SOLUTION BRIEF

# Manage Third-Party Risk Exposure in Healthcare with Armis Centrix™

Supporting zero-trust security for the full spectrum of healthcare technology, vendors, and systems.

# Overview

Cybersecurity is only as strong as its weakest link. Healthcare is consistently a prime target for advanced cyberattacks, including ransomware and data breaches, intensified by its increasing reliance on technology to support innovative patient care. With sprawling technology and expansive third-party vendor connections underpinning every aspect of patient care, without robust security measures for every point of connection, healthcare delivery organizations are left exposed and unsure of where the gaps exist.

Key concerns for healthcare delivery organizations include limited visibility into their networks and third-party connections, managing large vendor ecosystems without complete oversight, and lack of control over remote access solutions.

Armis Centrix™ supports effective cybersecurity and protection for every technology asset and every connection within your network, providing essential capabilities for an effective third-party Cyber Exposure Management (CEM) program. By providing immediate and complete visibility into all connected assets with a multi-detection engine, anomalous behavior monitoring, early warning of potential risks before they're weaponized, patient-centric vulnerability management and risk scoring, compliance reporting, and streamlined enforcement and remediation, Armis Centrix™ proactively protects and secures every exposure and keeps healthcare delivery organizations operational.

# Key Challenges

**More exposures, more breaches -** 62% of organizations experienced a third-party data breach or cybersecurity incident in 2024.

**Minimal access control -** 70% of healthcare organizations with third-party breaches attribute the incident to giving too much privileged access to outside parties.

**Limited visibility and blind spots -** Less than half of healthcare organizations trust that they have a comprehensive inventory of all third parties with access to their network, leading to blind spots regarding connected assets, patch status, and device vulnerabilities.

**Underinvestment in cybersecurity -** Healthcare organizations, on average, spend a lower percentage (7%) of their IT budgets on cybersecurity compared to other industries. This, coupled with skill shortages and tight budgets, makes it difficult to secure adequate funding and resources to manage cyber risks effectively.

**Regulatory compliance and accountability -** Healthcare organizations must maintain effective security measures for the entire technology ecosystem, including third-party accountability. Failure to meet privacy and security regulations such as Health Insurance Portability and Accountability Act (HIPPA) and General Data Protection Regulation (GDPR) can lead to extensive fines and even legal action.

**Business continuity risks -** Disruptions caused by third-party failings, such as service downtime, can compromise patient care and operational continuity.

# A CTEM Approach to Third-Party Risk Management

Every added connection and digital tool helps make healthcare more efficient. Real visibility and protection must include a complete understanding of every connected asset.

Armis Centrix™, the cyber exposure management and security platform, allows healthcare delivery organizations to see, protect, and manage every asset and vendor in their ecosystem. In order to protect the delivery of healthcare and clinical operations, Armis Centrix™ supports a Continuous Threat Exposure Management (CTEM) methodology to enable comprehensive awareness and threat exposure management for every technology asset that powers the patient journey from intake to discharge. Adopting a CTEM approach powers effective third-party risk management by discovering every asset, assessing and prioritizing all risks, orchestrating remediation, measuring compliance, and facilitating detailed reporting on progress and risk reduction.

# Building a Comprehensive Third-Party Risk Management Strategy

To mitigate risks effectively, healthcare organizations must adopt a comprehensive approach that goes beyond visibility. Here are some key considerations for more strategic protection:

01 **Maintain Full Visibility of Your Network -** Understanding what devices and vendors are connected to your network is the foundation of any exposure management strategy. First, identify all assets and third-party connections and review data handling practices of connected devices.

02 **Conduct Vendor Risk Assessments -** Before onboarding a vendor, conduct a thorough risk assessment to evaluate their security posture. Key areas to evaluate include data encryption practices, regulatory compliance, and past incidents of security breaches.

03 **Segment Your Network -** Implement network segmentation to isolate critical systems and limit the potential damage from a breach. For example, by creating separate zones for sensitive medical devices, office equipment, and guest Wi-Fi, or by ensuring vendors only have access to the systems or data necessary for their work.

