticality to the business. Armis Centrix™ for Vulnerability Prioritization and Remediation offers triaged risk-based vulnerability management that enables security teams to quickly identify and remediate the vulnerabilities that are most likely to be exploited and negatively impact the business. It's time to prioritize remediation efforts based on real risks to your operations and enable continuous security posture management and compliance. You can also integrate with your organizational playbooks to take action with SIEM, SOAR, and SOC processes.

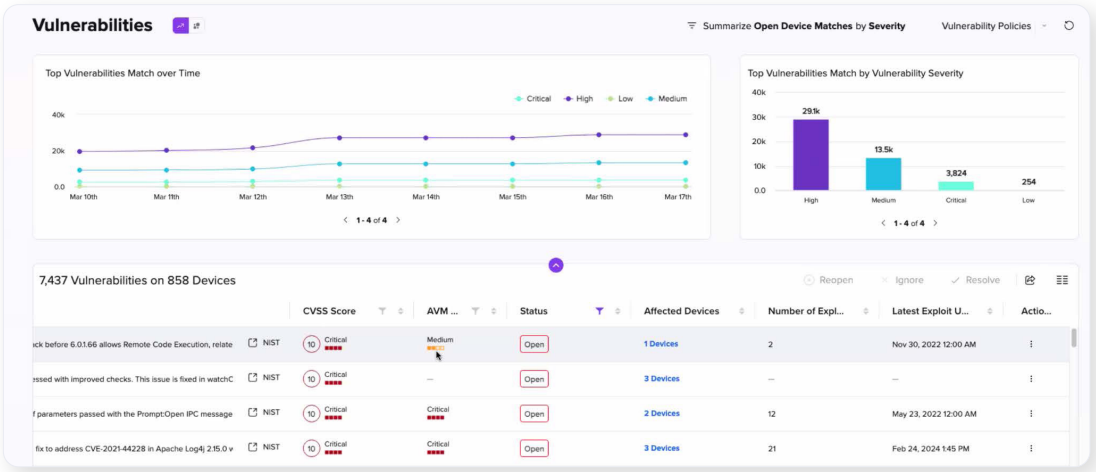


Achieving Adherence to Regulations and Security Frameworks

Safeguard your organization against cyber threats and ensure compliance and safety throughout pharmaceutical production and distribution.

Pharmaceutical organizations operate under strict regulatory frameworks, including HIPAA (Health Insurance Portability and Accountability), FDA (Food and Drug Administration), and GMP (Good Manufacturing Processes) regulations, as well as local regulations and guidelines like the EU General Data Protection Regulation (GDPR). A cyber attack can result in regulatory investigations, audits, and fines if an organization is found to have failed to protect sensitive patient data or uphold cybersecurity standards.

Maintaining a proper paper trail is essential to comply with regulatory and cybersecurity standards. Armis Centrix™ deep awareness of every device's state, characteristics and behaviors can help organizations align with required regulatory compliance standards and security frameworks. Proactive compliance reports can be generated to help demonstrate compliance with both. Automated recall assessments streamline pharmaceutical manufacturing processes and save hours of manual reconciliation efforts. Scheduled reports and dashboards help teams stay on top of new advisories and track remediation efforts.

