WHITE PAPER

15 WAYS THE ARMIS PLATFORM UNDERPINS EFFECTIVE MEDICAL DEVICE OVERSIGHT AND SECURITY.

The most comprehensive asset management for managed, unmanaged, and IoT devices

Without complete asset visibility, there is no security or optimal efficiency and use of resources. Today organizations must not only get an accurate inventory of all devices IT, cloud, IoT, OT, IoMT, 5G and edge – managed and unmanaged – inside and outside their walls but must also understand the risks and usage trends associated with each device. Armis provides both types of information.

Rapid digital transformation across healthcare organizations has information security, clinical engineering, and operations teams scrambling to keep up with rapidly evolving security threats and compliance requirements. Today, the proliferation of everything from connected medical devices, such as MRIs, infusion pumps and other IoMT devices, to smart assets like TVs and thermostats pose risks across the patient journey. Especially when you consider there were 1.5 billion attacks on smart devices in 2021 alone. [source]

The management challenges with digital devices run deep. Information security teams need the right mix of capabilities to protect every device and ensure compliance. And clinical engineering teams need to ensure that the patient care delivery process goes off without a hitch. It's a huge ask on both sides, given that more than 50 percent of connected medical devices have known vulnerabilities [source], and traditional security and management solutions lack the comprehensive capabilities needed to secure and monitor every asset on the network.

The Armis advantage

- **Complete visibility**
  - Powerful discovery
  - Unified asset inventory
- **Contextual intelligence**
  - Multidimensional views
  - Comprehensive analytics and intelligence
- **Continuous security**
  - Vulnerability assessment
  - Policy enforcement
- **Rapid time to value**
  - Modern cloud architecture
  - Industry leader, trusted partner

The Armis platform stands alone in its ability to deliver complete visibility into the medical device ecosystem along with capabilities for:

- Visualizing and mitigating threats
- Understanding device inventory, utilization, and performance
- Locating devices
- Assessing clinical risk
- Improving compliance

This white paper highlights 14 ways that the Armis platform bolsters device oversight and security so information security, clinical engineering, and operations teams can work more efficiently and effectively.

Device visibility

Armis automatically discovers every connected device in your environment — managed and unmanaged, medical and IT, wired and wireless, on or off your network including cloud assets. The ability of the Armis platform to discover devices is much broader than traditional systems. For example, in addition to normal computers that are used by personnel in the clinical environment, the Armis platform can discover:

- Medical devices such as infusion pumps
- Imaging devices
- Crash carts
- Smartphones
- Tablets
- Smart TVs

- Wireless access points
- Printers
- Security cameras
- Building automation control systems.

For each device, Armis automatically discovers a wide range of device characteristics that you can automatically input into your computerized maintenance management system (CMMS), including:

- Manufacturer
- Model
- Operating system version
- Serial number
- Location
- Connections
- FDA classification
- And more.

In addition to the asset inventory details mentioned above, the Armis platform also provides complete visibility into the behaviors of all devices. The insights include all network activity, such as DNS queries, TCP sessions, and HTTP requests, in addition to device utilization and application usage. You can use this information in different ways to secure and manage medical devices. For example, identifying the different services and systems medical devices communicate with to segment the network, or to identify all medical devices that do not have endpoint protection software deployed.

The Armis Device Knowledgebase can also alert your teams to anomalous device behaviors, such as MRI machines connecting to social media sites. The behavioral analysis is important as it enables more accurate device classifications. For example, the Armis platform will classify a medical imaging workstation as what it is rather than just a computer. Similarly, it identifies devices such as iPads running patient care applications as medical support devices rather than just general-purpose tablets.

Because Armis continuously monitors your environment in real-time, all device data remains up to date, eliminating the need for lengthy site visits by clinical engineering and facility operations teams and the manual maintenance of inventory spreadsheets. The Armis platform also helps ensure the appropriate team remains aware of all patient care and ancillary support devices in the environment, regardless of which clinical department purchased or manages them. For example, new glucose monitors procured by the diabetes clinic or smart water pressure meters installed by facilities management in buildings with operating rooms.

