SOLUTION BRIEF

Patient-Centric Vulnerability Management for Healthcare

Contextualize, Prioritize, Manage, and Reduce Risk Throughout Every Step of the Patient Journey

Overview

Traditional vulnerability management falls short in healthcare. A missed patch or delayed remediation can mean more than data loss; it can mean compromised patient safety. Armis Centrix™ redefines how healthcare organizations manage and mitigate cyber risk by shifting the focus to what truly matters: protecting patients and care delivery.

With Armis Centrix™, vulnerability management becomes intelligent, automated, and clinically aligned. Instead of drowning in alert fatigue and manual processes, healthcare security and clinical engineering teams gain a unified understanding of every security finding across the full care ecosystem.

Our platform assigns ownership, launches remediation workflows, and ranks issues based on patient proximity, device criticality, and operational impact, ensuring that resources are directed to where they'll make the most impact. By removing bottlenecks, automating triage, and embedding clinical context into every step, Armis Centrix™ empowers healthcare providers to minimize risk, prevent costly downtime, and deliver safe, uninterrupted care.

Armis Centrix™ at a Glance:

80% reduction of manual risk assessment with risk consolidation, deduplication, and AI-driven contextualization of findings

50% faster time to patch critical vulnerabilities, reducing the risk of breaches

7x increase in closed findings annually with streamlined processes

90% reduced operational overhead with automated ownership and ticketing

Millions of dollars saved by neutralizing high-impact threats and ransomware attacks

The Downfalls of Traditional Vulnerability Management in Healthcare

The healthcare industry is one of the most targeted by advanced cyberattacks, with widespread threats from ransomware, third-party risks, and data breaches. Increased innovation in technology-assisted patient care translates to more assets and a tangled web of interconnections between them, bringing a new influx of cyber exposure risks. Without a clear prioritization strategy, the volume of alerts and security findings can overwhelm already underresourced teams, creating massive security gaps that can compromise patient safety and the continuity of care.

From imaging systems and wearable monitors to supporting IT infrastructure and even building management systems (BMS), security teams at healthcare delivery organizations must consider the entire attack surface, not just medical devices. To minimize the risk of exploits, impacts on care availability and patient outcomes, all vulnerabilities, as well as risk factors such as end-of-life (EOL) assets, must be viewed through both a cyber exposure management and clinical lens for effective prioritization and remediation.

60%

of cyberattacks exploit known but unpatched vulnerabilities and **53% of medical devices have known vulnerabilities.**

While initial response to cybersecurity threats can take

1 to 5 hours,

full resolution can take days or weeks.

Ransomware attacks take

21 days

on average for full remediation.

With 17 connected devices per hospital bed and up to 23 vulnerabilities on each medical device, the average hospital can have

over 50,000

vulnerabilities directly touching patients.

Key Components of Patient-Centric Vulnerability Management

Armis Centrix™ offers a patient-centric approach to vulnerability management in healthcare by prioritizing risks to patient safety, care delivery, and operational continuity. By addressing the downfalls of traditional methods with holistic attack surface coverage, proactive risk alerts, clinical asset context, risk-based prioritization, automated remediation, and comprehensive reporting, healthcare delivery organizations can provide true protection for their patients across every technology asset they interact with.

