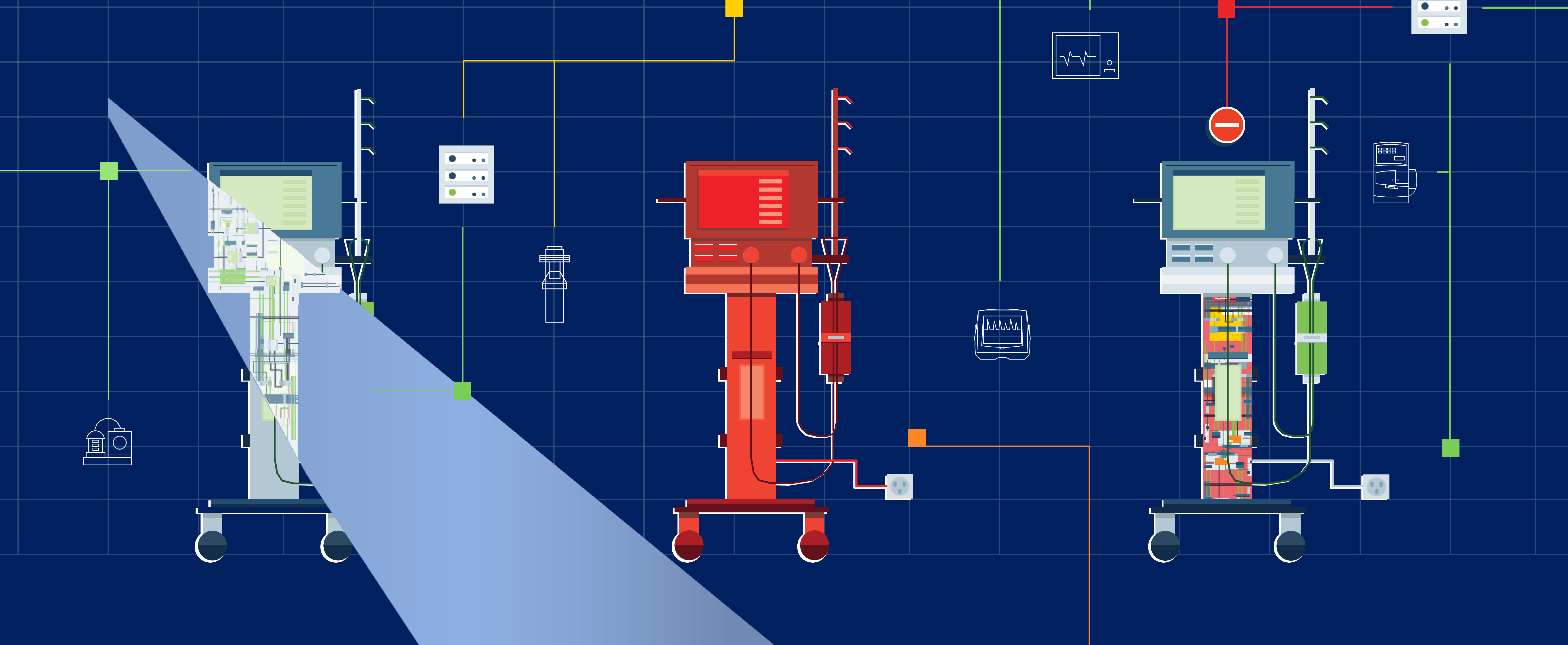
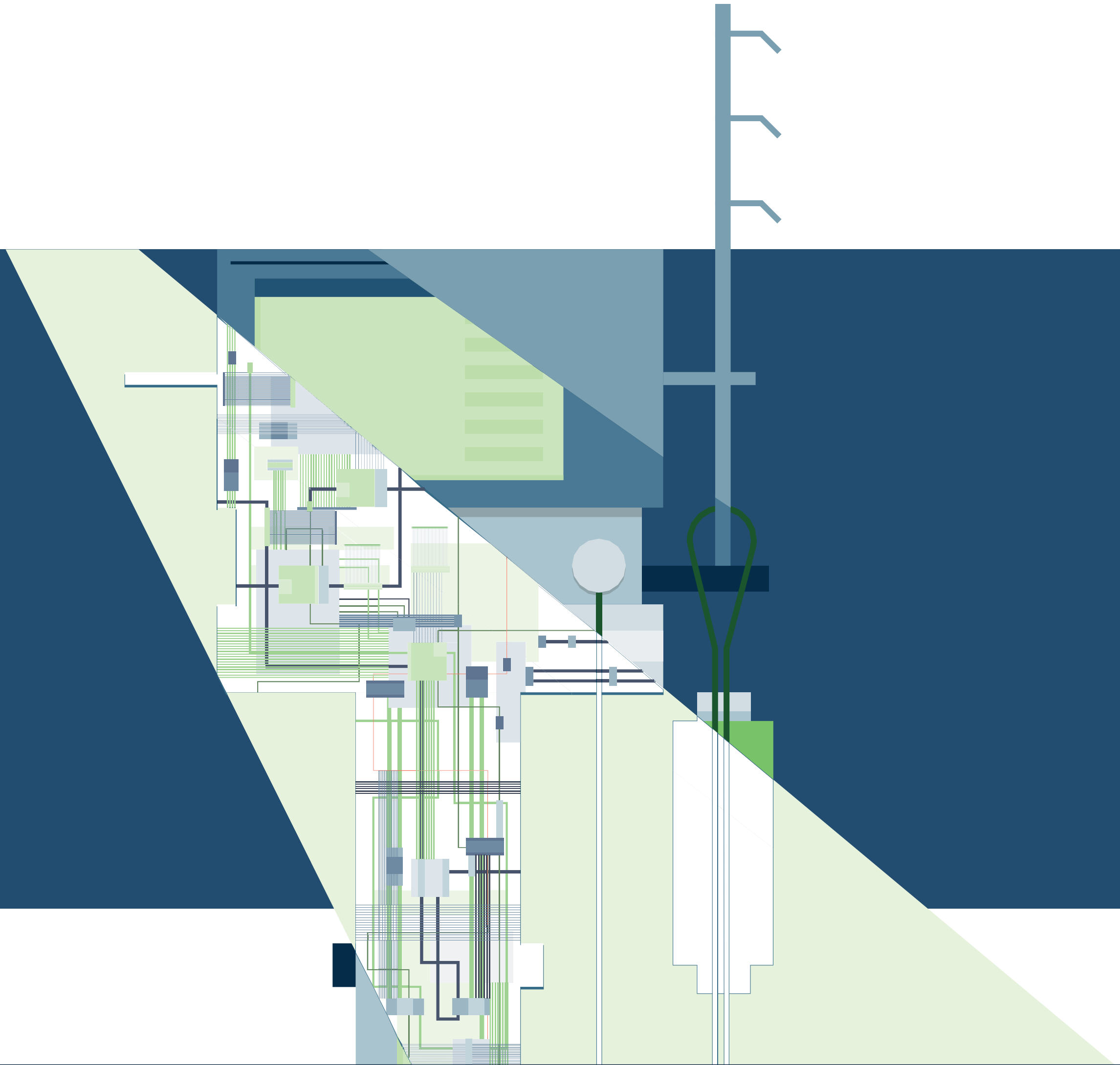
HEALTHCARE CYBER RISK MITIGATION FOR CONNECTED MEDICAL DEVICES



THE RISK MITIGATION FOR CONNECTED MEDICAL DEVICES

Connected medical devices represent a huge challenge for healthcare leadership. They are inherently vulnerable to cyber threats and successful cyber attacks 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 explain the problem of connected medical devices and present a three-phase process for identifying and mitigating risks. Establishing cybersecurity layers for medical devices is a multi-staged, ongoing process, which can be successful when it starts from a strong foundation and takes a methodical, systematic approach.



