ARMIS

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 commissioned study conducted by Forrester Consulting on behalf of Armis, 63% of healthcare delivery organizations have experienced a security incident related to unmanaged and IoT devices over the past two years.[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 cover 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 which 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 new security risks. There are three distinct security challenges:

1 **No Security**
The devices cannot accommodate a security agent, therefore they cannot be directly monitored or controlled by traditional IT security products or processes.

2 **New Connection Protocols**
The devices frequently communicate over wireless protocols including Wi-Fi, Bluetooth, Zigbee and other radio frequency protocols that are beyond the scope of traditional network security management tools.

3 **Vulnerable Operating Systems**
Many of the more sophisticated devices (for example, MRI scanners) are based on old, vulnerable operating systems including Windows 2000, Windows XP, and Windows 7. These devices function like black boxes, outside the reach of healthcare IT departments. There are no diagnostic cyber security tools that a hospital can use to identify malware on these devices, nor can these devices be patched using normal IT management systems. The manufacturer is responsible for patching, and they have a poor history of delivering those patches in a timely fashion. Other devices (for example, patient monitors and infusion pumps) typically use an embedded real-time operating systems such as VxWorks or OSE. Security fixes for these devices are even more complicated because updated firmware needs to be manually installed when a vulnerability needs to be fixed.

Medical devices like the ones described above, as well as other devices to run operations, are common in healthcare delivery organizations. According to the 2019 Forrester Consulting study, 64% of healthcare delivery organizations estimate that at least half of all devices on their network are unmanaged or IoT devices, including medical devices.[2]

HEALTHCARE IS A FREQUENT TARGET

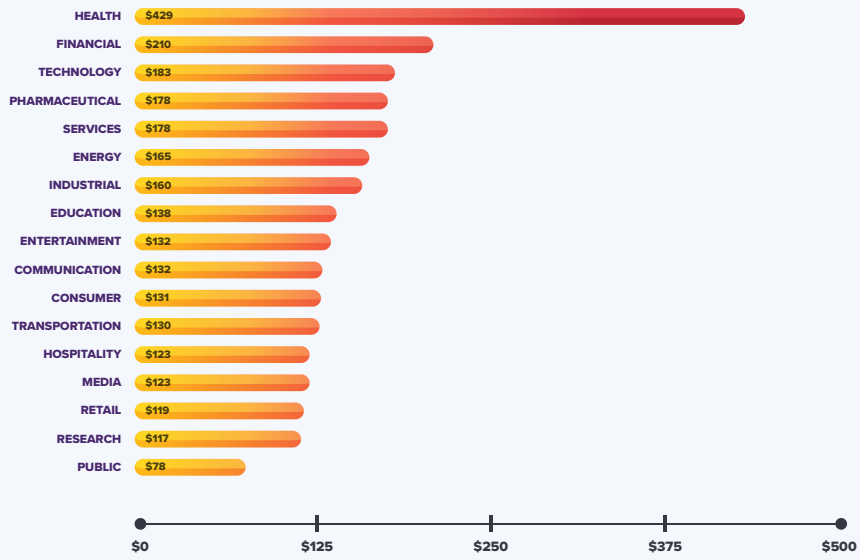
Statistics show that healthcare delivery organizations are hackers' new favorite targets. Why? Because medical records contain contain information that can be used for identity theft. As a result, the resale price for a healthcare record is approximately 50x times the resale price of a stolen credit card number.

Since hacking healthcare organizations is now so lucrative, the number of security breaches experienced by healthcare institutions has skyrocketed. In June 2017 it was reported that healthcare is the top-targeted vertical for cybercrime.[3] And the HIPAA Journal reported that 2018 was another record year for hackers, with 365 breaches of 500 or more records being reported.[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 a study conducted by Ponemon, the average cost to the healthcare organization per stolen record in 2018 was $429, almost double the cost of the next most sensitive target which is financial firms.[5] The average total cost of a data breach for healthcare providers was $6.45 million, Ponemon researchers found.