04 **Deploy Anomaly Detection Systems -** Use anomaly detection systems to identify unusual behavior or potential threats early. For instance, flag irregular activity in a vendor's access pattern to identify potential breaches proactively.

05 **Establish Patient-Centric Risk Assessment -** Since healthcare is ultimately about patient outcomes, vulnerability management should prioritize patient safety. Conduct risk assessments with a focus on how vulnerabilities might impact patient care and score risks accordingly.

06 **Invest in Early Warning Systems -** Equip your systems with proactive tools that can identify emerging threats, such as vulnerabilities in third-party software, so you can address them before they become critical risks.

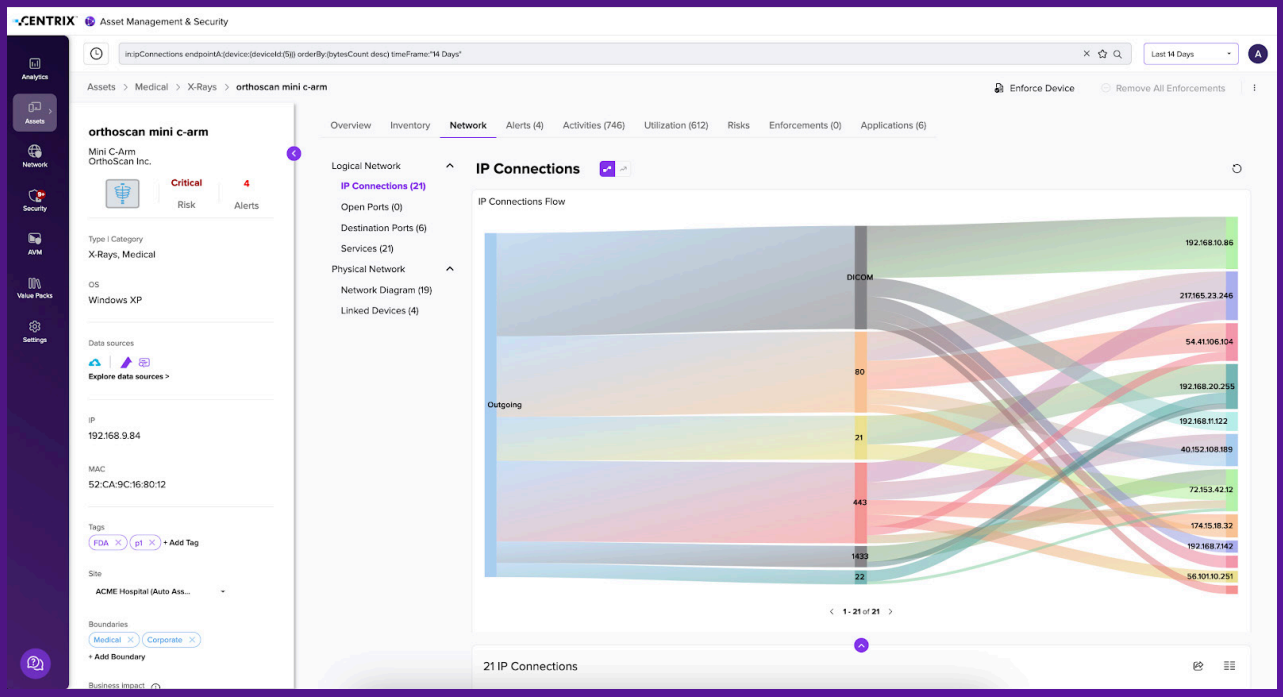
07 **Demand Vendor Accountability -** Hold vendors accountable for maintaining security standards. Define clear policies, and require regular attestation of compliance. Ensure vendors undergo periodic audits and have a structured incident response plan in place.

# Key Capabilities

## 1. Visibility of All Assets and Risks

Healthcare organizations rely on multiple technology assets, medical devices, and third-party providers to provide top-quality patient care. These expansive technology ecosystems require a single viewpoint of every asset, from IT equipment like laptops to IoT, OT, and medical devices, to effectively manage the associated third-party risks.