Traditional cybersecurity measures cannot be applie d to these devices, and may even risk interfering with critical clinical operations.

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 continuously perform theses phases—surveying the environment, assessing risks, and addressing security issues they discover on a day-to-day basis.

01 FIRST PHASE

Understanding the Connected Device Environment

Discovering which devices exist, accurately classifying them, understanding their clinical context, and identifying their networking needs

02 SECOND PHASE

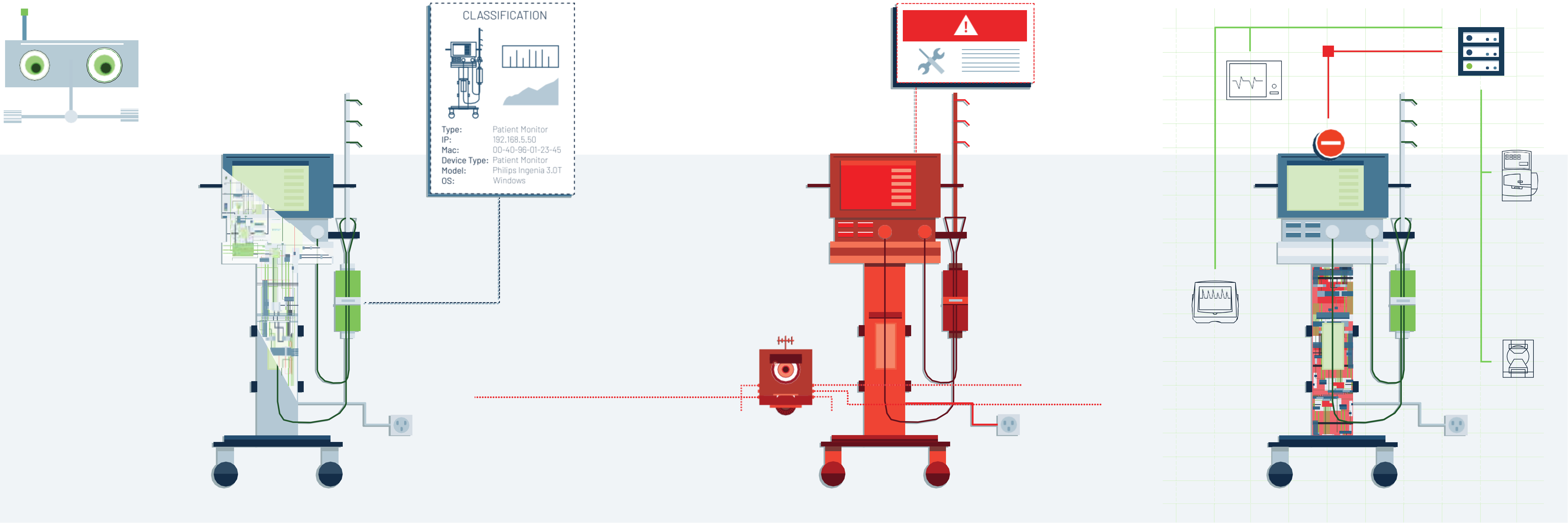
Risk Assessment

Identifying device vulnerabilities and network-related risks, assigning each device a risk index, and providing recommendations for remediation

03 THIRD PHASE

Protecting Connected Devices

Addressing 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



CLASSIFICATION

Type: Patient Monitor
IP: 192.168.5.50
Mac: 00-40-96-01-23-45
Device Type: Patient Monitor
Model: Philips Ingenia 3.0T
OS: Windows

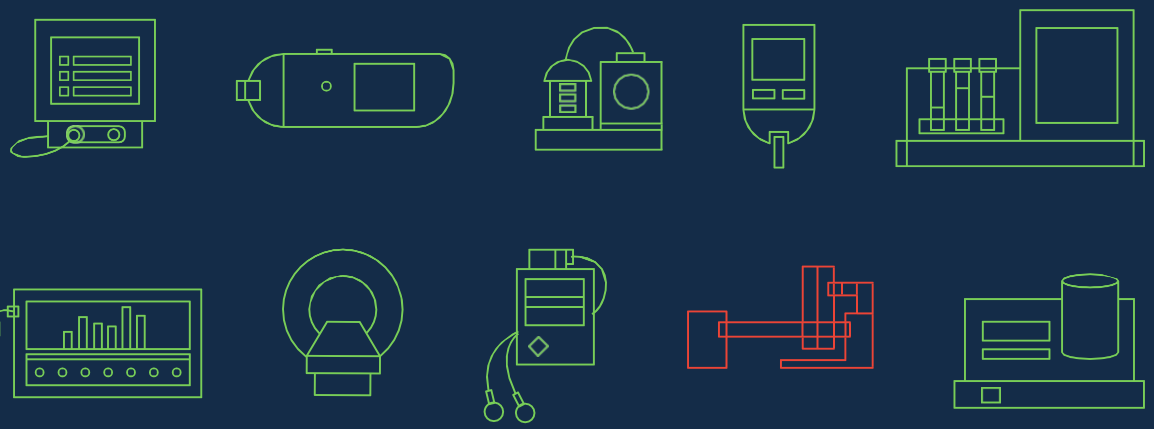
How Vulnerable Are Medical Devices to Cyber Attack?

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 so 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

Many of these devices are not secure and are not actively managed, opening the door to a wide range of cybersecurity threats.



How Big Is the Problem?

81%

compromised

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

32%

top concern

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

10–15

devices per bed

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

Source: 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 a coarse but highly useful classification of device risk levels.

Tier 1
Higher Cybersecurity Risk

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

Tier 2
Standard Cybersecurity Risk

The device is:

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

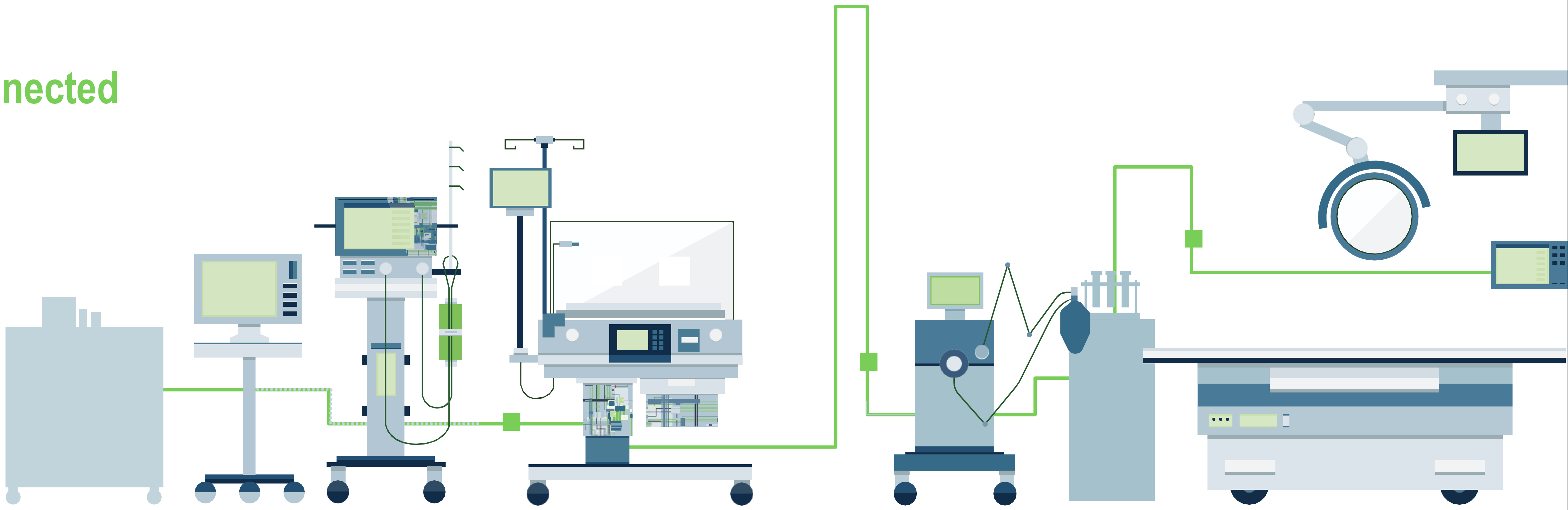
To get a more granular evaluation of risk, use a framework like the CVSS risk calculation. Take the following factors into account when assessing cybersecurity risk:

- Software Vulnerabilities
- Authentication
- Networking
- Patient Safety
- Privacy
- Service Disruption

For more details on risk assessment, refer to the Second Phase below.

01 FIRST PHASE

Understanding the Connected Device Environment



UNDERSTANDING THE CONNECTED DEVICE ENVIRONMENT

The first step to solving a problem is recognizing it exists and understanding its scope. The problem of connected medical devices is not well understood by IT and IS 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. Information about these devices does exist in healthcare organizations, but cannot be readily accessed by security teams.

■ **The problem of connected medical devices is not well understood by HDO IT and IS teams due to extremely limited visibility.**

The following important questions are left unanswered:

How many devices are connected?

What types of devices are they?

Which other devices or networks do they communicate with?

Is network behavior normal and expected or anomalous?

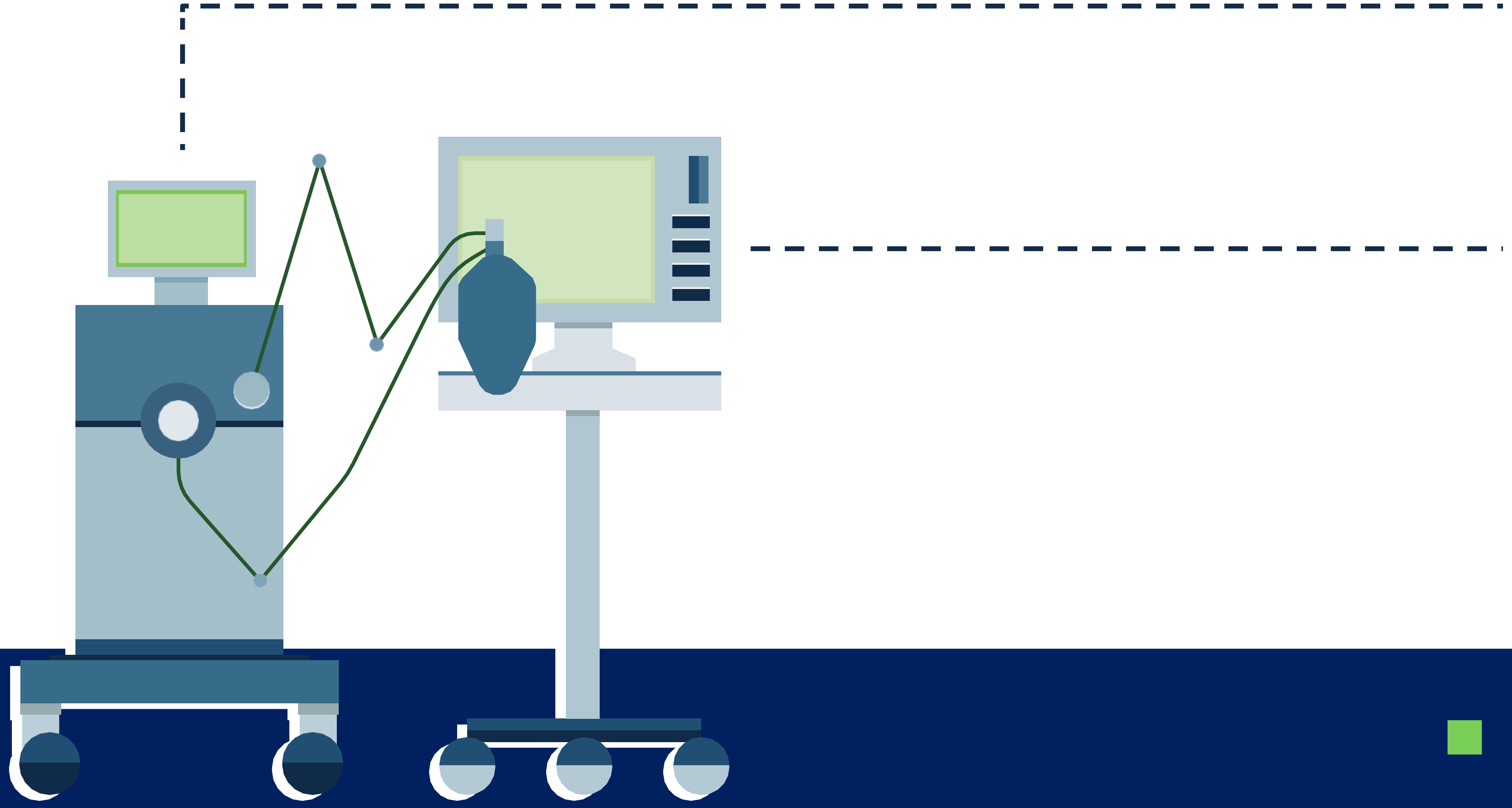
Why Is It Difficult to Create an Inventory of Connected Medical Devices?

You cannot simply run a network scan and identify medical devices like you would on a regular IT network:

- **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 falsely indicate 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 needs to be ongoing.

Step 1. Discovery

Aim to build a database of medical devices with data about each device.



