Armis Centrix™ for Medical Device Security | Ransomware Detection

Proactively detect ransomware attacks and prevent patient care disruption

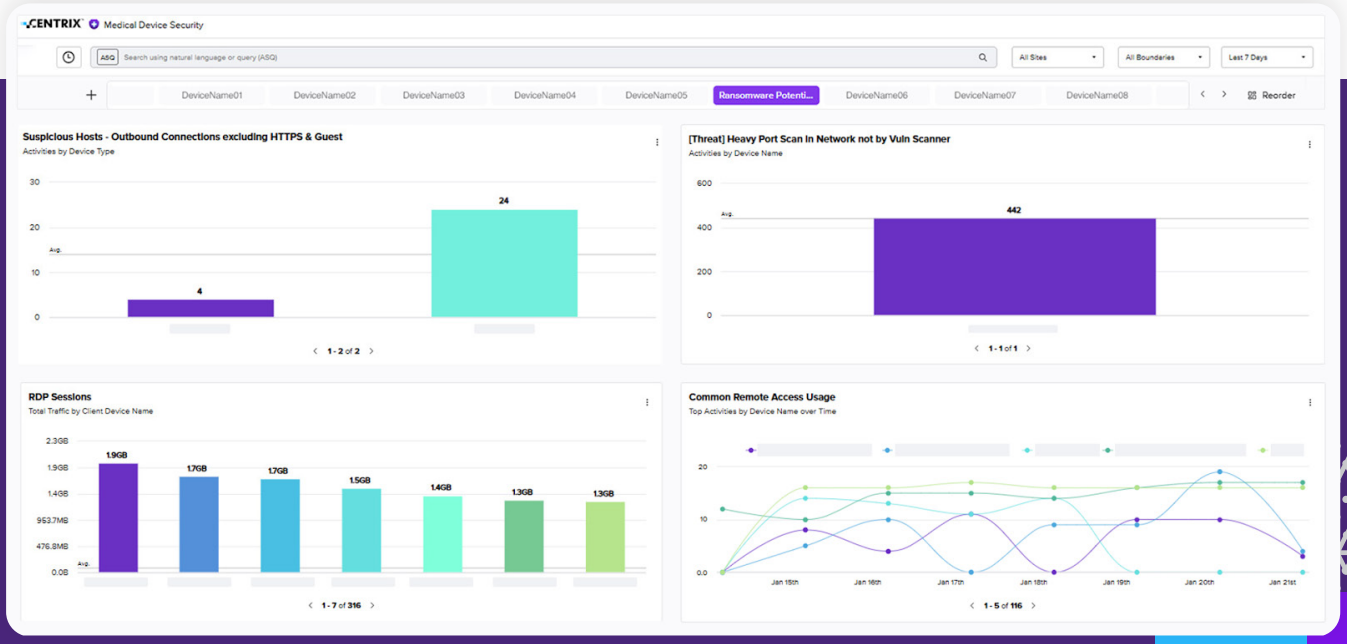
Protect Patient Care Continuity with Armis Centrix™ Ransomware Detection

Healthcare remains one of the most lucrative industries for ransomware attacks in the world. Over half of healthcare organizations have experienced more than one cyberattack. Proactive ransomware protection can play a major role in maintaining patient services, ensuring sensitive data is protected, and disruptions do not jeopardize essential healthcare operations putting patient lives at risk.

The Armis Approach

Armis Centrix™, the cyber exposure management platform, allows you to move the dial from reactive to proactive and leverage best-in-class cybersecurity to get ahead of ransomware attacks. Understanding organizational assets and risks in real time establishes the fundamental awareness needed to identify and prioritize critical assets, data, and systems within your organization.

Teams are empowered with timely and accurate information about every asset. The Armis Asset Intelligence Engine leverages artificial intelligence (AI) to enrich asset profiles and better classify abnormal behavior. With Early Warning alerts based on deception technology, threat intelligence, and research, healthcare organizations can get ahead of potential threats and make real-time assessments to address vulnerabilities before they can impact the organization. Traffic anomaly detection, advanced network segmentation, and policy automation take the guesswork out of ransomware detection and allow you to take action immediately at a threat's most granular level.



Armis Centrix™ sample dashboard for ransomware detection and monitoring

See, protect and manage your entire attack surface with Armis Centrix™

Visit **Armis.com** to find out more

Key Ways Armis Enables Ransomware Threat Detection:

Anomaly Detection
The Armis threat detection engine uses machine learning and AI to detect when a device operates outside its "known-good" baseline.

Multi-Detection Engine
Our multi-detection technology supports anomaly detection and policy-based detection for more comprehensive protection. Monitor any device's communication in your environment for fast and effective threat response and mitigation.

Early Warning Alerts
Real-time threat intelligence about tactics attackers use and their potential impact helps protect against zero-day vulnerabilities and ransomware threats.

Ransomware Detection
Itemize device activity including DNS queries, web surfing, callouts to suspicious domains, lateral movement, and encryption. Immediately identify potential exploits and potential lateral movement and contain the threat.

Automated Alerts
Quickly identify risks and get alerted to any changes in behavior in real time.

Policy Enforcement & Automation
Create policy enforcement rules per device type to ensure your business remains operational and services are not disrupted. Enforce actions, quarantine the device, remove network access, and take proactive measures against detected threats.

Vulnerability Prioritization and Remediation
A data-centric, AI-driven approach for prioritizing the most critical risks in a healthcare environment. Prioritize mitigation efforts based on asset criticality or proximity to patient care. Identify and action the most critical risks, and facilitate an end-to-end remediation lifecycle.

Ransomware Detection in Healthcare

Challenges in Healthcare	The Armis Solution
Difficult to identify visible and hidden assets, vulnerabilities, misconfiguration, and other risks.	**Maintain operations and availability for patient services** with proactive monitoring, real-time alerting and intelligent network segmentation
Greater connectivity and digital transformation contribute to influx of assets that need protection	**Protect patient safety and enhance care capacity** with total, real-time visibility of every IoT, IT, OT, and IoMT device in the healthcare environment
Outages can result in poor patient outcomes or even fatalities, raising the stakes from financial losses to life-threatening risks	**Manage clinical and operational risk** with a cyber exposure management platform powered by an AI-driven Asset Intelligence Engine
Time-consuming and manual approaches to cybersecurity and threat detection take valuable hours away from essential operations	**Save time and reduce threat exposure** with an end-to-end approach for security findings and vulnerability consolidation, prioritization, and remediation

"I was surprised to see how quickly you were able to determine what a device was. You could see our vital cart machines, the make, the model, when it was being used. You could see when we were running tests on patients."

Brian Schultz
Director of Network Operations,
Burke Rehab Hospital