5 CRITICAL CONSIDERATIONS FOR YOUR MEDICAL DEVICE SECURITY STRATEGY

EBOOK

ARMIS

INTRODUCTION

Cybersecurity vulnerabilities in medical devices offer multiple avenues of access to cybercriminals. The presence of these vulnerabilities may enable hackers to remotely take control of medical devices then take malicious actions like disrupting their operations, triggering a denial of service attack, and causing logical flaws or information leakage.

As an example of this, in March 2020, the U.S. Food and Drug Administration (FDA) informed manufacturers of potential cybersecurity vulnerabilities in specific medical devices with Bluetooth low energy.

Healthcare systems require medical devices to connect to the Internet, while hospital networks use them to acquire enhanced features that help healthcare providers treat patients more effectively. As a result, malicious actors exploiting vulnerabilities in medical devices can lead to severe repercussions for device manufacturers, healthcare providers, and patients.

In this ebook, we will explore traditional vulnerability management approaches. We'll also outline five critical considerations for your medical device security strategy, which will help medical device manufacturers, patients, and healthcare providers better understand common cybersecurity vulnerabilities and the appropriate solutions to combat them.

> *"Network-connected/configured medical devices that are infected by malware can disable a device from properly performing its clinical function. This, in turn, could lead to a patient safety concern.*

Suzanne Schwartz

Director at FDA Center for Devices and **Radiological Health**

THE LIMITATIONS OF APPLYING TRADITIONAL VULNERABILITY MANAGEMENT PROGRAMS TO HEALTHCARE ENVIRONMENTS

Traditional vulnerability management approaches present several challenges within modern healthcare IT environments. New devices and technical limitations can make traditional methods largely ineffective and present critical issues such as:

Lack of visibility and context

Before any scan, it's crucial to know which devices exist on a network and where they are being utilized. However, traditional scanners often don't provide context and can increase patient risk.

Sensitive and critical nature of medical devices

Medical devices' sole purpose is to aid workflows that support patient care. They are extremely sensitive to even slight deviations in normal operating behavior.

Direct risk to patient care

Medical device malfunction and data output errors can directly affect patient care. Traditional scanners can actually increase the risk by hindering the care delivery and decision-making process.

Proprietary operating systems and protocols

Medical devices operate on various operating systems and protocols that traditional scanners can struggle to fingerprint and assess or identify vulnerabilities effectively.

Specialized vulnerabilities

Traditional technologies lack the context required to assess the risk of new vulnerabilities. This can lead to alarm fatigue and see organizations miss potential threats.

Vendor managed network segments

Devices and networks are increasingly vendor-managed, which can lead to blind spots for traditional scanners. They need to be placed on unique gateways on dedicated patient care networks.

Scanning cadence

The variety of medical device types and features means there's no 'one-size-fits-all' scanning cadence. This often makes admin tasks complex and can defeat the purpose of traditional processes.

Limited remediation capabilities

Detecting vulnerabilities is a small part of the process; they also need to be remediated. But patching options for many medical devices remain limited.

Resource constraints

In addition to technical limitations, many organizations lack the personnel and resources to compensate for them. This could include extensive site surveys plus analysis, planning, testing, and implementation.

THE NEED FOR A **NEW APPROACH** TO VULNERABILITY MANAGEMENT

We need to transition from this legacy approach to a continuous monitoring vulnerability management methodology. To do so, we need to understand how to take advantage of the capabilities that exist in legacy platforms and add innovations with new approaches that take into account:

- **Network behavior**
- **Communication methodology (peer to peer/airspace like Zigbee, Z-Wave)**
- **Real-time passive event-based vs. scheduled scanning**
- **Utilization data**
- **Baselined device behavioral telemetry**

Utilizing these approaches allows for the creation of an architecture that takes into account not only the technology footprint but also the workflow impacts in an operational setting. This is critical for healthcare organizations, as operational environments such as Biomed / clinical engineering often consists of devices ranging from 30-year-old lab monitoring equipment to the latest imaging modalities. As the next step, when you take into account the role that building management systems plays in a healthcare environment, it becomes clear that vulnerability management is no longer just a security tool kit but an essential component of continuity of operations.