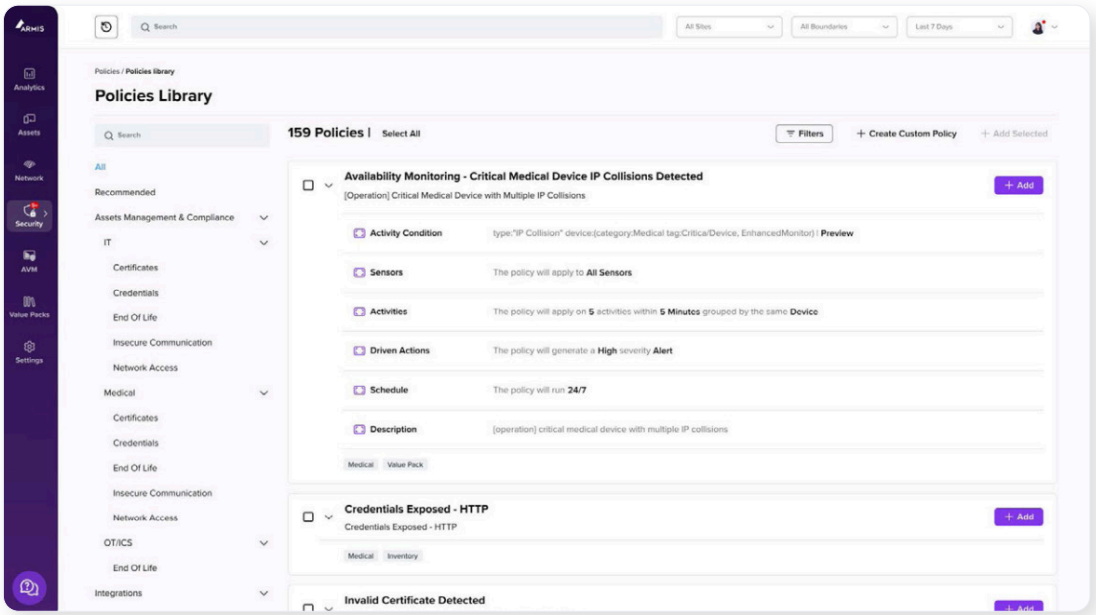


Securing the Entire Supply Chain

Avoid disruptions to production and distribution of life-saving materials and maximize ROI

Managing pharmaceutical manufacturing operations from R&D to production and distribution, along with the reliance on third-party interconnections requires real-time control and precision. Implementing comprehensive asset security measures without causing delays or disruptions in the production process is crucial for maintaining efficiency as well as the integrity of the manufacturing process.

Incorporating Armis Centrix™ into your organization's cybersecurity strategy delivers more than just protection. It enhances the overall operational efficiency and production agility. Securing converged IT and OT systems ensures comprehensive and effective security resourcing. This agility leads to secured and assured productivity, reduced downtime, and ultimately, a positive impact on the ROI.

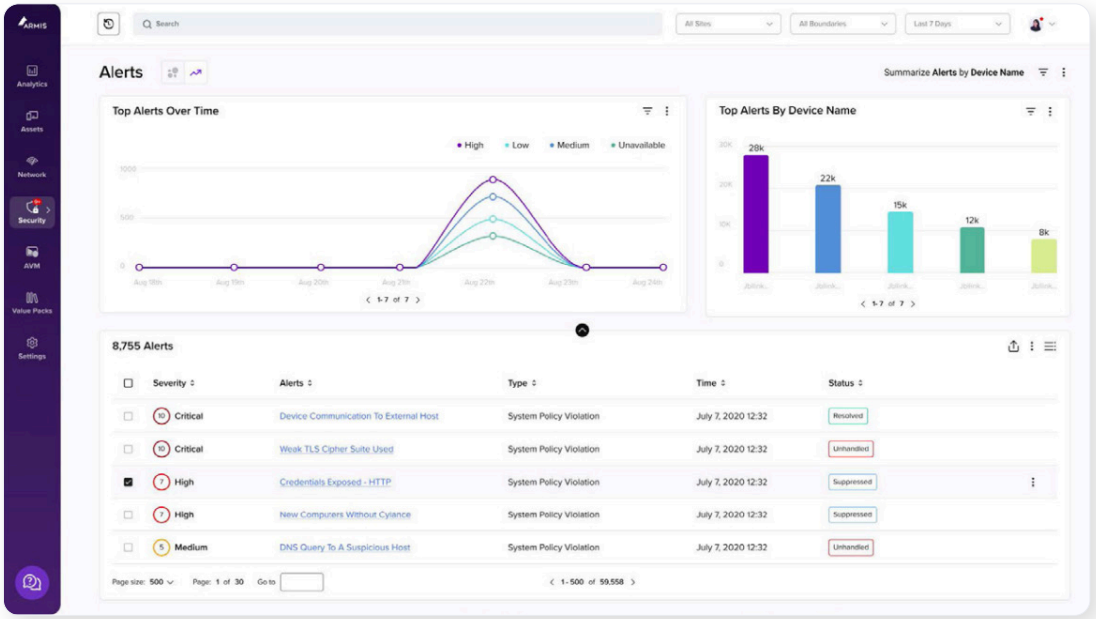


Predict and Protect Against Emerging Threats

Proactively protect manufacturing environments, understand threat impact, and resolve before operations are impacted

Attacks in pharmaceutical manufacturing can impact intellectual property theft, production record or system errors, or worse, defective products reaching patients, resulting in recalls or impacts to patient health. Proactive security and maintenance measures are essential to ensure the entire pharmaceutical journey remains uninterrupted.

Leveraging a combination of AI and machine learning, Armis Centrix™ for Actionable Threat Intelligence is an early warning system that empowers you with early warning intelligence to anticipate threats, understand their potential impact, and take preemptive action to neutralize them, effectively moving the security posture from defense to offense. Armis Centrix™ for Actionable Threat Intelligence offers a revolutionary AI technology that leverages dark web, dynamic honeypots and HUMINT to stop attacks before they impact your organization.