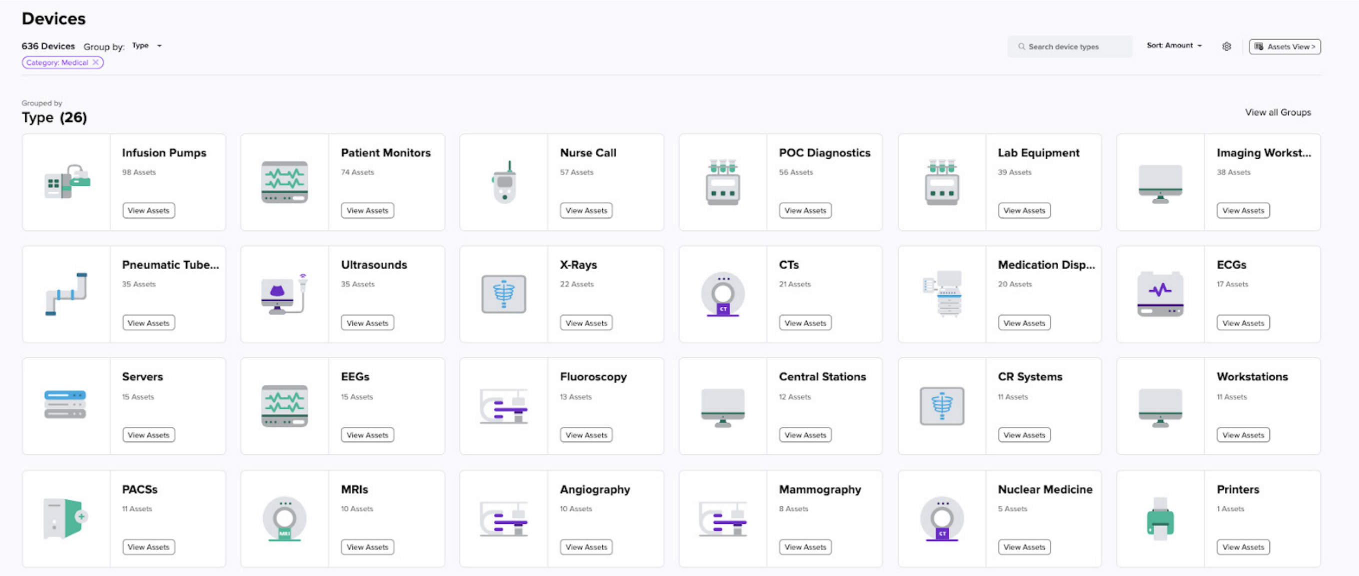
1. **Holistic Attack Surface Coverage**
2. **Early & Proactive Risk Alerts**
3. **Clinical Asset Context**
4. **Clinical Risk-Based Prioritization**
5. **Automated Remediation & Response**
6. **Compliance & Reporting**

1. Holistic Attack Surface Coverage

Power proactive risk mitigation and cyber resilience with visibility and protection of the entire patient care technology ecosystem. Detect early signs of compromise from anomalous behavior to minimize risk and maintain uptime.

- **Dynamic Inventory -** Complete visibility of your entire technology ecosystem, spanning medical devices, IT, OT, IoT, and medical device assets, whether physical, logical, or virtual, for a view of every asset supporting the patient journey.
- **Advanced Analytics -** Asset intelligence compares asset behavior to a known good baseline. Alerts and policies can effectively mitigate risks as soon as the earliest threat indicator is detected.
- **Multi-detection Engine -** Employs multiple configurable detection methods, including network traffic or behavior-based anomaly detection, in order to find more and secure more.
- **Integration with Diverse Tech Stacks -** Maximize your existing investments and provide comprehensive visibility and protection by leveraging our hundreds of pre-built integrations.

The Armis Impact: A single pane of glass view of every technology asset in your environment.



Devices

636 Devices Group by: Type

Category: Medical

Grouped by

Type (26)