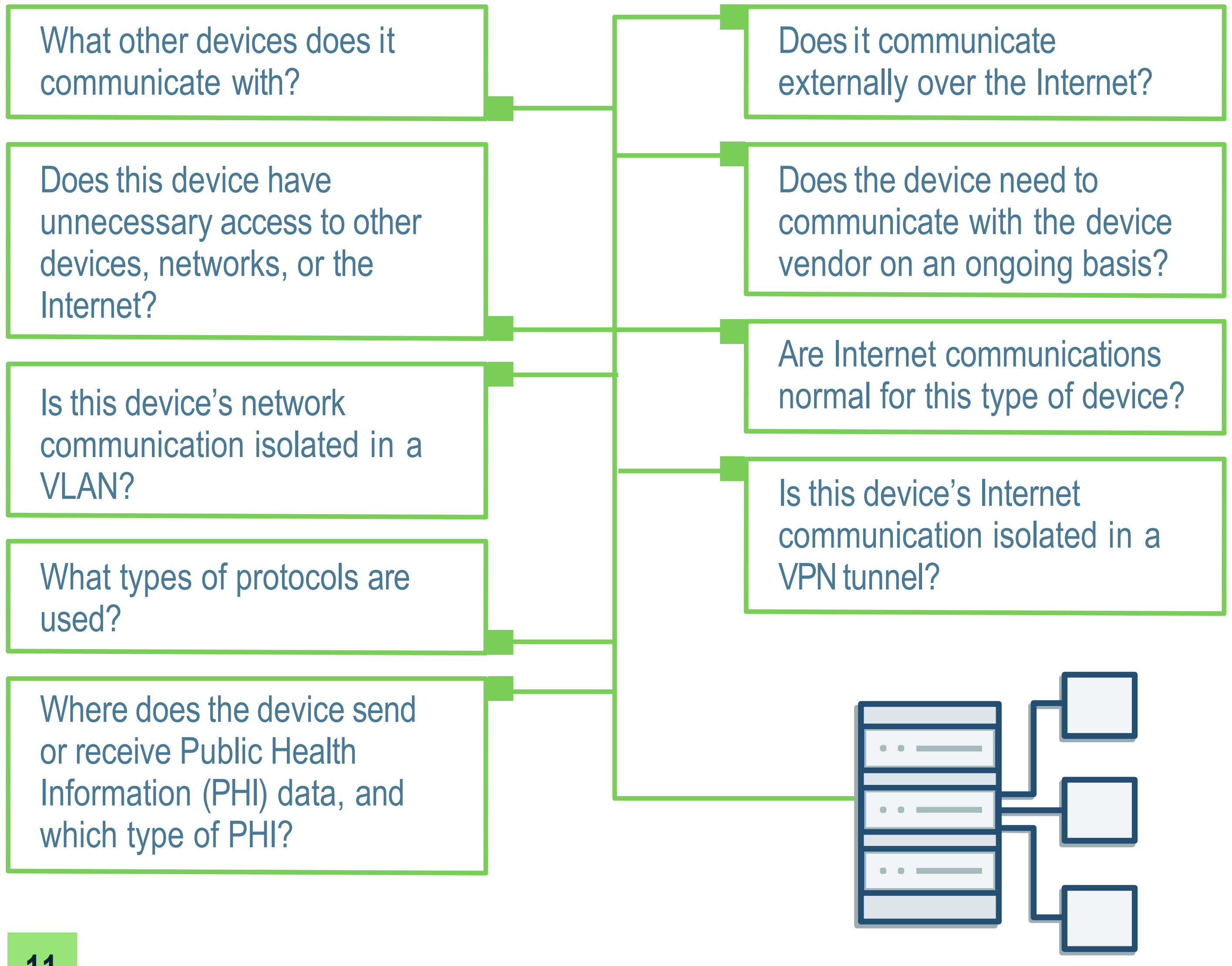
Focus on high-quality data that can help you determine risks and vulnerabilities. In particular:

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

Focus on high quality data that can help you determine risks and vulnerabilities.

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?

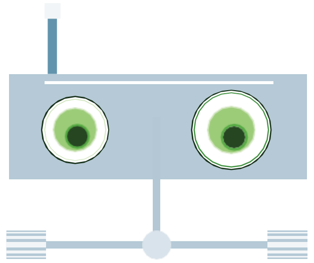
Does the device need to communicate with the device vendor on an ongoing basis?

Are Internet communications normal for this type of device?

Is this device's Internet communication isolated in a VPN tunnel?

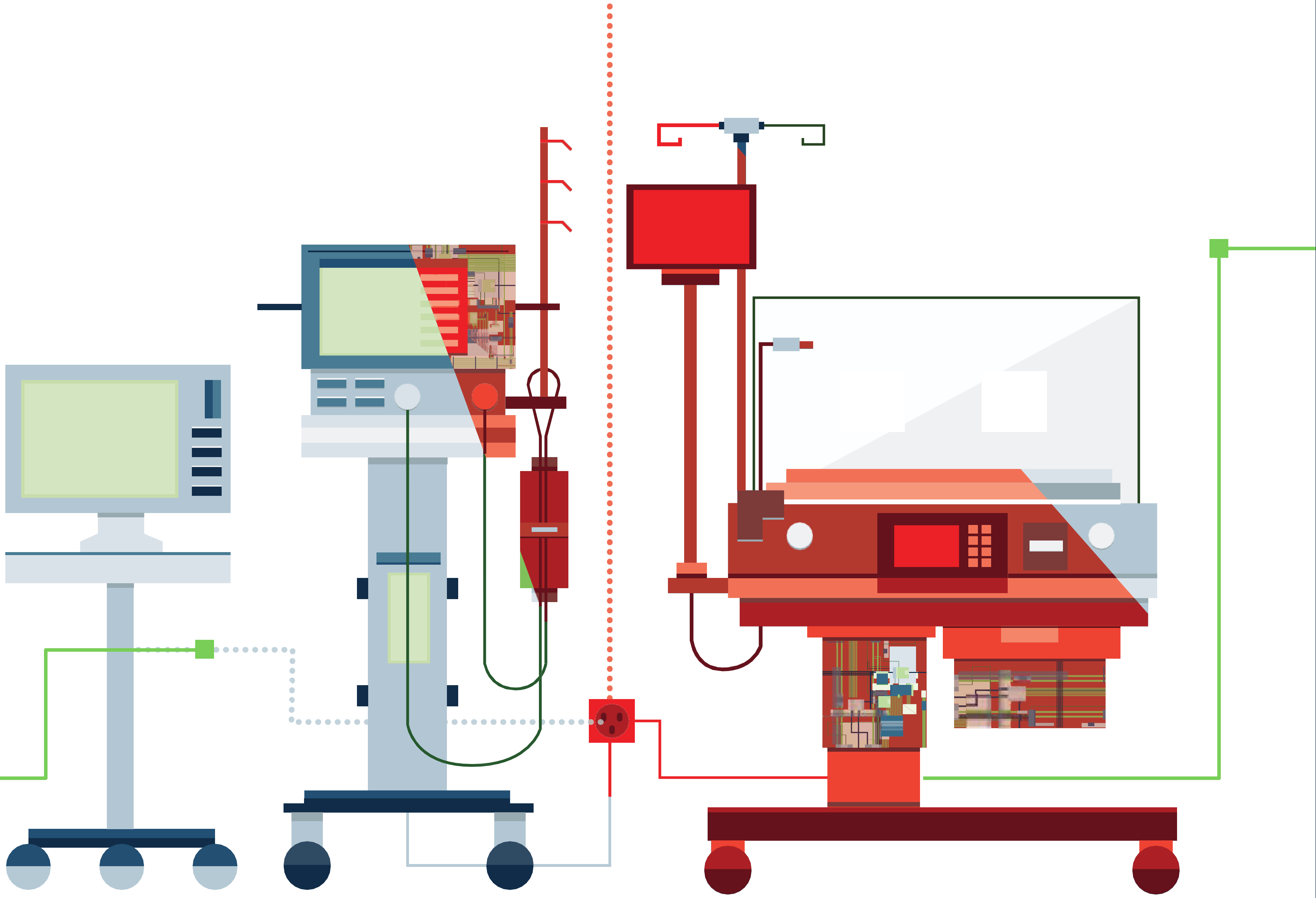
Clarify the clinical use of each device and, by extension, its exposure to risks. This data can be extremely difficult to obtain without the aid of automated tools.