AVERAGE COST PER RECORD BY INDUSTRY SECTOR

Source: Ponemon 2019 Cost of a Data Breach Report



> By 2020, more than 25% of identified attacks in healthcare delivery organizations will involve the IoT.[6]
>
> – Gartner

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 – Remote ICU telemetry
- Tele-ology (teleneurology, teledermatology)

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

REAL-TIME LOCATION SERVICE (RTLS) DEVICES

- Asset tracking – Wheelchairs, infusion pumps, smart cabinets, medication carts, par-level management, rental management
- Employees – Physicians, nursing staff, ancillary staff
- Patients – Infant abduction and wandering systems
- Visitors – Wayfinding and digital signage

FACILITY MONITORING DEVICES

- Security – Video surveillance, door locks and entry systems, fire alarms
- Building management – Power monitoring, power distribution, energy consumption and management, elevators
- Environmental controls – HVAC, lighting, room control, water quality, humidity monitoring, tissue and blood refrigerators

FROM HACKING PATIENT DATA TO HACKING PATIENT CARE

Recently we have seen cyber attackers expand their focus. They are no longer content with extracting healthcare records and patient data. Now they are trying to gain control over medical devices and threaten the safety of patients.

> Unsecured medical devices are putting hospitals and patients at risk.[7]
>
> – Forrester Research

The first wave of such attacks took the form of ransomware which has literally shut down hospital operations until the ransom has been paid or until hospital systems could be restored from backup systems - each carrying a high cost. In January 2018, Cyberscoop reported an Indiana hospital had to shut down systems after a ransomware attack.[8] And another ransomware attack cost an Erie County Medical Center almost $10 million to get back online.[9]

But now attacks are moving to medical devices. Here is a list of recent attacks against medical devices and vulnerabilities discovered by the security community.

- In 2017, Forbes reported that an MRI contrast injector was shut down by a ransomware attack in the US.[10]
- In February 2018, Sophos reported how WannaCry malware impacted MRI and CT scanners which ran on Windows XP operating systems.[11]
- In April 2018, the FDA warned that hackers could exploit a cybersecurity vulnerability in implantable cardiac defibrillators made by Abbott Laboratories (formerly St. Jude Medical).[12]
- In March 2019, the Cybersecurity and Infrastructure Security Agency (CISA), a division of the U.S. Department of Homeland Security, issued a Medical Advisory bulletin advising that Medtronic cardiac defibrillators were vulnerable to a wireless attack, with a vulnerability score of 9.3, close to the top of the 10-point scale. The bulletin stated that an unauthorized individual with a "low skill level" could gain access to the equipment's setting and possibly change them.[13]
- In April 2019, security researchers showed how an attacker could tamper with DICOM medical images produced by MRI machines and CT scanners[14] Evidence of cancer could be either added or removed from the images, and the changes would be undetected.
- In July, 2019, CISA warned that an attacker with a low skill level could remotely modify GE Healthcare anesthesia machines.[15]
- In July 2019, Armis announced and demonstrated how URGENT/11 vulnerabilities allow the takeover of a patient monitor, potentially changing the readings on the device without notice. And, in October 2019, Armis, the FDA, and DHS jointly announced additional medical devices at risk due to URGENT/11.[16]

These risks were reflected in the 2018 HIMSS Cybersecurity Survey Final Report which showed that patient safety was the top concern of healthcare delivery organizations.[17]

Concern	Percent
Patient safety (e.g., patient harm or serious injury)	39.0%
Data breach	26.0%
Spread of malware to other devices on the same network	13.6%
Liability concerns	5.8%
Device loss or theft	4.5%
Intellectual property theft (e.g. clinical trials, research, etc.)	1.9%
Other	2.6%
Don't know	6.5%

THE NEW HEALTHCARE CYBER ATTACK

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

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

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:

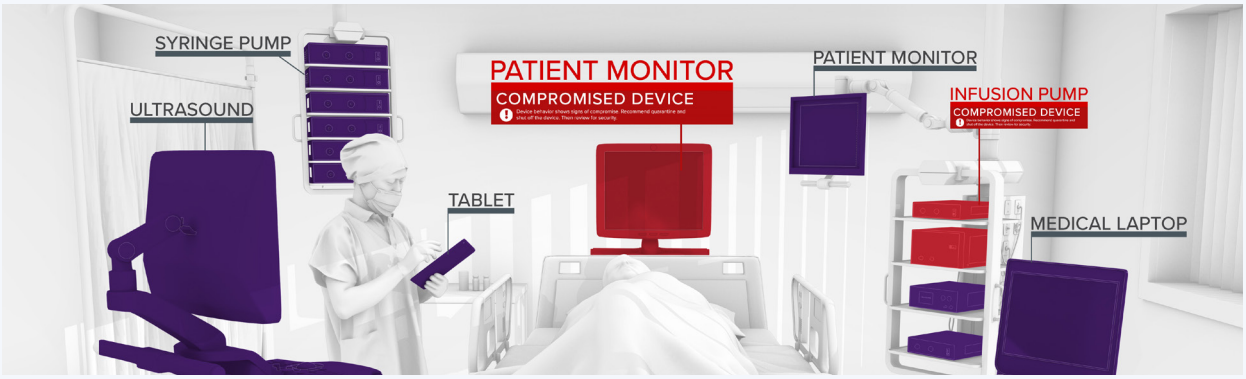
- Systems locked and inoperative
- Systems operating incorrectly
- Disruption of scan signals
- Altering results
- Altering radiation exposure

For entrance into the healthcare facility network, cyber attackers usually prefer the easiest route which is a device that is exposed directly to the Internet. Use of the search engine Shodan might find security cameras, HVAC systems, or other such devices that can be attacked. If that fails, a more up-close approach may be pursued, such as introducing a WiFi or Bluetooth pineapple into the lobby or nearby parking lot. Armis frequently finds pineapples in enterprise environments even if the organization has invested heavily in security tools and personnel. Another easy way to penetrate the environment is to use an airborne attack such as BlueBorne or KRACK. Finally, there are various remote attacks that can be used to bypass or compromise the firewall, such as URGENT/11 or DNS rebinding.

An example would be 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 6 that could allow an attacker to take over a medical or other device. Armis demonstrated how an attacker could take over a patient monitor.[18]

A MEDICAL DEVICE EXPOSURE

After the initial announcement of URGENT/11 vulnerabilities impacting Wind River VxWorks in July 2019, hospitals using Armis identified additional medical devices with the impacted IPnet vulnerability. Armis confirmed 6 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) in October 2019. Armis worked with the FDA and DHs and an impacted device manufacturer, BD Alaris, to address the vulnerabilities and issue advisories. The vulnerabilities including the ability to exploit and 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.[19] They also recommended locating control system networks and remote devices behind firewalls, and isolate them from the business network. BD provided its own advisory as well.[20]



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 you cannot scan.

