ARMIS

Seeing vulnerable clinical asset blind spots in the patient journey .

The innovation and increasing adoption of connected medical devices and IoMT, IoT, and other smart assets propel the patient journey, but many hospitals are still not prioritizing cyber security.

The risks to patients and operations are real, pervasive, and exist across each stage of the journey. And the potential compliance and accreditation implications are all too real.

>50%

of connected medical devices are unmanaged assets and are **unable to support security agents**

>63%

of healthcare organizations have dealt with one or more security incidents **related to unmanaged IoT devices**

>50 MILLION

the number of individuals in the U.S. impacted by **healthcare data breaches** in 2021 alone

At a glance:

The monetary costs of threats:

$9.4 million

average cost of a healthcare data breach

$4.2 million

average cost of a ransomware attack in healthcare

$50 million

amount of revenue one medical center estimated losing from mitigation efforts after refusing to pay a ransom

11%

percentage of hospitals prioritizing cybersecurity spending

Connected assets are pervasive across the patient journey.

Just consider these examples in each stage.

Admission

- Check-in kiosks
- Label printers
- Tablets and iPads
- Handheld scanners
- Wireless printers
- Security cameras
- Digital signage displays
- Elevator control systems

Threat spotlight:

150,000
hospital surveillance feeds breached

Treatment

- CT scanners
- MRI scanners
- X-ray machines
- Lab analyzers
- Code blue infrastructure
- Pneumatic tube systems
- HVAC systems
- Porter communication systems

Threat spotlight:

$4 billion
in losses from WannaCry ransomware attacks

Aftercare

- Nurse call systems
- Central nursing stations
- Drug dispensing cabinets
- Pneumatic tube systems (PTS)
- Patient service robots
- Implantable devices

Threat spotlight:

80%
of US hospitals impacted by PwnedPiper vulnerability

Discharge

- Tablets
- Billing and payment systems
- Telemedicine solutions
- Cardiac monitors
- Portable dialysis machines
- Smart glucometers

Threat spotlight:

20ft
Remote hacking range of cardiac implant devices

So many assets, so many points of **vulnerability.**

Security teams...

struggle to gain complete visibility of all assets to understand and manage true risk, protect their most critical and vulnerable assets, and respond quickly to security incidents.

Biomedical and clinical engineering teams...

struggle with resource intensive, manual workflows for inventorying and locating clinical devices, identifying FDA recalls, and providing technical information in response to cybersecurity threats.

CISOs, CIOs, and CTOs...

are challenged with managing risk in a highly targeted industry, responding to an increasing number of cyber threats, and establishing cyber resiliency in legacy networks without compromising patient safety.

1.5 Billion

attacks on smart devices in 2021

>25

Why having 25 or more IT management and security solutions in house still doesn't cut it.

Most healthcare organizations have an array of tools to monitor, manage, and secure enterprise assets, but they fall short of what's needed for comprehensive device visibility and protection of the healthcare device ecosystem.

Most asset inventory and management tools...

May be able to aggregate a view of all your managed enterprise devices, but the majority can't:

- Be installed on vendor-certified or proprietary medical devices
- Provide a complete, holistic view of all unmanaged IoT, IoMT, and OT devices
- Provide behavioral context of the device
- Passively identify and dynamically

Most risk assessment tools...

Only provide a point-in-time comparison of activity differences over time and can't:

- Conduct assessments on medical or IoT and OT devices due to incomplete inventory
- Factor in clinical context and utilization of clinical devices or critical OT devices
- Perform real-time continuous risk assessments based on device properties and behaviors
- Provide intelligence about what happened in between time periods

Most vulnerability scanners...

Only provide point-in-time information about managed devices and can't:

- Scan the entire network due to the sensitivity of medical and IoT/OT devices
- Provide real-time updates about new or transient IoMT and IoT devices and connections
- Perform real time vulnerability assessments

Most network access control and monitoring solutions...

Are designed to assess traditional enterprise assets so they can't:

- Identify the vast array of IoMT, OT, and IoT devices found in healthcare ecosystems
- Factor in behaviors and clinical context of devices when assessing the risk and identity of devices
- Continuously monitor and dynamically apply policies based on anomalous behaviors

ARMIS

The Armis platform gives your organization **complete asset visibility.**

The ability to see and understand every connected asset...

Track all things physical and virtual across the patient journey in real-time

- IT
- Medical devices
- IoMT
- IoT
- Building management system devices
- 5G
- Virtual
- Cloud

...with contextual intelligence...

Understand asset truths.

- Fingerprint unknown assets
- Understand clinical context
- Assess true clinical risk
- View real-time utilization metrics
- Assess behavioral anomalies
- Resolve asset conflicts

...and cyber threat support.

Secure your environment.

- Real-time threat intelligence for every asset
- Zero-day vulnerability identification
- Adaptive risk scoring
- Dynamic trust policy assignment
- Seamless security tool integration
- Automated response actions

4

ways that complete asset **visibility** helps support patient care delivery

- Rapid identification and enhanced monitoring of critical patient care devices
- Protect the entire healthcare device ecosystem from cyber attacks and downtimes
- Real time clinical risk assessment streamlines workflows for biomedical teams
- Ensure optimal patient care delivery through real-time utilization analytics

But remember... **complete visibility** is easier said than done...

- Agents only work on managed devices and cannot be installed on medical and IoT devices.
- Active scanning of medical devices can result in devices being knocked offline and put patients at risk.
- Medical devices are evolving out of their traditional profiles, so understanding device context is more important than ever.
- Threats are evolving rapidly and targeting unmanaged blindspots that are difficult for security teams to detect and secure.

Discover more about how Armis can help you gain complete visibility and control over every asset and **secure the patient journey.**

ARMIS

See and secure everything.