WHITE PAPER

MEDICAL AND IOT DEVICE SECURITY FOR HEALTHCARE.

Managing risk and ensuring patient safety with 21st century healthcare

With the advent of the Internet of Things (IoT), businesses are experiencing a digital transformation bigger than the PC and mobile revolutions combined–and healthcare is no exception. The new breed of connected medical devices brings the promise of improved patient care, better clinical data, improved efficiency, and reduced costs–but they also bring increased security risks. According to a Forrester Consulting study, 63 percent of healthcare delivery organizations have experienced a security incident related to unmanaged and IoT devices.[1]

This white paper will examine the security risks of medical devices that affect healthcare delivery organizations and the patients that they serve. We will also explore a solution to the security problem—one that encompasses not just biomedical devices, but all the various "smart" devices that are present in healthcare delivery organizations that add to the risk.

The medical device healthcare exposure

Connected medical devices offer the potential to improve patient care and operational efficiency, but they also introduce three distinct security challenges:

Lack of visibility and inventory capabilities

An accurate inventory forms the basis for any security or risk program. The problem is that medical devices and other smart devices in a healthcare ecosystem are difficult to discover and inventory. Since unmanaged IoMT, IoT, and smart devices don't support inventory agents and are often missed by network discovery scans, security teams relying on traditional inventory methods struggle to get a clear understanding of their true risk.

Even when biomedical teams have an inventory of the devices their departments support, usually in the form of spreadsheets, the inventories are often outdated and require resource-intensive efforts to update. Moreover, the device list is limited to what the biomedical team manages and wouldn't include other devices, such as those managed by the diagnostic imaging or diabetes teams. The challenges are further complicated by the fact that different departments and teams often purchase devices and other innovative technologies in a decentralized manner independent of the security team, creating potentially enormous blind spots.

The Armis advantage

- ➤ **Complete visibility**
  - Powerful discovery
  - Unified asset inventory
- ➤ **Contextual intelligence**
  - Multidimensional views
  - Analytics and intelligence
- ➤ **Continuous security**
  - Vulnerability management
  - Adaptive trust
- ➤ **Rapid time to value**
  - Modern cloud architecture
  - Industry leader, trusted partner

Inherent security control limitations

Beyond asset visibility, there are limitations on the security controls that can be applied to medical devices. While traditional enterprise devices, such as laptops and servers, support a host of traditional security tools, including inventory and patching agents, medical devices simply cannot. For example, many devices, such as Alaris PCU pumps run proprietary operating systems (OSs) that do not support agents.

In other cases, despite running a mainstream OS, such as Microsoft Windows, the devices are certified by the vendor with specific configuration parameters. In these cases, relying on traditional agent-based security tools, or even installing native Windows security patches, can result in unresponsiveness or unexpected behavior that can impact patient safety. This inability to patch or upgrade has resulted in millions of devices in healthcare environments running decades-old legacy OSs and vulnerable software, further amplifying risks to patients and organizations.

Inability to contextualize clinical and device risk

Healthcare device ecosystems are full of unmanaged devices. And with different departments using an array of new device types, understanding their unique contexts is critical to the risk assessment process. And it's also impossible to achieve through the traditional security software stack. For example, although vulnerability scanners can identify common vulnerabilities and exposures, they treat each endpoint as the same (a compute device running vulnerable OS and software).

In a clinical environment, however, a legacy workstation embedded into a large MRI scanner actively providing patient care poses a significantly higher risk compared to the same OS with the same vulnerabilities on a workstation found in a non-clinical environment. Manufacturing Disclosure Statements for Medical Device Security (MDS^2) files also provide an abundance of privacy and security functions of the device that healthcare organizations must take into consideration.

Proven value for HDOs

The Armis unified asset intelligence platform delivers a wide range of business value for healthcare delivery organizations, including the following benefits.

- **Protect patient safety** – Alert security managers to cyberattacks and compromised devices, including medical, clinical, and smart devices of all types. The ability to complete contextualized risk analysis, such as understanding clinical risk related to FDA recalls, allows teams to prioritize securing the most critical at-risk patient care devices.
- **Maintaining availability of patient care services** – Proactively monitor for network issues and manage risk across all devices that can impact patient care service. Enable enhanced monitoring and real-time alerting for the most critical clinical devices.
- **Protecting patient privacy** – Monitor for the various ways patient privacy is put at risk, from detection of external transfer of unencrypted PHI, to clinical system service account compromise, or compromised IP cameras streaming out to the internet.
- **Enable patient care innovation safely and securely** – Empower research and clinical departments to improve patient care delivery through the secure adoption of innovative technologies and migration from legacy methods and systems.
- **Ensure audit and regulatory compliance** – Streamline auditing of systems and ensure compliance with regulations, such as HIPAA or PCI-DSS for payment systems, and various audit requirements.
- **Automate device inventory** – Reduce person-hours focused on tracking devices with a dynamically updated real-time view of all hardware and software assets in the environment.
- **Reduce costs with data-driven purchasing decisions** – Generate a complete, real-time inventory of all medical and other devices, find lost equipment, more efficiently utilize existing equipment, and leverage utilization analytics to justify purchasing additional equipment, ultimately reducing cost of over-investment in equipment.
- **See and stop ransomware attacks** – Identify WannaCry and other ransomware in real time, reducing the risk of operational downtime and reputational damage.
- **Deliver faster vulnerability and threat detection** – Real-time passive identification of vulnerabilities and detection of threats ensures attack surface management and faster time to response for incidents, minimizing the risk and impacts of cyberattacks.
- **Streamline incident response** – Fine-tune SOC workflows and achieve faster response through automated enforcement of security controls in the event of an incident. Automatically contain and remediate cyber threats as they happen in real-time, reducing overall operational risk and downtime.

Ultimately, traditional security tools simply do not capture the true contextualized device risk, including the behavioral and clinical factors. And this leads to an inaccurate quantification of a healthcare organization's true security posture and risk.

It's not just medical devices that impact patient care

Medical devices like the ones described above are not the only unmanaged devices that pose a risk. They are also not the only devices that can directly impact patient care. Just consider a few parts of the ecosystem that supports the patient journey:

- Check-in kiosks
- Tablets and iPads
- Handheld scanners
- Security cameras
- Digital signage displays
- Elevator control systems
- Smart thermostats
- Smart TVs
- HVAC systems controlling humidity and temperature
- Porter communication systems
- And more

Malfunction or downtime of building management systems, such as the HVAC units that regulate humidity levels in an operating room, can result in canceled surgeries. This is a prime example of a non-medical device that directly impacts patient care. The implications are striking when you consider that 64 percent of healthcare delivery organizations estimate that at least half of all devices on their network are unmanaged or IoT devices, including medical devices.[2] While hospital and security teams tend to focus on medical device security, it is imperative to 'zoom out' and include other IoT and smart devices as part of the risk assessment scope.