Clinical Context Information	How It Can Help
Which connections to and from this device are clinical data transfers? Which are non-clinical communications such as control channels?	▪ Any security effort must avoid interfering with critical dataflows ▪ By recognizing clinical workflows, you can accurately identify anomalies that could impact important information flows
Does this device transfer or store Protected Health Information (PHI)?	▪ Devices with PHI are more likely to be targeted by cyber criminals ▪ There is a need to secure data as well as the device itself ▪ The device needs to comply with relevant standards and regulations
Is the device directly involved in patient care? For example, patient monitors, infusion pumps, and pacemakers. Is it an FDA Class III device (a device that sustains or supports life)?	▪ Prioritize security efforts on connected devices that are directly involved in patient care or may cause direct harm to patients



02 SECOND PHASE

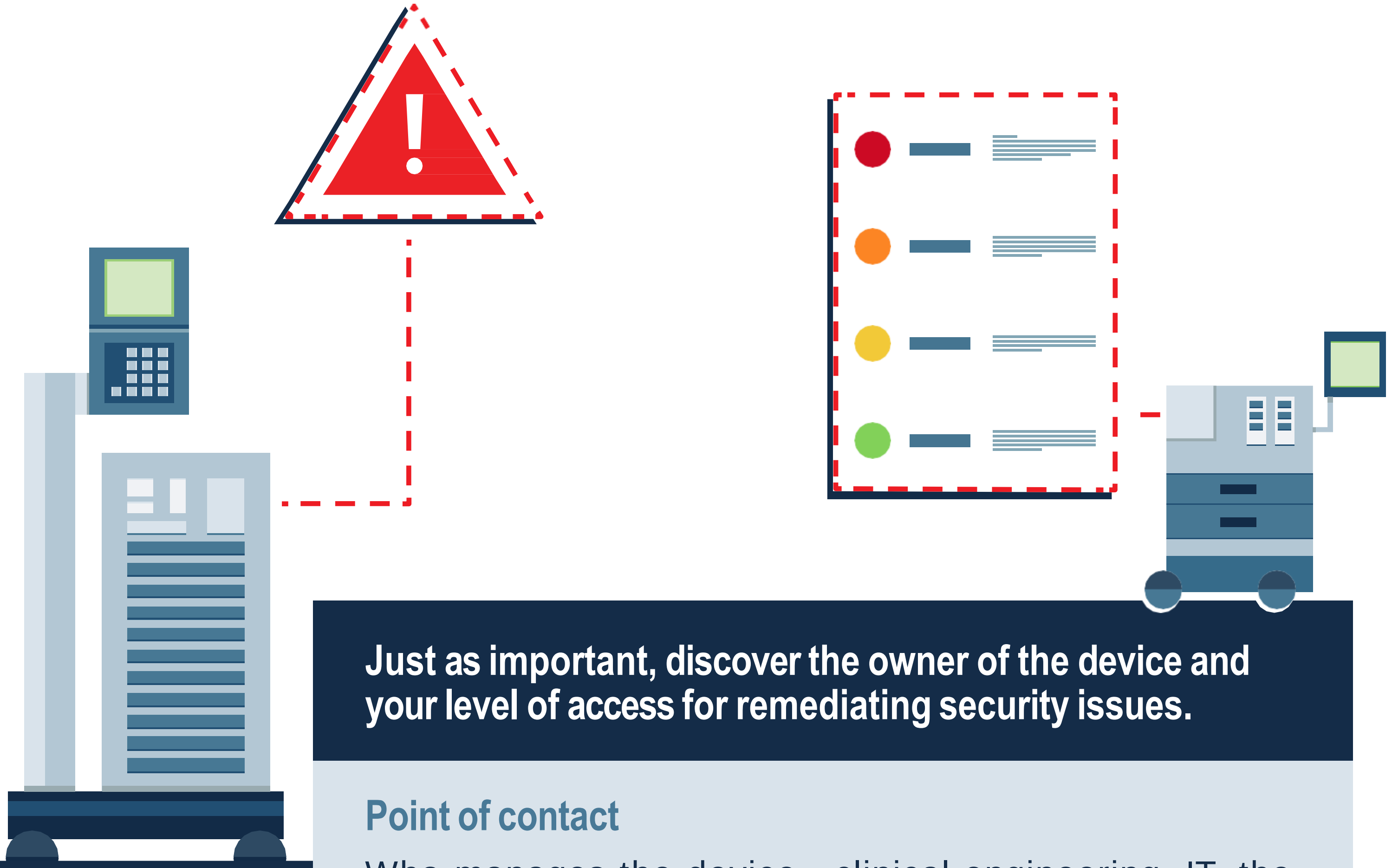
Risk Assessment



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, and 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.

Encryption

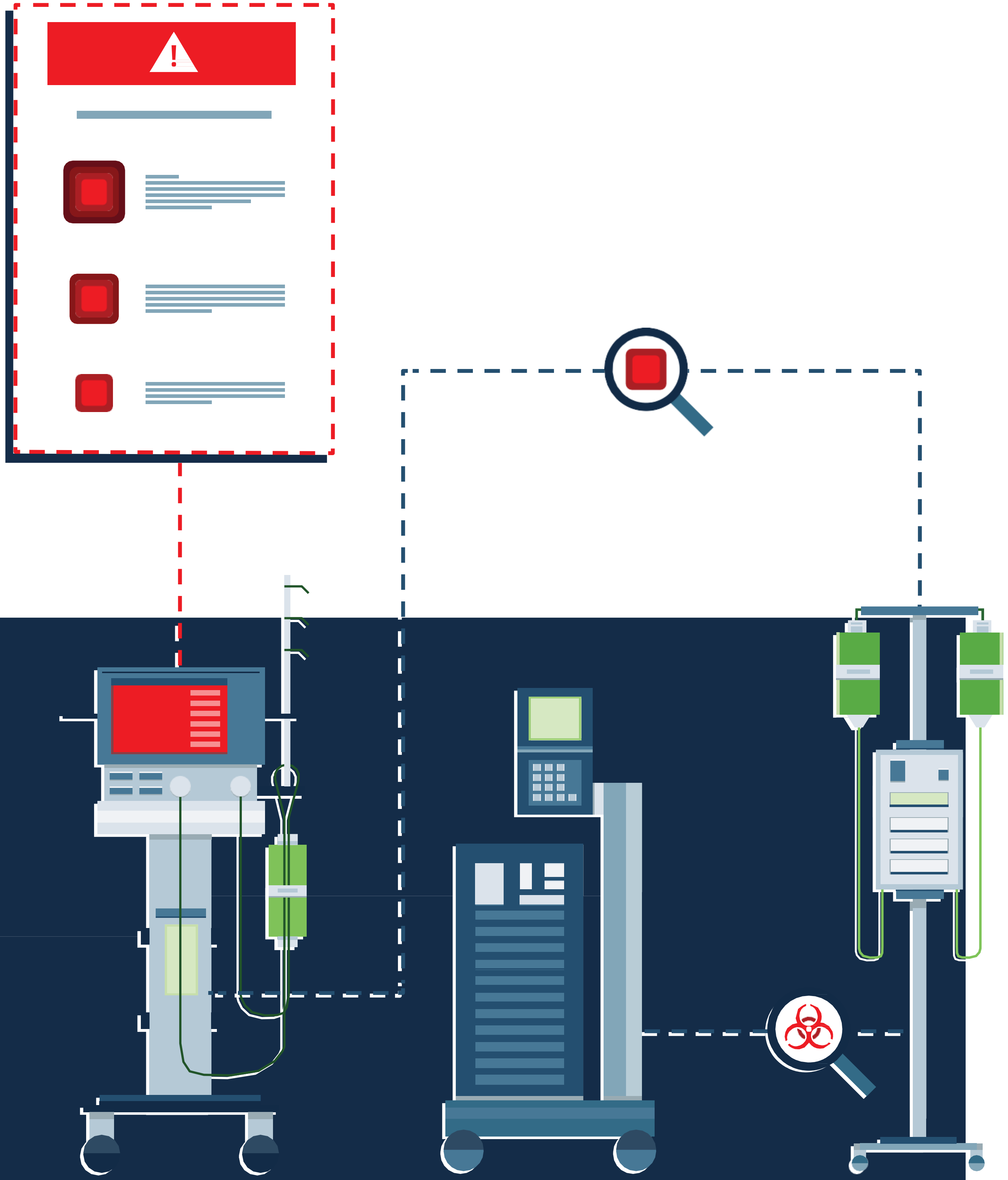
Check if the device transmits or receives unencrypted dataflows.

