ARMIS

Public Sector

SOLUTION BRIEF

See and Secure Everything

Unified asset visibility and security for medical universities and teaching hospitals

Cyberattacks on healthcare organizations worldwide are on the rise and they show no sign of subsiding anytime soon. The healthcare sector suffered approximately 295 reported breaches in the first half of 2023 alone, according to the HHS Office for Civil Rights (OCR) data breach portal. More than 39 million individuals were implicated in healthcare data breaches in the year's first six months.

Advances in technology are essential to improve the speed and quality of care delivery, but with increasingly connected care comes a much larger attack surface, one that most tools cannot cope with. Smart hospitals are expected to deploy 7.4 million connected IoMT devices globally by 2026, according to Juniper Research.

Medical universities and teaching hospitals, which have enterprise campuses and medical facilities to manage and protect, sit at the intersection of cyber and clinical risks. They are uniquely positioned to protect not only enterprise IT, OT, and IoT assets but also medical and IoMT devices involved in clinical workflows, patient data, and building management systems.

On the clinical side, effective delivery of care depends on the uptime of connected medical devices, and any cyber attack or malfunction could be life-threatening. On the enterprise IT side, CIOs and CTOs are tasked with ensuring operational efficiency and mitigating risks of cyber threats on the network and those posed by unmanaged devices connecting to the network. Knowing what devices a medical university or teaching hospital has, where they are located, how they are being used, and if they pose any security risk is critical.

However, implementing a medical device security strategy for medical universities and teaching hospitals involves navigating multiple security risk frameworks alongside disparate solutions with limited threat context. This leads to ineffective security operations when taking action on medical device visibility data that lack risk context.

Armis Centrix™

> Armis Centrix™, the Armis Cyber Exposure Management & Security Platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, protects, and manages billions of assets around the world in real time.
>
> Armis Centrix™ is a seamless, frictionless, cloud-based platform that proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats and protects your entire attack surface.

Often, point solutions are implemented, but they need more features and capabilities when taking action along the lines of identifying medical devices, conducting contextualized risk assessments, and prioritizing remediation efforts.

With IoMT vulnerabilities and healthcare cyberattacks on the rise, now more than ever, it's crucial to build a security program that protects every connected device, IT network, and building management system with complete visibility and continuous contextualized monitoring. But you can't protect what you can't see. Securing medical universities and teaching hospitals requires a holistic view of risk, from asset inventories, application payloads, and custom protocols to connected medical devices critical to patient care.

ARMIS
Public Sector

Armis Asset Intelligence Engine

The Armis Asset Intelligence Engine is an AI-powered knowledge base, monitoring billions of assets world-wide in order to identify cyber risk patterns and abnormal behaviors.

It powers the Armis Centrix™ platform with continuous unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface.

Unified Asset Management

puts comprehensive device identity and classification all in one place.

Agentless Technology

that won't impact your network or critical devices.

Dynamic Risk Assessment

helps you proactively understand and reduce your attack surface.

Continuous Threat Detection and Response

that mitigates threats and attacks automatically.

Frictionless Deployment and Integration

that delivers immediate time-to-value.

See and Secure Everything

Armis provides unified asset visibility and security in a single platform purpose-built for this elevated threat landscape. Armis Centrix™ is the industry's most comprehensive asset intelligence platform, offering complete visibility and maximum security across all managed or unmanaged medical devices, clinical assets, and the entire healthcare device ecosystem—with zero disruption to patient care.

Complete Asset Inventory Visibility and Context

Armis Centrix™ provides medical universities and teaching hospitals with a holistic view that bridges the gap in securing new smart healthcare systems and legacy platforms for medical devices. Armis discovers and classifies every device and traditional managed and unmanaged devices in your environment. The comprehensive device inventory Armis generates includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications.

FDA and Regulatory Compliance

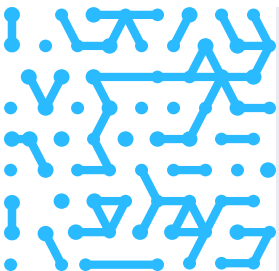
Armis can detect detailed properties and attributes based on the various device types. For medical devices, Armis helps automate the association of FDA recalls to streamline clinician workflow. This information is critical for responding to and complying with FDA recalls and vulnerabilities promptly. It is also vital to ensure you comply with HIPAA and HICP regulations.

Threat and Ransomware Protection

Armis' cloud-based threat detection engine uses machine learning and artificial intelligence to detect when a device operates outside its normal "known good" baseline. This deviation can be caused by a device misconfiguration, a policy violation, abnormal behavior such as inappropriate connection requests or unusual software running on a device, or threat intelligence that indicates the device has been compromised.

Continuity of Operations

Armis Centrix™ delivers early warning alerts about vulnerabilities threat actors are exploiting in the wild. This facilitates proactive cybersecurity to mitigate risks and maintain operations. By understanding the full scope of risk to your continuity of operations, Armis Centrix™ provides high-fidelity information, security data visualization, and response capabilities through the entire workflow context to help improve the quality of care and reduce inefficiencies simultaneously.



Medical Device Utilization and Optimization

Armis provides clinical teams insights into medical device utilization metrics to understand when and how devices are being used. Clinical team management can rely on up-to-date asset usage data to make informed purchase decisions and avoid a patient backlog.

Risk Prioritization and Vulnerability Identification

Armis can help medical universities and teaching hospitals focus on high-risk vulnerabilities that can cause costly disruption by assessing the risk associated with every asset and prioritizing remediating critical vulnerabilities to reduce the attack surface quickly. Armis Centrix™ prioritizes the most critical security findings based on risk, context, and likelihood of exploit. Assign ownership and automate ticketing with actionable remediation guidance.

"Metrics and accountability are key to understanding how to protect the hospital's network, and Armis has a major role in making the relevant data available to us in an easy-to-access manner."

Dr. Michael Connolly
Chief Information Officer (CIO)

Mater Misericordiae University Hospital.

"Armis immediately provided us with visibility into what devices were plugging into the network,"

Brian Schultz
Director of Network Operations and Security

Burke Rehabilitation Hospital.

Armis at-a-glance

Asset discovery

- Identify all OT devices, including SCADA, PCS, DCS, PLC, HIM, MES, plus other devices in your educational institution environment
- Determine the make, model, OS, IP, location, etc
- Track connection and activity history through Profibus, Profinet, Modbus, and many other OT protocols
- Integrate with asset inventory systems like CMMS and CMDB

Risk management

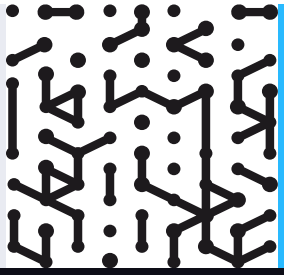
- Passive, real-time, continuous risk assessment
- Extensive CVE and compliance databases
- Risk-based policies

Threat detection

- Detect changes in device state or behavior
- Detect behavior anomalies
- Detect policy violations

Prevention

- Quarantine devices automatically
- Integrate with firewall, NAC, SIEM policies
- Reduce dwell time
- Improve incident response



ARMIS
Public Sector

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
Free Trial