ivanti Neurons

Healthcare IT, Biomedical, Security

Guide to Improving Visibility and Security Risk Mitigation for Medical Devices

Table of Contents

Introduction

Connected medical devices represent a huge challenge for healthcare IT, biomedical and security organizations. They are inherently vulnerable to cyberthreats, and successful cyberattacks can have terrible consequences. Yet traditional cybersecurity measures cannot be applied to these devices and may even risk interfering with critical clinical operations.

In this guide we go through a three-step process to help increase visibility into medical devices and improve security risk mitigation. Establishing cybersecurity layers for medical devices is a multi-stage, ongoing process, which can be successful when it starts from a strong foundation and takes a methodical, systematic approach.

Learn how to discover, assess, and mitigate cybersecurity risks associated with connected medical devices. The three phases we present in this guide are not a one-time process, but rather should be treated as a cycle. IT and security teams at healthcare centers should perform these phases continuously — surveying the environment, assessing risks and addressing security issues they discover day to day.

How vulnerable are medical devices to cyberattack?

An increasing number of medical devices are connected to networks or to other devices, creating a major security vulnerability for hospitals and healthcare providers. Many of these devices are not secure and are not actively managed, opening the door to a wide range of cybersecurity threats.

Why are medical devices vulnerable?

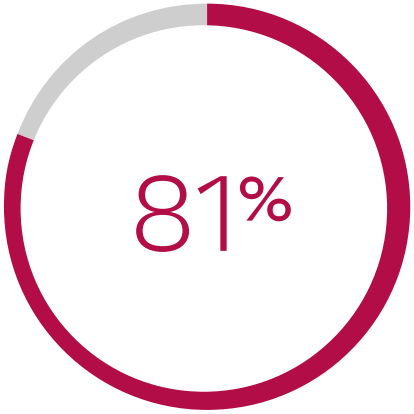
- Software code has not undergone security review.
- Authentication is weak or nonexistent.
- Data-transfer channels are often insecure and unencrypted.
- Limited visibility over which devices are actively used.
- Inability to monitor device activity and security incidents.
- Decommissioned devices are not securely disposed of.
- Software updates are unavailable, or rarely deployed.

Understanding the environment
Discover which IT and medical devices exist, classify them accurately, understand their clinical context, and identify their networking needs.

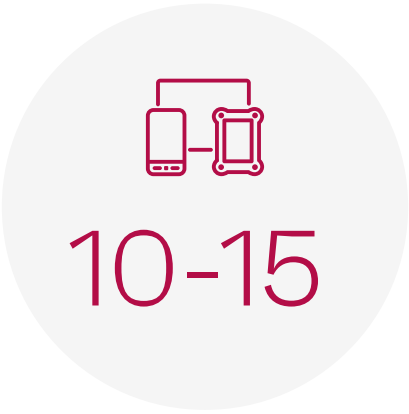
Risk assessment
Identify device vulnerabilities and network-related risks, assigning each device a risk index, and providing recommendations for remediation.

Protecting devices
Address security at the device level, isolating devices within the LAN and preventing unwanted communication over LAN/WAN, and preparing a strategy for detecting security incidents when they occur.

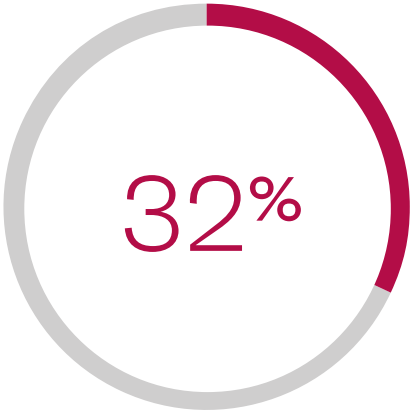
How big is the problem?



81% of healthcare organizations reported being compromised by a cyber-attack in the past two years.



Hospitals maintain 10 – 15 connected medical devices per bed, with over 3.7 million devices in active use.



32% of healthcare organizations say medical devices are their top security concern.

Sources: KPMG, Wired

What threat vectors affect medical devices?

Malware
Medical devices typically have no endpoint protection and are especially vulnerable to malware.

Inside threats
Due to weak authentication, malicious insiders can easily gain unauthorized access and tamper with devices.

Web application attacks
Some medical devices are manageable via a web interface, creating a range of cyber risks such as code injection, cross-site scripting (XSS), and path traversal.

Device misuse
Connected medical devices are often based on Windows PCs. Hospital staff can use the machines to browse the internet or install software, creating additional risk.