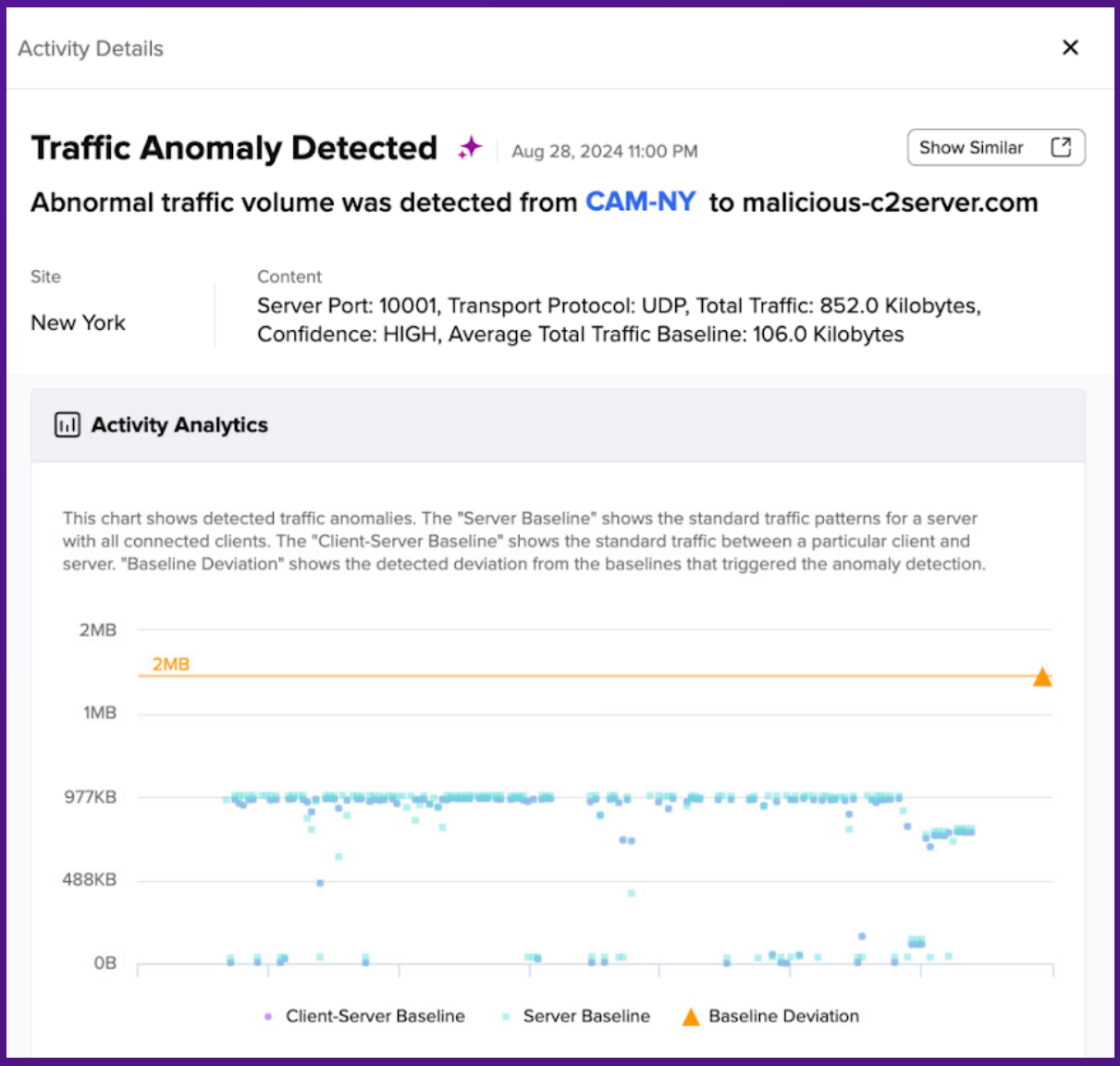
Armis Centrix™ offers complete visibility and best-in-class security across the entire healthcare device ecosystem—with zero disruption to patient care. This comprehensive visibility is crucial for identifying and mitigating risks introduced by third-party vendors, devices, and connections. Out-of-the-box integration capabilities ensure you can access all your information in a single location, consolidating data to better assess and manage third-party vulnerabilities and compliance. Armis Centrix™ gives you the full picture of every asset and risk in your environment, empowering you to keep your healthcare environment safe, your patients protected, and your third-party risk management robust.



