ARMIS

USE CASES FOR HEALTHCARE

ARMIS USE CASES FOR HEALTHCARE

How Healthcare Delivery Organizations (HDOs) Are Using The Armis Platform

This document is intended to help Armis' prospective customers understand how Armis' existing healthcare delivery customers are using the Armis platform to reduce their cyber risk, improve compliance with security frameworks such as NIST CSF and CIS CSC, and improve compliance with regulations such as HIPAA. Armis also helps improve efficiency of processes such as inventory management, threat detection and response. This document is designed to supplement (not replace) Armis' standard marketing materials.

Business Use Cases

1. Protect Patient Health

Protecting patient health is paramount. By detecting vulnerabilities, malware and other cyber threats within your healthcare delivery environment, Armis is able to reduce risk to your patients. Some of the risks are obvious, such as the presence of malware on an infusion pump that is connected to a patient. Some of the risks are less obvious, such as an attacker's ability to alter DICOM images that are transmitted without encryption in your environment. Armis' security platform provides proactive and real-time information to your security team to allow them to lower your cyber risks. Benefits include:

- Protect patient care
- Lower risk of litigation, brand damage, or regulatory penalties

2. Completely Automated Device Inventory Process

Armis' ability to automatically discover every connected device in your environment — managed and unmanaged, wired and wireless, on or off your network — greatly streamlines your asset inventory processes. Armis' scope is much broader than traditional inventory systems and includes devices such as infusion pumps, imaging devices, crash carts, smartphones, tablets, smart TVs, wireless access points, printers, security cameras, temperature control systems — and even normal computers that are used by people. For each device, Armis automatically discovers a wide range of device characteristics such as manufacturer, model, OS version, serial number, location, connections, FDA classification, and more. This information can be automatically imported into your IT asset management or CMDB system (e.g. AIMS by Phoenix Data Systems). Benefits include:

- Fewer manual steps
- Manpower savings
- Improved accuracy
- More comprehensive inventory

3. Reduce risk of personal health information (PHI) exposure

Armis has the unique ability to detect when PHI is being transmitted in unencrypted format, which can put the information at risk of alteration or theft, which can be a HIPAA violation. For example, Armis can identify medical devices sending unencrypted information such as passwords, unencrypted patient files and DICOM images, and other types of files. We have seen such transmissions coming from CT machines, ultrasound machines, and nuclear imaging machines. Traditional security products can see that these transmissions are unencrypted, but they do not have context -- they don't know that these transmissions are coming from medical devices, and they don't know that they are sending ePHI – so they fail to issue alerts. Benefits include:

- Reduced risk of data tampering, which can lead to misdiagnosis and patient harm
- Reduced risk of HIPAA violations and fines

4. See and Stop Ransomware Attacks

Ensuring medical equipment from MRIs to X-Ray machines to ventilators is operational and delivering care is key for any HDO. Armis is able to safely determine whether any of your existing medical devices are vulnerable to WannaCry or other kinds of ransomware attacks, which allows your security team to take proactive measures to protect these devices from attack. Armis can also discover malware present in your network that your existing threat detection systems often don't discover (ex: WannaCry on medical devices such as MRI machines). Once a detection is made, Armis issues an alert and can break the kill chain by interacting with your existing network infrastructure (switches, routers, wireless LAN controllers) and/or security tools (NAC, firewall, etc.) to block communications from the infected device. Benefits include:

- Avoid business disruption
- Avoid damage to your brand and reputation
- Lower risk to patient health

5. More Efficient Audit Processes

Armis' ability to automatically generate information for many of the security controls that are required by internal and external auditors (e.g. NIST CSF, HIPAA) lets you reduce the number of person-hours spent on auditing processes. Benefits include:

- Manpower savings
- Fewer non-compliance findings

6. Mergers and Acquisition Cyber Risk Assessment

When merging with or acquiring new organizations, you typically don't have a clear view into the target organization's security posture. Armis provides the ability to discover IT assets and vulnerabilities with essentially no intrusion or disruption to existing IT infrastructure; this can help an organization assess the cyber risk of another organization during the due-diligence phase prior to the merger or acquisition. Post-acquisition, the acquiring company will be able to use Armis as a centralized system that provides visibility to all devices and associated security risks connected to the acquired company's locations anywhere in the world. Benefits include:

- Improve understanding of cyber risks prior to M&A
- Improve centralized visibility of disparate organizations and remote networks
- Create security plan and policies to address any security requirements

7. Reduce Wasted Expenditure on Software Licenses

Armis' ability to discover software that is actually being used on each corporate-owned computer may let you reduce the number of software licenses that you purchase and maintain on an ongoing basis. Benefits include:

- Save money by avoiding purchasing and maintaining unneeded software licenses

8. Better Manage Your Equipment Inventory

Armis' platform gathers medical equipment utilization information across your entire enterprise, giving you intelligence about device usage, hours of operation, and underutilization. This can help you plan purchases, right-size your inventory levels, and maximize efficiency.