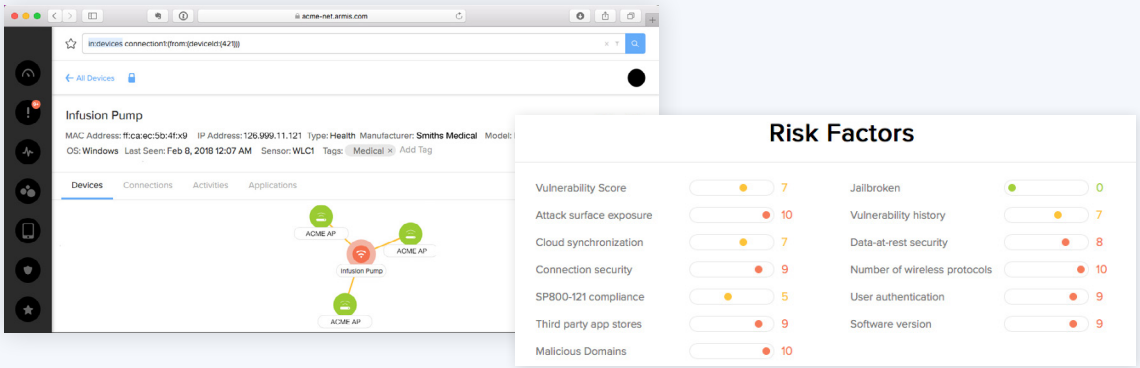
1 Discover

Armis allows you to see all devices in your environment, both on your network and in your airspace. This is critical because we find that most healthcare providers are unaware of approximately 40% of the devices in their environment. And they have zero visibility into airborne exploits such as BlueBorne, KRACK and Broadpwn to compromise devices over the air, without any interaction with the network.

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 the devices and the connections that exist, including connections to unmanaged devices or rogue networks that you might not be aware of.

The Armis platform utilizes our proprietary Device Knowledgebase – a crowd-sourced, cloud-based knowledgebase tracking over 110 millions devices with 10 million device profile characteristics. This lets Armis accurately classify every device in your environment–managed and unmanaged endpoints as well as non-traditional devices that are commonly found in healthcare environments such as laboratory instruments, heart monitors, infusion pumps, X-ray systems and clinicians' handheld devices.

The comprehensive device inventory that Armis generates includes critical information like device manufacturer, model, serial number, location, username, operating system, installed applications, FDA classification, and connections made over time.



The Armis platform discovers risky medical devices and malicious behavior on your network.

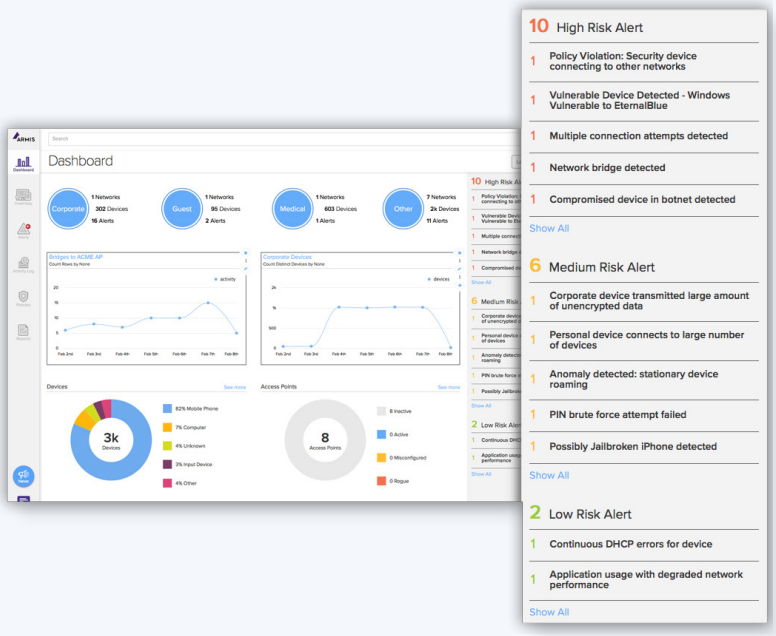
In addition to discovering and classifying a device, Armis calculates a risk score for every device based on factors like vulnerabilities, known attack patterns, and the behaviors associated with each device. This risk score helps your security team understand your attack surface and meet compliance with regulatory frameworks (e.g. the NIST framework) that require identification and prioritization of vulnerabilities.