## 2. Behavioral Analysis and Anomaly Detection

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. With dynamic, AI-driven anomaly detection powered by the world’s largest aggregated asset intelligence dataset, Armis uncovers complex attack patterns that traditional signature-based detection might miss, enabling proactive identification of risky third-party activities. Armis Centrix™ easily identifies appropriate baselines of behavior for over 6.5 billion assets to speed up detection and ensure precise prioritization and response. Advanced policy management and network segmentation facilitate security for even the most sensitive assets that don’t allow traditional security solutions, further mitigating third-party risks.

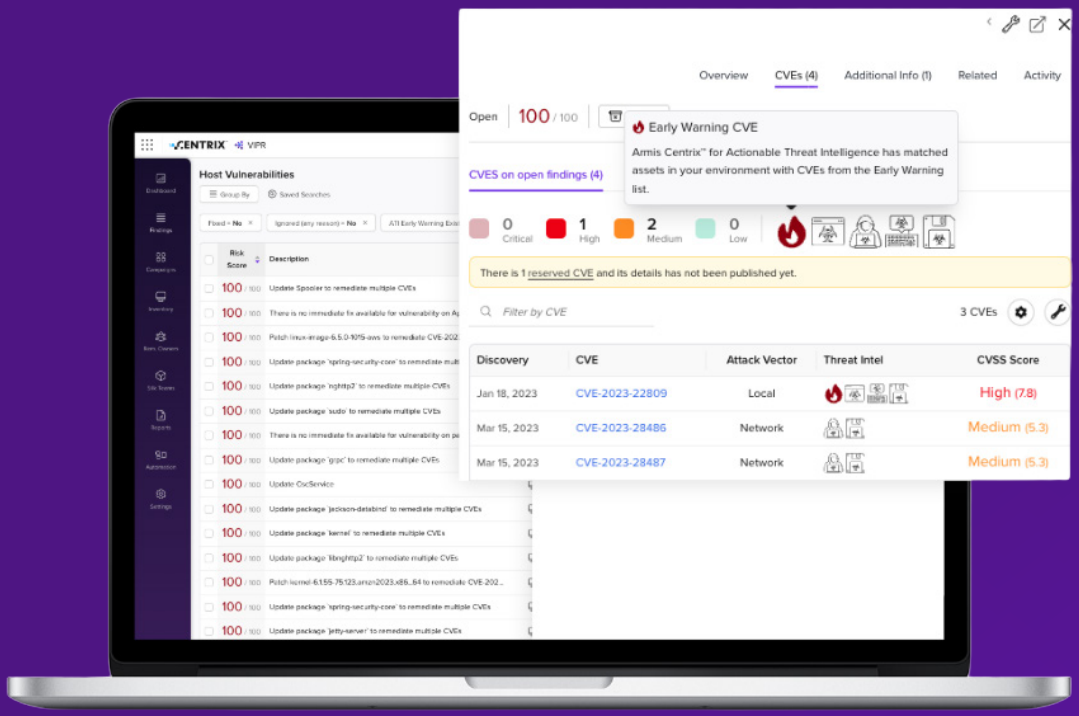
Reduce alert fatigue by identifying true anomalies, detecting indicators of ePHI transmission, or malicious behavior for early detection and response, crucial for managing risks associated with third-party access and systems.



## 3. Early Warning Alerts to Preempt Threats

Armis Centrix™ for Early Warning allows healthcare organizations to move “left of boom” by preempting emerging threats and vulnerabilities, including ransomware attacks, for unparalleled coverage and accuracy in managing third-party risks. 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.

