Armis Centrix

Patient-centric, agentless cyber exposure management platform for securing all medical, IoT, and IT assets in healthcare environments.

https://www.armis.com/platform/armis-centrix-for-medical-device-security/

Overview

Armis Centrix™ for Medical Device Security is a comprehensive, agentless cyber exposure management platform designed specifically for Healthcare Delivery Organizations (HDOs). It provides total, real-time visibility and protection for the entire healthcare ecosystem, including all connected medical devices (IoMT), operational technology (OT), Internet of Things (IoT), and traditional IT assets .

The platform is powered by the Armis AI-driven Asset Intelligence Engine, which continuously discovers, classifies, and profiles every asset without the need for agents, eliminating security blind spots and preventing disruption to patient care . It leverages a massive, crowdsourced knowledge base of billions of asset profiles to establish a "known-good" behavior baseline for anomaly detection and accurate threat identification .

Key Benefits for Healthcare:

Patient Safety & Care Continuity: Proactively identifies and mitigates risks to life-saving medical devices, ensuring continuous operation and patient safety .
Compliance & Audit Readiness: Provides automated compliance reporting and helps enforce policies to meet regulations like HIPAA and GDPR .
Operational Efficiency: Offers medical device utilization insights to optimize resource allocation, device lifecycle management, and proactive maintenance scheduling .
Unified Security: Consolidates visibility and risk management for IT, OT, IoT, and IoMT onto a single, frictionless platform, reducing the complexity of siloed security tools .
Main Features and Capabilities:

Agentless Device Discovery and Classification .
Real-time Asset Inventory and CMDB Enrichment .
AI-Powered Risk Assessment and Vulnerability Prioritization (VIPR) based on clinical risk and business criticality .
Automated Network Segmentation and Policy Enforcement .
Continuous Threat Detection and Response, including ransomware monitoring .
Asset Behavior Monitoring and Compliance Tracking (e.g., unencrypted PHI transmission) .

The platform is cloud-native (SaaS) and integrates seamlessly with existing security and IT tools, allowing for automated workflows and efficient incident response .

Key Features

- Agentless Device Discovery & Classification
- AI-Powered Risk Assessment & Prioritization
- Automated Network Segmentation & Enforcement
- Real-time Threat Detection & Response
- Unified Asset Inventory (IT, OT, IoT, IoMT)
- Medical Device Utilization Insights
- Compliance Reporting & Gap Analysis
- CMDB Enrichment & Workflow Automation

Pricing

Model: enterprise

Contact vendor for custom enterprise pricing. The model is subscription-based, typically priced based on the number of assets/devices monitored.

Target Company Size: medium, enterprise

Integrations

ServiceNow, Splunk, IBM QRadar, Cisco, Palo Alto Networks, Check Point, Rapid7, Tenable, Qualys, AWS Security Hub, Azure, Google Cloud Platform

Compliance & Certifications

HIPAA (BAA Available), SOC2 Type II, ISO 27001, GDPR, FedRAMP Moderate, DoD IL4, C5, CSA STAR Level 1