Benefits of asset visibility through the Armis platform include:

- Fewer manual steps
- Human effort savings
- Improved accuracy and real-time updates
- Automated and comprehensive inventory
- Centralization of distributed asset inventories to a single pane of glass
- Continuous device monitoring
- Complete contextual classification of devices
- Scalable deployment model utilizing cloud-to-cloud integrations

2. Device location and utilization

The Armis platform gathers medical equipment utilization information across your entire enterprise providing intelligence about device usage, hours of operation, and underutilization. This can help you plan purchases, schedule maintenance downtimes, right-size your inventory levels, and maximize efficiency through the entirety of the medical device lifecycle. Visibility not only ensures optimal uptime and operations of critical medical devices, it also enables the following:

- Compare usage across facilities for better equipment distribution
- Use device data to improve asset data in IT governance and electronic health record applications
- Identify offline or unused medical devices and bring them back into service
- Find misplaced or intentionally hidden devices
- Identify where end-of-life medical devices are still being used
- Identify recalled devices and schedule maintenance windows
- Correlate recalled unstable device reporting with location data to proactively investigate potential safety incidents
- Discover when devices travel from one site to another
- Understand usage patterns and adjust schedules
- Make better-informed purchasing decisions
- Save money by avoiding purchasing additional inventory to replace “lost” items

3. Third-party and vendor-managed device and network discovery

Armis enables you to discover computers and devices on your network that are owned and operated by third parties, including outsource suppliers, vendors, consultants, patients, and visitors. You can view the location, external connection, and software vulnerabilities associated with each device. You can use this comprehensive device visibility to help optimize physical security, information security, and risk management.

The ability to catalog not only a device’s properties but also its software inventory is of paramount importance in unmanaged devices given emerging threats, such as Log4J, from legacy libraries and software stacks. These antiquated libraries are often used in medical devices and systems that may not be updated, in some cases, for decades. The Armis platform automatically discovers every device on your network and correlates the firmware versions, operating systems, application catalog, and even the TCP/IP stack, with vulnerabilities that would otherwise go unnoticed.

4. Rogue device discovery

The Armis platform continuously looks for devices that may be masquerading as authorized devices and allowed onto your network by your existing Network Access Control (NAC) system. Armis uses a more sophisticated method than traditional NACs to identify devices and can easily identify things like MAC address spoofing. This includes devices masquerading as medical devices or medical network access points attempting to steal corporate credentials and patient data.

Armis also sees everything in the enterprise airspace, including devices that communicate via Wi-Fi, Bluetooth, and many other peer-to-peer protocols that are invisible to traditional security tools. This not only provides an added layer of protection against potential network intrusion and data exfiltration points, but it also enables the Armis platform to deliver a more complete inventory of devices than traditional tools that see only IP addresses. For instance, you can leverage the airspace visibility feature on the Armis platform to inventory and locate devices that are not directly connected to the network, such as defibrillators, in addition to consumer IoT devices, such as smart lights and smart locks.

5. Risk scoring for all devices

Through 100% passive monitoring, the Armis platform generates a risk score for every device in your environment. It does this without agents or any pre-programming or pre-knowledge of what a device is or how it should be configured. The risk score is based on the following a detailed list of risk factors that the Armis platform assesses, including:

- Attack surface exposure
- Cloud service access
- Connection-level security posture
- Boundary evasion
- Third-party application repository access
- Malicious domain access
- Vulnerability history
- Data-at-rest security
- External connectivity
- User authentication
- Software version
- Certificate reuse
- Manufacturer reputation
- Device model reputation including information contained in the Manufacturer Disclosure Statement for Medical Device Security (MDS2) for each device

In addition to providing risk scores, Armis can detect network level disruptions, such as IP collisions, network latencies, and packet loss. This information combined with device utilization data enables the Armis platform to detect and diagnose issues so you can respond to potential safety incidents and care disruption.

6. Contextualized risk assessment for medical devices

The Armis platform performs real-time risk assessment for medical devices. Because Armis takes a completely passive approach, there is no impact to the flow of medical device traffic or active probing of sensitive medical devices, which can cause interruption to patient care. The key to any effective medical device risk assessment approach is factoring in the clinical context of devices and not just considering known technical vulnerabilities. By leveraging behavioral analysis and utilization analytics, the Armis platform provides a contextualized risk score that also includes clinical risk for each device.