How can you evaluate cybersecurity risk and the impact of an attack?

The FDA guidelines for medical devices provide useful classification of device risk levels.

Tier 1: Higher cybersecurity risk	Tier 2: Standard cybersecurity risk
The device is:	**The device is:**
Capable of connecting to another medical or non-medical product, to a network, or to the internet OR A cybersecurity incident affecting the device could directly harm one or more patients	Capable of connecting to another device or network, but cannot directly harm patients OR Capable of directly harming patients but cannot connect to a network

To get a more granular evaluation of risk, use a framework like the CVSS risk calculation. Take the following factors into account when assessing cybersecurity risk:

- Software vulnerabilities
- Patient safety
- Authentication
- Privacy
- Networking
- Service disruption

Phase I:

Understanding the connected-device environment

The first step to solving a problem is recognizing its existence and understanding its scope. The problem of connected medical devices is not well understood by IT, biomedical and security teams at hospitals and healthcare organizations due to extremely limited visibility.

Security teams see medical devices as black boxes, or cannot see them at all

Security for medical devices is becoming a shared responsibility of clinical engineering teams and IT departments. While information about these devices exists in healthcare organizations, it can't be readily accessed by security teams.

The following important questions are left unanswered:

1. How many devices are connected?
2. What types of devices are they?
3. Which other devices or networks do they communicate with?
4. Is network behavior normal and expected or anomalous?

Why is it difficult to create an inventory of connected medical devices?

You cannot simply run a network scan and identify medical devices like you would on a regular IT network. That's because:

- Devices are sensitive. Active network scanning can disrupt medical device operation, so you must use passive discovery.
- Invisible to network discovery tools. Traditional tools will not discover the vast majority of connected medical devices, or may indicate falsely that the device is a Windows workstation. Most connected medical devices do not advertise their information, and detecting them over the network requires careful analysis of traffic at the application layer.
- Large number and variety of devices. There may be tens of thousands of devices of different types, vendors and versions.
- Ongoing flux. Devices are constantly added, replaced or removed from the network, often without involving IT, so discovery and inventory must be an ongoing process.

Step 1. Discovery

Aim to build a database of medical devices with data about each device. Focus on high-quality data that can help you determine risks and vulnerabilities. In particular:

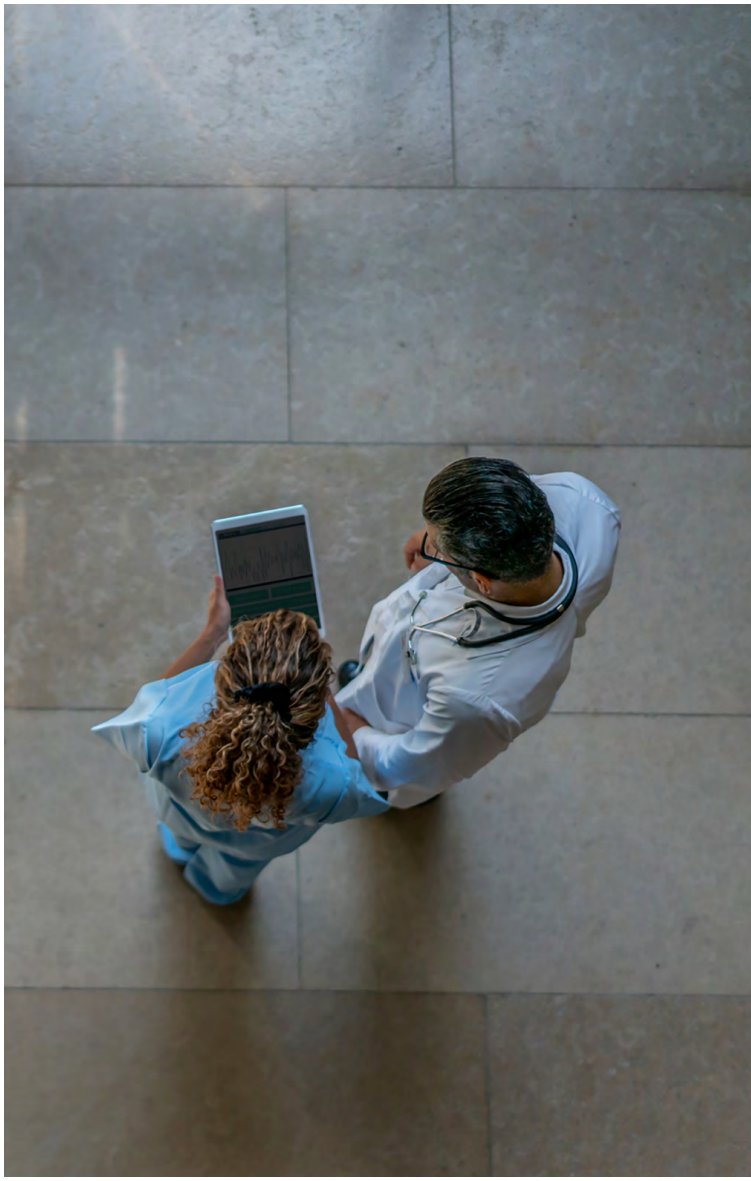
- Device type
- Department and room
- Vendor
- Model
- IP address
- Operating system
- Application software version
- Latest security patch