Healthcare is a frequent target

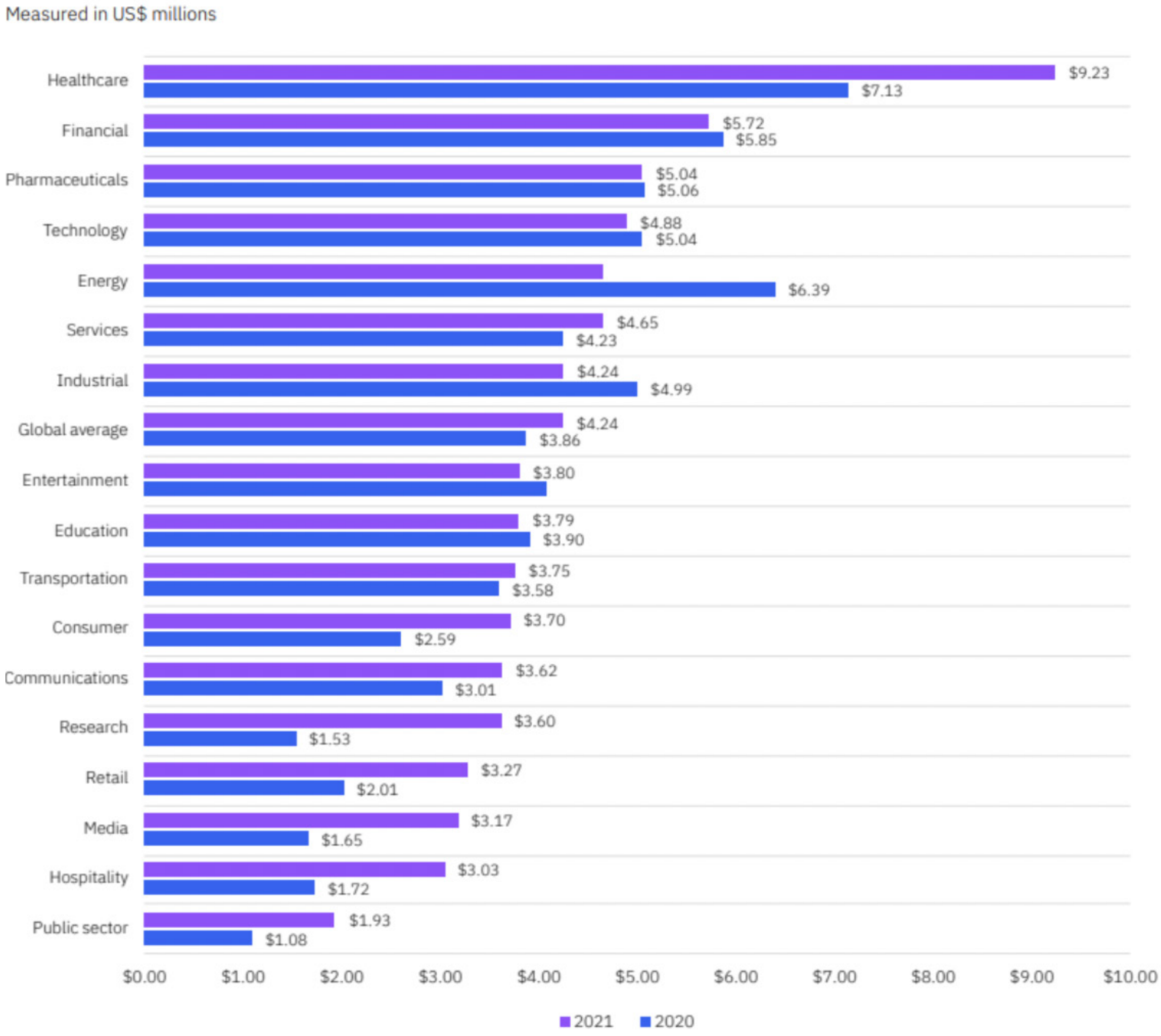
Statistics show that healthcare delivery organizations are among hackers' favorite targets. Why? Because medical records contain information that can be used for identity theft. As a result, the resale price for a healthcare record is orders of magnitude more than the resale price of a stolen credit card number.

Since hacking healthcare organizations is now so lucrative, the number of security breaches experienced by healthcare institutions has skyrocketed. And all it takes is a quick Internet search to see that healthcare is top target for cybercriminals year after year. In fact, the HIPAA Journal reported that 2021's biggest healthcare data breaches rank amongst the worst of all time with nearly 45 billion records compromised across nearly 700 breaches.[3]

Nearly 50 million records were compromised in healthcare data breaches in 2021.

– HIPPA Journal[4]

To make matters worse, data breaches are more costly for healthcare providers than for any other type of business. This is due to the stringent penalties and costs that are mandated by HIPAA regulations. According to the Ponemon Institute, the average cost of a data breach for healthcare providers was more than $9.23million.[5]



Average cost of a data breach by industry.[6]

Securing medical devices and more

Patient monitoring devices

- Medical devices – Smart medical devices, infusion pumps, ventilators, incubators, telemetry, smart stethoscopes, medical imaging
- Clinical monitors – Electrocardiogram (ECG), heart rate, pulse oximetry, ventilators, capnography monitors, depth of consciousness monitors, regional oximetry, biopatch technology, and respiratory rate
- Smart patient room – Smart beds, hand hygiene, fall detection
- Virtual care and telemedicine – Remote health telemetry and care delivery

Patient experience devices

- Registration devices – Kiosks, label printers, tablets, and pagers
- Digital Signage – Smart TVs, wait time screens, electronic whiteboards
- Patient transport – Elevator systems, porter communication devices, lab specimen transport

Building management system monitoring devices

- Emergency response – Code blue infrastructure, fire alarms and suppression, dedicated telephony, helipad lightings and control
- Security – Video surveillance, door locks and entry systems, security communication systems
- Utilities and power – Power monitoring, emergency generators, power distribution, water supply and quality monitors
- Environmental controls – HVAC, lighting, room control, humidity monitoring, tissue and blood refrigerators

Remote wellness and chronic disease monitoring devices

- Implantable devices – Pacemakers, defibrillators, neurostimulators
- Wearables – Wristbands, biopatches, smartwatches, ear buds
- Remote clinical monitors – Spirometer, pulse oximeter, ECG, glucometer, fall detection

From hacking patient data to hacking patient care

Cyber attackers continue to expand their focus and are no longer just concentrating on extracting healthcare records and patient data. For example, ransomware gangs have focused on gaining control over medical devices and demanding payment for returning control. And their financial success has resulted in increasingly frequent and costly cyberattacks and constant news headlines over the past several years. In 2018, for example, an Indiana hospital lost access to systems for a day after a ransomware attack, only restoring them after paying the attackers $180,000.[7] In 2021, a ransomware attack on a Georgia-based health system disrupted its network for multiple days and jeopardized the records of 1.4 million patients.[8] And the threats to healthcare organizations persist; in 2021 the healthcare industry saw the most ransomware attacks of all critical infrastructure sectors, according to the FBI.[9]

Today, given their inherent vulnerabilities, attackers are increasingly looking to medical devices and other unmanaged assets as onramps for ransomware and other types of attacks. To understand why, just consider a few vulnerabilities discovered by the security community.