Some of the factors the Armis platform analyzes for the holistic assessment include:

Device properties

- Operating system/firmware version
- Manufacturer risk analysis
- Device make/model
- Network-level details, such as number of open ports

Vulnerabilities

- Operating system vulnerabilities
- Application vulnerabilities
- Network-level vulnerabilities, such as TCP/IP stack and Bluetooth vulnerabilities

Device behaviors

Rather than simply tying risk scores strictly to vulnerabilities, the Armis platform also analyzes device behavior to provide additional context, such as:

- Malicious traffic and exploit attempts
- Transmission of unencrypted PHI
- Port scan activity
- Use of unencrypted protocols (for example, FTP or Telnet)
- Anomalous behaviors that deviate from normal operation, such as accessing external sites or connecting between corporate and guest networks

FDA recalls

The Armis platform assesses medical devices for the existence of the different classes of FDA recalls. Direct links to the FDA databases enable clinical engineering teams to quickly and easily obtain more details for each FDA Recall.

MDS^2 properties

The Armis platform links MDS2 properties and files directly to medical devices. MDS2 provides additional guidance to securing medical devices and contributes to the risk assessment in cases where security controls, such as patches or endpoint security, cannot be applied.

Because Armis is a real-time and continuous solution, it provides the most up-to-date risk assessment for all devices in the environment without having to wait for, or execute, manual scans. You can tie policies to the discovery of risks or updating of risk scores to assist in limiting the attack surface of devices. For example, automatically creating tickets for the clinical engineering team to review only when new high-risk medical devices are added to the network.

Overall, the risk assessment benefits in the Armis platform include:

- A multi-pronged, comprehensive risk assessment approach that incorporates a device's role, properties, vulnerabilities, and behaviors
- Real-time and continuous monitoring ensures risk factors remain updated and accurate

- Direct integration with the NIST database, advisories, and available patches aid in remediation of vulnerabilities
- FDA recall information and MDS2 properties are linked directly to the device in the Armis console
- Passive vulnerability assessment ensures critical medical devices are not impacted and uptime is maintained
- Proprietary threat detection engine identifies malicious activity on all device types with the ability to automate remediation
- Customized reporting capabilities on any aspect of risk assessment to quickly generate reports or build policies
- Interoperability with clinical engineering workflow management solutions

7. Detection and visibility in custom healthcare networking environments

The Armis platform can inventory devices that are placed on segregated vendor-managed networks which can create blindspots. With the Armis platform, you can see devices and traffic on these networks, providing you with the visibility, security, and control required, while still supporting segmented networks and all the benefits they bring.

Without agents, Armis passively monitors device traffic, including data passed from VLANs through a dedicated gateway and on to the hospital Intranet. There is nothing to install on the devices, and no scans to disrupt them or tip them over. Armis' ability to passively monitor network traffic, allows for the discovery of medical devices in your environment, including those that use the proprietary protocols. This includes visibility into device utilization such as when devices are actively monitoring patients, any network issues that can impact performance, such as IP collisions, as well as device location details.

8. Reduce risk of ePHI exposure and privacy breaches

Exposures and breaches of ePHI can result in reputational damage, regulatory violations, and financial repercussions, including class-action lawsuits. Armis has the unique ability to detect when ePHI is being transmitted in unencrypted format, which can put the information at risk of alteration or theft, and can be a security and/or privacy policy violation. Moreover, privacy breaches don't only stem from unencrypted PHI; various new IoT and smart devices also pose risks.

The Armis platform assesses healthcare environments for ePHI exposure and privacy breaches in numerous ways. For example, Armis can identify medical devices sending unencrypted information like passwords, unencrypted patient files, DICOM images, lab test results, and other types of files. Armis has seen such transmissions coming from CT machines, ultrasound machines, and nuclear imaging machines, and in some cases being transmitted out to the internet to malicious servers. The presence of unsanctioned IoT and smart devices can also pose a threat to patient privacy. For instance, by continuously recording information or even containing unencrypted credentials that can be used to access patient record databases. Traditional security products may have visibility into the data, but they lack the device and workflow context that enables appropriate alerting.

Examples and benefits of how the Armis platform can protect an organization include:

- Reduced risk of data tampering, which can lead to misdiagnosis and patient harm
- Reduced risk of financial and reputational damage resulting from non-compliance with applicable security and privacy regulations

- Enhanced detection and identification of unsanctioned or misconfigured devices used for monitoring patients with privacy breach potential. For example:
  - Detect smart cameras set up in patient units streaming out to cloud portals.
  - Identify the presence and usage of virtual assistants, such as Amazon Echo in shared patient rooms, which can record and share confidential information.
- Increased ransomware protections through the ability to detect indicators of data exfiltration that are leveraged by newer variants of ransomware to steal patient data prior to encrypting files.

