Cynerio

The State of Healthcare IoT Device Security 2022

A Cynerio Research Report

An industry report that examines the current outlook of connected medical device security in hospitals of all sizes.

Table of Contents

Background

For decades, patient care has seen improvements resulting from the data, insight and timeliness provided by connected devices. However, as the number of these devices has grown, so too have the number of threats, vulnerabilities, and entry points for bad actors within healthcare networks.

This Cynerio research report shines a light on the sorely under-addressed risks, threats and security issues related to IoT and related devices within healthcare environments. The information in this report is based on our analysis of over 10 million IoT and IoMT devices collected from current Cynerio implementations at over 300 hospitals and other healthcare facilities in the US and around the world, fully anonymized and analyzed by our Data Team. With hospitals under an unprecedented amount of strain from both the pandemic and the explosion of ransomware attacks on healthcare facilities, it has never been clearer that digital safety and patient safety are intimately intertwined, and that protecting the devices providing the care patients depend on is ultimately about safeguarding their health, safety and well-being.

Executive Summary

IV Pumps Are the Most Common Healthcare IoT Device and Possess the Lion's Share of Risk

The ubiquitous IV pump makes up 38% of a hospital's typical healthcare IoT footprint, and a whopping 73% of those IV pumps have a vulnerability that would jeopardize patient safety, data confidentiality, or service availability if it were to be exploited by an adversary.

53% of IoMT and IoT Devices Contain Critical Risks

More than half of connected medical and other IoT devices in hospitals have a known critical vulnerability. If attacked, these will impact patient safety, service availability or data confidentiality, either directly or as part of an attack's collateral damage. A third of bedside healthcare IoT devices, the devices closest to patient care that patients most depend on for optimal health outcomes, have an identified critical risk.

Urgent11 and Ripple20 Made Headlines, but the Most Common Device Risks Are Old Standbys

The most common IoMT and IoT device risks are connected to default passwords and settings that attackers can often obtain easily from manuals posted online. In contrast, vulnerabilities such as Urgent11 and Ripple20 were great for raising IoMT security awareness, but only affected about 10 percent of devices with attack vectors that are difficult for attackers to leverage successfully.

Healthcare IoT Running Outdated Windows Versions Dominate Devices in Critical Care Sectors

Medical devices running versions of Windows older than Windows 10 only make up a small part of a typical hospital's healthcare IoT infrastructure, but they account for the majority of devices used by pharmacology, oncology, and laboratory devices, and make up a plurality of devices used by radiology, neurology, and surgery departments. This leaves patients connected to those devices vulnerable, since those older versions of Windows are already past end of life and replacing the machines they run on will still take several years in most cases.

Most Healthcare IoT Devices Are Used Regularly, Making Them Difficult to Securely Update

Almost 80% of healthcare IoT devices get used monthly or more frequently, giving them little downtime for hospital security teams to analyze them for risks and attacks, apply the latest patches, and carry out segmentation to protect the devices on the network.

Linux Is the Operating System of about Half of Healthcare IoT Devices, the Other Half Is a Grab Bag

The open-source Linux platform is a popular choice for healthcare IoT operating systems, followed by dozens of mostly proprietary operating systems with small chunks of the overall footprint. This makes most IT security designed overwhelmingly for Windows machines a poor fit for healthcare IoT cybersecurity.

Network Segmentation Is Hugely Beneficial for Reducing Critical IoMT and IoT Risk

Segmentation that takes medical workflows and patient care contexts into account addresses over 90 percent of the critical risks presented by connected devices in hospitals and is the most effective way to mitigate and remediate most risks that connected devices present.

Introduction

The Healthcare IoT Cybersecurity Landscape - A Perfect Storm of Threats and Risks, Clouded by a Lack of Visibility

Over

500

healthcare breaches in 2021 -

US Department of Health and Human Services (HHS)

Ransomware attacks on hospitals increased

123%

in the past year -

2021 SonicWall Cyber Threat Report

Ransomware cost hospitals nearly

$21B

last year -

Comparitech

The percentage of healthcare breaches caused by connected devices is

=

To the percentage of healthcare breaches caused by phishing -

Ponemon Research Report: The Impact of Ransomware on Healthcare During COVID-19 and Beyond

The average hospital loses

$8M

per ransomware incident and takes 287 days to fully recover -

Emsisoft Report: The State of Ransomware in the US

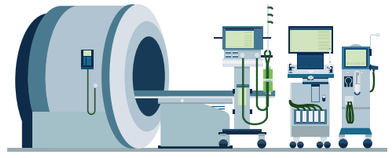
Healthcare is more targeted for cyberattacks than any other industry, absorbing 100 to 200% more attacks than the runner-up. It is healthcare that has led among all industries in how much their data breaches end up costing for over a decade now. Thanks to the volume of sensitive Personal Health Information (PHI) they contain that is useful for perpetrating identity fraud, medical records can fetch up to 50 times the amount that stolen credit cards get on the black market. Unfortunately, hospitals often lack visibility into the critical risks and attacks targeting the mushrooming array of connected medical, enterprise IoT, and industrial OT devices that are becoming increasingly common at all levels of patient care, with disastrous consequences. With the information in this report, collected and analyzed by Cynerio's data and research team from our platform's implementations at many different hospitals in the US and around the world, we hope to bring connected device security risks out of the shadows and into the light. What follows are hard numbers about the kinds of connected devices hospitals tend to have, the critical risks those devices contain, and how to best protect them as threats and attacks continue to evolve.