Device Lifecycle Management

Track and manage device lifecycles, predict maintenance windows, and ensure device reliability in essential manufacturing environments.

Pharmaceutical manufacturing processes contribute to a wider network of essential healthcare services. Any outages or downtime can delay medication or pharmaceutical device delivery.

Armis Centrix™ provides a view of vulnerabilities and necessary updates to all assets in the manufacturing environment and facilitates proactive maintenance or mitigation to avoid any unexpected delays. Monitor asset behavior and assess device properties and compliance for a single pane of glass view of all devices and functionality.

"Of all the vendors we looked at, Armis provided the fastest time to value and the widest coverage. Because it's cloud-based, it's simple to manage. Thanks to Armis, we've already uncovered a series of potential cyber risks. Without the Armis deployment, we never would have known they existed. It has already paid for itself."

Mike Towers
Chief Security and Trust Officer
Takeda Pharmaceuticals

Armis AI-Driven Asset Intelligence Engine

The Armis Asset Intelligence Engine is a collective AI-powered knowledge base, monitoring billions of assets worldwide in order to identify cyber risk patterns and behaviors. It feeds the Armis Centrix ™ platform with unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface.

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.

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, OT/ICS and IoT assets Armis has seen across all our customers.

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

A modular approach to address key security challenges

Managed Services

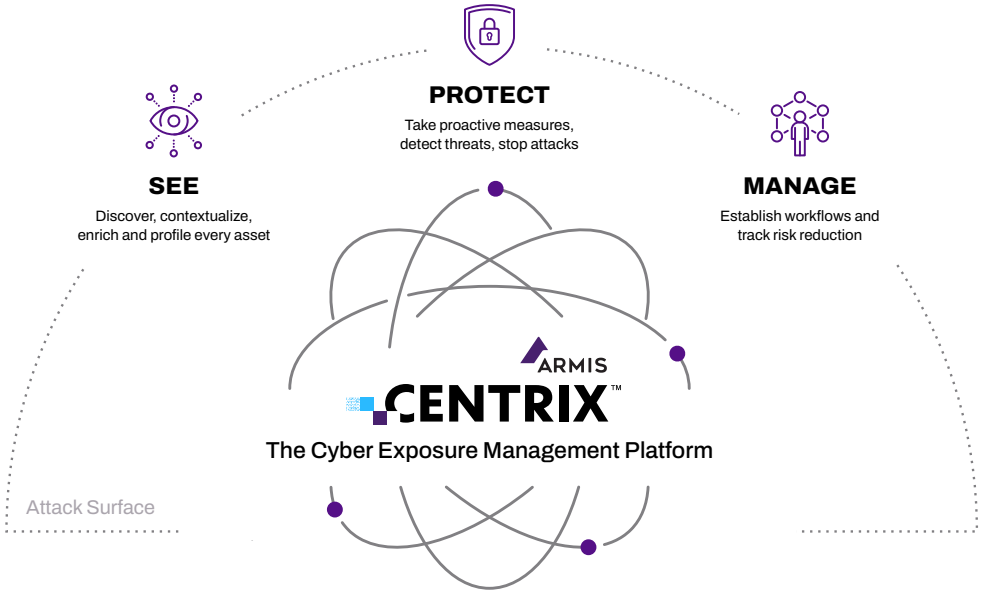
Asset Management and Security
Complete asset inventory of all asset types allowing any organization to see and secure their attack surface

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

OT/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

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



Business Outcomes and Benefits

Cyber resilience with complete asset discovery

Visibility of all assets from the factory floor to R&D labs and the corporate office. Empowers swift detection, response, and mitigation of potential threats, even in dispersed facilities.

Protect precise formulas and data

Enhance operational efficiency by significantly reducing the risk of cyber attacks. Real-time and proactive monitoring capabilities help reduce disruptions to essential pharmaceutical production and minimize downtime.

Life-sustaining supply chain integrity

Protect production ability and the flow of medical supplies to healthcare delivery organizations and patients. Achieve full situational awareness and comprehensive security to ensure reliable service for patients.

Compliance and safety across the entire production process

Proactively demonstrate compliance with security policies, regulations, and guidelines such as HIPAA for heath data, FDA regulations, Good Manufacturing Practices (GMP) for the production of medications, and international standards such as GDPR.

Operational resilience

Address evolving cyber threats and the convergence of new digital equipment and legacy technology. Compare asset behavior against known baselines in our AI-powered Asset Intelligence Engine and stop attacks in their tracks.