TLStorm

In spring 2022, Armis researchers discovered a set of three critical vulnerabilities in APC Smart-UPS devices, a widely used emergency backup power source in healthcare environments. Attackers could exploit the vulnerabilities in numerous ways. For example:

- Installing malicious firmware on a device to establish a stronghold for more attacks
- Remotely altering the power supply to sensitive medical assets connected to the device
- Bridging the cyber and physical realm by causing devices to go up in smoke and cause physical damages
- Initiating a ransomware attack, threatening to take control of the backup power supply to a data center supporting critical ICU applications, for example.[10]

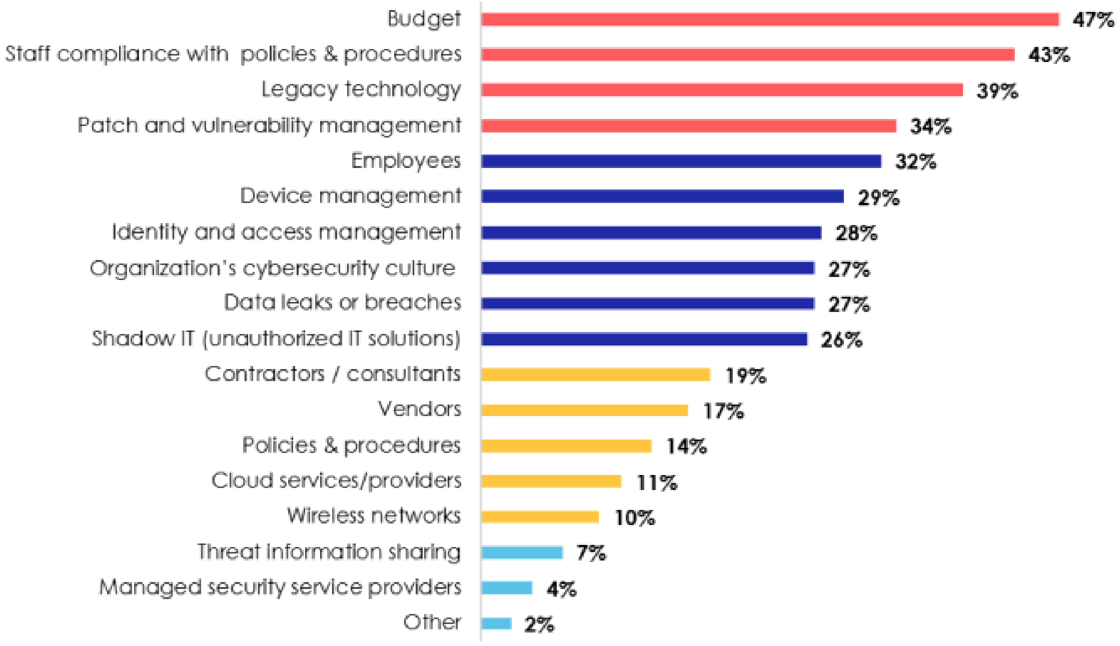
Log4j vulnerabilities

In January 2022, the U.S Department of Health and Human Services (HHS) Cybersecurity Program warned health organizations about Log4j vulnerabilities, noting that “health sector adversaries are actively leveraging these vulnerabilities” and that “vulnerabilities in ubiquitous apps will present similar issues in the future.”[11]

URGENT/11

In recent years, the Armis announcement of URGENT/11 illustrates the potential unknowns and patching challenges associated with any given vulnerability. For example, in 2019 Armis demonstrated how URGENT/11 vulnerabilities allow the takeover of a patient monitor, potentially changing the readings on the device without notice. Not long after the initial announcement, Armis, the FDA, and DHS jointly announced additional medical devices at risk due to URGENT/11.[12] By early 2022, researchers at a third-party organization demonstrated that the majority–75 percent–of 200,000 analyzed infusion pumps still included a host of security gaps, including URGENT/11.[13] The actual number of devices in the marketplace still at risk from URGENT/11 vulnerabilities could range from hundreds of thousands to millions.

Couple the potential security holes in unmanaged assets with the fact that patch and vulnerability management and device management are among healthcare security teams biggest challenges, and it’s easy to understand attackers’ motivations



The biggest security challenges facing organizations, according to the 2021 HIMSS Cybersecurity Survey Report.[14]

The new healthcare cyberattack

A typical healthcare provider will have a variety of traditional IT security tools, such as firewall, intrusion detection, endpoint security, and encryption controls as mandated by HIPAA. The organization also typically includes a variety of healthcare equipment such as:

- Blood gas analyzers
- Diagnostic equipment (for example, PET scanners, CT scanners, MRI machines)
- Therapeutic equipment (for example, infusion pumps, medical lasers, and LASIK surgical machines)
- Life support equipment (for example, heart-lung machines, medical ventilators, extracorporeal membrane oxygenation machines, and dialysis machines)
- PACS and imaging systems

For entrance into the healthcare facility network, cyber attackers usually prefer the easiest route which is either a phishing attack, or a device that is exposed directly to the Internet. In both cases, legacy and unpatched devices have security flaws that attackers can exploit for drive-by downloads and ransomware execution. And once they've compromised an asset, cyber attackers can quickly and easily move laterally through traditionally flat hospital networks and infect many other devices, including medical devices, and entire care systems

The Shodan search engine might reveal security cameras, HVAC systems, or other such devices that can be attacked. Attackers even plant rogue devices to compromise networks, such as introducing a WiFi pineapple into the lobby or nearby parking lot. Armis frequently finds pineapples in enterprise and healthcare environments even if the organization has invested heavily in security tools and personnel. Finally, there are various remote attacks that can be used to bypass or compromise the firewall, such as CDPwn, URGENT/11, or DNS rebinding.

Just take the URGENT/11 vulnerabilities announced by Armis. Companies such as GE Healthcare, Philips, Drager, Spacelabs, and BD issued advisories that their products were impacted by URGENT/11. There were 11 vulnerabilities, including six that could allow an attacker to take over a medical or other device. Armis demonstrated how an attacker could take over a patient monitor.[15]

ACCESS POINT
ULTRASOUND
WORK STATION
TABLET
COMPROMISED DEVICE
BP MONITOR
HEART MONITOR

Targeting hospital devices

Attackers have moved from health care systems to health care devices. There are documented cases of MRIs and CT scanners impacted by malware. Potential consequences include:

- Locked and inoperative systems
- Systems operating incorrectly
- Disruption of scan signals
- Altered results
- Altered radiation exposure

SYRINGE PUMP
ULTRASOUND
PATIENT MONITOR
COMPROMISED DEVICE
TABLET
PATIENT MONITOR
INFUSION PUMP
COMPROMISED DEVICE
MEDICAL LAPTOP

A medical device exposure

After the initial announcement of URGENT/11 vulnerabilities impacting Wind River VxWorks, hospitals using Armis identified additional medical devices with the impacted IPnet vulnerability. Armis confirmed six additional real-time operating systems were impacted (OSE by ENEA, Integrity by Green Hills, ThreadX by Microsoft, Nucleus RTOS by Mentor, ITRON by TRON Forum, and ZebOS by IP Infusion). Armis worked with the FDA, DHS, and an impacted device manufacturer, BD Alaris, to address the vulnerabilities and issue advisories. The vulnerabilities included the ability to gain entry via firewalls and simple devices like printers, as well as medical devices. The DHS recommended that hospitals minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.[16] They also recommended locating control system networks and remote devices behind firewalls, and isolating them from the business network.