5 CRITICAL CONSIDERATIONS FOR YOUR MEDICAL DEVICE SECURITY STRATEGY

Resilience is quickly becoming the guiding strategy for health IT investment. As a result, information security teams are having to pivot their approach to risk management, incident response, and recovery processes.

To help align with that, there are five innovative approaches to vulnerability management that enable healthcare organizations in five ways:

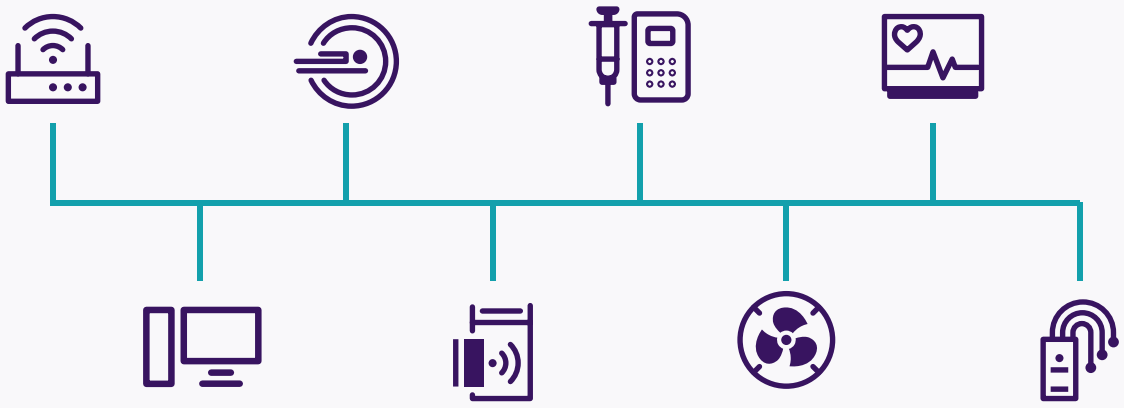
1. **Passive, real-time, continuous monitoring**
2. **Baselined device behaviors & threat telemetry**
3. **Risk assessment for medical devices**
4. **Visibility into airspace**
5. **Utilization data**

1 PASSIVE, REAL-TIME, CONTINUOUS MONITORING

Healthcare Delivery Organizations (HDOs) are not prepared to protect the broad attack surface that medical devices create. These devices cannot easily receive software updates, lack inherent security controls, and cannot be managed or seen by traditional security systems whose medical device vulnerability management is suboptimal.

HDOs and clinicians need an agentless passive architecture that helps them to automatically discover every connected device in their environment. This includes managed and unmanaged medical and IT devices, wired and wireless devices on or off their network, including IaaS environments and vendor-managed network segments. In addition, this security solution should also provide complete visibility into the behavior of all devices. This includes all network activity, such as DNS queries, TCP sessions, HTTP requests, device utilization, and application usage. The passive architecture also ensures complete asset inventory and near real-time vulnerability information without the risks and limitations of a traditional vulnerability methodology.

2 BASEDLINED DEVICE BEHAVIOURS & THREAT TELEMETRY



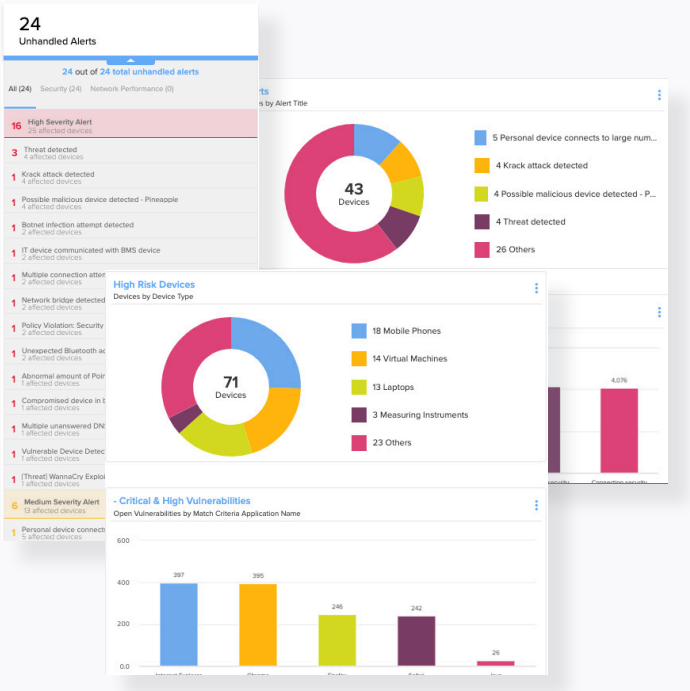
A medical device security strategy is critical to monitoring the traffic of wired and wireless medical devices. You also need to understand the behaviors of these devices without creating disruption. Each device includes unique characteristics, such as manufacturer, model, OS version, serial number, location, connections, FDA classification, and more. Your security strategy should analyze this information and use device profiles and behavioral data from its “Device Knowledge Base” to identify each device, assess its risks, detect cyber threats, and quarantine malicious devices automatically.