Infusion Pumps 98 Assets

Patient Monitors 74 Assets

Nurse Call 57 Assets

POC Diagnostics 56 Assets

Lab Equipment 39 Assets

Imaging Workst... 38 Assets

Pneumatic Tube... 35 Assets

Ultrasounds 35 Assets

X-Rays 22 Assets

CTs 21 Assets

Medication Disp... 20 Assets

ECGs 17 Assets

Servers 15 Assets

EEGs 15 Assets

Fluoroscopy 13 Assets

Central Stations 12 Assets

CR Systems 11 Assets

Workstations 11 Assets

PACSs 11 Assets

MRIs 10 Assets

Angiography 10 Assets

Mammography 8 Assets

Nuclear Medicine 5 Assets

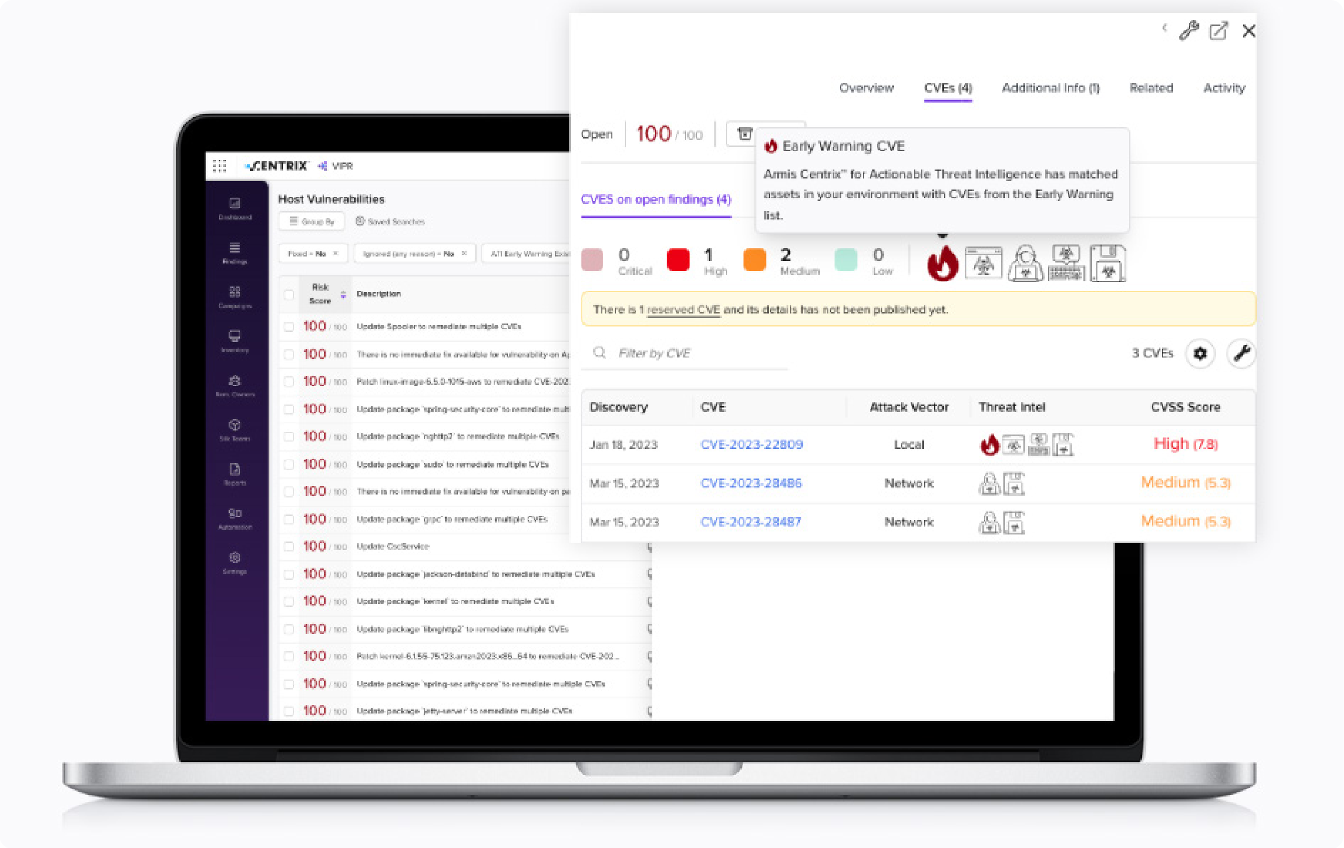
Printers 1 Assets

2. Early & Proactive Risk Alerts

Proactively identify actively exploited vulnerabilities using AI and threat intelligence, including zero-day and ransomware, enabling timely mitigation and protecting healthcare organizations from disruptions. Focus efforts on the small percentage of risks that matter most before they're exploited.

- **Early Warning Intelligence -** 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.
- **Timely Alerts -** Notifications of impending threats and Early Warning threat alerts provide insights into potential exploits before a CVE is published.

The Armis Impact: 98% reduction in the vulnerabilities you need to worry about with proactive threat insights.



Host Vulnerabilities

Risk Score	Description
100 / 100	Update Spooler to remediate multiple CVEs
100 / 100	There is no immediate fix available for vulnerability on Ap
100 / 100	Patch linux-image-6.5.0-1015-aws to remediate CVE-202
100 / 100	Update package 'spring-security-core' to remediate mult
100 / 100	Update package 'nghttp2' to remediate multiple CVEs
100 / 100	Update package 'sudo' to remediate multiple CVEs
100 / 100	There is no immediate fix available for vulnerability on pa
100 / 100	Update package 'grpc' to remediate multiple CVEs
100 / 100	Update CscService
100 / 100	Update package 'jackson-databind' to remediate multiple CVEs
100 / 100	Update package 'kernel' to remediate multiple CVEs
100 / 100	Update package 'libnghttp2' to remediate multiple CVEs
100 / 100	Patch kernel-6.1.55-75.123.amzn2023.x86_64 to remediate CVE-202...
100 / 100	Update package 'spring-security-core' to remediate multiple CVEs
100 / 100	Update package 'jetty-server' to remediate multiple CVEs

Early Warning CVE

Armis Centrix™ for Actionable Threat Intelligence has matched assets in your environment with CVEs from the Early Warning list.