The Armis solution

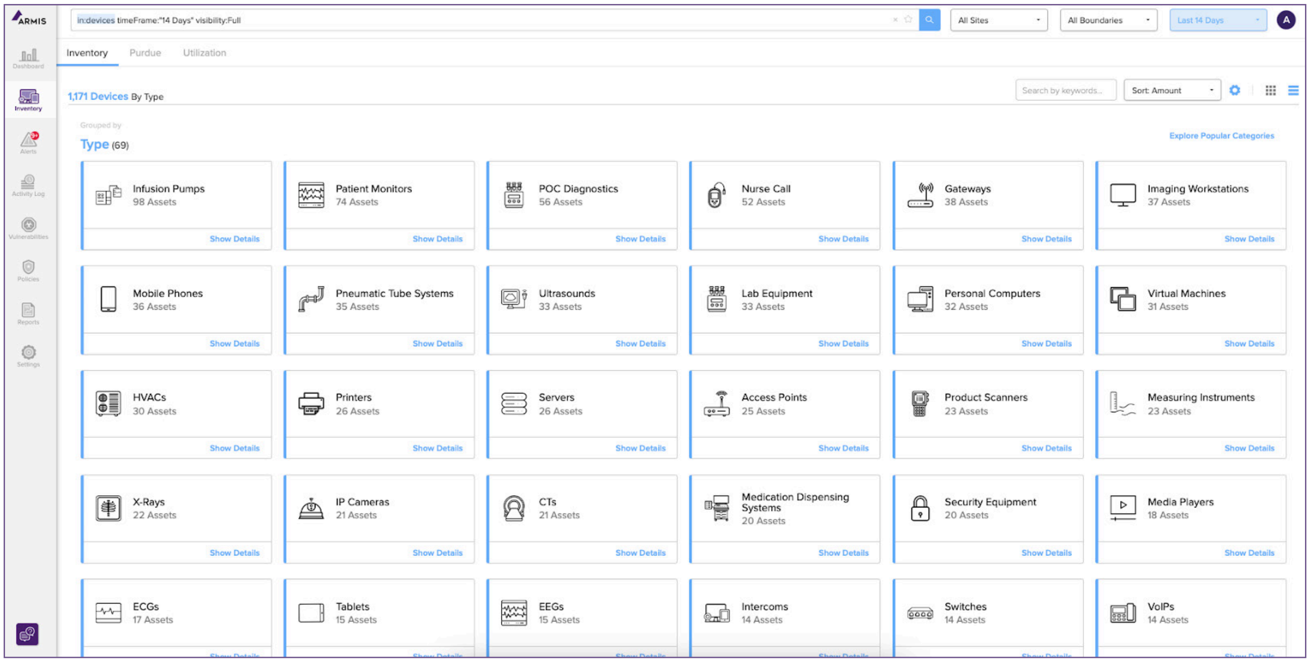
Armis is purpose built to address the need for medical and IoT device security by today's healthcare delivery organizations. Armis is an enterprise-class agentless and passive device security platform that provides three essential capabilities:

Armis is agentless and passive—critical for medical devices that can't take an agent or that you cannot scan.

Discover

Armis allows you to see all managed and unmanaged devices in your environment by type, both on your network and in your airspace. This is critical because we find that most healthcare providers are unaware of approximately 40 percent of the devices in their environment. The Armis platform operates in a completely agentless and passive manner, running without the need for software installation on devices or intrusive scanning. Armis provides visibility in near real-time, dynamically updating the inventory as new devices come online or changes are detected, ensuring teams have the most up-to-date view of their environment.

Through a simple out-of-band connection to your network, the Armis platform profiles and classifies devices, users, connections, applications, and operating systems throughout your environment. Armis shows you existing devices and the connections, including connections to unmanaged devices or rogue networks that you might not be aware of. This out-of-band connection also ensures no interruption or latency is introduced to the production network, making it a completely seamless deployment.



in:devices timeFrame:"14 Days" visibility:Full

All Sites | All Boundaries | Last 14 Days

Sort: Amount

1,171 Devices By Type

Grouped by

Type (69)

Infusion Pumps 98 Assets	Patient Monitors 74 Assets	POC Diagnostics 56 Assets	Nurse Call 52 Assets	Gateways 38 Assets	Imaging Workstations 37 Assets
Mobile Phones 36 Assets	Pneumatic Tube Systems 35 Assets	Ultrasounds 33 Assets	Lab Equipment 33 Assets	Personal Computers 32 Assets	Virtual Machines 31 Assets
HVACs 30 Assets	Printers 26 Assets	Servers 26 Assets	Access Points 25 Assets	Product Scanners 23 Assets	Measuring Instruments 23 Assets
X-Rays 22 Assets	IP Cameras 21 Assets	CTs 21 Assets	Medication Dispensing Systems 20 Assets	Security Equipment 20 Assets	Media Players 18 Assets
ECGs 17 Assets	Tablets 15 Assets	EEGs 15 Assets	Intercoms 14 Assets	Switches 14 Assets	VoIPs 14 Assets

Example of the asset inventory by type dashboard on the Armis platform.

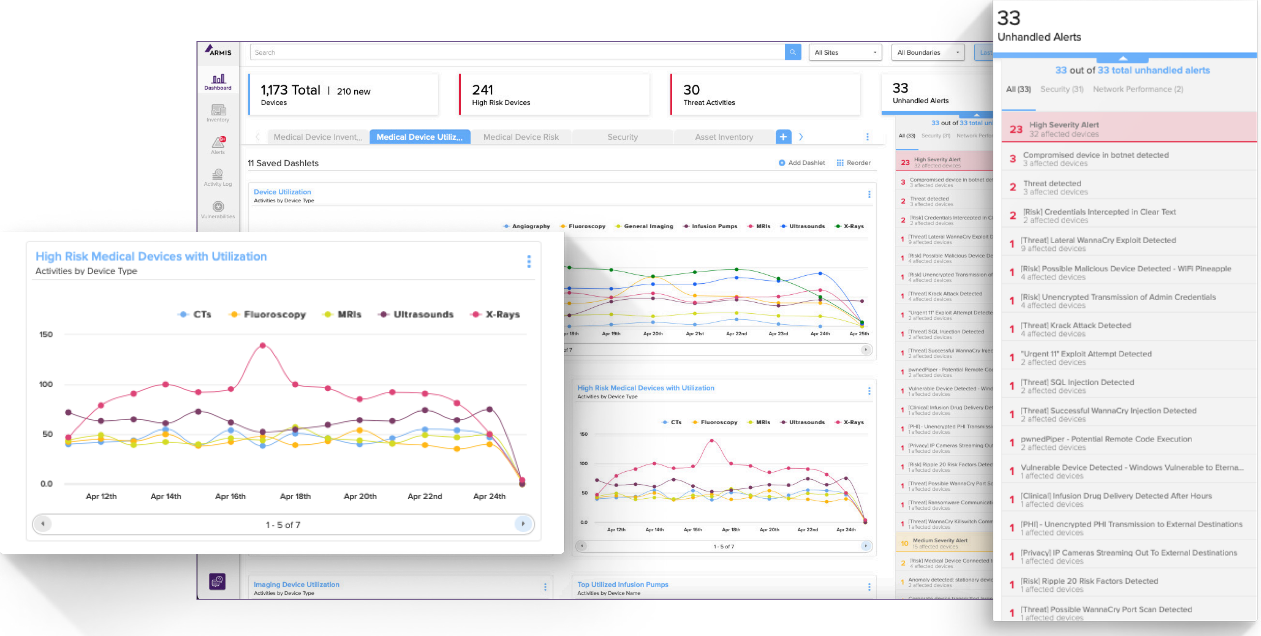
The Armis platform utilizes our proprietary Armis Intelligence Engine—a crowd-sourced, cloud-based knowledgebase tracking over 2 billion devices with 20 million device profile characteristics. This lets Armis accurately classify every device in your environment, including managed and unmanaged endpoints as well as non-traditional devices found in healthcare environments, such as laboratory instruments, heart monitors, infusion pumps, X-Ray systems and clinicians' handheld devices.