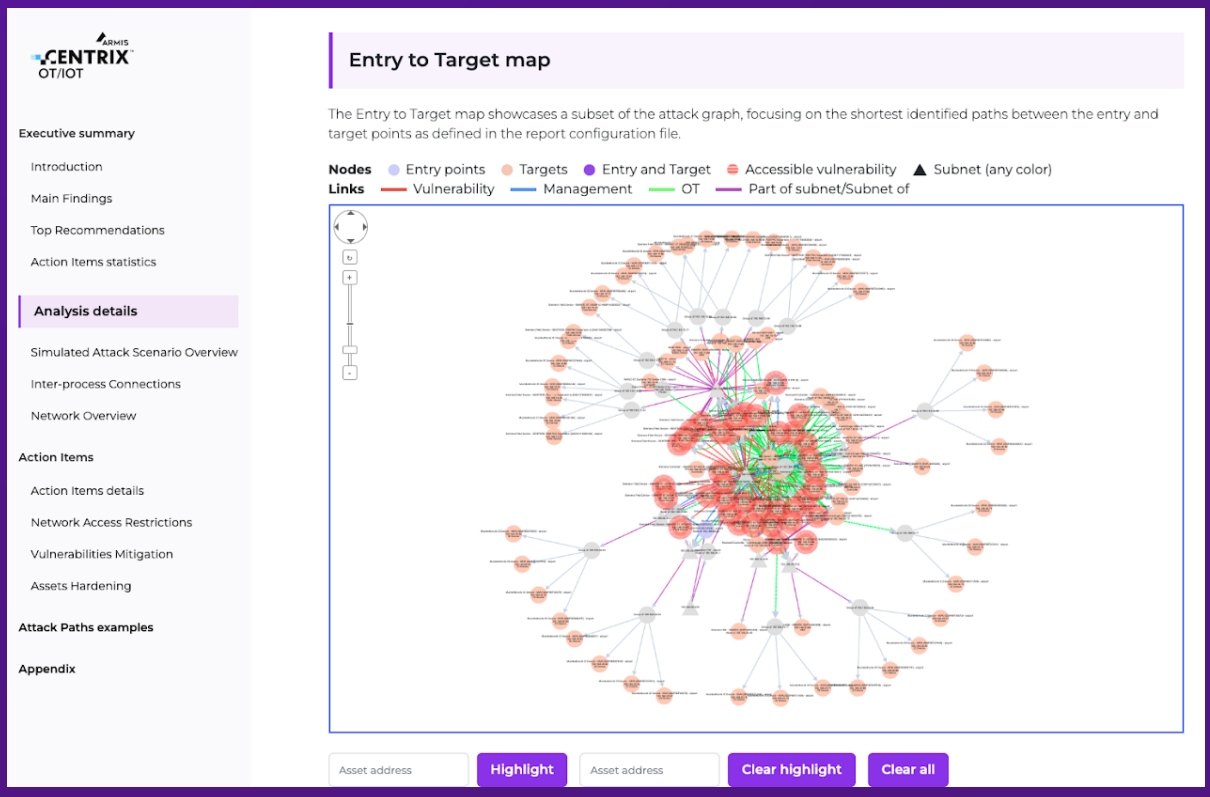
Armis Centrix™ leverages AI-driven actionable intelligence and machine learning that scours the dark web, coupled with deception technology and human intelligence to deliver an early warning system for vulnerabilities that threat actors are preparing to exploit. These early indicators of potential attacks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