There is 1 reserved CVE and its details has not been published yet.

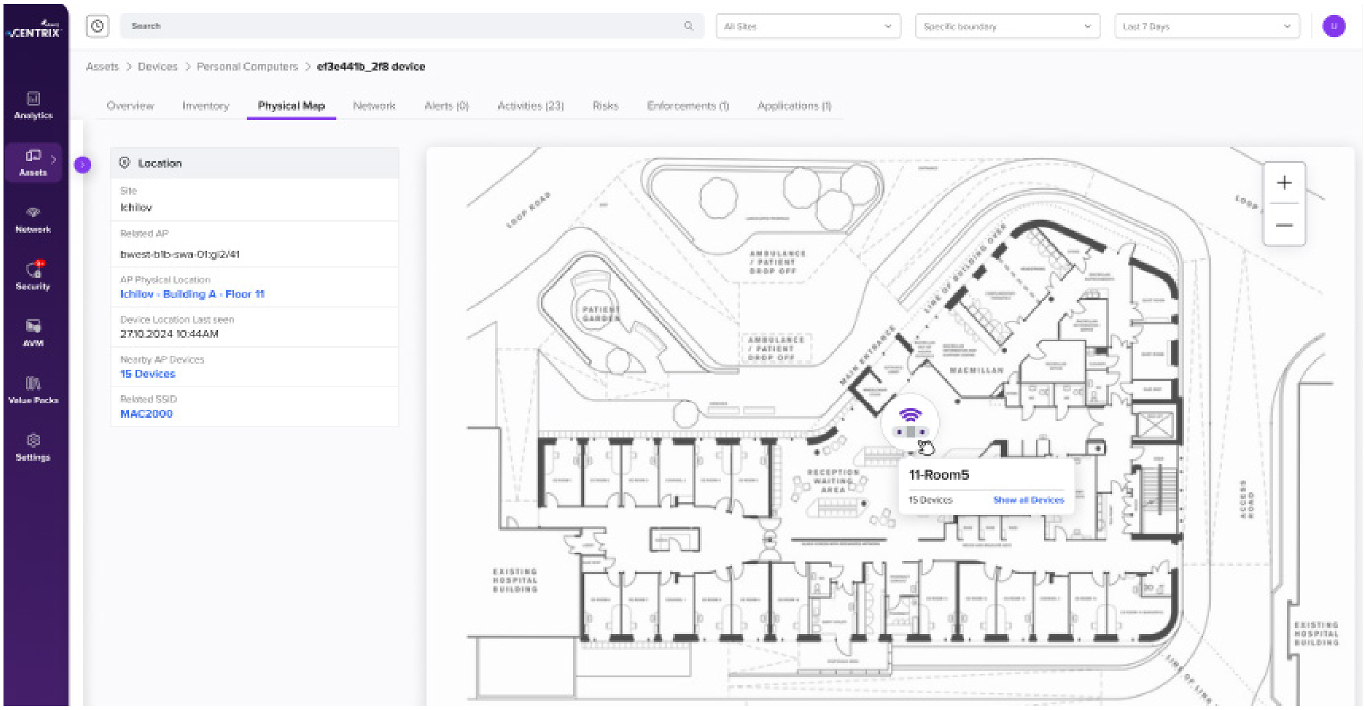
Discovery	CVE	Attack Vector	Threat Intel	CVSS Score
Jan 18, 2023	CVE-2023-22809	Local		High (7.8)
Mar 15, 2023	CVE-2023-28486	Network		Medium (5.3)
Mar 15, 2023	CVE-2023-28487	Network		Medium (5.3)

3. Clinical Asset Context

Standard asset visibility is not enough to secure smart hospitals and modern healthcare environments. Detailed asset insights about clinical usage, location, patient proximity, and behavioral context is necessary to power comprehensive cybersecurity.

