SOLUTION BRIEF

Armis Centrix™ for Healthcare

Proactive Cybersecurity for Every Patient Care Delivery Asset

53%

of medical devices have known vulnerabilities that are still exploited.

Legacy medical devices are often impossible to patch or upgrade, which prevents healthcare organizations from keeping up with security and compliance.

HALF

of healthcare organizations reported experiencing a cyberwarfare incident in 2024.

62%

of data breaches caused by **third party vendors.**

$11M

the average cost of a healthcare data breach in 2023.

Armis Centrix™ at a Glance:

Protect complex and sensitive healthcare environments with complete end-to-end cybersecurity, from asset discovery and monitoring to vulnerability prioritization and early ransomware detection

Manage clinical and operational risk with a cyber exposure management platform powered by an AI-driven Asset Intelligence Engine

Protect patient safety and enhance care capacity with total, real-time visibility of every medical/IoMT, IoT, IT, and OT device in the healthcare environment

Save time and reduce threat exposure and risk of ransomware attacks or data exfiltration with an end-to-end approach for security findings and vulnerabilities consolidation, prioritization and remediation

Demonstrate compliance to regulations and frameworks with comprehensive cybersecurity, reporting, and preventive risk mitigation

Maintain operations and availability for patient services with proactive monitoring and real-time alerting

An Explosion of Assets and Threats, While Cyberattacks Continue to Increase

Healthcare organizations deliver lifesaving and life-improving care every day and rely on a wide array of technology devices to help patients, ensure better outcomes, and provide continuous care from intake to release. Healthcare Delivery Organizations (HDOs) are also one of the world's largest targets for ransomware attacks. In an industry permeated by technology, from infusion pumps and MRIs to mobile devices or building management systems, it is more important than ever for healthcare to bolster its defenses to prevent cyberattacks.

Top Healthcare Cybersecurity Threats

- **Ransomware Attacks** - Targeting healthcare networks, including connected medical devices, to disrupt operations and demand ransom. These attacks lead to operational downtime and risks to patient safety. Ransomware attacks have doubled in frequency over the past two years.
- **Unpatched Software and Firmware** - 53% of medical devices have known vulnerabilities that are still exploited. Outdated systems with known vulnerabilities can lead to unauthorized access or manipulation of device functionality.
- **Third-Party Risk** - 62% of organizations experienced a third-party data breach or cybersecurity incident in 2024. Unauthorized remote access via unsanctioned or unsecured apps on unmanaged vendor servers remains a top risk vector. High-profile attacks have exposed sensitive records, impacting millions of patients worldwide.
- **Data Breaches** - Exploiting devices to steal patient health information (PHI) or sensitive operational data. 2023 was a record-breaking year for data breaches. 725 breaches were reported to the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and exposed or impermissibly disclosed more than 133 million records. Breaches violate privacy laws and risk financial and reputational damage.