9. Compliance

The Armis platform aligns organizational views with a number of regulatory frameworks and requirements, including:

- NIST CyberSecurity Framework (CSF)
- MITRE ATT&CK Framework
- HIPAA Security Rule
- PCI-DSS
- FDA medical device compliance

The platform can help healthcare teams quickly assess security posture and compliance for digital assets across the environment. It also includes the capability to report on either adherence to or noncompliance with the various components of these regulations and standards. This approach helps ensure the healthcare network and medical devices provide maximum protections for patient health and data by always remaining secure and operational.

- Compliance benefits include the ability to:
- Ensure compliance to industry frameworks and regulations
- Minimize attack surface and prevent breaches
- Get real-time updates on activity and compliance status of devices
- Rely on scheduled or on-demand reporting for framework compliance
- Automate alerts, containment, and remediation of non-compliant devices
- Create customized compliance status dashboards
- Follow direct links to advisories and compliance databases
- Conduct detailed audits on all devices, activities, users, applications, operating systems, vulnerabilities, and risks

10. Medical device segmentation

The Armis platform supports network segmentation initiatives by identifying all communications between medical devices, subnets, and protocols used in your environment. You can leverage this information to create access control lists (ACLs) for segmentation projects. The Armis platform also augments network access control (NAC) solutions by providing visibility into medical, IT and IoT devices that is not available through traditional security controls. Armed with knowledge from the Armis platform, you can set granular policies and automate device segmentation based on medical device identification, attributes, behavior, and communication. Armis ensures medical devices are connected to their appropriate secured segments and are not connected in error to unsecured networks, such as guest wireless networks.

In addition to lacking visibility into medical and IoT devices, traditional NAC solutions are rule based and mostly act as gatekeepers for devices trying to join the network. Once a device is on the network, NAC solutions lack the visibility or ability to enforce rules based on changing device behaviors. The Armis platform can augment NAC solution capabilities with continuous monitoring. Through the ability to detect threats and the risky or anomalous behavior of virtually any device, you can enforce NAC policies on any device to ensure the appropriate segmentation, integrity, and availability of critical healthcare networks.

- Get help creating ACLs for network segmentation by identifying traffic properties, such as services and protocols used by medical devices
- Automate segmentation by leveraging NAC solutions for all devices types, including managed, unmanaged, IoT, and medical devices
- Extend and enforce NAC policies to unmanaged IoT and medical devices deviating from sanctioned network segments
- Maintain a secure medical device network by continuously monitoring for risky behavior and leveraging NAC solutions to automate containment of threats

11. Network segmentation and performance

The Armis platform also understands network segmentation and can alert you when one or more of your network segments (physical or logical) have lost integrity. For example, Armis shows you unauthorized connections between your lab network and your patient network, and Armis can see when laptop computers are connected to a network that is supposed to only contain medical devices. Existing healthcare customers have leveraged the Armis platform Armis to:

- Uncover medical devices connected to insecure hospital guest networks,
- Identify data exfiltration activities
- Find medical devices responding to suspicious connections attempts.

Beyond enhancing segmentation capabilities, the Armis platform can detect and alert you to network performance degradation that could impact proper medical device function. Many medical devices can only tolerate very low network latency to ensure real-time monitoring of patients, and any communication delays between medical devices, such as bedside monitors for vital signs, could put patients at risk. The Armis platform can assess various aspects of network performance and alert teams based on thresholds or anomalous behavior. Benefits include:

- Identifying network-related degradation and disruptions to critical medical devices, including:
  - IP collisions
  - DNS/DHCP retransmits and timeout
  - Network latency and jitters
  - Access point failures
- Preventing downtime through real-time alerting of network performance degradation and anomalies
- Ensuring optimal medical device operations by appropriate network resource allocation
- Identifying and remediating misconfigured medical devices on the network

12. Zero trust network principles

Healthcare organizations leverage Armis to apply Zero Trust principles to their medical device and IT

security. With visibility into the various pillars that comprise a zero trust model the Armis platform can analyze each layer to identify risks and threats and help organizations secure their environment. Below are some examples of how Armis can apply Zero Trust principles for medical devices in each pillar.