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.

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 cyber attack 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 cyber attack 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:

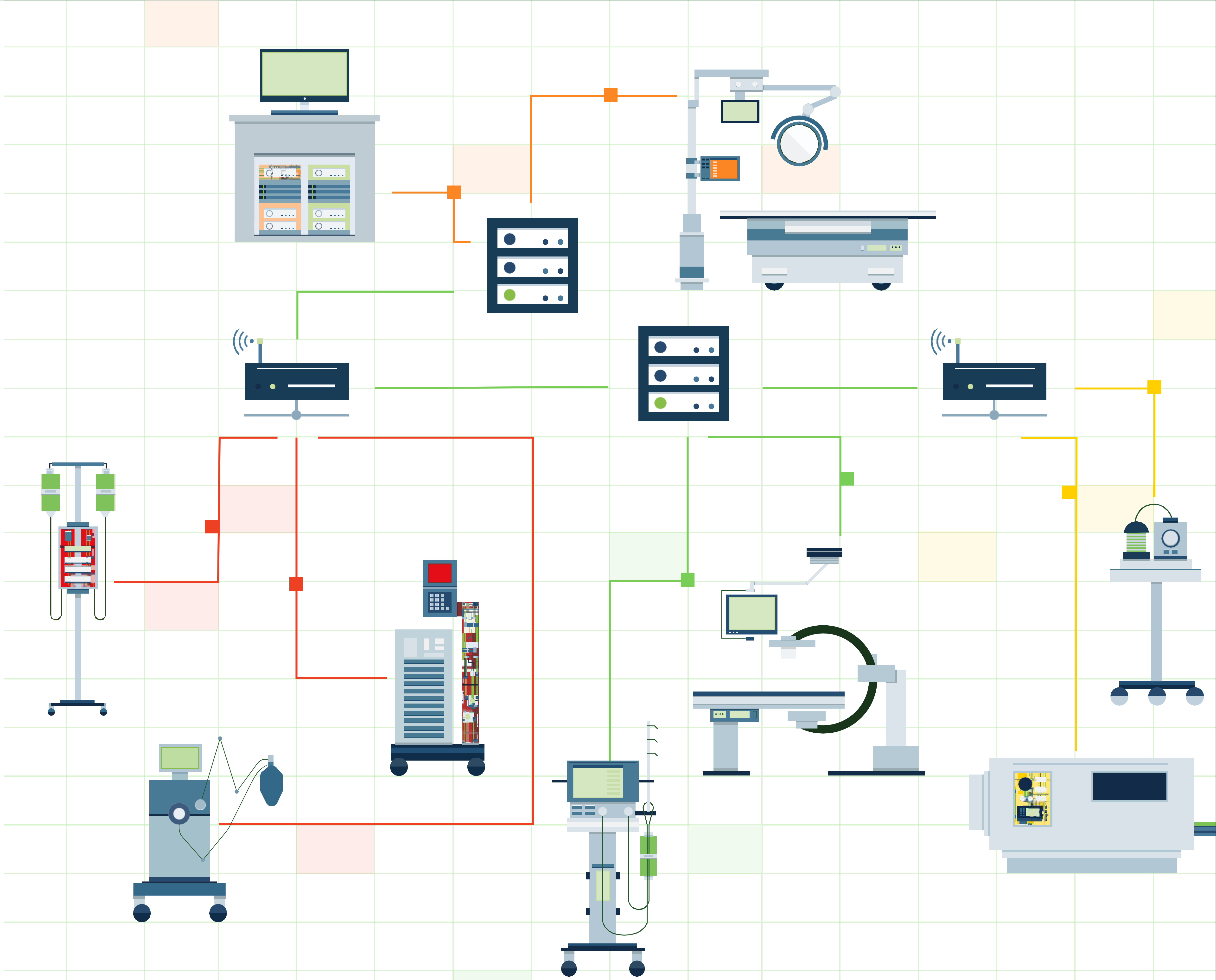
- **Confidentiality** — corresponds to the risk exposure of Protected Health Information (PHI) stored in or transmitted by the device
- **Integrity**—corresponds to the risk to patient safety for devices directly used in patient care
- **Availability**—corresponds to the risk of service disruption

	Patient Safety	Privacy	Service Disruption
Low	FDA Class I Medical Device; low-to-moderate risk to the patient or user	Device does not store PHI	Device failure cannot disrupt patient care
Medium	FDA Class II Medical Device; moderate-to-high risk	Device stores a small amount of PHI for a limited time period around a test or treatment	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	Device stores large amounts of PHI across multiple tests or treatments	Device failure can disrupt critical medical treatment such as surgery, respiratory equipment, or delivery of life-sustaining medication

- A successful cyber attack could disrupt clinical care and cause direct harm to patients.