Prioritize vulnerabilities by business impact

Save hours of manual sorting through vulnerabilities and other security findings, deduplicate alerts, and address the most urgent threats based on context and potential impact to the business.

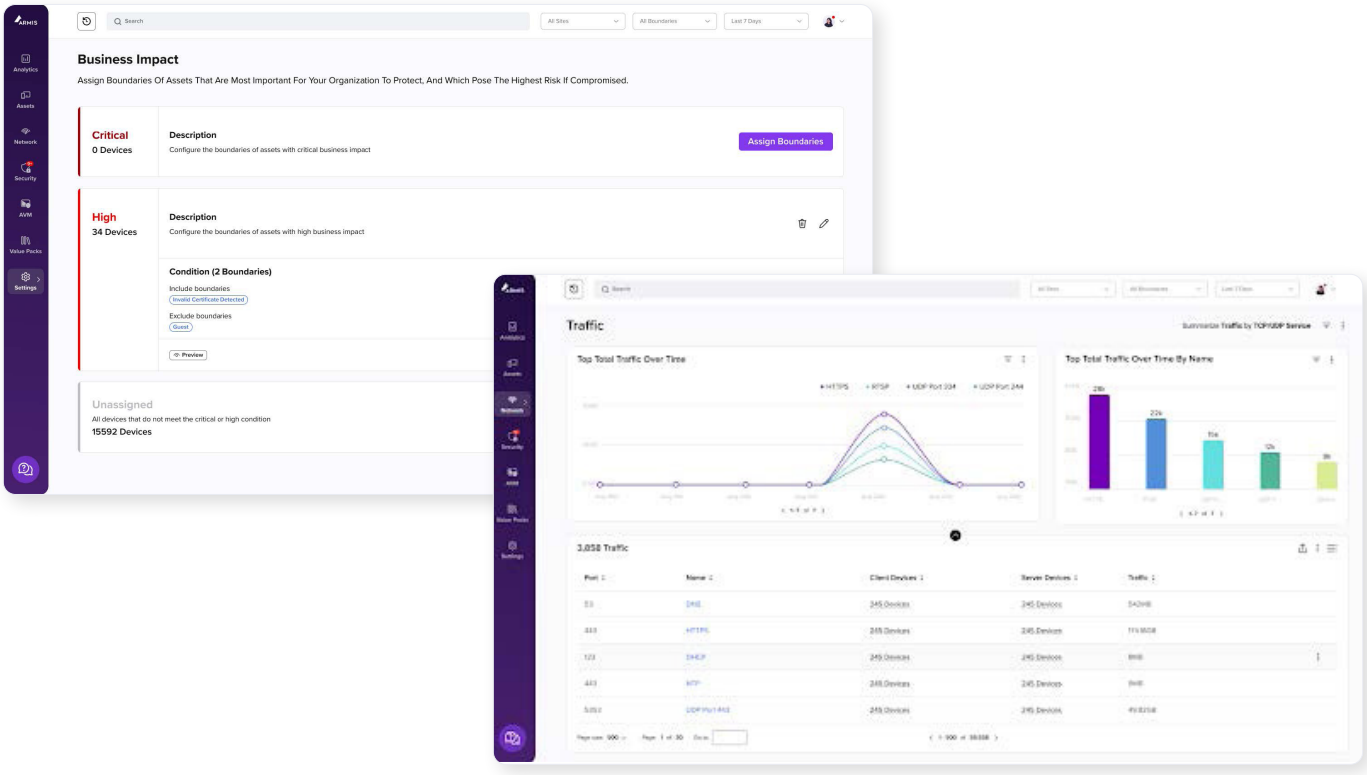
Reputation, trust, and safety

Prevent disruption, faults, or attacks that can pose unacceptable risks to patient lives and the quality of their care. Protect essential production machinery, intellectual property, sensitive patient information with leading cybersecurity practices. Uphold production quality standards to keep your organization and patients safe.

"Armis has helped increase the lifecycle management of our critical assets and overall secure our environment. The biggest value Armis brought to Fortive and our respective operating companies, has given the teams a toolset of information of the overall health of the IT environment, and now extending into IoT and other areas of focus."

Victor Fetter
Chief Information Officer
Fortive

Armis Centrix™ is the industry's most comprehensive IoMT, IoT, OT, and IT security solution, enabling pharmaceutical manufacturers to secure the assets, devices, and technologies that are the foundation of connected care innovation. Armis provides the data, insight, and action needed for pharmaceutical and biotech manufacturers to produce the highest quality materials and ensure an uninterrupted flow from facility to healthcare providers while ensuring integrity of the manufacturing process.



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