Healthcare IoT Devices Covered by This Report and Methodology

Before we get started, it is probably a good idea to define our terms clearly.
When it comes to healthcare IoT, we are dealing with several different categories of devices:

IoT (Internet of Things)

This is a blanket term for any network-connected device or other asset that is not considered traditional information technology (IT). Examples include security cameras, VOIP phones and smart door locks, but wouldn't include computers or servers.



IoMT (Internet of Medical Things)

These are IoT devices that have medical functionality. Examples abound in any hospital: MRI machines, IV pumps, heart monitors, glucometers. Perhaps these devices didn't have many internet connections a decade ago but going forward they almost always will.

OT (Operational Technology)

OT refers to hardware, software and communications systems that keep large-scale industrial equipment and assets running. For the purposes of hospitals, this usually includes devices like HVAC (Heating, Ventilation and Air Conditioning) systems, elevators, and electrical grids.

Connected Devices

These devices are remotely connected and controlled and are often simpler than any other device referenced above. Examples include a light switch or a coffee machine.

Methodology

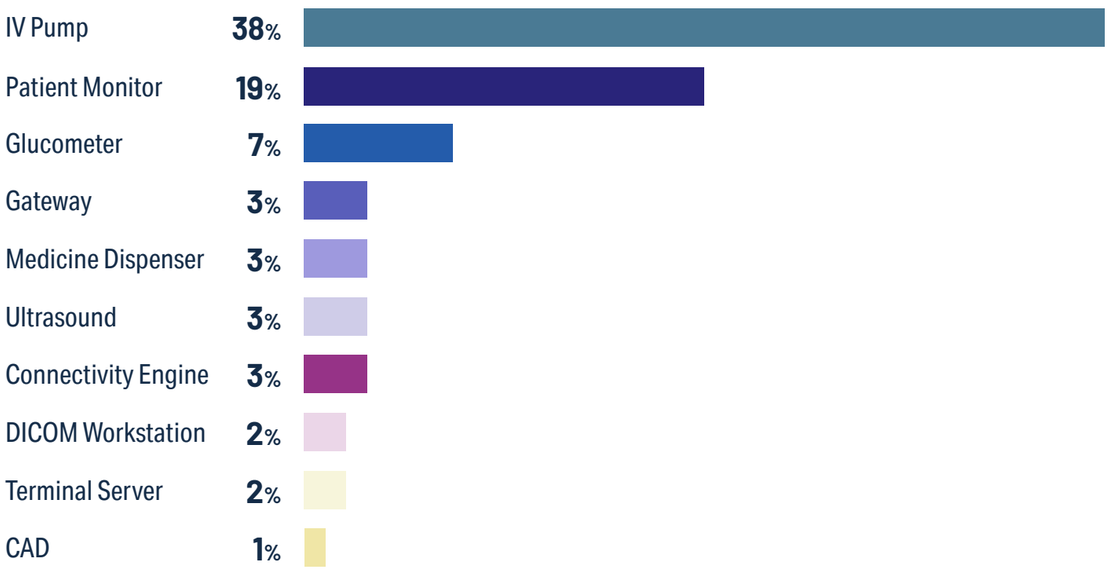
Cynerio collects detailed information about a hospital's connected device footprint through a patented connector that is typically placed on the core switch's SPAN port. This allows Cynerio to passively monitor the network traffic of connected devices immediately without putting confidential data at risk. Using our research team's deep healthcare expertise Cynerio can parse hundreds of proprietary device protocols to analyze device metadata, classify devices, and compile information about their risks and vulnerabilities. Analysis is performed through a combination of meticulous investigation by the Cynerio research team and artificial intelligence. Cynerio does not analyze or collect any electronic personal health information as part of this process. The data in this report is based on our analysis of over 10 million IoT and IoMT devices collected from current Cynerio implementations at over 300 hospitals and other healthcare facilities in the US and around the world. All data is completely anonymized.

What Healthcare IoT Device Footprints Look Like Right Now

What are the most common healthcare IoT devices in hospitals?