- Compare usage across facilities to for better equipment distribution
- Identify offline devices and bring them back into service
- Find misplaced or intentionally hidden devices
- 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

9. Get More Value from Your Existing Security Investments

Armis easily integrates with your existing security tools, letting you leverage existing investments to achieve greater value and more automated response. Armis enriches your existing investments in the following ways:

- Give your firewall the intelligence to block traffic from compromised devices
- Enrich your network access control (NAC) system with better information to more accurately classify devices and segment your network
- Give your SIEM visibility to risks and threats stemming from unmanaged devices which produce no logs and cannot accommodate agents
- Alert your vulnerability assessment system to the presence of transient devices that have just joined the network so they can be formally assessed
- Trigger action in other security systems like opening a ticket or initiating a workflow in an orchestration system
- Feed real-time asset discovery information into your ITAM and CMDB including systems such as AIMS by Phoenix Data Systems

10. Monitor Remote Sites Without Additional Resources

Large organizations often have remote offices without dedicated IT staff. For these organizations, Armis provides an easy way for the centralized security team to monitor what is happening at remote offices--what devices are on the network, and whom they are communicating with. Since Armis does not require deployment of agents or additional hardware, the impact on the remote offices is low. Benefits include:

- Manpower savings
- Improved governance over remote sites

Technical Use Cases – Discover

1. Asset Inventory

Armis detects, classifies, and profiles every device in your environment – managed, unmanaged, and IoT – giving you a complete, real-time device inventory and an unprecedented level of visibility to activity on your network and in your airspace. Whether you have one site or many, Armis provides a depth of information not found in other products, such as:

- Device name
- Mac and IP address
- Manufacturer
- Model
- OS & OS version
- User
- Applications
- Connection history
- Link to each device's Manufacturer Disclosure Statement for Medical Device Security (MDS2)

2. Shadow IT Discovery

Armis is able to automatically discover all devices in "hidden" parts of your network, eliminating any possibility of "shadow IT" devices. This is possible because Armis does not utilize any sort of active scanning and does not need to be told in advance about your network topology.

3. Rogue Device Discovery

On an ongoing basis, Armis discovers devices that may be masquerading as authorized devices and have been allowed onto your network by your existing NAC system. (Armis uses a more sophisticated method to identify devices than NAC does and can easily identify situations such as MAC spoofing.)

4. Third-party Device Discovery

Armis lets you discover computers and devices on your network that are owned by third-parties (outsource suppliers, vendors, or consultants). You can see where they are, the internal and external connections that they make, and the software vulnerabilities that they bear.

5. Discover Bluetooth Devices, Risks and Threats

Armis 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 allows Armis to detect risks and threats in your environment. It also helps Armis produce a more complete inventory of devices than traditional tools that see only IP addresses.

6. Discover the Risk of Every Device

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

- 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

7. Improve Compliance with Security Frameworks

Traditional security tools that are commonly used to implement security frameworks such as NIST CSF or the CIS Critical Security Controls are typically not effective against IoT and other “un-agentable” devices. Thus, there is a gap in coverage. Armis is an agentless security platform that has been specifically designed to help you implement many of the security controls listed in the various frameworks for both managed and unmanaged devices, including the Internet of Things.

8. Assess Security Posture of Managed Computers

Through 100% passive monitoring, Armis is able to detect when agents on managed computers are installed and working properly. When this is not the case, Armis can issue an alert and open a ticket in an incident response system.

Technical Use-Cases – Analyze and Protect

1. See and Stop Malware and Ransomware Attacks

Armis' cloud-based Threat Detection Engine is able to discover malware present in your network that your existing threat detection systems often don't discover (ex: WannaCry, Locky, and Zeus Panda ransomware). Once a detection is made, Armis issues an alert and can break the kill chain by interacting with your existing network infrastructure (switches, routers, wireless LAN controllers) and/or security tools (NAC, firewall, etc.) to block communications from the infected device.

2. Identify and Stop Unencrypted Data Transmission (e.g. HIPAA Violations)

Armis is able to detect when data that should be encrypted (e.g. DICOM images, credentials, ePHI, etc.) is being transmitted in clear text. Once detected, Armis issues an alert and can optionally take actions such as quarantine the device, open a ticket, etc.

3. Identify Network Segmentation Failures

Armis 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.

4. Agentless EDR for Unmanaged Devices

Armis observes and records the communications of all unmanaged and un-agentable devices on your network and in your airspace and retains this information for at least three months. This can be used by security analysts performing forensic analysis after a security incident.

About Armis

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately-held company headquartered in Palo Alto, California.