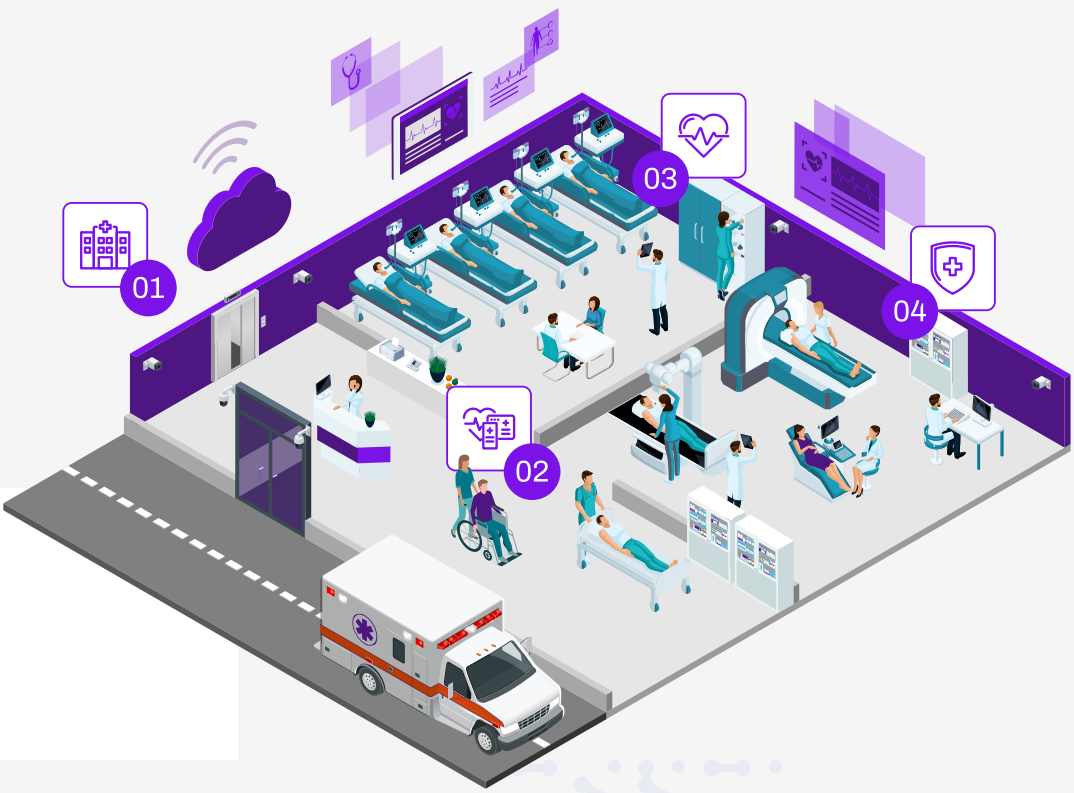
The Healthcare Attack Surface

As healthcare delivery organizations continue to adopt innovative technology, the cyber attack surface is dynamic and constantly expanding.

The average hospital uses thousands of network-connected devices—about 17 per hospital bed.

90% of attacks originate in IoT devices, highlighting the need for a comprehensive security strategy that protects the entire healthcare environment.

See, Protect, and Manage the Entire Healthcare Environment, including:



01 Overall facility

- HVAC systems
- Building Management Systems
- IT and WiFi networks
- CCTV cameras
- Building security systems
- Staff scheduling systems
- Elevators
- Printers and FAX machines

02 Patient & Emergency Admission

- Hospital apps
- Electronic Patient Records
- Digital signage
- Queue management systems
- PA system

03 Triage and Medical Examination

- Patient entertainment systems
- Intercom
- Monitors
- Pagers & staff messaging apps
- Clinician mobile devices
- Medical devices

04 Treatment, Surgery, Procedures, Diagnosis

- Medication cabinets
- Medical devices for scans, imaging
- Third parties (pathology labs, etc)
- AI diagnostics tools
- Surgical robotic arms

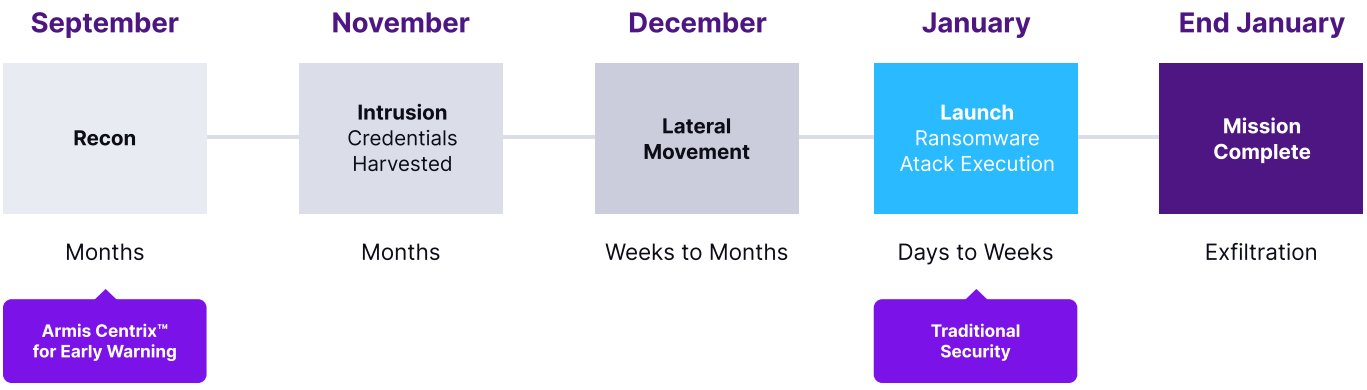
Anatomy of a Healthcare Cyberattack

Cyberattacks in healthcare are often lurking undetected within technology environments for weeks, even months, before their devastating impacts are felt. Attackers exploit vulnerabilities like stolen credentials or weak authentication to gain entry, then move laterally through the system to identify and exploit valuable data.

Early detection and intervention are critical. If these exploit attempts are left unchecked, attacks can cause catastrophic disruptions to operations, compromising patient care and potentially putting lives at risk.