Infusion pumps were by far the most common connected device in hospitals, accounting for 12 percent of all connected devices, and 38 percent of all IoMT devices detected by Cynerio. Why are IV pumps so common compared to any other device? Most patients will need fluid administered during their hospital stay, and infusion pumps help medical personnel reduce the margin of error when doing so by regulating the amount and rate of fluids being given.

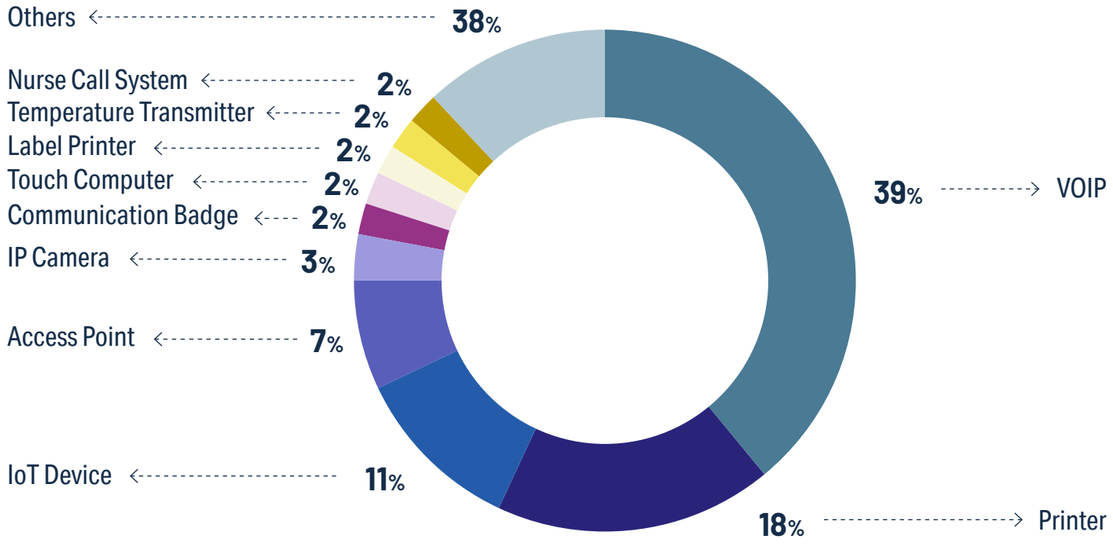
Top Connected Devices in Hospitals (as a percentage of all IoT/IoMT devices)



What are the most common non-medical IoT devices in hospitals?

While the devices listed here are not medical devices per se, they do facilitate medical outcomes. VOIP phones permit doctors to communicate with the lab where patient results are determined. Printers allow lab reports to be generated and stored for later reference. Access points determine who can get in or out of a restricted area like an operating room. If these devices are disabled in the event of a ransomware attack, the knock-on effects could easily affect patient health outcomes. While Cynerio was originally designed to specifically address the risks of medical devices, our healthcare customers immediately helped us realize that all connected devices in hospitals can present risks to patient safety and data confidentiality, and as a result Cynerio works to secure all connected devices in medical environments.

Top "Non-Medical" Connected Devices in Hospitals (as a percentage of all IoT/IoMT devices)



What percentage of healthcare IoT devices are used regularly?

Most devices get used at least once a month. While this is great in terms of hospitals getting a good return on their investment when it comes to device utilization, this has consequences for the security of those devices. If they are constantly in use, it means that it can be difficult to find a good time to update the security of devices that may need a patch or get a system upgrade.