Healthcare providers are unaware of approximately 40 percent of the devices in their environment.

The comprehensive device inventory generated by Armis includes critical information like device manufacturer, model, serial number, physical location, username, operating system, installed applications, and connections made over time. Armis also detects medical device specific properties including FDA recalls, MDS^2 files and properties and utilization metrics.

Armis even detects medical device specific risk, such as the transmission of unencrypted Patient Health Information (PHI), MDS^2 files and properties and utilization metrics.

This risk score helps your security team understand your attack surface and meet compliance with regulatory frameworks (for example, the NIST framework) that require identification and prioritization of vulnerabilities.



1,173 Total | 210 new Devices

241 High Risk Devices

30 Threat Activities

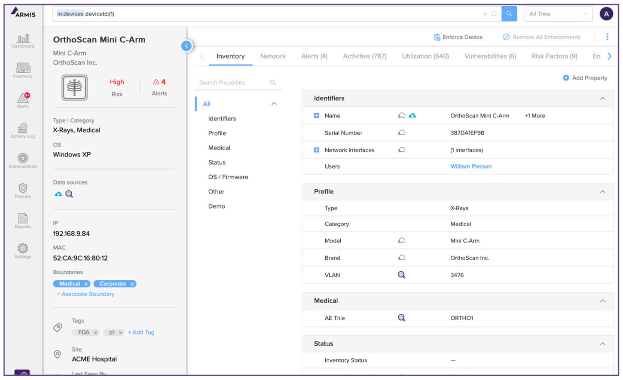
33 Unhandled Alerts

11 Saved Dashlets

33 out of 33 total unhandled alerts

All (33) Security (31) Network Performance (2)

- 23 High Severity Alert — 32 affected devices
- 3 Compromised device in botnet detected — 3 affected devices
- 2 Threat detected — 3 affected devices
- 2 [Risk] Credentials Intercepted in Clear Text — 2 affected devices
- 1 [Threat] Lateral WannaCry Exploit Detected — 9 affected devices
- 1 [Risk] Possible Malicious Device Detected - WiFi Pineapple — 4 affected devices
- 1 [Risk] Unencrypted Transmission of Admin Credentials — 4 affected devices
- 1 [Threat] Krack Attack Detected — 4 affected devices
- 1 "Urgent 11" Exploit Attempt Detected — 2 affected devices
- 1 [Threat] SQL Injection Detected — 2 affected devices
- 1 [Threat] Successful WannaCry Injection Detected — 2 affected devices
- 1 pwnedPiper - Potential Remote Code Execution — 2 affected devices
- 1 Vulnerable Device Detected - Windows Vulnerable to Eterna... — 1 affected devices
- 1 [Clinical] Infusion Drug Delivery Detected After Hours — 1 affected devices
- 1 [PHI] - Unencrypted PHI Transmission to External Destinations — 1 affected devices
- 1 [Privacy] IP Cameras Streaming Out To External Destinations — 1 affected devices
- 1 [Risk] Ripple 20 Risk Factors Detected — 1 affected devices
- 1 [Threat] Possible WannaCry Port Scan Detected — 1 affected devices



in:devices deviceId:(1)

OrthoScan Mini C-Arm
Mini C-Arm
OrthoScan Inc.

High Risk | 4 Alerts

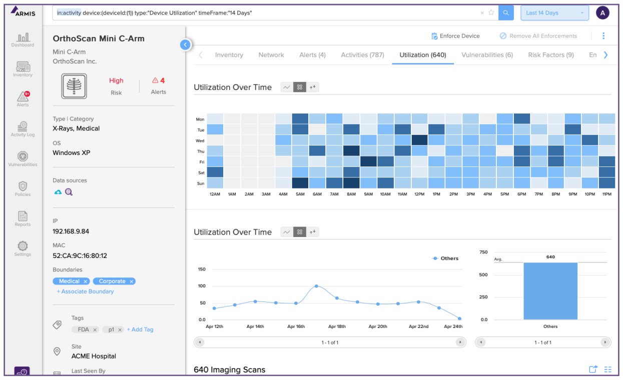
Type | Category: X-Rays, Medical
OS: Windows XP
Data sources
IP: 192.168.9.84
MAC: 52:CA:9C:16:80:12
Boundaries: Medical, Corporate
Tags: FDA, p1
Site: ACME Hospital
Last Seen By

Identifiers	
Name	OrthoScan Mini C-Arm +1 More
Serial Number	387DA1EF9B
Network Interfaces	(1 interfaces)
Users	William Pierson

Profile	
Type	X-Rays
Category	Medical
Model	Mini C-Arm
Brand	OrthoScan Inc.
VLAN	3476

Medical	
AE Title	ORTHO1

Status	
Inventory Status	—



in:activity device:(deviceId:(1)) type:"Device Utilization" timeFrame:"14 Days"

OrthoScan Mini C-Arm
Mini C-Arm
OrthoScan Inc.

High Risk | 4 Alerts

Type | Category: X-Rays, Medical
OS: Windows XP
Data sources
IP: 192.168.9.84
MAC: 52:CA:9C:16:80:12
Boundaries: Medical, Corporate
Tags: FDA, p1
Site: ACME Hospital
Last Seen By