Phases of a Cyberattack Can Include:

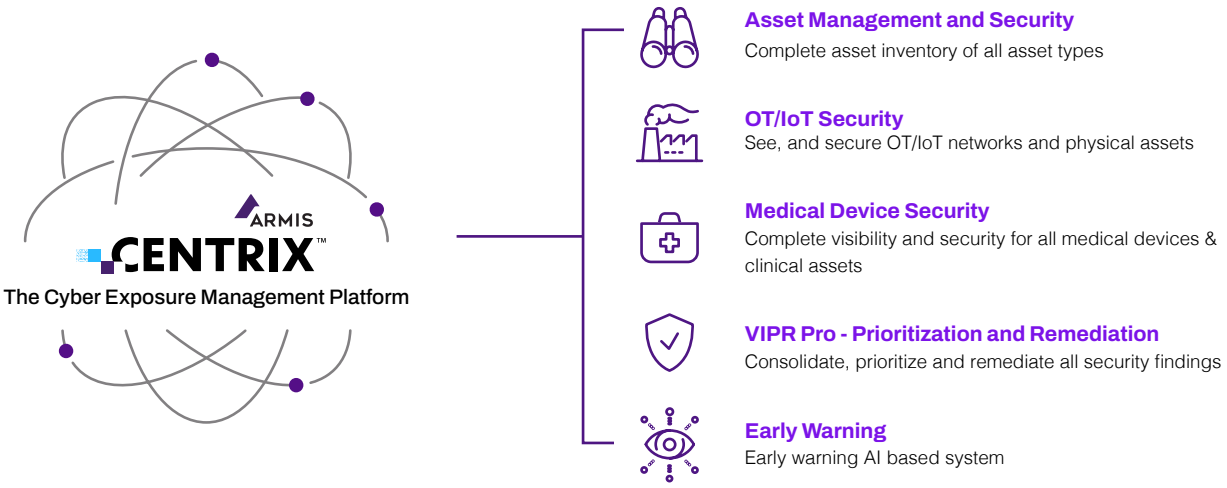
- Reconnaissance - Harvesting stolen credentials
- Access to network via exploit
- Access to patient and sensitive data
- Exploit or vulnerability weaponization
- Ransomware deployment & installation
- Exfiltration of data externally
- Threat actor control, operational disruption
- Procedure standstill and rescheduling
- Financial and legal fallout
- Restoration and reputational damage control



Armis Centrix™ for Early Warning empowers organizations to preempt cyber attacks with early indicators of vulnerabilities that threat actors are exploiting in the wild or are about to weaponize.

Introducing Armis Centrix™

Armis Centrix™, the Armis Cyber Exposure Management Platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, protects, and manages billions of assets worldwide in real time. Armis Centrix™ is a cloud-based platform that proactively identifies and mitigates all cyber asset risks, remediates security findings and vulnerabilities, and protects your entire attack surface.



The Armis Healthcare Security Suite

Armis revolutionizes healthcare cybersecurity by addressing the unique challenges of protecting complex, sensitive medical devices and the broader healthcare environment. Designed for Healthcare Delivery Organizations (HDOs), the Suite seamlessly integrates with existing systems to deliver:

- Visibility of All Assets and Risks
- Contextual, Real-time Asset Intelligence
- Comprehensive Protection of the Entire Expanded Attack Surface
- Continuous Device Behavior Insights
- Early Warning Alerts to Preempt Threats
- Streamlined Risk Prioritization, Mitigation, and Remediation

“The biggest security challenge that we faced before Armis was getting real insights into all the assets that we effectively manage on the network.”

“Armis delivered fast results effectively and efficiently.”