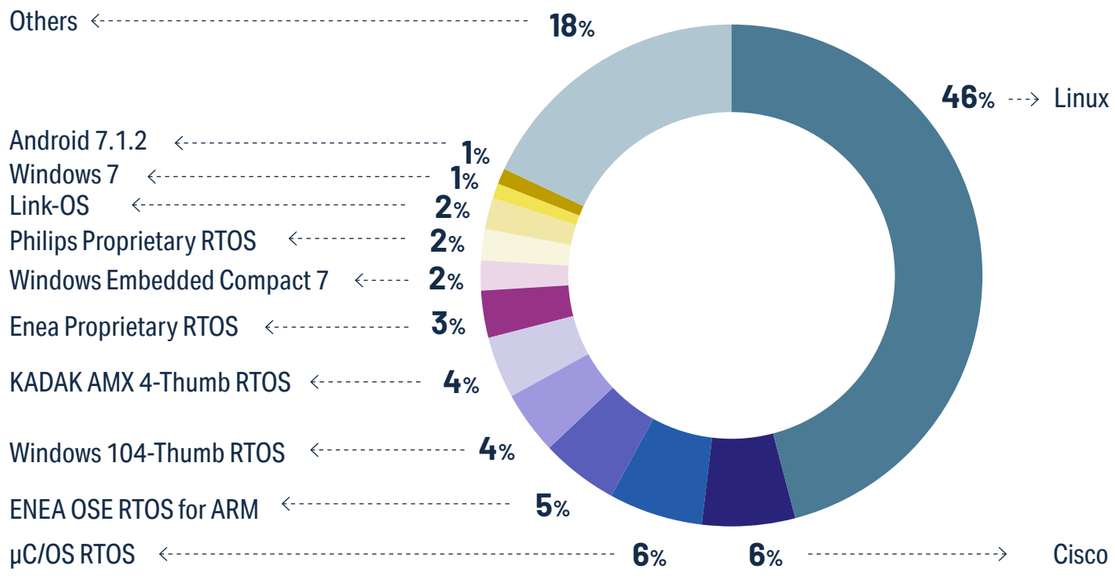
79%
Devices Used in the Past 4 Weeks

21%
Devices Not Used in the Past 4 Weeks

What Are the Most Common Operating Systems in Healthcare IoT Devices?

Unlike the IT world, where Microsoft Windows dominates the desktop, healthcare IoT is all over the map. In terms of security, this makes solutions like Endpoint Detection and Response (EDR) agents almost impossible to deploy – there is no way for those kinds of solutions to address the vast variety of operating systems that power devices created by different manufacturers for different medical purposes. IoT security needs to be tailored to the device level, since it is unlikely that hospitals will have solutions for most proprietary and diverse operating systems. That being said, nearly half of medical devices run on Linux, an open source platform renowned for its stability and possibilities for customization.

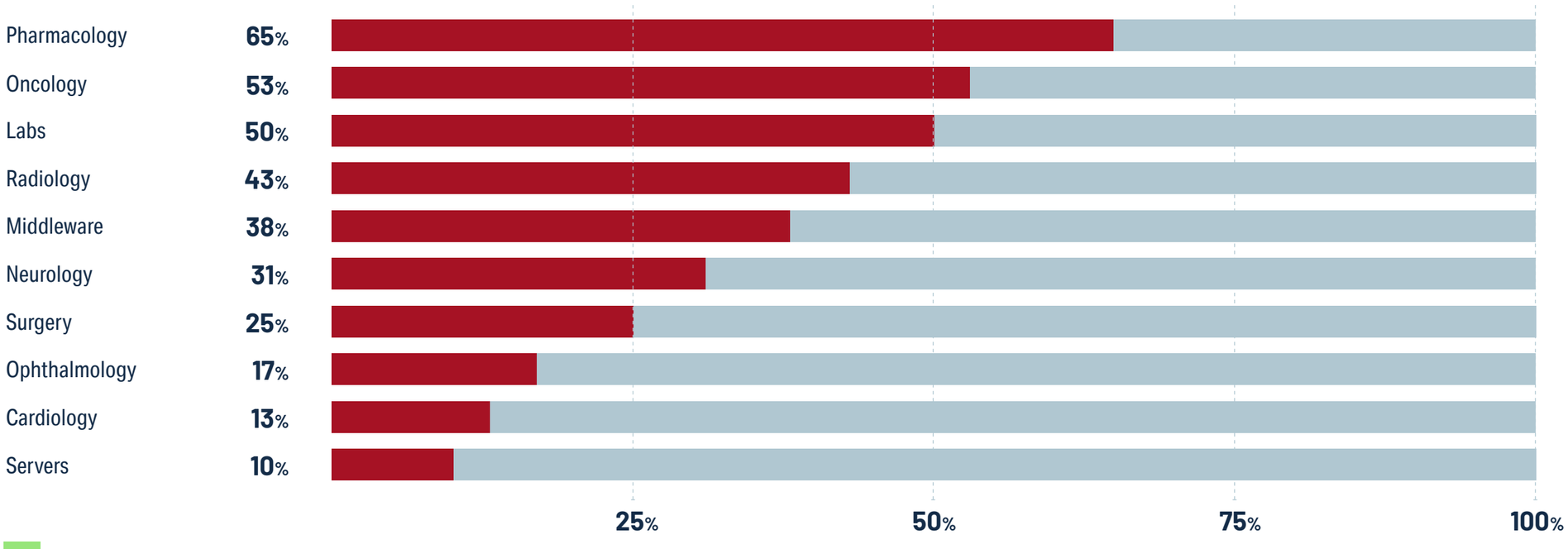
Top Operating Systems of Healthcare IoT Devices (by percentage of total IoT devices)



Which Hospital Departments Depend the Most on Windows Devices Running a Version Older than Windows 10?

Windows devices are not the biggest chunk of IoT and IoMT device operating systems, but where they do exist, they tend to concentrate in departments of the hospital responsible for the direct care of patients. The security implications of Windows dominating in these critical departments is that most malware and ransomware is designed to attack Windows devices, and will more easily threaten devices running on that operating system, especially if they are older devices running versions of Windows that are no longer updated or patched. This can leave the patients connected to those devices vulnerable, as well as the data those devices contain. Windows 10 offered significant security improvements, so identifying and addressing the risks of prior versions should be considered an IT priority.