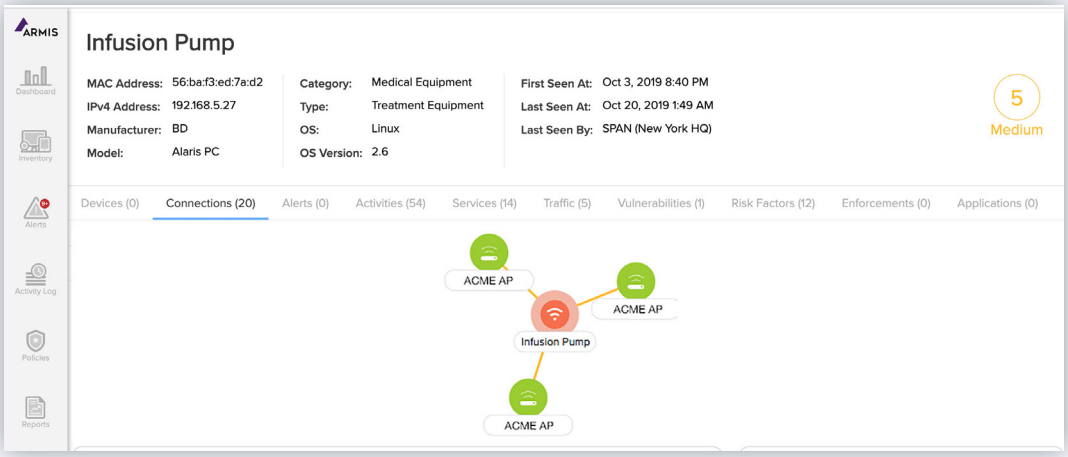
2 Analyze

Like an agentless Endpoint Protection and Response (EDR) system for unmanaged and medical devices, Armis continuously monitors the state and behavior of all devices on your network and in your airspace for indicators of attack. When a device operates outside of its known-good profile, Armis issues an alert or triggers automated actions. The alert can be caused by a misconfiguration, a policy violation, or abnormal behavior such as inappropriate connection requests or unusual software running on a device.

- **Behavior** - Compares real-time device activity to established, “known-good” baselines that are stored in the Armis Device Knowledgebase. 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.
- **Configuration** - Compares the configuration of each device to other devices within your environment, looking for anomalies.
- **Policies** - Lets you create policies for each device or type of device, and identifies violations.
- **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 this threat intelligence, as well as taking into account the presence of vulnerabilities and other risk factors, in order to detect actual attacks with higher confidence.

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





Armis device inventory contains a broad range of information.

Armis displays alerts corresponding to the risks and threats that we perceive on and around your network. Each alert includes drill-down capability so you can see the basis for each alert. Armis scores each device on the basis of more than 20 different characteristics and behaviors.

If you have a SIEM, you can utilize all of the data that we gather and all of the analyses that we make regarding risks and attacks. Typically, the Armis platform is the primary source of information for IoT devices and the sole source of information for devices that communicate through Bluetooth, BLE, WiMax, Zigbee, and other IoT protocols.

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

3 Protect

Once the Armis threat detection engine determines that there is malicious behavior on your network, or once Armis sees that one of your security policies has been violated, Armis allows you to take action either automatically or manually. One such action is to restrict access or quarantine the malicious device. Since Armis operates out-of-band, these actions are taken by your existing network infrastructure such as your switches, wireless LAN controller, firewalls, or whatever network access control system you might have in place. Armis is able to integrate with these systems and send triggers when needed.