Kurt Gielen
IT Manager, Ziekenhuis Oost-Limburg

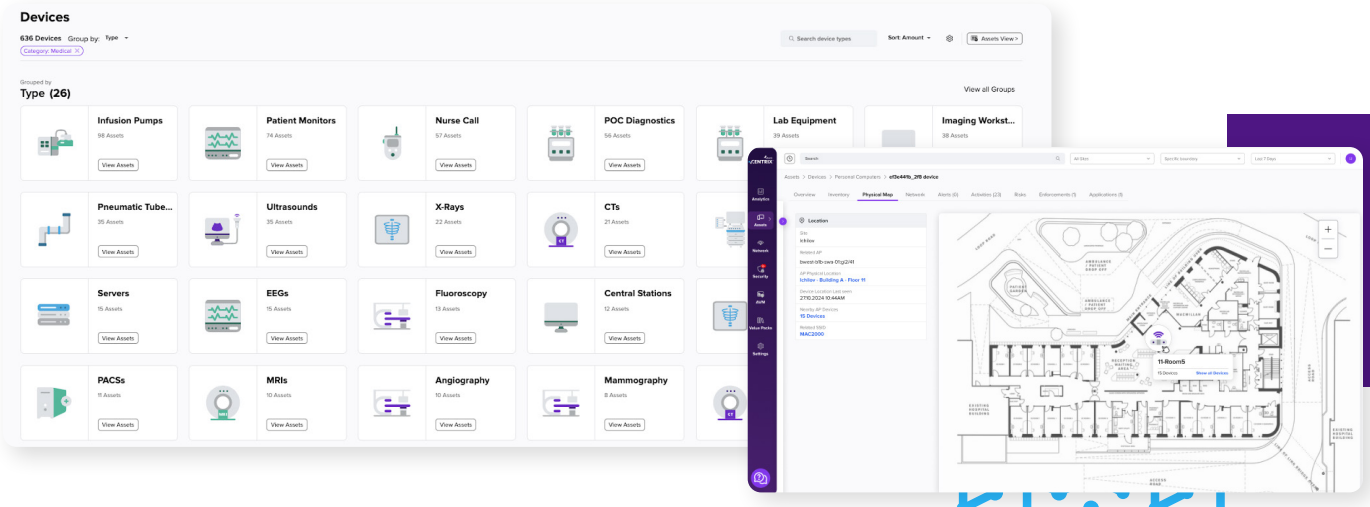
1. Visibility of All Assets and Risks

The Challenge: Healthcare organizations have multiple asset and device types, many of which are legacy devices that are unseen or unmanaged.

To deliver advanced, quality patient care, healthcare organizations are adopting massive numbers of connected medical devices. But unlike conventional IT assets, such as laptops and desktop computers, most of these existing, legacy medical devices are unmanaged and un-agentable, which means your traditional security solutions can’t see or secure them. And when those assets go unchecked, your patients’ safety, records, and privacy are at risk.

Armis Centrix™ is the industry’s most comprehensive exposure management and security platform. It offers complete visibility and best-in-class security across the entire healthcare device ecosystem – with zero disruption to patient care. Physical map capabilities allow you to easily pinpoint the location of your devices to power effective risk scoring and decision-making, as well as streamlined remediation. Out-of-the-box integration capabilities ensure you can access all your information in a single location to leverage the full power of your security stack.

Armis Centrix™ gives you the full picture of every asset and every risk in your environment, to keep your healthcare environment safe and your patients protected.



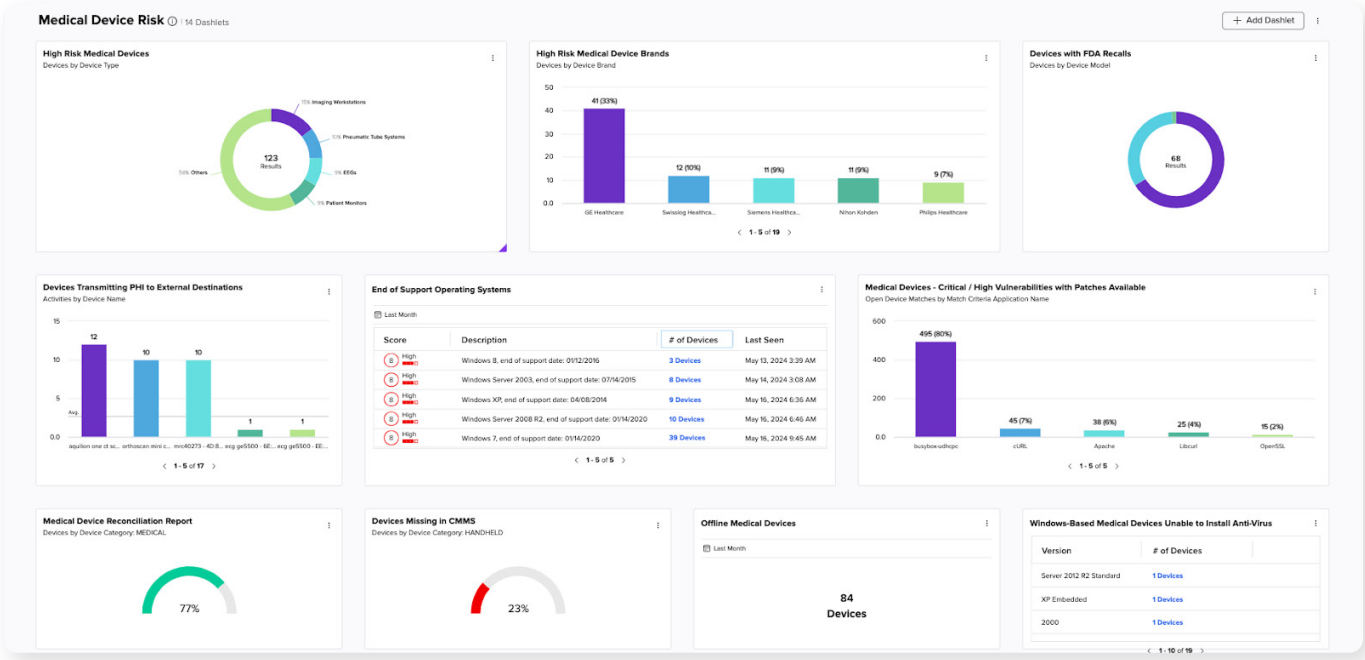
2. Contextual, Real-Time Asset Intelligence

The Challenge: Traditional asset inventory is limited and static, doesn't consider clinical context and usage.