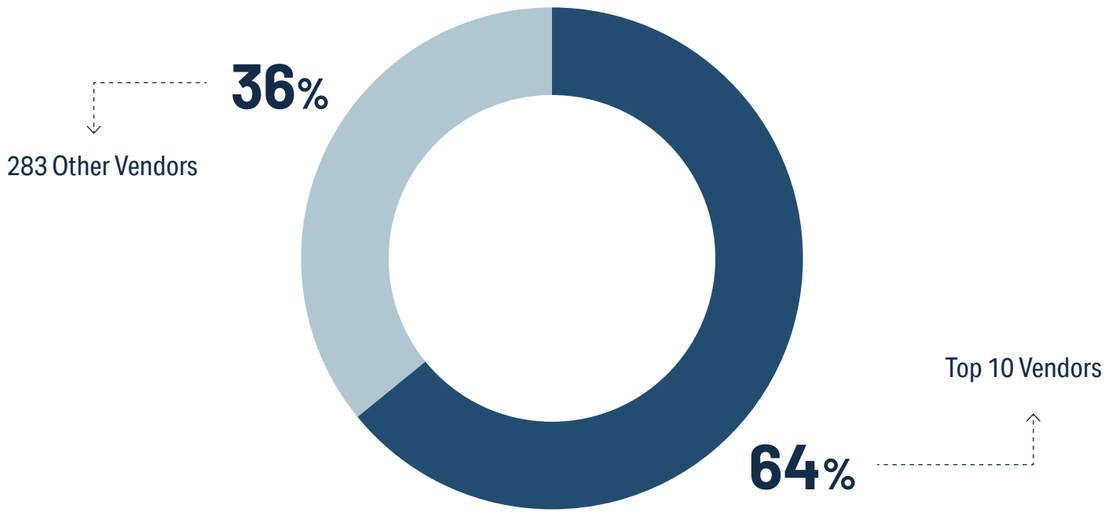
Hospital Departments Using the Most Devices with Outdated Windows Versions (by percentage of total devices)

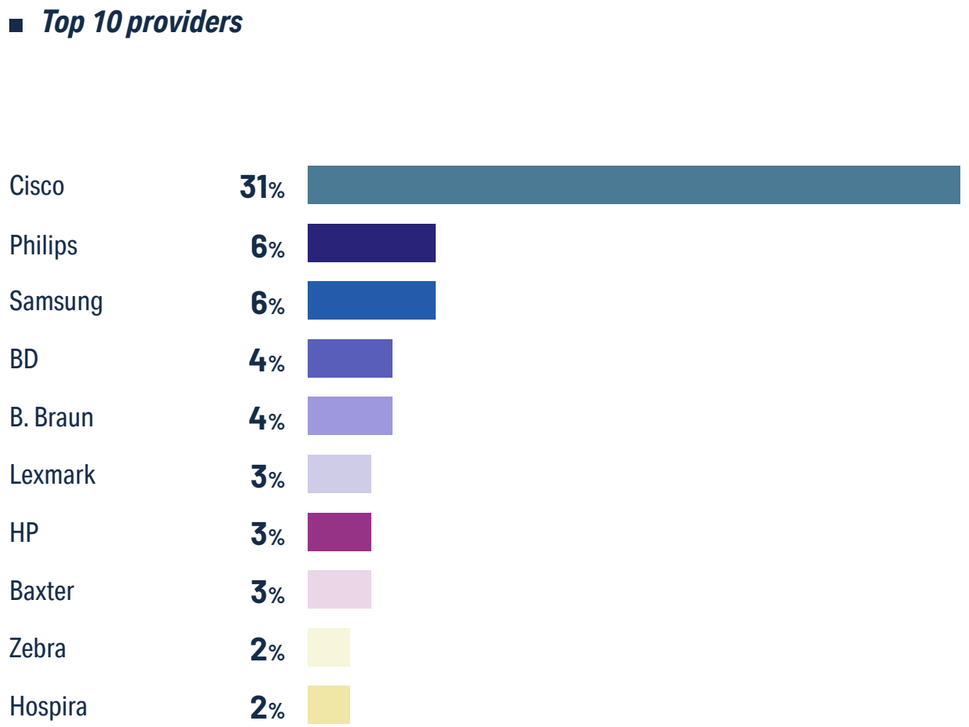


What Are the Most Common Device Manufacturers in Healthcare IoT?

Device vendors are a much more diverse lot than computer or mobile phone manufacturers, where a few big names tend to dominate. Aside from Cisco, whose dominance of many telecommunications devices is well-documented, device manufacturers tend to vary based on the type of device. This creates complexity when it comes to healthcare security – without specialized expertise in the security vulnerabilities of each device at scale, it becomes too labor-intensive to manually secure each kind of device as new vulnerabilities and risks appear.