## 4. Attack Path Mapping

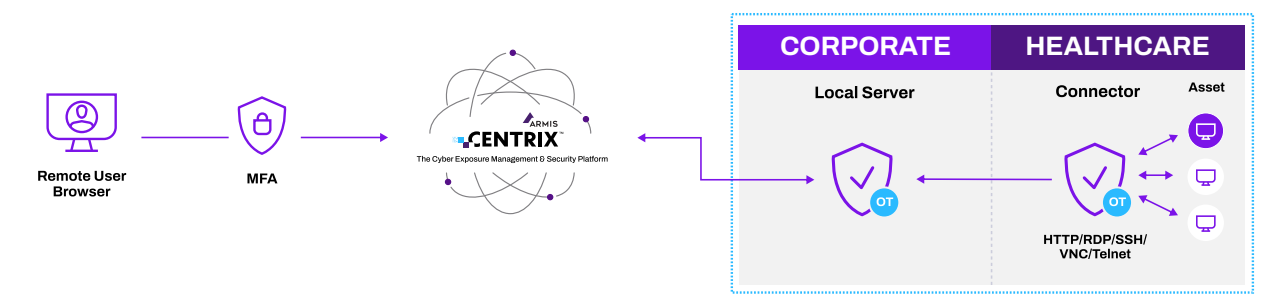
Attack Path Mapping is the process of systematically identifying, visualizing, and analyzing potential attack vectors within your environment. By going beyond simple device inventory, mapping attack paths empowers organizations to gain a proactive understanding of how an adversary might exploit vulnerabilities to move laterally via east-west traffic attack proliferation.

Armis Centrix™ offers a best-in-class attack path mapping solution that provides deep insights on potential weak spots and lateral movement pathways for essential protection insights for healthcare organizations. Armis leverages extensive asset context data and healthcare expertise to provide unified protection and security for all medical devices, IT, OT, and IoT assets, automated risk prioritization based on clinical and business impact, and remediation recommendations regarding adjustments to firewall rules, restriction of connections, hardening of assets, and mitigation of vulnerabilities that enable lateral movement toward critical targets. By leveraging advanced attack path mapping capabilities, organizations can enhance resilience, ensure compliance, and protect essential healthcare infrastructure from dynamic cyber exposure threats.