- **Asset Intelligence Engine -** Core to the Armis platform is our Asset Intelligence Engine, the largest crowd-sourced, cloud-based asset behavior knowledgebase in the world, tracking billions of assets. Identify, classify, aggregate, and enrich assets with context about usage and known good behavior.
- **Utilization Data -** Insights about medical device utilization, including high and low-frequency usage times, inform better resource allocation and patient flow, maximizing the lifespan of your devices.
- **Location -** Visualize devices in their actual locations on detailed floor maps for improved situational awareness, location-based policies, and streamlined medical device management across floors and sites.

The Armis Impact: Reduce manual utilization analysis by 50% to optimize asset lifecycle management and procurement.



Location

Site
Ichilov

Related AP
bwest-b1b-swa-01:gi2/41

AP Physical Location
Ichilov · Building A · Floor 11

Device Location Last seen
27.10.2024 10:44AM

Nearby AP Devices
15 Devices

Related SSID
MAC2000

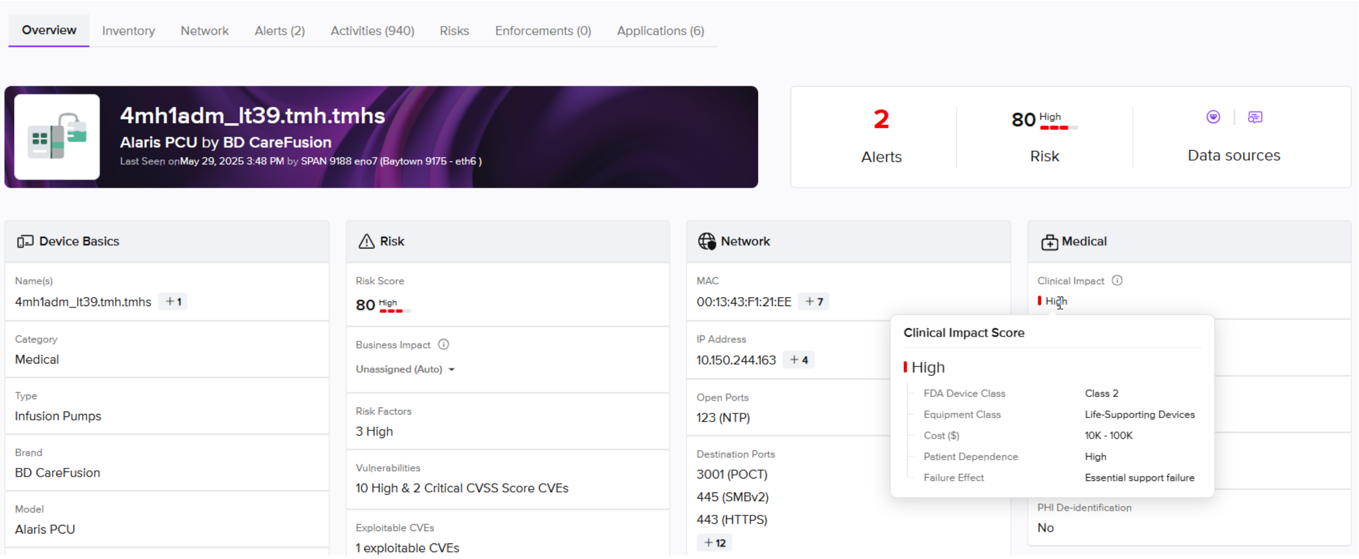
11-Room5
15 Devices

4. Clinical Risk-Based Prioritization

Effective hospital risk prioritization considers patient safety, operational continuity, and medical device security. Armis Centrix™ prioritizes remediation based on clinical risk and asset criticality, avoiding unnecessary delays and downtime.

