



Armis Centrix™ for Healthcare

Proactive Cybersecurity for Every Touchpoint
of the Patient Journey

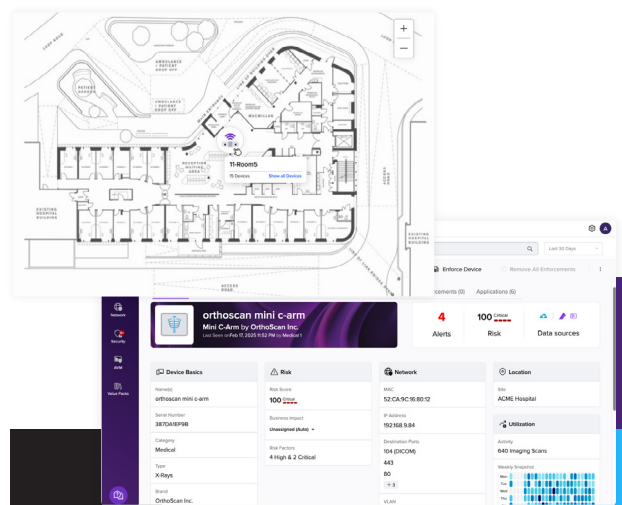
Patient-Centric Cybersecurity, Risk Reduction, and Future-Proofed Protection

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 assets – **about 17 per hospital bed**.

Armis Centrix™ identifies and mitigates all cyber exposure risks, remediates security findings and vulnerabilities, and protects your entire attack surface.

Effective Cyber Risk Management for Secure Patient Care

Armis revolutionizes healthcare cybersecurity by addressing the unique challenges of protecting complex, sensitive medical devices and the broader healthcare environment. Designed for leading hospitals, clinics, and healthcare systems, Armis Centrix™ seamlessly integrates with your existing systems for comprehensive coverage, total protection of every asset, and real risk reduction that keeps your patients and equipment safe.



Armis Centrix™ for Healthcare – A Single Platform for Every Technology Asset:

Proactive Threat Intelligence and Alerts

Protect your healthcare organization from emerging attack methods to prevent downtime or disruptions. Armis Centrix™ for Early Warning delivers real-time threat intelligence about tactics, techniques and procedures (TTPs) attackers use and their potential impact to protect against zero-day vulnerabilities and threats including ransomware. Prioritize mitigation efforts based on the current threat landscape and asset criticality to the business and migrate your security posture from reactive to proactive. Protect your healthcare organization with the most proactive warning system.

Medical Device Behavioral Insights

Armis Centrix™ for Medical Device Security provides detailed asset intelligence within a single platform for better resource allocation, asset lifecycle management, and optimized patient flow. View behavioral insights for how your assets are behaving and get alerted for any anomalous or potentially risky behavior. View and manage asset risks while gaining unique health-related insights including FDA recalls, device utilization, and MDS2 information, improving collaboration between clinical engineers and IT security. Locate devices on a physical map, view peak utilization times, and effectively manage your clinical operations.

Actionable Risk Remediation

Armis Centrix™ for VIPR - Prioritization and Remediation drastically reduces the effort involved in vulnerability management, allowing you to target mitigation and remediation efforts based on the biggest risks to patient safety and operational continuity. Deduplicate, contextualize and prioritize findings into actionable fixes, make the best use of your resources and tangibly improve your security posture.

See, protect, and manage your entire attack surface

Visit [Armis.com](https://www.armis.com) to find out more



Key Features that make Armis the Go-To Platform for Cyber Exposure Management

Complete asset visibility of the technology used throughout the patient journey, spanning medical devices, IT, IoT, cloud, and OT assets including building management systems.

Usage analytics improve patient care, device utilization hours, and facilitate an optimized schedule for asset maintenance.

Automated and detailed inventory of every connected asset in your environment, even across dispersed locations.

Integration with diverse tech stacks, maximizes your existing investments, enabling a quicker time to value and visibility.

CMMS workflow integration communicates the most up-to-date information about every medical and technology asset. Automatically create work orders for efficiency and faster resolution time.

FDA recall, MDS2, advisory tracking, and remediation automatically alert you to affected devices, timely alerts such as NHS Cyber Alerts, the security controls that can be applied on each asset, and their location for streamlined fixes.

Out-of-the-box healthcare dashboards and customizable views give your clinical engineering, executive, and IT security teams the information most important to their work, reducing overall noise by quickly getting to the data most relevant to the specific role.

Multi-detection engine that employs multiple configurable detection methods in order to find more and secure more.

Early warning feed powered by Armis Centrix™ for Early Warning allows you to leverage our insights derived from Armis Labs in addition to our AI-powered pre-attack threat hunting, and deception technology.

Vulnerability and risk assessment reduces MTTR with AI-based detection, deduplication, contextualization and prioritization and remediation process that considers business impact, patient risk, and criticality.

Remediation campaigns and predictive ownership connect security findings to the fix, speeding up time to remediation and eliminating manual effort and guesswork.

Key Benefits

Full-scope visibility and protection reduce outages and business impact to 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.

Clinical asset context powered by the Armis Asset Intelligence Engine, an AI-powered knowledge base identifies cyber risk patterns and behaviors.

Real-time intelligence and early warning alerts for proactive protection.

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 – IoMT, IT, OT, and IoT – 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.