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

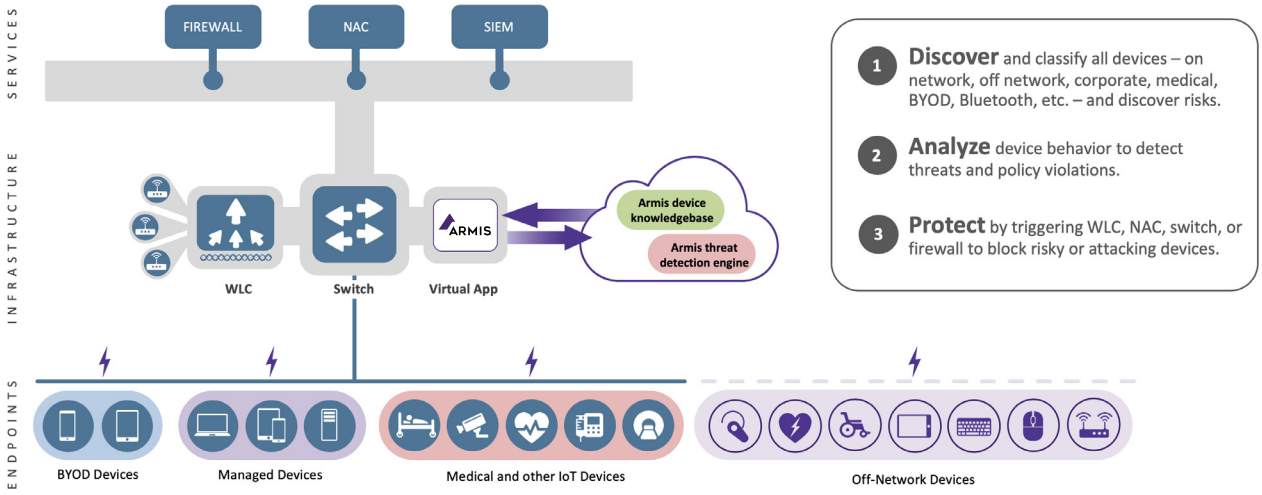
In addition, Armis helps your threat research team investigate the security incident. Like a traditional EDR solution, Armis continuously records information about the state and connections made by each device – managed or unmanaged – on your network so that when a security incident occurs, your security team can scroll back in time to see the scope of the breach—what communications occurred, over what protocols, how much data was transmitted, recent OS or application updates, abnormal traffic patterns, or even devices changing locations.

For deeper analytics and threat mitigation, Armis integrates with existing security solutions such as Palo Alto Networks and others to deliver a multi-data feed integration that provides a 360 degree view across an organization, and providing insight so those solutions can also apply policies and mitigation against a threat. Armis integrates with SIEMs such as Splunk and many others.

Frictionless Installation

Most medical devices and other kinds of IoT devices can't take an agent. For this reason, Armis has been designed to deliver all of these capabilities without any need for an agent. The Armis solution is 100% passive and non-disruptive. There is no remote scanning or other kinds of invasive access to endpoints. 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 and, optionally, connections to your wired network via a SPAN port and to your existing firewalls. Complete installation typically take only minutes to a few hours, depending on the environment.



PROVEN BUSINESS VALUE FOR HDOs

The Armis platform provides not just security but a wide range of business value for healthcare delivery organizations. The following is a partial list of business value.

- **Protect Patient Safety** — Alert security managers to cyber attacks and compromised medical, clinical, and other devices.
- **Completely Automated Device Inventory** — Reduce person-hours, and discover every connected device in your environment automatically.
- **Track Device Utilization** — Generate a complete, real-time inventory of all medical and other devices, find lost equipment, more efficiently utilize equipment, and ultimately reduce their over-investment in equipment.
- **See and Stop Ransomware Attacks** — Identify WannaCry and other ransomware in real time, thus reducing the risk of operational downtime and potentially catastrophic impact to the healthcare delivery organization's reputation.
- **Deliver Faster Threat Detection** — Identify other threats and reduce shorter dwell time, which limits the amount of time that a cyber attacker can accomplish his objective and, thus, reduces the organization's risk of experiencing devastating data breach.
- **Enables Faster Incident Response** — Address exploited medical devices faster, which reduces the amount of operational downtime associated with cyber attacks.

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. With every technological advance and device, there are new security risks. Those new security risks are real. Today, medical devices are not built with security in mind. Statistics show that hackers are targeting healthcare organizations more than any other industry.

As these devices bring greater promise in the delivery of healthcare and the well being of a patient, we must now pay special attention to ensure those devices do not inadvertently do harm to patient care.

Armis can be installed in just a couple of hours, and within a week you can have a complete inventory of devices along with risk scores and suggestions for remediation. Initial remediations are usually done manually, but as more confidence is gained, automated policies can be deployed that will be able to detect and stop attacks of all types, from ransomware to device tampering.