- **Clinical Impact Score -** Determine the clinical impact of device malfunction or exploit based on FDA class, equipment class, patient dependence, and the effect of failure. Triage risks to patient safety and operational resilience, and manage vulnerabilities and risk accordingly.
- **Medical Device Recalls -** Armis Centrix™ offers a direct integration with the FDA recall database, as well as other advisory databases, including CISA. Recalls and advisories are then amalgamated in the Armis Centrix™ platform, automatically associated with each relevant device.
- **MDS² -** Armis Centrix™ catalogs all medical devices, provides the relevant MDS² file, and associates it with each device. All privacy and security attributes are extracted and visible directly in the Armis Centrix™ platform to facilitate easy action and reporting. View detailed risk assessments per device based on MDS² properties.
- **Customizable Risk Scoring -** Adjust risk scores based on your environment and/or unique use cases. Your hospital, your risks.and sites.

✓ **The Armis Impact:** Efficient recall management and remediation cuts open FDA recalls in half, protecting patient care delivery



4mh1adm_lt39.tmh.tmhs
Alaris PCU by BD CareFusion
Last Seen onMay 29, 2025 3:48 PM by SPAN 9188 eno7 (Baytown 9175 - eth6)

2 Alerts
80 High Risk
Data sources

Device Basics

Name(s)
4mh1adm_lt39.tmh.tmhs +1

Category
Medical

Type
Infusion Pumps

Brand
BD CareFusion

Model
Alaris PCU

Risk

Risk Score
80 High

Business Impact
Unassigned (Auto)

Risk Factors
3 High

Vulnerabilities
10 High & 2 Critical CVSS Score CVEs

Exploitable CVEs
1 exploitable CVEs

Network

MAC
00:13:43:F1:21:EE +7

IP Address
10.150.244.163 +4

Open Ports
123 (NTP)

Destination Ports
3001 (POCT)
445 (SMBv2)
443 (HTTPS)
+12

Medical

Clinical Impact
High

PHI De-identification
No

Clinical Impact Score

High

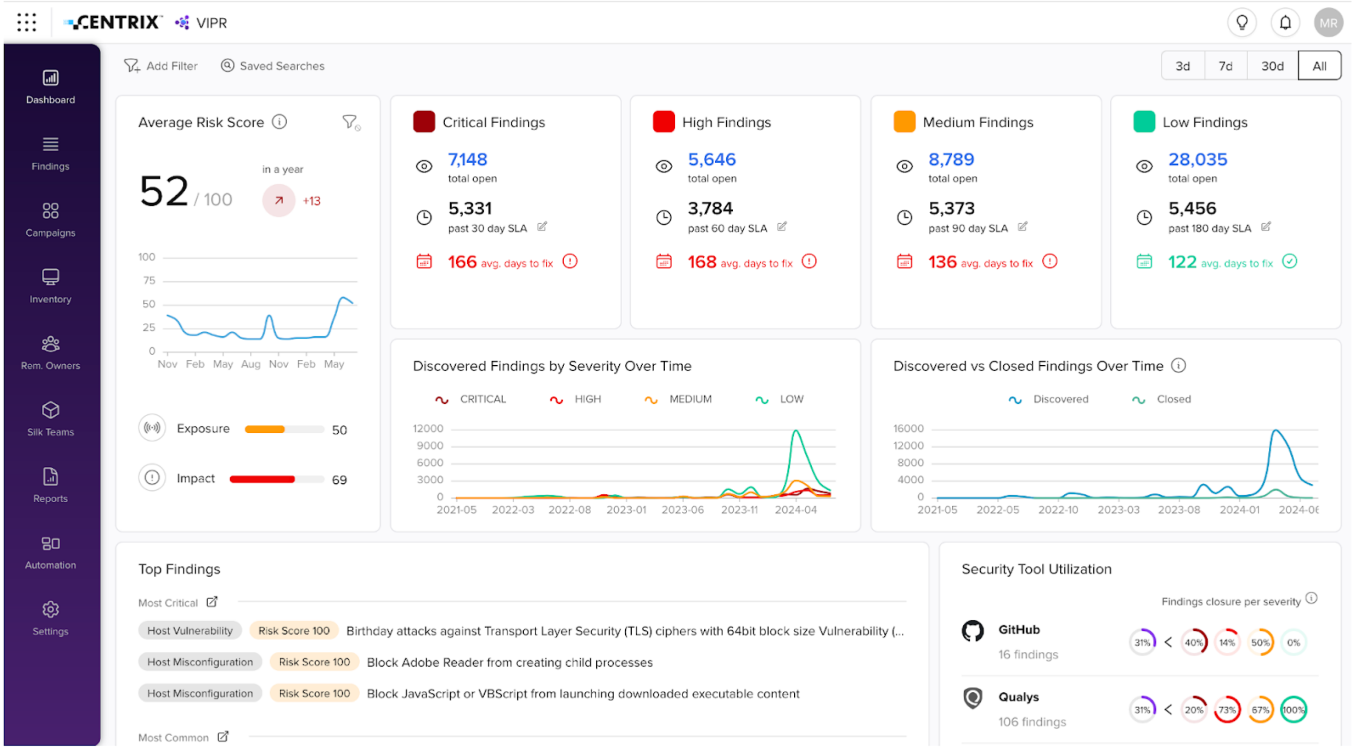
FDA Device Class	Class 2
Equipment Class	Life-Supporting Devices
Cost ($)	10K - 100K
Patient Dependence	High
Failure Effect	Essential support failure