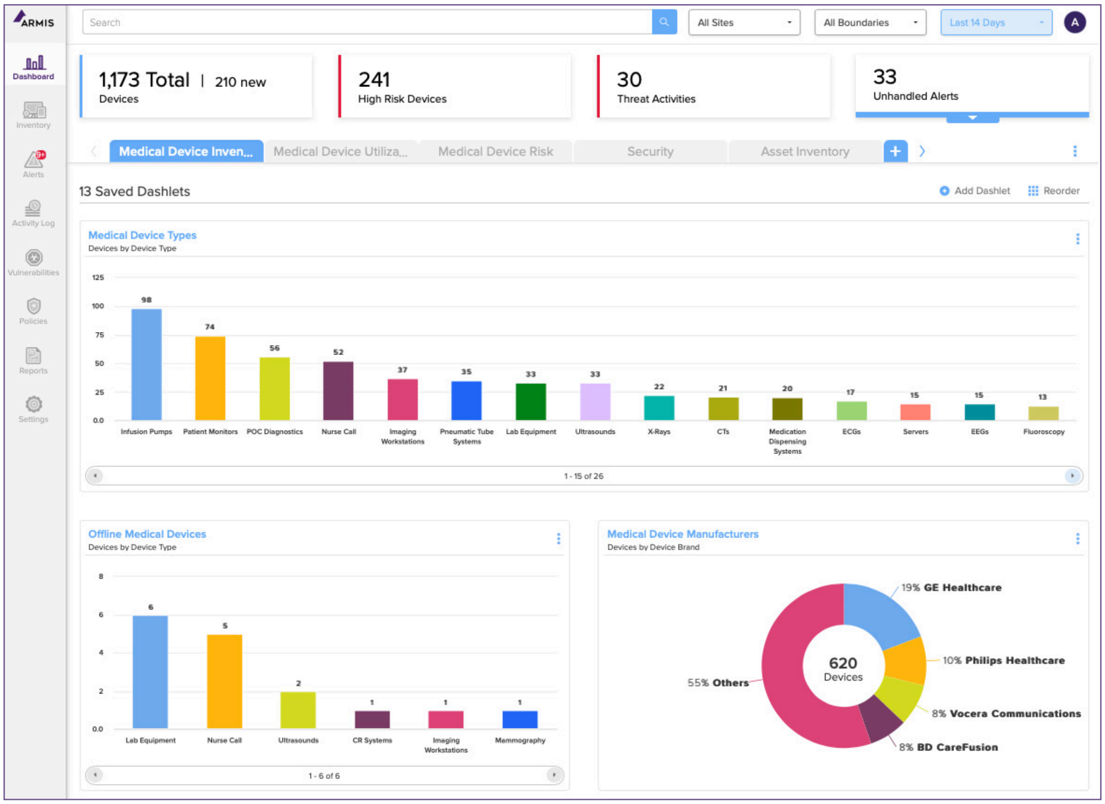
640 Imaging Scans

The Armis platform shows you everything from the big picture of assets in your environment down to granular device views.

Analyze

In addition to discovering and classifying a device, Armis calculates a risk score for every device based on factors like vulnerabilities, known attack patterns, and the behaviors associated with each device. Armis even factors in the clinical risk of devices, such as the presence or transmission of PHI, or the presence of active FDA recalls. This helps teams put risks into context, allowing them to quickly identify, assess, and remediate high-risk devices in a prioritized manner.

Like an agentless endpoint detection and response (EDR) tool for unmanaged and medical devices, Armis also continuously monitors the network for indicators of attack. When a device operates outside of its “known-good” profile, Armis issues an alert or triggers automated actions based on the policies you set for each device type. Everything from a misconfiguration to a policy violation to abnormal behavior, such as inappropriate connection requests or unusual software running on a device, can trigger an alert.



1,173 Total | 210 new
Devices

241
High Risk Devices

30
Threat Activities

33
Unhandled Alerts

13 Saved Dashlets

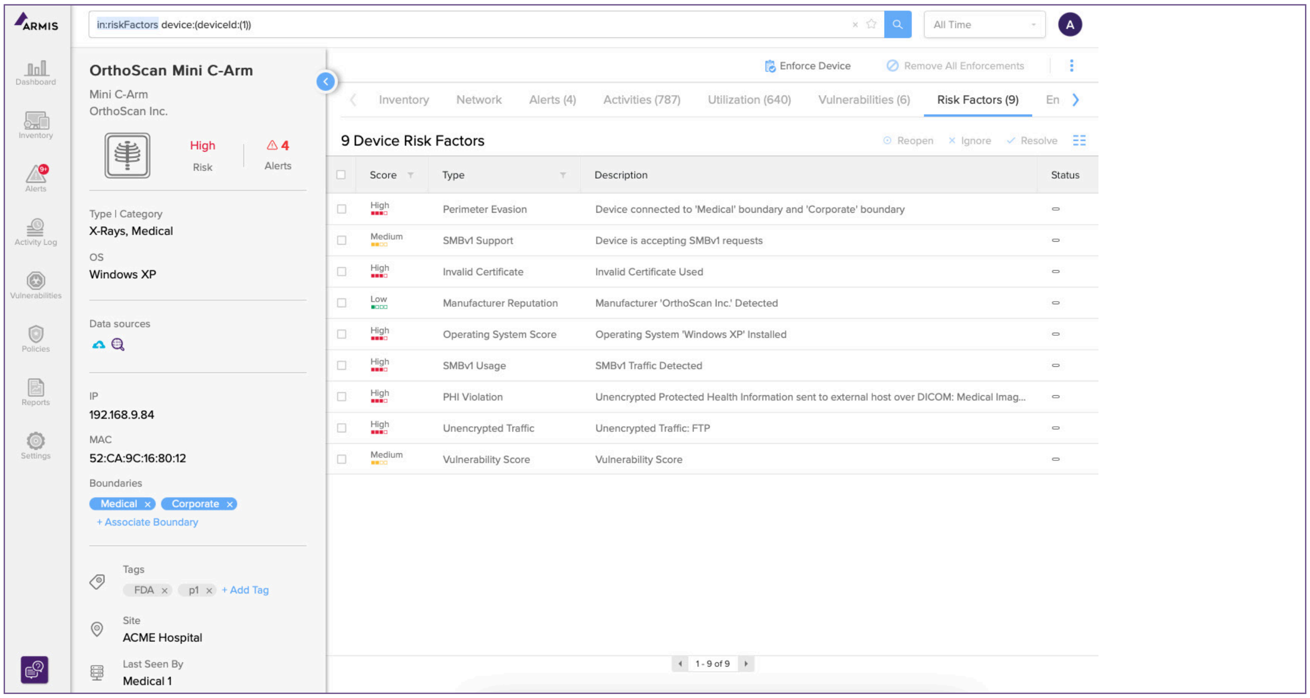
The Armis Risk Analysis Engine discovers a wide range of hidden threats on your network.

- Behavior – Compares real-time device activity to established known-good baselines that are stored in the Armis Intelligence Engine. These are based on the historical behavior of the device, behavior of similar devices in your environment, and the behavior of similar devices in other environments.
- Clinical risk – Calculates clinical risk into the assessment of devices, facilitating enriched prioritization and strategic remediation.
- Configuration – Compares the configuration of each device to other devices within your environment, looking for anomalies.
- Threat intelligence – Utilizes premium threat intelligence to inform the Threat Detection Engine of real world attack activity and patterns. The Threat Intelligence Engine then correlates observed activity in your network with the latest threat intelligence, factoring in vulnerabilities and other risk factors to detect actual attacks with higher confidence.

Armis displays alerts corresponding to the risks and threats that are detected on and around your network. Each alert includes drill-down capability so you can see the basis for it; Armis analyzes more than 20 different characteristics and behaviors to score each device.

If you have a SIEM solution, you can use all the data gathered by the Armis platform, along with analyses of risks and attacks, in your SIEM workflows. Typically, organizations rely on the Armis platform as the primary source of information for IoT and unmanaged devices as well as a discovery and analytics engine.

The Armis platform maintains a complete history of devices in your environment including their connections and behaviors. This is useful for forensics following an observed attack.



in:riskFactors device:(deviceId:(1))

OrthoScan Mini C-Arm

Mini C-Arm
OrthoScan Inc.