03 THIRD PHASE

Protecting Connected Devices



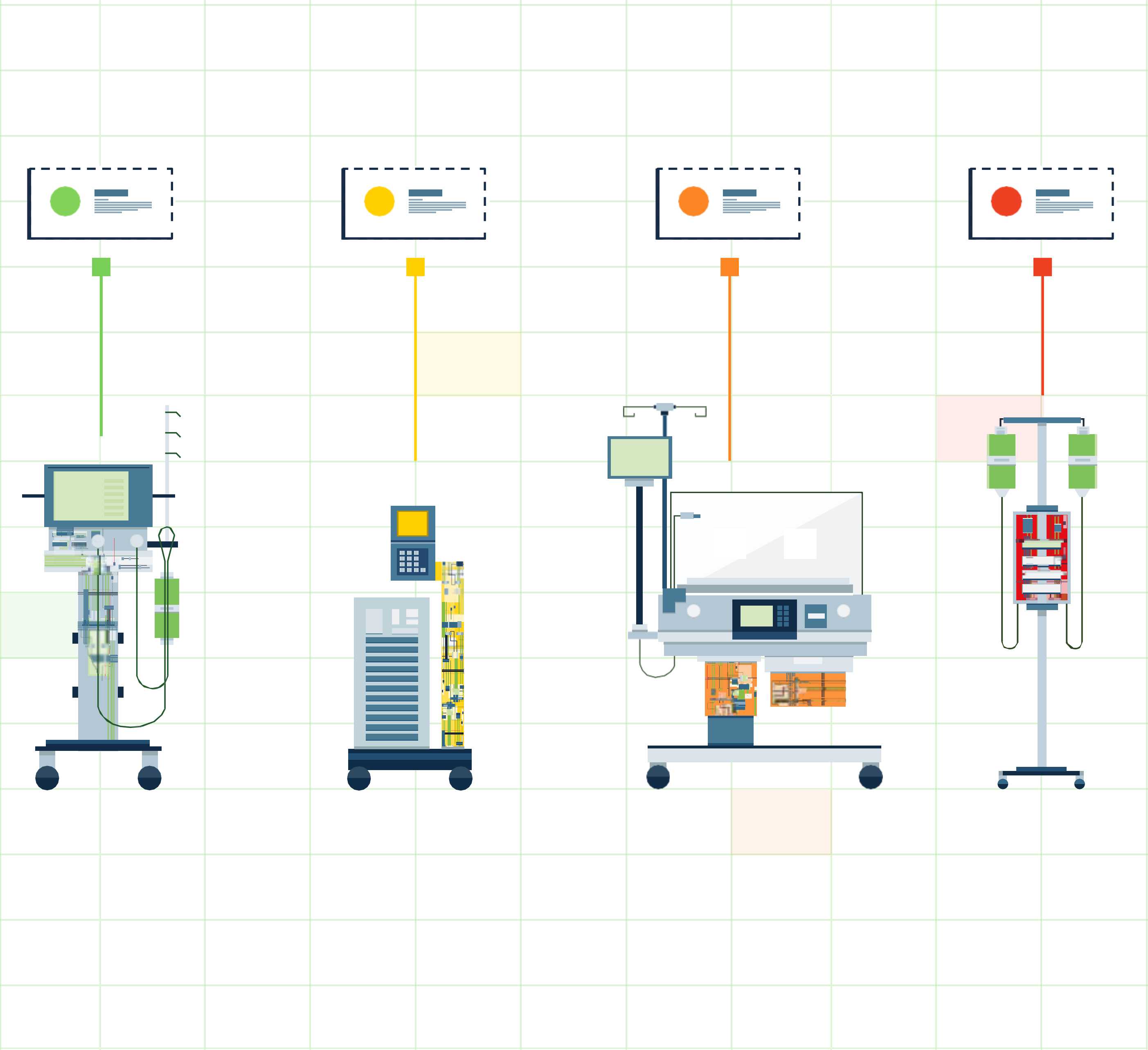
PROTECTING CONNECTED DEVICES

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, and the security team can focus on protecting devices whose risk score is beyond the acceptable level and apply the appropriate security measures to devices with different risk scores.

We advise protecting connected medical devices in four steps:

- **Protecting the device layer** — patching, disabling vulnerable services, adopting best-practice configuration
- **Protecting the network layer**—isolation at the LAN level, blocking unneeded communication within the local network, and isolation at the WAN level, allowing the device to communicate only with known external entities
- **Incident detection**—having a strategy in place to detect security incidents when they occur
- **Metrics and analysis**—ongoing analysis of security program results, adjustment, and improvement

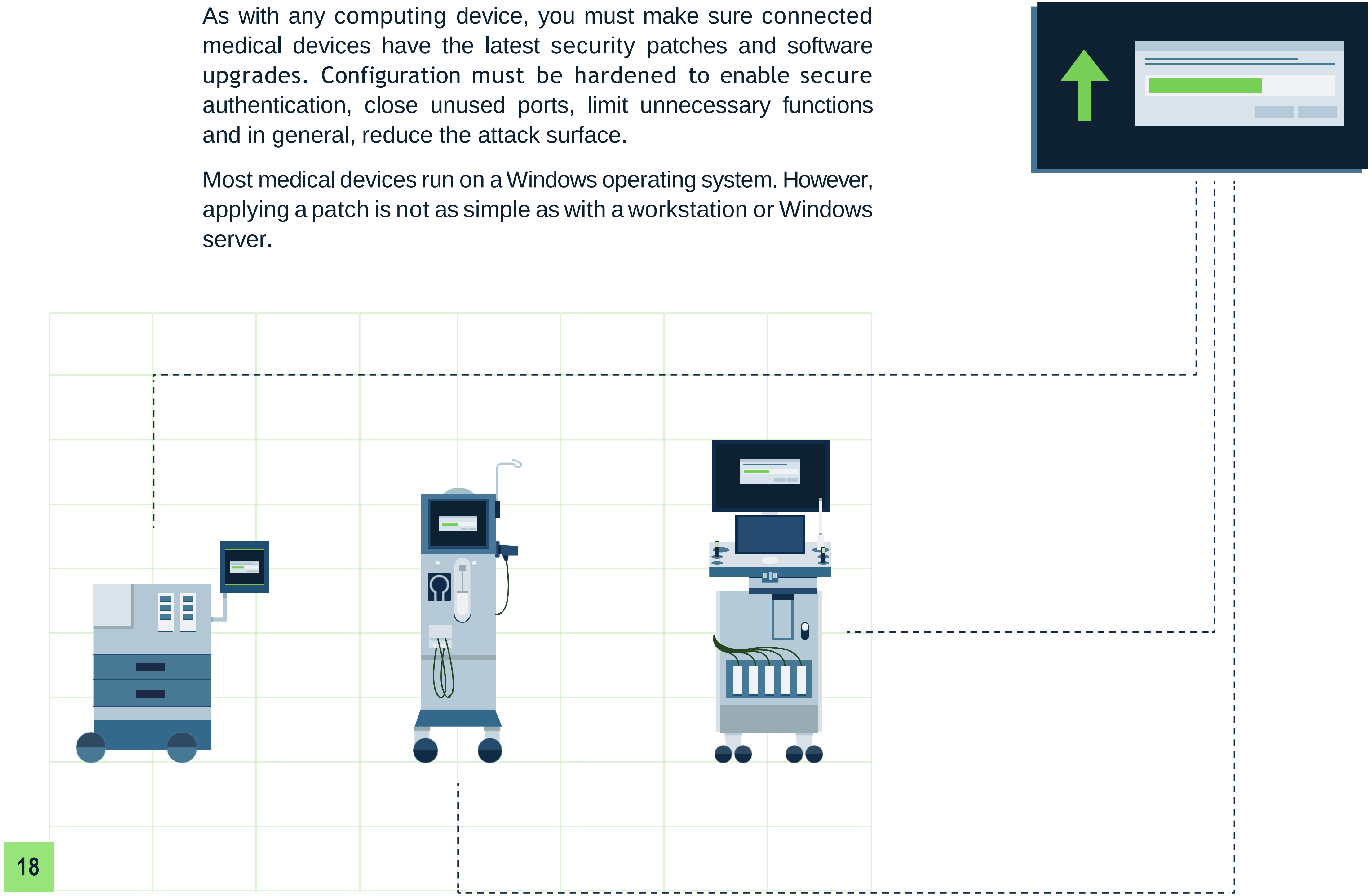


Each device should have a risk impact score

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 need to 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