5. Automated Remediation & Response

Streamline remediation with a single platform for security, IT, compliance, and clinical teams. Leverage automation to reduce manual intervention bottlenecks.

- **Automated Ownership Assignment -** 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 and care.
- **Compensating Controls -** Apply either manual or automated network segmentation according to device type, firewall rules, and application controls for rapid containment of high-risk vulnerabilities.
- **Workflow Integration -** Connect vulnerability management to ITSM platforms (ServiceNow, JIRA)—Automate ticket creation and tracking within a centralized platform.

✓ **The Armis Impact: 80% reduction in manual vulnerability management efforts,** for more efficient, timely protection



Average Risk Score

52 / 100 in a year +13

Exposure 50

Impact 69

Critical Findings	High Findings	Medium Findings	Low Findings
7,148 total open	5,646 total open	8,789 total open	28,035 total open
5,331 past 30 day SLA	3,784 past 60 day SLA	5,373 past 90 day SLA	5,456 past 180 day SLA
166 avg. days to fix	168 avg. days to fix	136 avg. days to fix	122 avg. days to fix

Top Findings

Most Critical

Host Vulnerability	Risk Score 100	Birthday attacks against Transport Layer Security (TLS) ciphers with 64bit block size Vulnerability (...
Host Misconfiguration	Risk Score 100	Block Adobe Reader from creating child processes
Host Misconfiguration	Risk Score 100	Block JavaScript or VBScript from launching downloaded executable content