Top Healthcare IoT Device Vendors (by percentage of total IoT devices)





Among the vendors identified, many may not be expected in healthcare environments. Care is not always about the core medical treatment. In many cases it is about patient comfort, resulting in manufacturers such as Sony, Nintendo, Roku and even Tesla introducing risk to patients.

The Real Healthcare IoT Risk Landscape

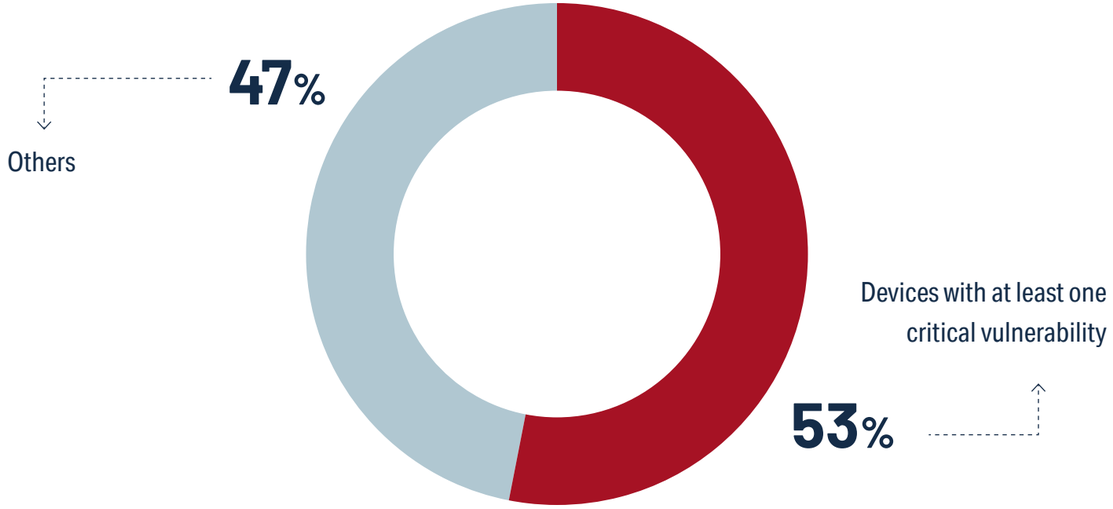
A Note about Cynerio's Risk Scoring Methodology

To measure the risk of healthcare IoT devices, Cynerio uses an adjusted CVSS (Common Vulnerability Scoring System) level that is standardized according to the NIST Cybersecurity Framework and adjusted based on temporal and environmental factors. CVSS risk scores supply a good baseline for considering risk, but at Cynerio and in healthcare more generally it is important to include information related to whether a given vulnerability will affect patient safety, data confidentiality, or the provision of healthcare services if an attacker is able to exploit it.

Devices with at least one critical vulnerability that would affect patient safety, data confidentiality or service availability (as a percentage of all IoT devices)

What percentage of devices have a critical vulnerability that would affect patient safety, data confidentiality or service availability?

Without robust healthcare IoT security in place, hospitals are sitting on a ticking time bomb. A ransomware attack may be able to take down the majority of their IoT infrastructure and the hospital won't have any visibility into how to proactively prevent the attack or shut it down once it is launched. More than half of healthcare IoT devices currently in hospitals have a risk factor considered to be critical.



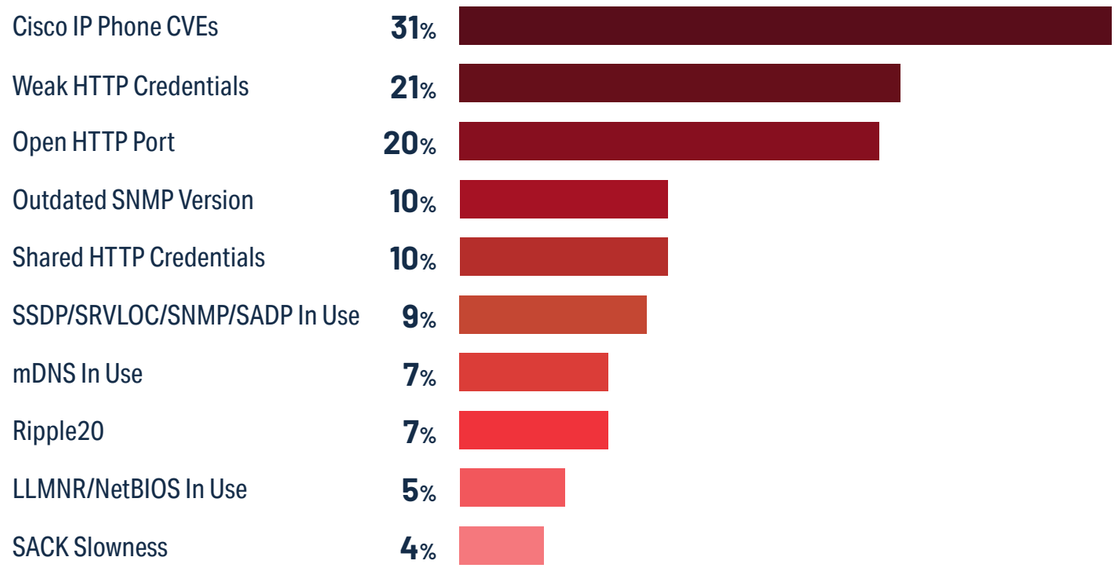
What Are the Most Common Healthcare IoT Device Vulnerabilities?

