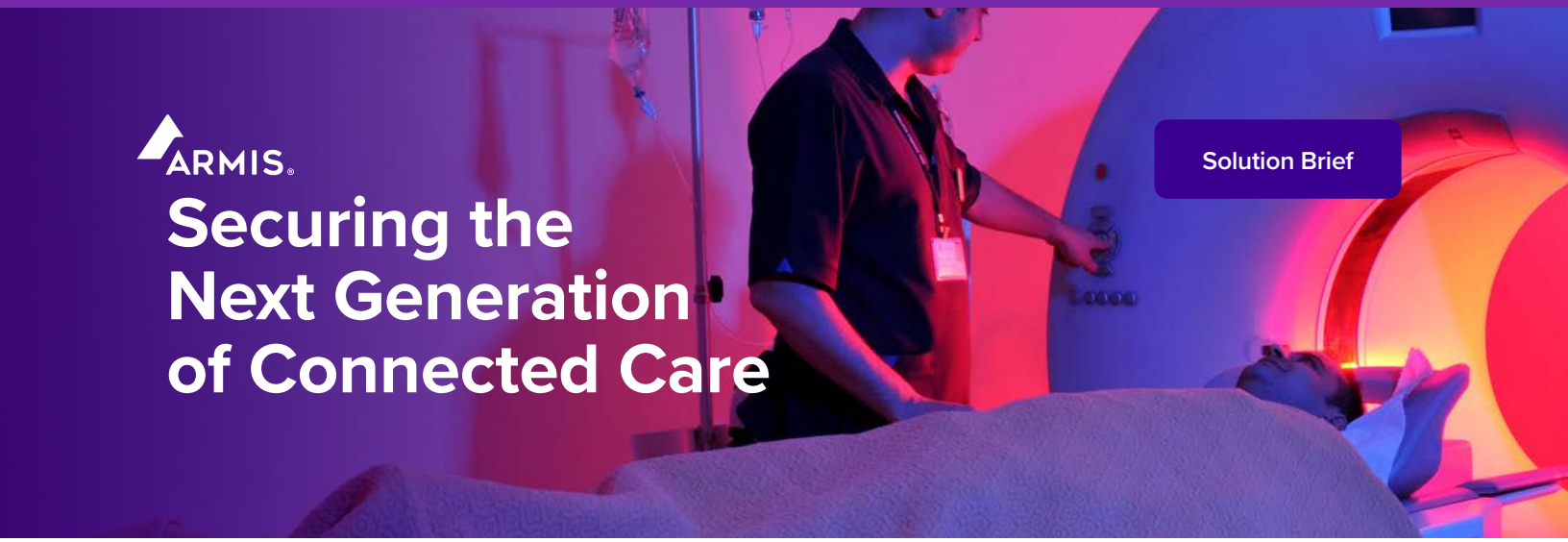

ARMIS.

Solution Brief

Securing the Next Generation of Connected Care

Connected medical devices help clinicians deliver faster, higher quality care, but they also create an attack surface that most healthcare delivery organizations (HDOs) aren't prepared to protect. These devices lack inherent security controls, they can't easily receive software updates, and they 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, IoT and OT devices cannot have agents installed, making them all but invisible to traditional security teams. Most organizations don't have an up to date or complete asset inventory, no understanding of how effectively assets are being utilized and no understanding of the attack surface that is exposed. This creates a large, mostly unmonitored cyber-attack surface that bad actors are successfully exploiting today. Silo'd ownership between operations, security and biomedical engineering teams often creates a disconnected approach to device management and security.

See it all. Secure it all

The Armis Platform 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 hospitals to confidently connect and operate all clinical assets across networks and ensure patient privacy and safety.

Delivered as an agentless passive technology, Armis identifies every managed and unmanaged device in a network. Whether IoMT, IoT, OT or IT, the Armis Collective Asset Intelligence Engine tracks anonymized data from over 3 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, 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:

IoMT, IoT, OT and IT Asset Discovery and Inventory

Armis uses agentless passive technology 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.

Asset Risk Analysis and Mitigation

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

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 uses AI and ML processing to baseline information for specific devices from the Armis Collective Asset Intelligence Engine, comparing information including unusual traffic patterns, malicious traffic destinations, unusual volumes of data, scanning of shares etc.

Medical Device Utilization and Insights

Armis aids biomedical 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.

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.

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.

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 passively detects, identifies and assesses the risk of every device.

Knowledge

The Armis Collective Asset Intelligence Engine contains detailed accumulated anonymized knowledge of more than 3 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.

Industry Leader

Armis has been recognized as a leader in healthcare device security including the SPARK Matrix: Connected Medical Device Security, Q4 2022 report.

Agentless

Many IoT, IoMT and OT environments are unable to have agents installed, leaving them outside of the scope of traditional security tools. Armis utilizes passive scanning. This enables detection of every device communicating on the network, removes the risk of crashing devices through active scanning 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

About Armis

Armis is the leading unified asset intelligence and security platform designed to address the new threat landscape that connected devices create. Our customers trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in San Francisco, California.

1.888.452.4011 | armis.com