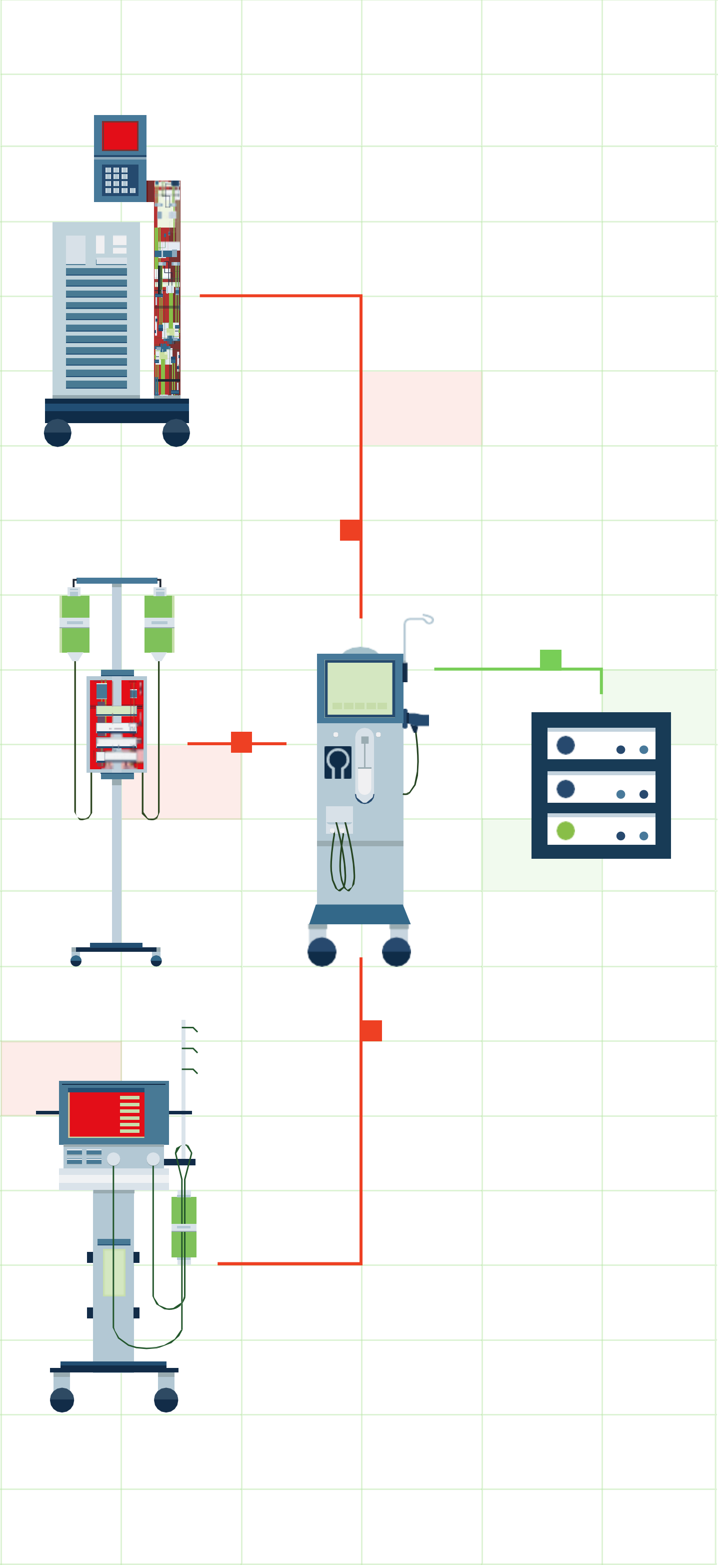
- You will not succeed in deploying all security patches or hardening all devices
- Focus on devices that have a high risk score
- Prioritize security patches or configuration changes that address the known vulnerabilities you identified in your risk assessment

Step 2.
Network Isolation

A key strategy to securing connected medical devices is to isolate them, as much as possible, from non-critical clinical communications, 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

> Isolation is key to securing connected medical devices and to limiting the attack surface.



Considerations When Isolating Medical Devices

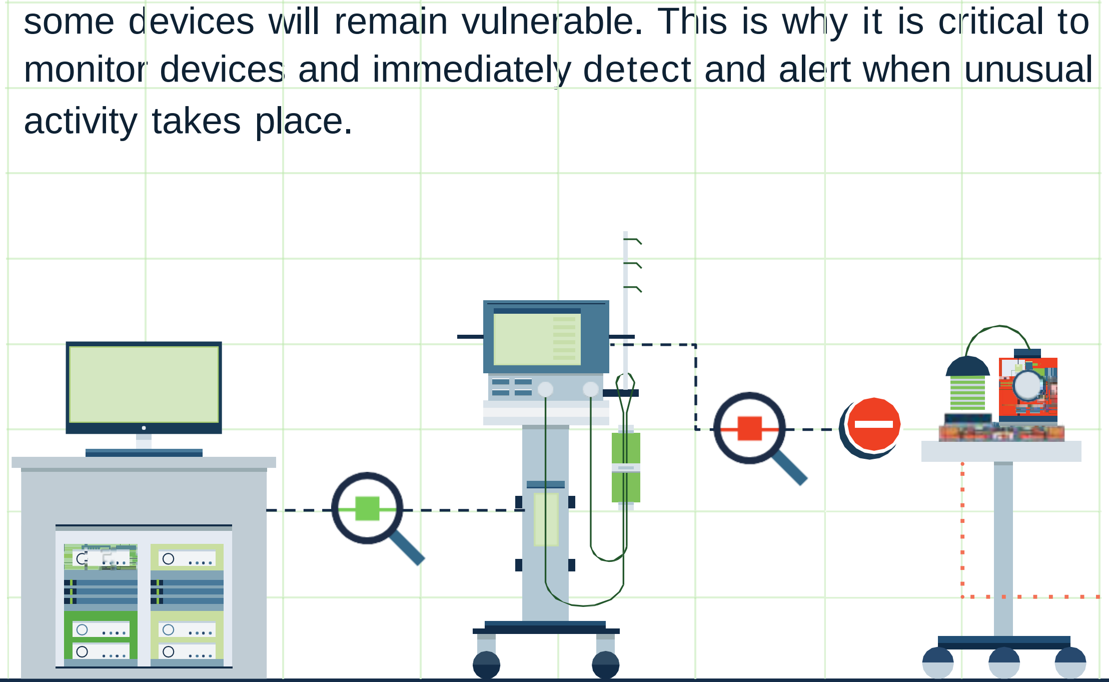
- Isolate clinical data flows from non-clinical data flows
- Clinical communications are essential, but any other communication should be blocked

Guidelines

- Set strict access policies and network segmentation to restrict non-essential communications 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
- Cooperate closely with clinical engineering and Healthcare Technology Management (HTM) to ensure you do not interrupt critical data flows

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, meaning 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 immediately detect and alert 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

- **There will always be critical legacy devices that cannot be replaced or fully patched or isolated, meaning the attack surface can be limited but not eliminated.**

Step 4. Metrics and Analytics

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

Create a Scorecard

Create a scorecard for medical devices with a timeline of risk scores, ensuring risk is reduced over time

Set KPIs

Set KPIs based on risk of important devices and monitor improvement; tie the KPIs to business goals like patient safety and service availability to get buy-in from leadership

Identify Activities

Identify activities and strategies that improved KPIs and reduced overall risk indexes

Collect Data

Collect data about risk indexes and historical behavior of devices, and use it for better procurement decisions