If you read healthcare IoT security headlines from the past year, you might get the idea that widely reported vulnerabilities like URGENT/11 or Ripple20 are the most common risks facing these devices. Of course, hospitals should make sure to protect against these vulnerabilities, and the many articles that were written about these security flaws were great for creating general awareness around healthcare IoT security, but they make up only a small part of the risk most healthcare IoT devices face.

The most common healthcare IoT risks are often much more mundane, and in line with the kinds of vulnerabilities we have seen across IT in the security industry for years. In many cases, a lack of basic cybersecurity hygiene is what is leaving healthcare IoT devices open to attack. Devices often come with default passwords and settings that remain unchanged, and are accessible in device manuals that can easily be found by attackers online. Without IoT security in place, hospitals don't have a simple way to check for these risks before attackers are able to take advantage of them.

Usually without healthcare IoT, security hospitals can still identify risky devices with lousy passwords, but shutting down services and changing passwords is going to be hugely difficult and complex. Most likely it just won't get done without a dedicated healthcare IoT security solution, leaving those devices vulnerable.

Top 10 Vulnerabilities and Percentage of Devices Impacted



URGENT/11 ranked 12th, making up 4% of total vulnerabilities.

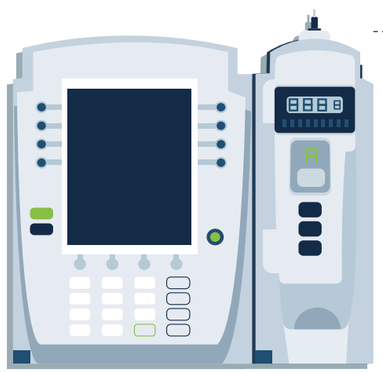
What Are the Bedside Healthcare IoT Devices with the Most Identified Vulnerabilities?

A glimpse into the devices closest to patients

The closer a healthcare IoT device gets to the patient's bedside, the higher the risk score of a vulnerability detected on it will increase, since it has a much greater chance of adversely affecting a patient's care. When Cynerio technology first enters a hospital environment where there has never been any healthcare IoT cybersecurity before, these are the devices that most commonly have a critical risk while connected to a patient.