High Risk | 4 Alerts

Type | Category
X-Rays, Medical

OS
Windows XP

Data sources

IP
192.168.9.84

MAC
52:CA:9C:16:80:12

Boundaries
Medical × Corporate ×
+ Associate Boundary

Tags
FDA × p1 × + Add Tag

Site
ACME Hospital

Last Seen By
Medical 1

9 Device Risk Factors

□	Score	Type	Description	Status
□	High	Perimeter Evasion	Device connected to 'Medical' boundary and 'Corporate' boundary	⊖
□	Medium	SMBv1 Support	Device is accepting SMBv1 requests	⊖
□	High	Invalid Certificate	Invalid Certificate Used	⊖
□	Low	Manufacturer Reputation	Manufacturer 'OrthoScan Inc.' Detected	⊖
□	High	Operating System Score	Operating System 'Windows XP' Installed	⊖
□	High	SMBv1 Usage	SMBv1 Traffic Detected	⊖
□	High	PHI Violation	Unencrypted Protected Health Information sent to external host over DICOM: Medical Imag...	⊖
□	High	Unencrypted Traffic	Unencrypted Traffic: FTP	⊖
□	Medium	Vulnerability Score	Vulnerability Score	⊖

Drill down capabilities enable you to quickly understand the specifics of device vulnerabilities.

Protect

Once the Armis Threat Detection Engine identifies malicious behavior on your network, or when the Armis platform detects a security policy violation, you can respond manually or rely on automatic responses. For example, although the Armis platform operates out of band, it can coordinate with existing network infrastructure, such as a switch, wireless LAN controller, firewall, or other network access control system, to enforce an action. The Armis platform also monitors for and automatically takes preventive and corrective actions in response to zero-day vulnerabilities, threats, and exploits such as Log4j.

Armis lets you see all the devices in your entire healthcare device ecosystem—medical, managed, unmanaged, and IoT. One solution for complete visibility and control.

In addition to triggering protection policies based on malicious behaviors, the Armis platform can also apply them proactively based on clinical risk or medical device properties. For example, proactively enforcing medical device segmentation policies to reduce the attack surface from the onset of the device joining the network. Or, with respect to clinical activities, terminating external network communications when the platform detects unencrypted PHI destined for unsanctioned external networks.

In addition, your threat research team can also rely on the Armis platform for help investigating the security incident. Like a traditional EDR solution, Armis continuously records information about the state and connections made by each device–managed or unmanaged–across your network so that when a security incident occurs, your security team can scroll back in time to see:

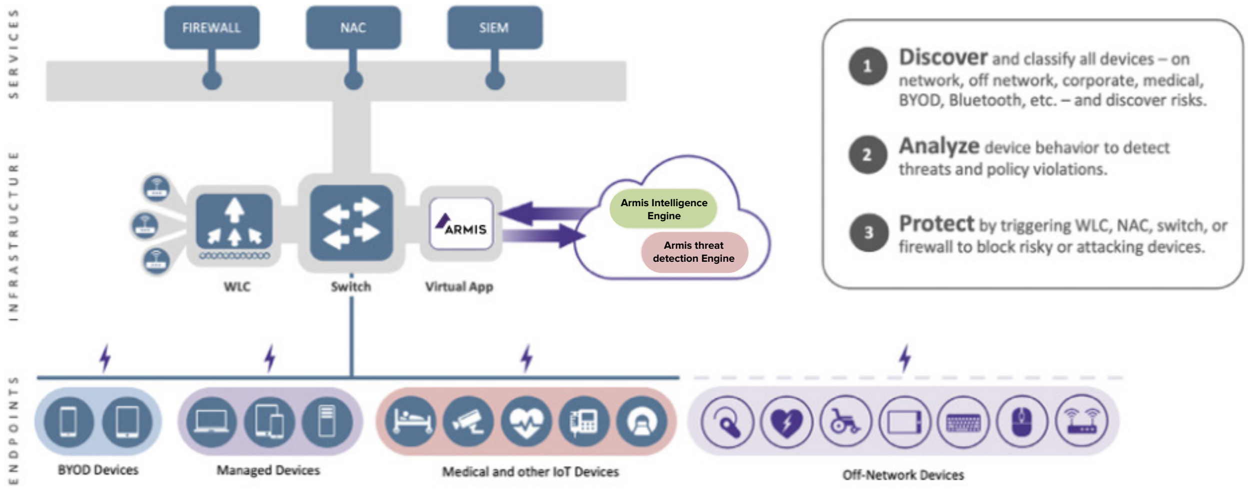
- The scope of the breach
- What communications occurred and over what protocols
- The amount of data transmitted
- Recent OS or application updates
- Abnormal traffic patterns
- Whether device locations have changed

For deeper analytics and threat mitigation, the Armis platform integrates with existing security solutions, such as Palo Alto Networks, to deliver a context-enriched, multi-data feed that provides a 360-degree view across an organization. These insights enable existing solutions to apply policies and mitigation against threats in a proactive manner to reduce the attack surface of the organization. The Armis platform integrates with a host of SIEMs, including Splunk.

Frictionless installation

Most medical devices and other kinds of IoT devices can't support an agent. For this reason, the Armis platform has been designed to deliver all its capabilities without the need for an agent. The Armis solution is 100 percent passive and non-disruptive, with no remote scanning or other kinds of invasive access to endpoints. In addition, the platform does not increase latency or impact the production network in any way. In healthcare environments, this is critically important to the safe operation of biomedical devices.

Armis runs on your network as a virtual appliance, passively collecting information. It requires a simple user account on your existing wireless LAN controller. You also have the option to connect it to your wired network via a SPAN port and to your existing firewalls. Complete installation typically takes only minutes to a few hours, depending on the environment.



1 **Discover** and classify all devices – on network, off network, corporate, medical, BYOD, Bluetooth, etc. – and discover risks.

2 **Analyze** device behavior to detect threats and policy violations.

3 **Protect** by triggering WLC, NAC, switch, or firewall to block risky or attacking devices.

The Armis platform is easy to install and integrate with your existing security and management tools.

Taking the next step

From the advent of the PC to the Internet to mobile devices to the cloud to IoT, history is a clear guide for the security risks associated with technological advances. And given that medical devices are built without security in mind, the risks to the patient journey are especially real and pressing. Today, hackers are targeting healthcare organizations more than any other industry.

New devices undeniably bring greater promise and innovation in the delivery of healthcare and the well-being of patients. But the security and clinical risks associated with managed and unmanaged devices are also all too real, so monitoring and securing them is key to ensuring the availability of patient care and minimizing risks to patient safety. The Armis platform underpins complete asset visibility and security. Your organization can install it within a couple of hours and have a complete inventory of devices in a week or less along with contextualized risk assessments of the entire environment and capabilities for automatically managing and reducing risk.

Without complete asset visibility there is no security, so now is the time to add IoT and medical device security to your comprehensive cyber-security strategy.