Now is the time for healthcare organizations to include IoT security as a part of their 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
Ellex Medical
Essilor
Fisher Paykel
Fluke Biomedical
Fresenius Medical Care
Fuji
Fukuda Denshi
Gambro Lundia
GE Healthcare
E 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
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

MEDICAL DEVICES THAT THE ARMIS PLATFORM CAN DISCOVER, CLASSIFY AND DISPLAY WITHIN ITS CONSOLE

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
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
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] Source: "State Of Enterprise IoT Security: A Spotlight On Healthcare", Forrester Consulting, September 2019. https://www.armis.com/resources/analyst-reports/forrester-state-of-enterprise-iot-security-a-spotlight-on-healthcare/

[2] Source: Ibid.

[3] Source: https://www.infosecurity-magazine.com/news/healthcare-the-toptargeted-vertical/

[4] Source: https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/

[5] Source: "2019 Cost of a Data Breach Report", conducted by the Ponemon Institute. https://www.ibm.com/security/data-breach?cm_sp=CTO-_-en-US-_-ZBZLY7KL

[6] Source: https://www.cio.com.au/article/613631/healthcare-cios-should-take-action-now-against-iot-security-risks-gartner/

[7] Source: "Best Practices: Medical Device Security", Forrester Consulting, May 21 2019

[8] Source: "Indiana hospital shuts down systems after ransomware attack", Cyberscoop, January 15, 2018. https://www.cyberscoop.com/hancock-hospital-ransomware/

[9] Source: "ECMC spent nearly $10 million recovering from massive cyberattack", The Buffalo News, July 26, 2017. https://buffalonews.com/2017/07/26/cost-ecmc-ransomware-incident-near-10-million/

[10] Source: "Medical Devices Hit By Ransomware For The First Time In US Hospitals", Forbes, May 17, 2017. https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#45e7782b425c

[11] Source: "Hospital MRI and CT scanners at risk of cyberattack", Sophos, Feb 1, 2018. https://nakedsecurity.sophos.com/2018/02/01/hospital-mri-and-ct-scanners-at-risk-of-cyberattack/

[12] Source: "Battery Performance Alert and Cybersecurity Firmware Updates for Certain Abbott (formerly St. Jude Medical) Implantable Cardiac Devices: FDA Safety Communication", US https://www.fda.gov/medical-devices/safety-communications/battery-performance-alert-and-cybersecurity-firmware-updates-certain-abbott-formerly-st-jude-medical

[13] Source: "Medical Device Vulnerable to Hackers", JD Supra, June 13, 2019. https://www.jdsupra.com/legalnews/medical-device-vulnerable-to-hackers-31159/

[14] Source: “CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning”, Yisroel Mirsky, Tom Mahler, Ilan Shelef, and Yuval Elovici. https://arxiv.org/pdf/1901.03597.pdf

[15] Source: “ICS Medical Advisory (ICSMA-19-190-01) GE Aestiva and Aespire Anesthesa”, US Dept. of Homeland Security ICS-CERT, July 24, 2019. https://www.us-cert.gov/ics/advisories/icsma-19-190-01

[16] Source: “URGENT/11: II Zero Day Vulnerabilities Impacting VxWorks, the Most Widely Used Real-Time Operating System (RTOS)”, Armis, August 2019 https://www.armis.com/urgent11/

[17] Source: “2018 HIMSS Cybersecurity Survey”, Healthcare Information and Management Systems Society (HIMSS), https://www.himss.org/2018-himss-cybersecurity-survey

[18] Source: “Takeover of a Spacelabs Xprezzon Patient Monitor Demo”, Armis. https://www.armis.com/urgent11/

[19] Source: “ICS Medical Advisory (ICSMA-19-274-01) Interpeak IPnet TCP/IP Stack (Update B)”, ICS-CERT, October 10, 2019. https://www.us-cert.gov/ics/advisories/icsma-19-274-01

[20] Source: “Interpeak IPNET TCP IP stack vulnerability”, BD, October 2, 2019. https://www.bd.com/en-us/support/product-security-and-privacy/product-security-bulletins/interpeak-ipnet-tcp-ip-stack-vulnerability

ABOUT ARMIS

Armis is the leading 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.

ARMIS™

1.888.452.4011 armis.com