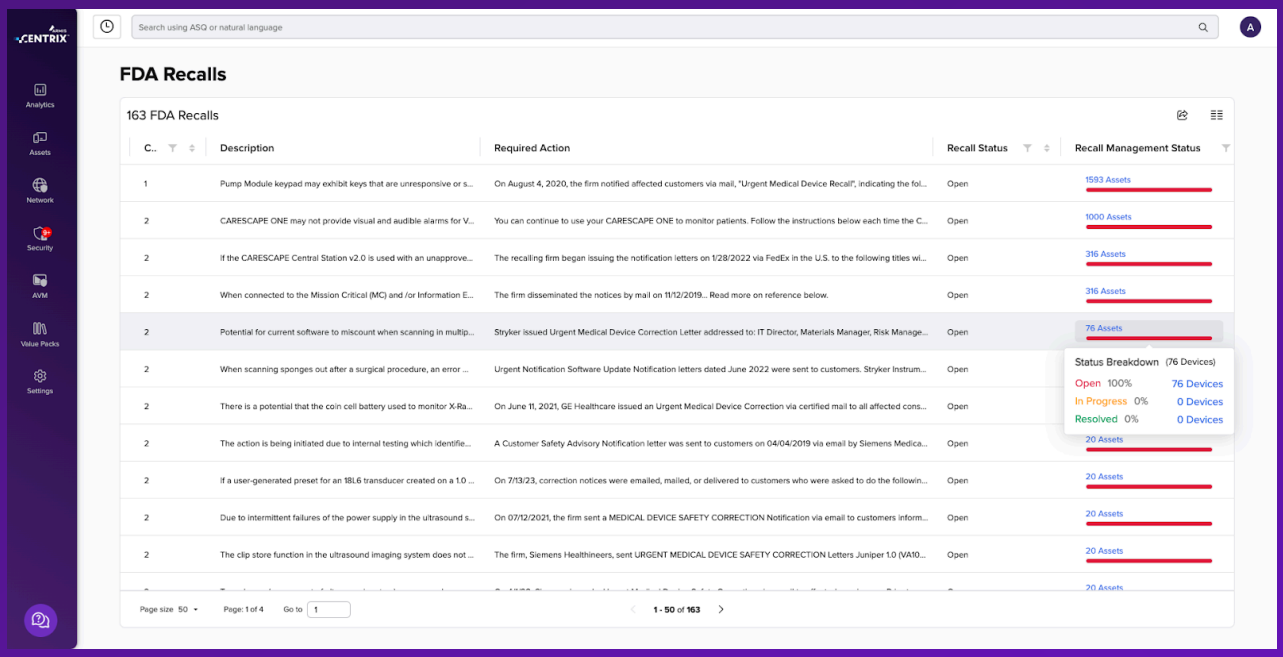
## 5. Secure Remote Access

Tighten security for third-party risk management with unique asset protocols. Manage user permissions and maintain full auditability. Adopt a scalable solution to future-proof your operations. Simplified secure remote access processes adhere to Zero Trust principles, with just-in-time access and multi-factor authentication for peace of mind. Armis Centrix™ improves real-time monitoring and insights, improving the overall security posture.




## 6. Compliance and Reporting

Armis Centrix™ allows healthcare organizations to document and demonstrate cybersecurity and resilience practices. In alignment with key directives, Armis provides total asset visibility with deep asset context, in-depth reporting and explainability, anomalous behavior detection, vulnerability management, and early threat detection and response. Armis Centrix™ facilitates automated response to minimize patient care disruption, proactive vulnerability management to mitigate patient care risks, and provides dashboards and overviews of the number of compliant or non-compliant devices for effective gap analysis. In addition, Armis Centrix™ tracks and manages FDA recall and MDS² information to improve visibility and collaboration across clinical engineering and IT security teams and provide a comprehensive view of every aspect of risk.



# How Armis Supports Zero Trust Security for Third-Party Connections

Zero Trust security is a strategic approach to cybersecurity that operates on the principle of “never trust, always verify.” It assumes that threats can exist both inside and outside the network, requiring strict identity verification for every user and device attempting to access resources, regardless of their location. Armis Centrix™ inherently aligns with Zero Trust frameworks by providing unparalleled visibility and continuous monitoring of all connected assets. This includes not only an organization’s internal devices but also critical third-party vendors, equipment, and supply chain components, ensuring that every connection, internal or external, is rigorously authenticated and authorized before granting access. This comprehensive approach establishes a robust security posture across the entire technology ecosystem.

## Zero Trust Security Benefits with Armis Centrix™

- **Full Situational Awareness** of all connected assets, including third-party vendors, equipment, and supply chain assets.
- **Reduced Risk of Cyberattacks** by mitigating cyber threats and ensuring complete visibility and protection of the technology ecosystem.
- **Proactive Threat Detection** with Early Warning alerts, granular anomaly detection, and automated response capabilities.
- **Operational Continuity and Patient Care Protection** by adopting proactive cybersecurity capabilities and preventing downtime and care interruptions caused by third-party breaches.
- **Regulatory Compliance** and alignment with stringent compliance requirements related to healthcare and cyber resilience practices.

# Why Armis

**Protect complex and sensitive healthcare environments** by ensuring complete end-to-end cybersecurity from your third-party vendors, encompassing asset discovery, monitoring, vulnerability prioritization, and early ransomware detection.

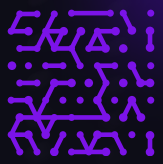
**Manage clinical and operational risk** associated with third-party vendors by leveraging a cyber exposure management platform powered by an AI-driven Asset Intelligence Engine.

**Protect patient safety and enhance care capacity** through total, real-time visibility of every medical/IoMT, IoT, IT, and OT device, both within your environment and introduced by external parties.

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

**Demonstrate compliance with regulations and frameworks** by ensuring comprehensive cybersecurity, reporting, and preventive risk mitigation are in place across your entire technology ecosystem.

**Maintain operations and availability for patient services** by implementing proactive monitoring and real-time alerting for all systems and services.



ARMIS®

## 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

**armis.com**

### Understand the Armis difference:

Comprehensive visibility, intelligent insights, proven outcomes.

**Try Armis Centrix™ Today**