Medical devices that the Armis platform can discover, classify, and display within its console

3M

AAEON Technology

Abbott Diagnostics

Abbott Optics

Abbott Point of Care

ACIST Medical Systems

Acteon Group

Advanced Sterilization Products

Advanced Medical Information

Advantage Pharmacy

Aeroscout

Alaris

Alaris Medical Systems

Alcon Laboratories

Alpinion Medical Systems

AmbiCom

American Telecare

Andon Health

Applied Biosystems

Applied Medical Technologies

Arkray

Avizia

Axis Shield

B Braun Melsungen

Bang Olufsen Medicom

Baxter Healthcare

Beacon Medical

Beckman Coulter

Becton Dickinson

BestCare Cloucal

Bio logic Systems

Bio Rad Lab

Biodevices

bioMerieux Italia

Bionet

BIOPAC Systems

BioSoundLab

Biospace

Biotage

BIOTRONIK

BK Medical

BL Healthcare

BMT Medical Technology

Boston Scientific

BriteMED

C8 MediSensors

Calypso Medical

Camtronics Medical Systems

Canon

CardioMEMS

CardioNet

Cardiopulmonary Corp

CardioTek

Care Everywhere

CareCom

CareFusion

CareFusion Alaris Pump

CarePredict

Carestream Health

CareTech

CareView Communications

Celectronic eHealth

Centrak

Cerner

CHG Hospital Beds

Cirtec Medical

Cirtec Medical Systems

CliniComp

Cogent Healthcare Systems

Colorado Med Tech

Compex

Compumedics

Conmed Linvatec

Convergent Bioscience

Corometrics Medical Systems

Criticare Systems

Cutera

Dainippon Pharma

Danaher Motion Kollmorgen

Datex Ohmeda

DENTSPLY Gendex

Diatek Patient Management

Dictum Health

Dixtal Biomedica

Draeger

Draeger Delta

Draeger M300

Dragerwerk

Durr Dental

Edwards Lifesciences

Ellex Medical

Essilor

Fisher Paykel

Fluke Biomedical

Fresenius Medical Care

Fuji

Fukuda Denshi

Gambro Lundia

GE Healthcare

GE Medical

GE Medical System

GEM Med

Getinge
Getinge IT Solutions
Getinge Sterilization
GN ReSound
Haag Streit
Health Advice Monitors
Health Hero
Health Life
HealthStream
Heart Force Medical
HemoCue
Heraeus Noblelight
Hitachi Aloka Medical
Hoana Medical
Hologic, Inc.
Honeywell
Honeywell HomMed
HORIBA Medical
Hospira
Huntleigh Healthcare
Imatron
Imricor Medical Systems
Indiana Life Sciences
InnerSpace
Innomed Medical
INSidE Technology
Integra Biosciences
Integra LifeSciences
Integrated Medical Systems
Intel GE Care Innovations
Interacoustics
Intuitive Surgical
Invivo
Ivoclar Vivadent
Ivy Biomedical
Johnson & Johnson Medical
Jostra

Karl Storz Imaging
KaVo Dental
KeyMed
Kodak Radiology
Kollmorgen
Kollmorgen Corp
Kollmorgen Servotronix
Kontron Medical
LABiTec
Laerdal Medical
Leica Biosystems
Leica Microsystems
LI COR Biosciences
LifeSync
LRE Medical
Maquet
Maquet Cardiopulmonary
Maquet CardioVascular
Maquet Critical Care
Maquet GmbH
Marconi Medical Systems
Masimo
Medav
MedAvant Healthcare
Mediana
Medicis
Medicore
Medison X Ray
Medrad
Medtronic Diabetes
Mennen Medical
Micropoint Biotechnologies
Mindray
MIR
MOCACARE
Mortara Instrument
NDS Surgical Imaging

Neural Image
Nicolet Instruments
Nicolet Neuro
Nihon Kohden
Nipro Diagnostics
Nonin Medical
Nova Biomedical
Novo Nordisk
Olympus
Olympus Image Systems
Omnicell
Omron Healthcare
Onyx Healthcare
Optimedical Systems
OrthoScan
ORTHOsoft Zimmer CAS
Ortivus AB Medical
Oticon
Pacific Biosciences
PaloDEx
Palomar
Panasonic Healthcare
Pharma Smart
Philips Analytical X Ray
Philips Careservant
Philips Healthcare PCCI
Philips Medical
Philips Oral Healthcare
Philips Patient Monitoring
Philips Respironics
Phonak Communications
Physio Control
Physiometrix
Planmeca Oy
Pointe Conception Medical
Power Medical Interventions
Progeny Midmark

Proteus Digital Health

Quantum Medical Imaging

Radiometer Medical

ResMed

Resurgent Health Medical

RF Surgical System

Robert Bosch

Roche Diagnostics

ScottCare

Secure Care

SenTec

Senticare

Shenzhen Lifesense Medical

Shimadzu

SHL Telemedicine

Siemens

Siemens Acuson Ultrasound

Siemens AG Healthcare Sector

Siemens Healthcare Diagnostics

Sigma

Sirona Dental Systems

Smiths Medical

SonoSite

Sonosite MicroMaxx Ultrasound

Soredex

Spacelabs Healthcare

Spectrum Medical Limited

Sphere Medical

St Jude Medical

Starkey Labs

Stratec Biomedical

Stryker

Sunol Molecular

Tecan Systems

Terumo

Thermo Fisher Scientific

Thoratec

Tiba Medical

Tokyo Boeki Medisys

Toyo Medic

tPlus Medical

Trendsetter Medical

Tunstall Healthcare

Valtronic

Varian Medical Systems

Versamed

Verto Medical

VIASYS Healthcare

Vigil Health Solutions

VitalCare

Vocera

Welch Allyn

West Com Nurse Call

Widex

Zimmer Elektromedizin

Zoe Medical

ZOLL Lifecor

Sources

1. "State Of Enterprise IoT Security: A Spotlight On Healthcare", Forrester Consulting, September 2019.
2. Ibid.
3. "Largest Healthcare Data Breaches of 2021", HIPPA Journal, December 2021.
4. Ibid.
5. 2021 Cost of a Data Breach Report, Ponemon Institute.
6. Ibid.
7. "Indiana hospital shuts down systems after ransomware attack", Cyberscoop, 2018.
8. "Ransomware attack on Georgia health system endangers info of 1.4M patients", Healthcare IT News, August 2021.
9. "2021 Internet Crime Report", Federal Bureau of Investigation.
10. "TLStorm: Three critical vulnerabilities discovered in APC Smart-UPS devices can allow attackers to remotely manipulate the power of millions of enterprise devices", Armis, 2022.
11. "Log4j Vulnerabilities and the Health Sector", HHS Cybersecurity Program, January 2022.
12. "URGENT/11: II Zero Day Vulnerabilities Impacting VxWorks, the Most Widely Used Real-Time Operating System (RTOS)", Armis, August 2019.
13. "Security Gaps in Smart Infusion Pumps Risk Patient Data", GovInfoSecurity, March 2022.
14. "2021 HIMSS Healthcare Cybersecurity Survey", HIMSS, January 2022.
15. "Takeover of a Spacelabs Xprezzon Patient Monitor Demo", Armis.
16. "ICS Medical Advisory (ICSMA-19-274-01) Interpeak IPnet TCP/IP Stack (Update B)", ICS-CERT, October 10, 2019.

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

20222804-1