Armis goes beyond a basic asset inventory and delivers actionable insights about your devices, where they are located, how they are being utilized, and their importance to patient care for more accurate, patient-centric risk scoring and recommendations. Consider the clinical risk of every asset and their proximity and criticality to patient care, allowing technology such as Electronic Patient Record (EPR) systems to be effectively classified and protected. Armis Centrix™ has the largest asset behavior knowledge base in the world, with our Asset Intelligence Engine, tracking over 5 billion assets and counting.

Easily identify new assets on your network and their "known good" baseline of behavior for effective categorization needed for policy management. Armis Centrix™ aggregates, normalizes, appends and contextualizes data from connected assets to enhance decision-making. Immediately understand what an asset is, how and where it is used and its behavior profile. Advanced policy management, anomaly detection, and network segmentation facilitate security for even the most sensitive assets that don't allow traditional security solutions.

The Armis Asset Intelligence Engine easily combines asset information, risk profile, and clinical context to manage risks effectively throughout the entire healthcare ecosystem.



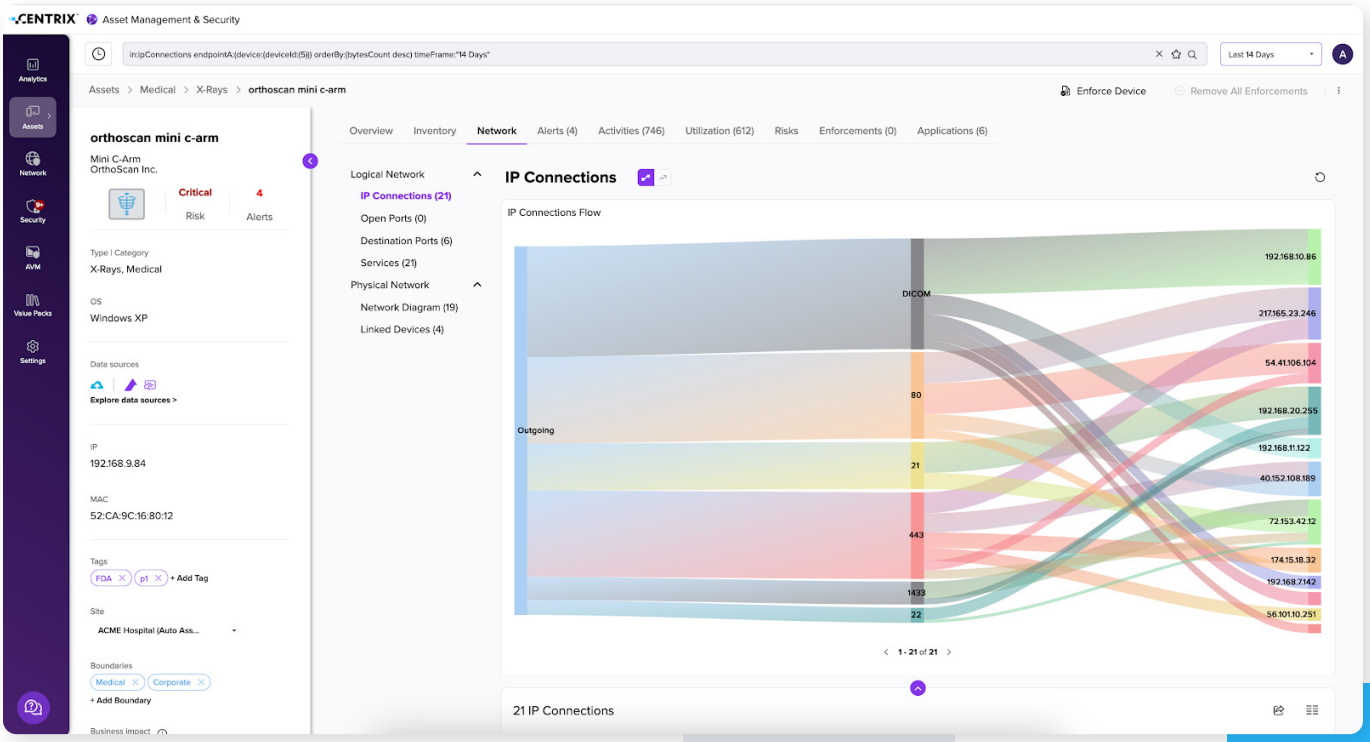
3. Comprehensive Protection of the Entire Attack Surface

The Challenge: Many solutions only protect medical devices or have limited coverage for the entire technology ecosystem used in healthcare environments.

