MEDICAL DEVICE SECURITY

AN AGENTLESS, PASSIVE SOLUTION FOR HEALTHCARE DELIVERY ORGANIZATIONS

Connected medical devices help clinicians deliver faster, higher quality care, but they also create an attack surface that most healthcare delivery organizations (HDOs) aren't prepared to protect. These devices lack inherent security controls, they can't easily receive software updates, and they can't be seen or managed by traditional security products. All of this puts sensitive data, day-to-day facility operations, and patient health at risk.

THE ARMIS SECURITY PLATFORM

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged medical and IoT devices. The Armis platform discovers every device (managed, unmanaged, medical, etc.) on and off of your network and analyzes behavior to identify risks to protect critical patient information and systems from attacks. It's cloud-based, agentless, and integrates easily with your existing network and security products.

Armis passively monitors wired and wireless traffic on your network and in your airspace to identify every device and to understand their behaviors without disruption. The Armis Risk Engine then analyzes this data and uses device profiles and characteristics from the Armis Device Knowledgebase to identify each device, assess their risks, detect threats, and quarantine suspicious malicious devices automatically.

SEE EVERY MEDICAL DEVICE, AND MORE

Armis discovers and classifies every medical device, as well as regular managed and unmanaged devices, in your environment. It can even identify off-network devices using Wi-Fi, Bluetooth, and other IoT protocols in your environment - a capability no other security product offers without

THE ARMIS PLATFORM

COMPREHENSIVE
Discovers and classifies all devices in your environment, on or off your network.

AGENTLESS
Nothing to install on devices, no configuration, no device disruption.

PASSIVE
No impact on your organization's network. No device scanning.

FRICTIONLESS
Installs in minutes using the infrastructure you already have.

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

In addition to discovering and classifying a device, Armis calculates its risk score based on factors like vulnerabilities, known attack patterns, and the behaviors observed of each device on your network. This risk score helps your security team understand your attack surface and meet regulatory requirements to identify and prioritize vulnerabilities.

Reduce Data Breaches

Healthcare has the highest data breach cost of any industry today, and breaches have regulatory consequences. PII and PHI continue to be valuable targets for hackers. Armis performs real-time, ongoing risk assessments with scoring that triggers notifications or automatic mitigation actions based on device behavior. Through behavioral analysis and security automation, security teams can reduce the likelihood and impact of potential breaches, and the theft of patient data.

Detect and Stop Ransomware Attacks

WannaCry and NotPetya attacks continue to impact HDOs, taking out critical medical devices like CT Scanners and X-Ray machines. Armis tracks device behavior to identify ransomware spread, and can quarantine devices, medical or otherwise, to stop attacks in real-time.

Protect Patient Safety

Today's medical devices are connected, gathering and transmitting information, and even administering patient care. However, these devices have no inherent security, and cannot have a security agent installed on them, and you can't scan them for fear of disrupting patient care. Armis is agentless, and can identify and track medical device behavior passively, without disruption, providing continuous, real-time device risk assessment and mitigation. It profiles all devices, connections, and identify anomalous behavior to protect patient care.

Track Medical Device Utilization and Inventory

Device usage and location are critical to the bottom line of any healthcare organization. You need to know where they are, how much they are used, or if they are sitting idle. Armis tracks each device, its IP, and where it is on the network, letting you track devices easily, even if they move between floors or buildings. It also sees traffic and associates use of each device for utilization reporting, helping you get the best return on investment for your medical assets.

ARMIS AT-A-GLANCE

Asset Discovery

- Automatic identification of all biomedical devices
- Make, Model, OS, IP, etc.
- FDA classified devices
- Connection and activity history
- Device location
- Integrate with asset inventory systems (CMMS, CMDB)

Risk Management

- Passive, real-time, continuous risk assessment
- Risk score of biodevices with context
- Extensive CVE and compliance databases
- FDA/ICS alerts
- Smart adaptive risk scoring
- Risk-based policies

Threat Detection

- Device attribution of activities
- Detect changes in device state
- Anomalies based on knowledgebase
- Automation of response
- Device context into every SOC tool and work flow (Splunk, Ticketing, FW, NAC)

Prevention

- Automatically quarantine devices
- Integrates with firewall, NAC, SEIM
- Reduce malware dwell time
- Improved medical device incident response

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 and headquartered in Palo Alto, California.

ARMIS

1.888.452.4011
armis.com