Device

- Gain complete visibility into all devices on the network
- Assess each device for risks, vulnerabilities, and behaviors
- Identify communication patterns between devices
- Identify devices running unsanctioned applications and connections

Network

- Gain visibility into each device's network traffic and limit communication to the minimum required for the medical device to operate
- Enforce Zero Trust by automating network segmentation based on device type
- Group together devices to form logical boundaries network segments based on subnet, function, groups, or device types
- Monitor network segments for suspicious and malicious behavior or unsanctioned cross-boundary communication

Identity

- Associate users with devices on the network
- Identify users behaving in risky ways, such as using malicious software
- Identify devices impacted by compromised user accounts
- Identify devices with unauthorized user logons
- Identify administrative credentials being transmitted in clear-text

Data

- Monitor each device's data transmission and receive alerts when sensitive data like ePHI or user credentials are unencrypted
- Detect and block data exfiltration attempts or transfers both internally and externally
- Closely monitor environments where critical data resides
- Improve third-party risk posture by utilizing logical boundaries for business associates and understanding data context

Visibility and analytics

- Monitor network traffic to detect behavioral anomalies
- Gain visibility into network and device analytics to identify compromises
- Identify security gaps or increased attack surfaces on devices
- Identify unsanctioned connections and applications running on devices

Automation and orchestration

- Automate remediation and enforcement of Zero Trust principles by leveraging integrations with existing infrastructure, management tools, and security controls
- Ensure CMDBs remain up-to-date with secure configuration information
- Enforce network segmentation policies designed for Zero Trust
- Leverage security controls such as firewalls, vulnerability scanners, and SOAR systems to ensure violations of Zero Trust principles are corrected immediately

Workload

- Discover, classify, and profile physical and virtual servers regardless of whether they are deployed on-premises or in cloud environments.
- Monitor traffic between devices and cloud environments
- Detect insecure configurations and run-states of cloud workloads
- Identify security gaps that exist as cloud assets without enterprise security tools spin up rapidly

Armis understands network segmentation and can alert you when one or more of your network segments (physical or logical) have lost integrity. For example, the Armis platform shows you unauthorized connections between your lab network and your patient network, and the Armis platform can see when laptop computers are connected to a network that is supposed to only contain medical devices. Healthcare customers relying on the Armis platform have uncovered scores of medical devices connected to insecure hospital guest networks. They have also been alerted to data exfiltration activities, and identified medical devices responding to suspicious connections attempts.

13. Threat detection and response

Armis' cloud-based Threat Detection Engine is able to discover malware present in your network that your existing threat detection systems may not protect against (for example, WannaCry, Locky, Ryuk, and Zeus Panda ransomware). Once Armis detects malware, it issues an alert and can break the kill chain by interacting with your existing network infrastructure (for example, switches, routers, and wireless LAN controllers) and/or security tools (for example, NAC or firewall) to block communications from the infected device. Clinical devices running traditional operating systems like Windows without endpoint protection agents as well as those running realtime operating systems (RTOS), such as VxWorks or ENEA's OSE, that contain lower level vulnerabilities such as URGENT/11 are also visible in the platform. Armis can detect active exploitation of these vulnerabilities and alert for immediate response and remediation. For example, a healthcare customer used the Armis platform to gain visibility into and combat a WannaCry infection. The customer uncovered nearly 20x more activities on the Armis platform than on its traditional security controls, including WannaCry activity on medical devices. The customer also tracked remediation activity through customized dashboards and reports created for the Board of Directors.

14. Alignment to mitre ATT&CK model

Threat hunters assisting Information Security and clinical operations teams use Armis to map to the knowledge base of adversary tactics and techniques contained in the MITRE ATT&CK framework. Benefits include:

- Identifying the most active threat actors targeting environments
- Understanding techniques most used by threat actors
- Prioritizing each technique based on probability and potential impact

- Assessing current defenses, understanding gaps, and planning improved defenses
- Using the data as a framework to update security operations play books in alignment with continuity of operations

15. Protection for “Un-agentable” devices

Armis observes the communications and records metadata and threat intelligence from all unmanaged and un-agentable devices on your network and in your airspace and retains this information for at least three months. Security analysts can use this data to perform forensic analysis for a security incident. All monitoring is continuous, passive, and is agentless. Our approach ensures detailed data is retained without any impact to the network and every device type, including managed, unmanaged, traditional devices like laptops, medical devices, and IoT devices like smart cameras.

Summary

Armis built our agentless device security platform to meet the needs of healthcare delivery organizations, helping IT and clinical engineering teams secure the devices clinicians use to deliver higher quality care without compromising the safety of patient’s health, safety, or sensitive medical information. In working with our customers, Armis has developed extensive experience with the use cases that are important to help clinical engineering achieve these goals.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies 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 Palo Alto, California.

armis.com

info@armis.com

20222904-1