Armis Centrix™ combines comprehensive risk scoring and detailed device profiles to power more proactive risk mitigation and cyber resilience. As devices are accurately cataloged and a baseline understanding of their role and function is established, this is used to detect early signs of compromise.

Advanced analytics, alerts, and policies can effectively segment and mitigate risks for medical vs non-medical assets once anomalous behavior is detected, and prevent further movement throughout your network. This minimizes risk and protects patient data from external transmission.

Armis Centrix™ delivers advanced risk scoring and insights for medical and non-medical devices for easier, proactive mitigation and protection.

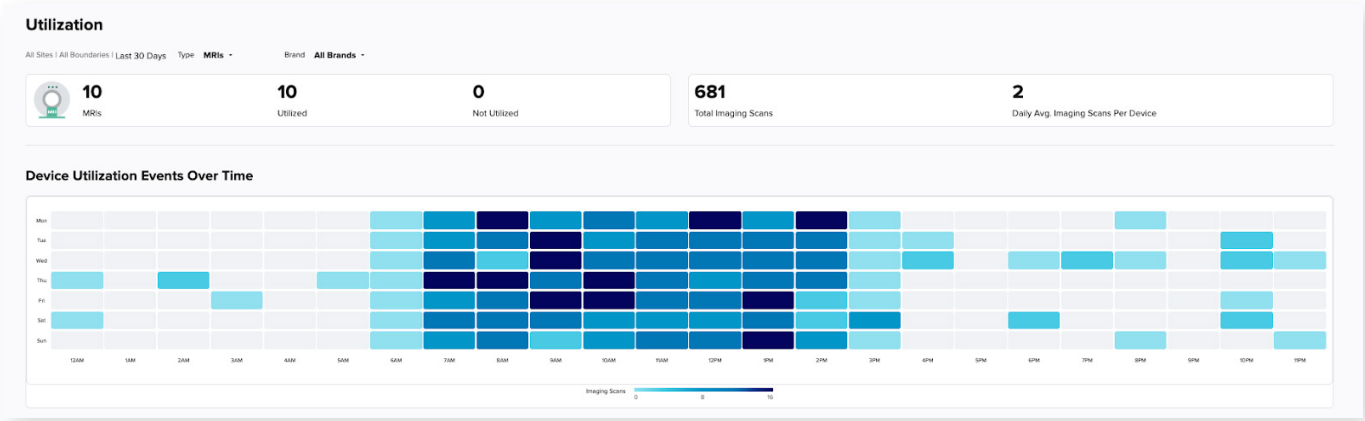


4. Continuous Device Behavior Insights

The Challenge: Healthcare delivery organizations require insights on their medical devices for resource allocation, budget forecasting, and better patient flow.

Armis Centrix™ for Medical Device Security provides comprehensive visibility into all assets and tracks medical device utilization over time. This facilitates better resource allocation, improved patient flow, optimized investment in medical devices, and extended lifespan through efficient utilization. By pinpointing the physical location of each asset, Armis enables better risk analysis and streamlined remediation. It also tracks and manages FDA recall and MDS² information, improving collaboration across clinical engineering and IT security teams. This comprehensive view of device security and utilization maximizes operational efficiency, ensures that all device information is accessible in a single platform, and enables the wider organization with insights for operational and financial decision-making.

Armis Centrix™ for Medical Device Security provides detailed device security and utilization insights to maximize operational efficiency and ensure that all device information is accessible in a single platform.