Most Common

Security Tool Utilization

GitHub 16 findings

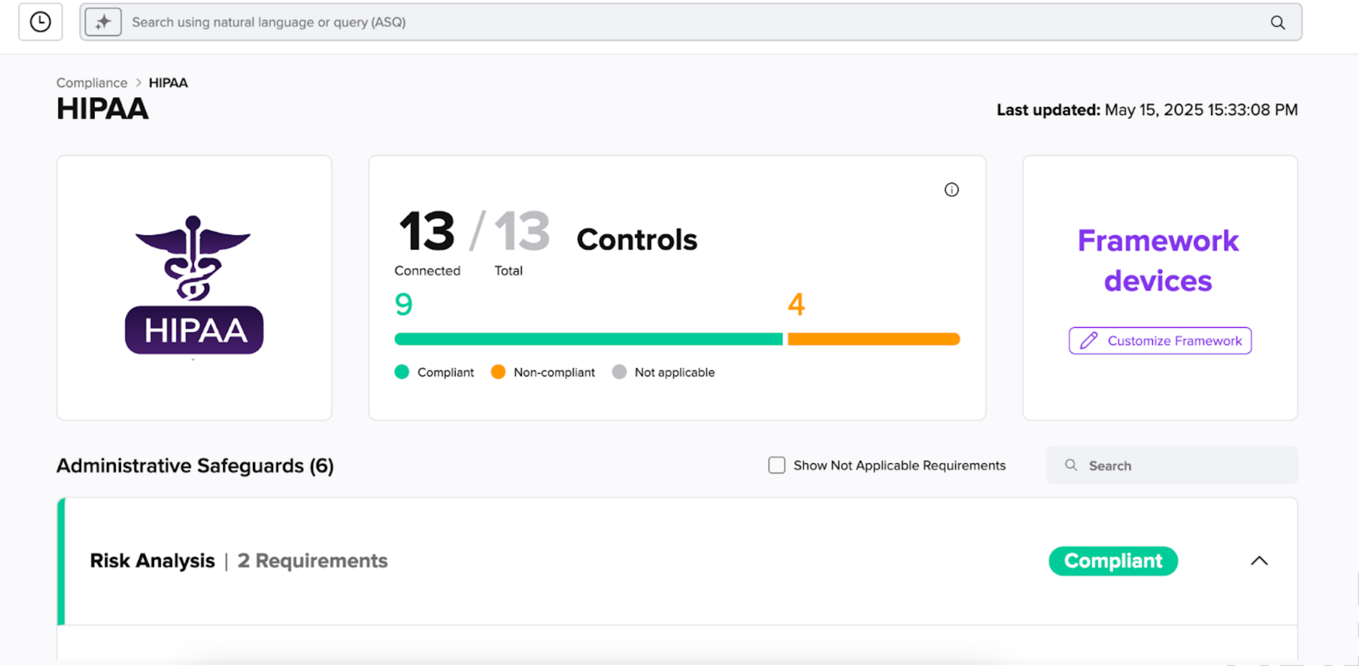
Qualys 106 findings

6. Compliance & Reporting

Demonstrate secure processes and manage compliance requirements with dashboards and reporting.

- **Automated Monitoring -** Monitor security advisories, medical device recalls, and manufacturer disclosure statements for full lifecycle management.
- **Protect Patient Data -** Manage HIPAA security requirements, protect patient data and ePHI to maintain trust and prevent costly data breaches.
- **Scheduled Reports & Dashboards -** Out-of-the-box healthcare dashboards and customizable views give your teams the relevant information needed to demonstrate risk reduction and reduce overall noise.

The Armis Impact: Maintain and demonstrate comprehensive compliance, with a **2x improvement in reporting speed and accuracy.**



Search using natural language or query (ASQ)

Compliance > HIPAA

HIPAA

Last updated: May 15, 2025 15:33:08 PM

13 / 13 Controls

Connected: 13, Total: 13

9 | 4

● Compliant ● Non-compliant ● Not applicable

Framework devices

Customize Framework

Administrative Safeguards (6)

□ Show Not Applicable Requirements

Search

Risk Analysis | 2 Requirements — Compliant

Key Vulnerability Management Capabilities

Unify

Ingest data from existing sources, including Armis Centrix™, EDR, on premise, cloud services, code, and applications. Translate millions of alerts into thousands of grouped findings.

Contextualize

Assign context to findings including threat intelligence, likelihood of exploit, and asset attributes like environmental information and business impact.

Prioritize

Automate prioritization based on business impact, clinical risk severity and likelihood of exploit, streamlining time spent on manual assessment by 80%. Focus on high-impact fixes that resolve the largest number of security issues.

Assign and Remediate

Leverage AI-driven ownership assignment for 75% improved MTTR. Benefit from bidirectional integrations with existing workflows and enable self-service for risk resolution.

Monitor and Report

Track and demonstrate progress for both individuals tasks, as for overall risk trends in the organization.

The Impact of a Patient-Centric Approach to VM

- **Total Visibility of the Entire Attack Surface – Every medical, IT, OT, IoT asset** used in the delivery of patient care.
- **Time Savings with Early & Proactive Risk Alerts –** Eliminate manual risk assessment, leverage AI-driven early threat indicators, and **reduce the scope of threats you need to worry about by 98%**
- **Clinical Risk Context –** Prioritize vulnerabilities based on clinical use, asset criticality, and operational risk. Enhance patient care resilience and prevent ransomware attacks, **potentially saving millions.**
- **Automation and Integrations:** Hundreds of pre-built integrations streamline deployment and maximize your existing technology investments. Automated workflows and key integrations **reduce operational overhead by 90%.**
- **Increased Remediation Capacity – Increase the number of closed findings by 7x annually**, preventing downtime costs and patient safety risks.
- **Streamlined Compliance and Security Reporting –** Protect patient data, easily manage medical device risks, and demonstrate compliance with key regulations and frameworks, **doubling reporting speed and accuracy.**

Armis Centrix™ keeps patients safe with proactive, comprehensive, and intelligent vulnerability prioritization and remediation. Our patient-centric approach to cyber exposure management and risk reduction enables healthcare organizations to focus on the biggest risks to patient care continuity and safety, minimize security gaps, and maximize operational efficiency.

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