This process can also alert you to anomalous device behaviors that deviate from their normal profile, such as MRI machines connecting to social media sites. Furthermore, an effective security approach enables you to discover computers and devices on your network that are owned and operated by third parties, such as outsource suppliers, vendors, consultants, patients, or visitors.

3

RISK ASSESSMENT FOR MEDICAL DEVICES

The FDA recommends risk assessment for medical devices since cybersecurity-related issues can harm patients in a variety of ways. For example, false negatives or false positives are crucial factors in diagnostics. If a diagnostic medical device gave an incorrect result, it could cause serious harm to the patient.



To prevent this, you need a real-time risk assessment for medical devices. Utilizing a completely passive approach prevents any impact on the flow of medical device traffic or active probing of sensitive medical devices, which can cause interruption to patient care.

Several factors are analyzed to provide a holistic and comprehensive assessment, including:

- Device properties
- Vulnerabilities impact to clinical workflows
- Device behaviors - Network and clinical protocol visibility
- FDA recalls & MDS2 Properties
- Alignment to NIST & MITRE ATT&CK frameworks

The ISO 14971 is an international standard for the risk management of medical devices. Its supporting document is ISO/TR 24971:2020. Healthcare organizations can purchase these documents from iso.org.

4

VISIBILITY INTO AIRSPACE

It is vital to see everything in the enterprise airspace, including devices that communicate via Wi-Fi and many other peer-to-peer protocols (Z-Wave & Zigbee) that are invisible to traditional security tools. This visibility allows you to identify potential network intrusion and data exfiltration points in your environment. In addition, your security strategy should produce a more complete inventory of devices than traditional tools that see only IP addresses. Healthcare customers need to leverage the airspace visibility feature to inventory and locate devices that are not directly connected to the network, such as defibrillators and devices that otherwise would not have been seen or inventoried, and consumer IoT devices, such as smart lights and smart locks.

A sound security strategy should also incorporate the development of a security profile for each medical device. This can be done by continuously performing tasks such as passive device profiling, vulnerability detection, and machine learning of network behavior through the use of wired and wireless network access devices. The security profile of medical devices helps security and Biomed administrators when onboarding medical devices and classifying their risks to the healthcare organization.

5

UTILIZATION DATA

It's crucial to implement a security strategy that helps you to gather medical equipment utilization information across your entire enterprise. It also needs to provide intelligence about device usage, hours of operation, and underutilization. Ensuring this allows you to plan purchases, schedule maintenance downtimes, right-size your inventory levels, and maximize efficiency through the entirety of the medical device lifecycle. Increased visibility ensures optimal uptime and operations of critical medical devices. It also enables operational departments to view the types of clinical procedures to assess for impact to operations.

All of this innovation leads to security and operations teams having appropriate, contextualized data that is already prioritized, taking into account organizational and clinical workflows. This leads to significant improvements in resource utilization and team efficiency for incident response and recovery operations.

Armis understands that healthcare operating margins are essential to the continuity of operations and, as such, is committed to helping organizations leverage their existing investments in automation technologies. To support that, Armis also provides integrations with industry-leading providers for clinical engineering workflow management, security orchestration, and automation solutions, as well as network/endpoint security platforms and security analytics solutions. The integrations, when leveraged correctly, can help healthcare customers realize the vision of information security being an organic extension of the clinical risk management process.

About Armis

Armis® is the leading unified asset visibility & security platform designed to address the new threat landscape created by connected devices. 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). The Armis platform 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

1.888.452.4011

20210401-1

ARMIS