Step 2. Network mapping and clinical context

Understanding a device's network behavior lets you understand how exposed it is to external and internal threats. Try to obtain the following information for each of your connected devices:

- What other devices does it communicate with?
- Does this device have unnecessary access to other devices, networks, or the internet?
- Is this device's network communication isolated in a VLAN?
- What types of protocols are used?
- Where does the device send or receive Public Health Information (PHI) data, and which type of PHI?
- Does it communicate externally over the internet?
- Does the device need to communicate with the device vendor on an ongoing basis?
- Are internet communications normal for this type of device?
- Is this device's internet communication isolated in a VPN tunnel?

Clarify the clinical use of each device and, by extension, its exposure to risks. This data can be extremely difficult to obtain without the aid of automated tools.



Phase II:

Risk Assessment

Once you have a better understanding of your connected medical devices and have built an inventory of the devices, their context, and network behavior, you can use this inventory to assess the risks affecting each device and their impact on the organization.

Step 1. Identify device vulnerabilities and remediation opportunities

Collect data about vulnerabilities for each of your device models, operating systems, and application versions.

Impact of software vulnerabilities
Use the CVSS risk calculation to identify the impact of known software vulnerabilities in your connected devices.

Misconfigurations
Check for general vulnerabilities such as hard-coded or default passwords, unpatched operating systems, or software.

Device authentication
Identify if the device has authentication and if so, how strong it is and whether secure passwords have been set. Just as important, discover the owner of the device and your level of access for remediating security issues.

Point of contact
Who manages the device—clinical engineering, IT, the manufacturer, or a third-party contractor?

Ease of access
Does the security team have access to this device to implement security controls or respond to incidents?

Backup
Does the device have backup or redundancy, and what is the impact of service disruption?

Step 2. Identify network-level risks

Medical device vulnerabilities are only one aspect of the risk. Analyze network connectivity and identify vectors by which attackers can connect to your devices.

Internet connection
Check if the device connects to other systems over the internet, for example to a third-party company or the manufacturer for maintenance or updates.

Connections to less-secure devices
Check if the device can connect to a less-secure device or endpoint, such as a physician's workstation, and whether it exposes management or data services like FTP or SSH.

Encryption
Check if the device transmits or receives unencrypted dataflows.

Non-secure protocols
Check if the device uses protocols that offer weak authentication, no authentication, or have vulnerabilities.

Step 3. Identify risk severity

Ask yourself: what would be the impact of a successful cyberattack on each of your devices? Unlike attacks on healthcare IT systems, the impact of an attack on connected devices is not limited to data security and privacy. A successful cyberattack could disrupt clinical care and cause direct harm to patients.

We recommend identifying risk severity according to the three impact metrics in the CVSS risk calculation:

- Confidentiality. Corresponds to the risk exposure of Protected Health Information (PHI) stored in, or transmitted by the device.
- Integrity. Corresponds to the risk to patient safety for devices directly used in patient care.
- Availability. Corresponds to the risk of service disruption.

Patient safety	Privacy	Service disruption
LOW: FDA Class I Medical Device; low-to-moderate risk to the patient or user.	**LOW:** Device does not store PHI.	**LOW:** Device failure cannot disrupt patient care.
MEDIUM: FDA Class II Medical Device; moderate-to-high risk	**MEDIUM:** Device stores a small amount of PHI for a limited time period around a test or treatment.	**MEDIUM:** Device failure can disrupt patient care but not critical medical treatment.
HIGH: FDA Class III Device; high risk, devices that sustain or support life, are implanted or present high risk of illness or injury.	**HIGH:** Device stores large amounts of PHI across multiple tests or treatments.y.	**HIGH:** Device failure can disrupt critical medical treatment such as surgery, respiratory equipment or delivery of life-sustaining medication.