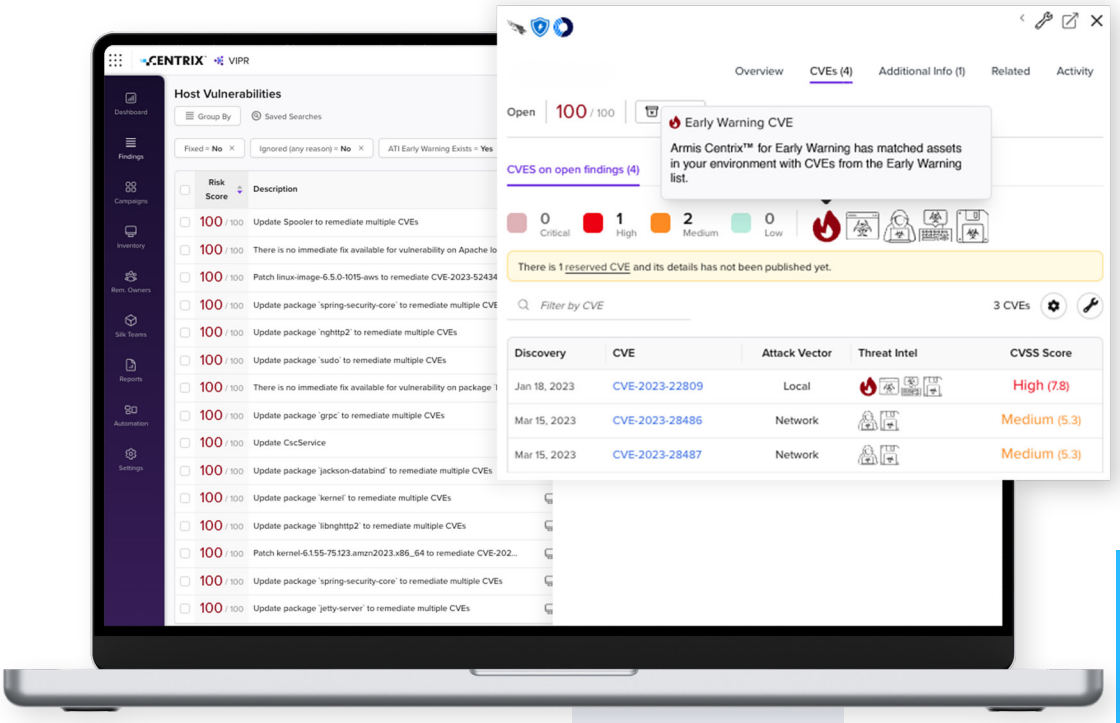
5. Early Warning Alerts to Preempt Threats

The Challenge: Organizations often focus remediation efforts on the newest vulnerabilities or overlook those actively exploited by attackers, reducing the ROI on security efforts.

Armis Centrix™ leverages AI-driven actionable intelligence and machine learning that scours the dark web, coupled with smart honeypots and human intelligence to deliver an early warning system for vulnerabilities that threat actors are exploiting. These early indicators of potential attacks empower you with insights that let you take action before a vulnerability is announced, before an attack is launched and before your organization is impacted.

Armis Centrix™ for Early Warning delivers real-time threat intelligence about tactics attackers use and their potential impact to protect against zero-day vulnerabilities and threats including ransomware for unparalleled coverage and accuracy. Prioritize mitigation based on the current threat landscape to remediate the biggest threats before attackers can leverage them, effectively moving the security posture from reactive to proactive.

Armis Centrix™ for Early Warning protects healthcare organizations from emerging attack methods to prevent downtime or disruptions.



