ARMIS®

SOLUTION BRIEF

Securing the Next Generation of Connected Care

Introduction

Connected medical devices help clinicians deliver faster, higher quality care, but they also expand an attack surface that most healthcare delivery organizations (HDOs) aren't prepared to protect. These devices lack inherent security controls, can't easily receive software updates, and can't be seen or managed by traditional security products. All of this puts sensitive data, day-to-day facility operations, and patient safety at risk.

You can't protect what you can't see

Many IoMT devices cannot have agents installed, making them all but invisible to traditional security teams. This lack of visibility means that most organizations don't have an up to date or complete asset inventory, and they have no understanding of how effectively assets are being utilized or how the attack surface is exposed. Siloed ownership between operations, security and biomedical engineering teams often creates a disconnected approach to device management and security. Together these factors create a large, mostly unmonitored cyber-attack surface that bad actors are successfully exploiting today.

See it all. Secure it all

Armis Centrix™ is the industry's most comprehensive IoMT, IoT, OT and IT security platform, enabling healthcare providers to secure the devices and technologies that are the foundation of connected care innovation. Armis provides the information and insight needed for HDOs to confidently see, protect, and manage all clinical assets across networks and ensure patient privacy and safety.

Whether they are IoMT, IoT, OT, or IT, Armis Centrix™ identifies every managed and unmanaged device in a network.

The Armis Asset Intelligence Engine tracks anonymized data from over 5 billion protected assets to identify a broad range of assets and highlight abnormal traffic or configurations that could indicate compromise.

Trusted by healthcare organizations worldwide, Armis helps customers protect against unseen operational and cyber risks, including ransomware, increase medical device efficiencies, optimize use of resources, and safely innovate with new technologies to deliver improved patient care.

A Unified Platform to Protect All Assets

Armis unites biomedical, security, and IT teams to deliver complete asset security, enabling healthcare organizations to improve:

1 IoMT, IoT, OT and IT Asset Discovery and Inventory

Armis Centrix™ is able to detect and identify every managed and unmanaged device in your environment. Integrations with security, network, and CMDB platforms enrich device context and accuracy. The resulting asset inventory is a single source of truth for all groups with connected device responsibilities, including healthcare technology management (HTM), OT and IT teams.

2 Asset Risk Analysis and Mitigation

Armis automatically groups every device to which an alert or recall applies, enabling fast prioritization and targeting for response teams. These alerts are then associated with public data from NIST CVE and CVSS, FDA, threat intelligence and MDS2 sources. Armis provides detailed information on the alert, including links to remediation sources such as required patches from vendor websites.

3 Anomaly Detection

Through detailed inspection of network traffic, Armis is able to identify anomalies in behavior, configuration, and utilization which may be indicators of compromise or attack. Armis Centrix™ uses AI and ML processing to baseline information for specific devices from the Armis Asset Intelligence Engine, comparing information including unusual traffic patterns, malicious traffic destinations, and unusual volumes of data.

4 Medical Device Utilization and Insights

Armis aids biomedical and clinical engineering teams in maximizing the efficiency of their devices by providing detailed device utilization data. When utilized for high-cost assets such as MRI and CT scanners, the resulting information can be used to compare times of high use and times of availability, identifying opportunities for relocation or altered scheduling. For high volume assets such as infusion pumps, Armis can identify devices that have not been utilized recently as a possible indication of unreported faults or forgotten devices, and identify devices that may have been missed during firmware upgrades.

5 Identify Medical Device Dependencies

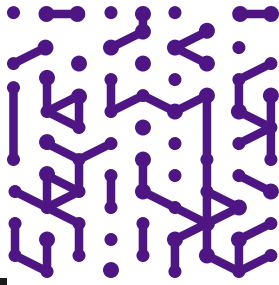
Armis adds context information to devices by identifying not only operating system information, but also what applications are running and what protocols are being utilized. This context allows Armis to identify and prioritize tablets or Raspberry pi devices which may be controlling portable scanners, or a Windows managed MRI machine over a back-office desktop.

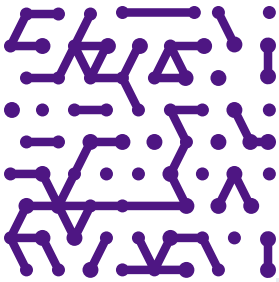
6 Protect from Cyber-attacks and Ransomware

Armis is able to identify Indicators of Compromise and Attack as well as identify forensic network information to help response teams understand how a breach may have occurred and what systems may have been compromised.

7 Secure PHI

Certain protocols and devices are known to communicate protected health information (PHI) as part of their network communications - often unencrypted. Armis can identify these assets and enable appropriate policy creation or network segmentation to protect data.





Why Armis?

Armis unites biomedical, security, and IT teams to deliver complete asset security, enabling healthcare organizations to improve:

Every Device - IoMT, IoT, OT and IT

Medical devices are not the only attack surface that healthcare needs to protect. IoT such as security cameras, OT such as building management systems, IT are supporting networks where patients attach their own devices - we've even seen cars. Armis Centrix™ detects, identifies and assesses the risk of every device.

Industry Leader

Armis has been recognized as a leader in healthcare device security and innovation by industry-leading analyst firms including Gartner, Forrester, Frost & Sullivan, KLAS, Quadrant Knowledge Systems and more.

Knowledge

The Armis Asset Intelligence Engine contains the detailed, accumulated, anonymized knowledge of more than 5 billion devices from Armis customers. When Armis finds a device on your network, it can instantly compare configuration and traffic pattern information, removing a learning period and yielding fast time to value.

Agentless

Many IoT, IoMT and OT environments are unable to have agents installed, leaving them outside of the scope of traditional security tools. Armis gives security teams the choice of both passive and active scanning. This enables detection of every device communicating on the network, removes the risk of crashing devices, and simplifies ongoing updating and maintenance.

"It has definitely filled in the gaps in our security arsenal by uncovering risks we never knew about previously. At first, I thought Armis was a nice-to-have, but now it's become an integral part of our cyber defense."

Dr. Michael Connolly
Chief Information Officer (CIO)
Mater Misericordiae University Hospital

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