Phase III:
Protecting connected medical devices

The advantage of our structured process for discovery and risk assessment is that you can rank devices according to the risks they represent. Each device should have a risk impact score (for patient safety, privacy and service disruption).

Your organization can define an acceptable level of risk. The security team can focus on protecting devices with risk scores beyond the acceptable level, and can apply the appropriate security measures to devices with different risk scores.

We advise protecting connected medical devices in four steps:

Step 1. Device hardening

As with any computing device, you must make sure connected medical devices have the latest security patches and software upgrades. Configuration must be hardened to enable secure authentication. Close unused ports, limit unnecessary functions, and in general, reduce the attack surface.

Most medical devices run on a Windows operating system. However, applying a patch is not as simple as with a workstation or Windows server.

Challenges with hardening medical devices:

- Windows security patches must be verified and approved by the device manufacturer.
- Clinical engineering must verify patches or updates that do not impact the functionality of the medical device.

Guidelines:

- You will not succeed in deploying all security patches or hardening all devices.
- Focus on devices that have a high risk score.
- Prioritize security patches or configuration changes that address the known vulnerabilities you identified in your risk assessment.

Step 2. Network isolation

A key strategy to securing connected medical devices is to isolate them, as much as possible, from non-critical clinical communication to limit the attack surface. This has two components:

- Defining network segmentation to ensure connected medical devices can only communicate with devices or systems that are part of their clinical process .
- Blocking external communication to ensure connected medical devices never connect to the internet, unless this is needed to communicate with the device vendor or other known entities.

Considerations when isolating medical devices

- Isolate clinical data flows from non-clinical data flows.
- Clinical communication is essential, but any other communication should be blocked.

Guidelines:

- Set strict access policies and network segmentation to restrict non-essential communication to/from devices.
- Set segmentation policy to address risks and vulnerabilities discovered in your impact analysis.
- Block the device from connecting to the internet unless absolutely needed for the device to function, and only to known entities.

Step 3. Incident detection and response

It is impossible to protect most connected medical devices from all potential threats because there will always be critical legacy devices that cannot be replaced and cannot be fully patched or isolated. This means you can limit the attack surface but not eliminate it. In addition, isolation can be a long process, and in the interim, some devices will remain vulnerable. This is why it is critical to monitor devices and detect and alert immediately when unusual activity takes place.

Considerations when monitoring for security incidents:

- Use passive monitoring such as a network TAP or mirror port to avoid interrupting device operations.
- Leverage information you collected about the clinical context of each device to understand what represents normal clinical communication.
- Compare current behavior to vendor specifications, past behavior, and to the behavior of a peer group of devices in your environment and in other organizations.

Guidelines:

- Continuously monitor all devices, with special emphasis on those with a high risk score.
- Establish a strategy for comparing ongoing communication to normal clinical communication.
- Alert security on any major deviation from normal behavior.
- Integrate with third parties that can help perform speedy remediation via remote action, such as on-demand network segmentation.

Step 4. Metrics and analytics

Medical device cybersecurity is a long process, which must be maintained and improved over time to adapt to a continuously changing threat landscape.

Tracing your progress can help you understand if you are moving in the right direction and make corrections if your work is not improving the security situation. Below are a few guidelines for tracking the progress of your medical device security project.

Guidelines:

- Create a scorecard for medical devices with a timeline of risk scores, ensuring risk is reduced over time
- Identify activities and strategies that improved KPIs and reduced overall risk indexes.
- Set KPIs based on risk of important devices and monitor improvement; tie KPIs to business goals like patient safety and service availability to get buy-in from leadership.
- Collect data about risk indexes and historical behavior of devices, and use it for better procurement decisions

Improve asset visibility and security risk mitigation for medical devices with Ivanti Neurons for Healthcare

Ivanti® Neurons for Healthcare improves asset visibility and security risk mitigation for medical devices. The solution discovers and intelligently profiles medical devices and Internet of Medical Things (IoMT), assessing security risks, reporting threats and reconciling device information across multiple data sources. Know more about the various healthcare-specific devices across your facilities, including device classification and usage information, with the details to reduce security risk or attend to anomalies. Collect and reconcile vendor data, creating a single source of truth for all your medical devices.

For more information, visit
ivanti.com/products/ivanti-neurons-healthcare

ivanti Neurons

ivanti.com/neurons
1 800 982 2130
sales@ivanti.com