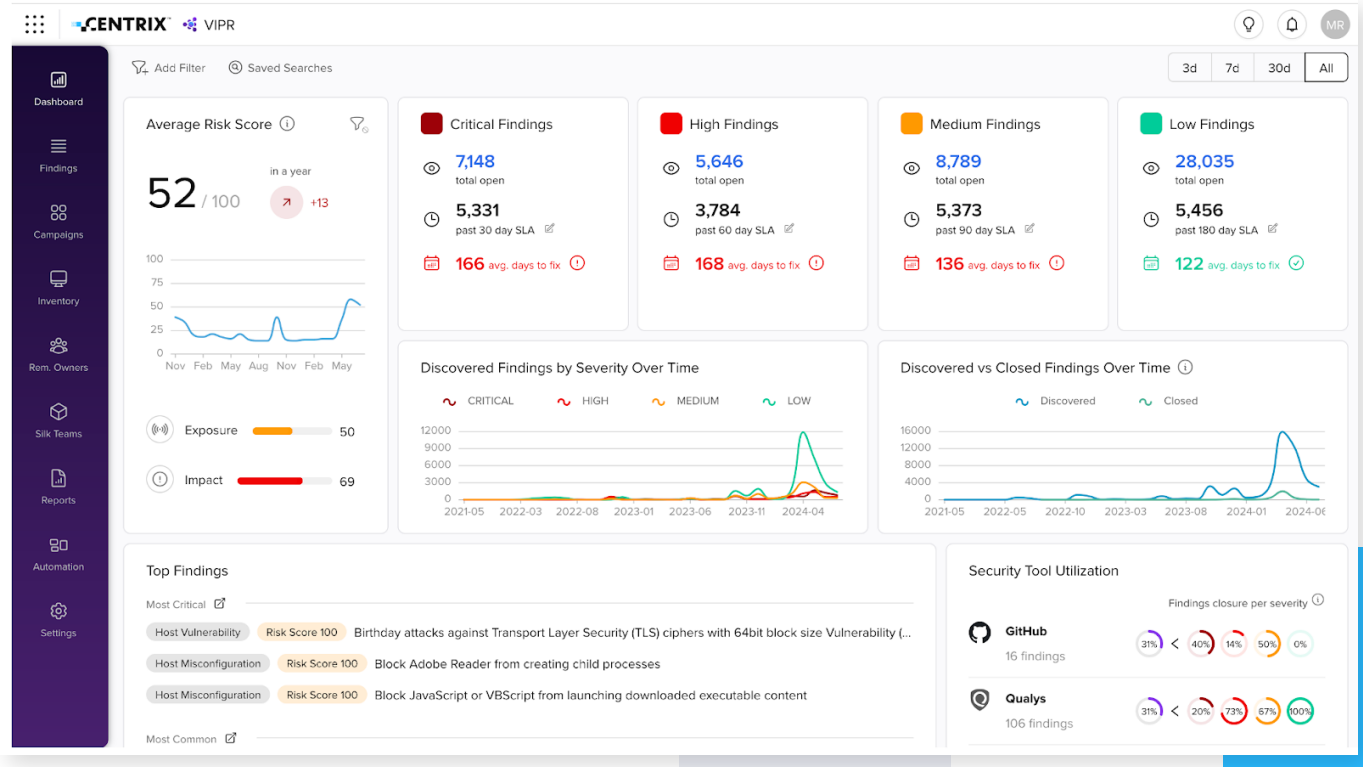
6. Streamlined Risk Prioritization, Mitigation, and Remediation

The Challenge: Security teams are inundated with vulnerabilities and dealing with fragmented processes and disparate tools with no clear mitigation steps.

Healthcare organizations are overwhelmed by the sheer volume of vulnerable assets in their environment at any given moment. With Armis Centrix™ for VIPR – Prioritization and Remediation, you can first address the biggest potential interferences in clinical care, and eliminate the time it takes to sort through alerts manually.

Consolidate vulnerabilities and other security findings. Collect, deduplicate, contextualize, and prioritize these findings based on the relative risk to the site. Automatically assign owners and initiate remediation workflows, prioritized based on asset criticality and clinical risk score, to focus efforts on addressing the biggest impacts on patient safety, data confidentiality, and potential disruptions of care. Avoid unnecessary delays in care or downtime of medical devices due to lengthy and complex processes.

Armis Centrix™ for VIPR – Prioritization and Remediation drastically reduces the effort involved in vulnerability management, allowing you to target efforts on the biggest threats to operations and patient safety. A single solution facilitates greater collaboration between IT security and clinical engineering workflows.



Key Benefits

- **Full-scope visibility and protection** reduce outages and keep your organization and patients safe
- **Streamlined clinical engineering workflows for managing recalls**, vulnerabilities and other security findings
- **Enhanced patient safety** with greater device security and data protection for EPRs
- **Comprehensive protection for every asset** within the healthcare attack surface within a single platform
- **Real-time intelligence and early warning alerts** for proactive protection
- **Faster vulnerability and threat detection** minimizes the risk and impacts of cyberattacks

The Armis Difference

Leader in Cybersecurity – Protecting the Entire Healthcare Ecosystem

The modern healthcare attack surface extends far beyond just medical devices. Armis Centrix™ provides the only platform that allows you to see, protect, and manage the risk of every device – IT, OT, IoT, and IoMT – all in one place. Our platform is consistently recognized as a leader by top industry analysts, including Gartner, Forrester, Frost & Sullivan, KLAS, and Quadrant Knowledge Systems, ensuring you get the best protection for your healthcare organization.

Industry Leading Asset Intelligence

Only Armis has an AI-driven Asset Intelligence Engine that understands 'known good' behavior baselines for over 5 billion assets. Identify, classify, aggregate, and enrich assets with context.

Risk Prioritization and Remediation

Only Armis prioritizes risks based on the organization's most critical assets, and when, where, and how it is used. Save hours of manual effort and quickly assign, action, and resolve the top-priority findings.

Accurate Profiling and Early Warning Threat Detection

Quickly discover, contextualize, enrich, and profile every asset using hundreds of pre-built integrations, network telemetry, and an AI-driven Asset Intelligence Engine. Early Warning data adds awareness of potential risks relevant to your industry before they can take hold.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. 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 stay 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