Bedside devices with highest rates of critical risk

■ 1



73%
IV Pump

■ 2

50%
VOIP

■ 3

Ultrasound

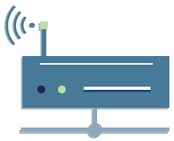
■ 4

Patient Monitor

■ 5

Medicine Dispenser

■ 6



Gateway

■ 7

IP Camera

■ 8

PACS Server

■ 9

Computerized Radiography System

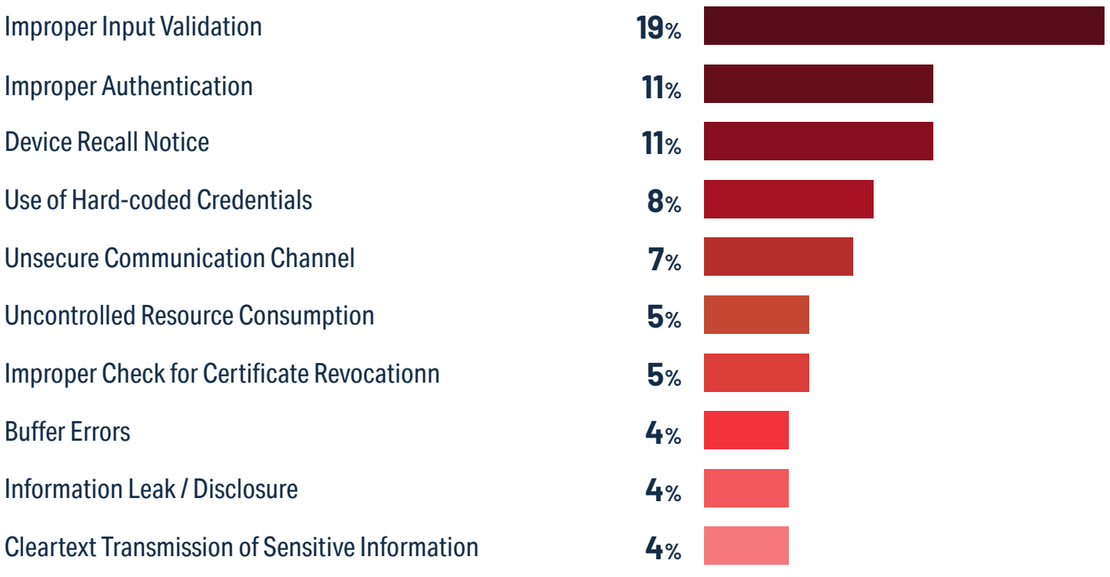
■ 10

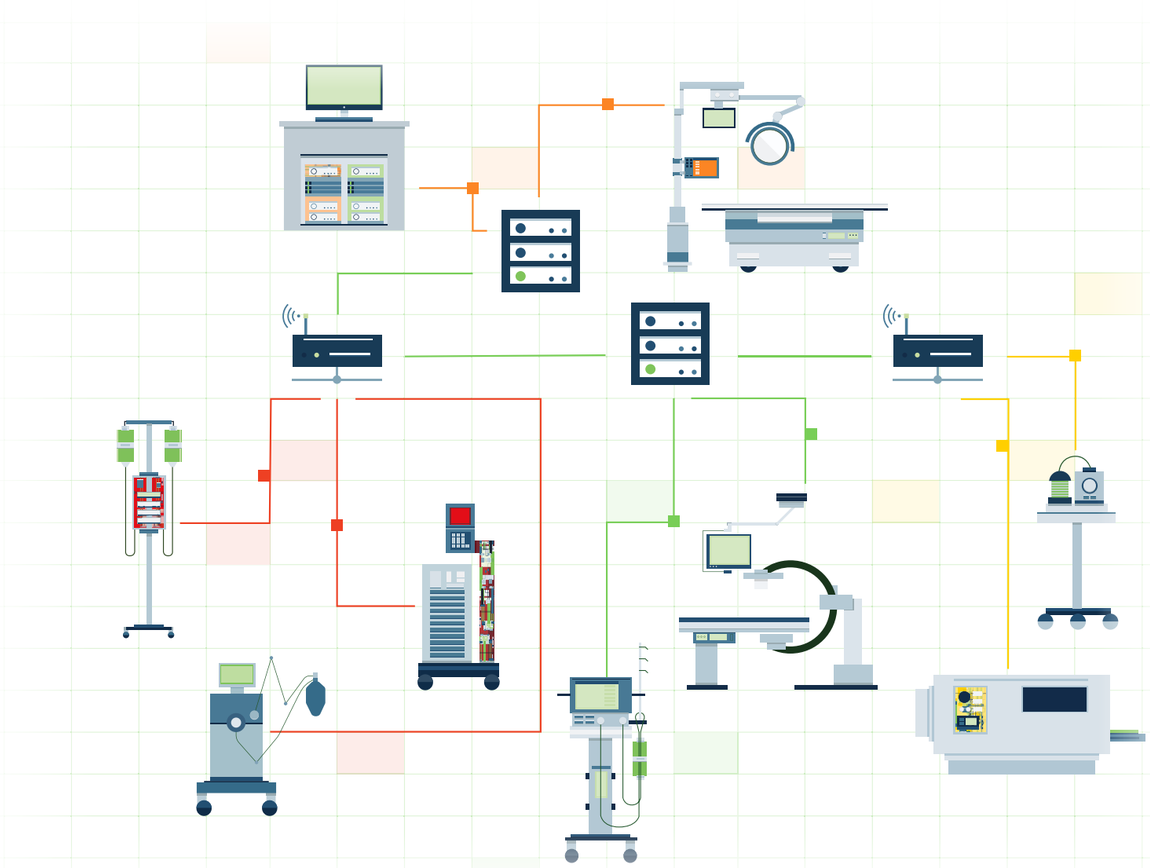
DICOM Workstation

What Are the Most Common Vulnerabilities of Bedside Devices?

Any vulnerability that appears while a device is connected to a patient takes on a higher risk profile simply because it will have an outsize effect on the potential health of the patient depending on that device. Major announced vulnerabilities from 2021 don't really add up to the biggest risks here; the top concern is that hospitals don't have enough visibility into very basic vulnerabilities like whether a device has an active recall or has been improperly authenticated. The good news is that common and basic vulnerabilities like these are easy enough to address with the right tools in place, as we will explore in the following sections.

Frequency of vulnerabilities found in bedside devices
(as a percentage of all devices with the vulnerability)





How To Effectively Address Healthcare IoT Risk

Before we dive into how to successfully manage healthcare IoT risk, it is important to define a few terms that tend to get used interchangeably when it comes to cybersecurity – remediation, mitigation, and acceptance of risk.

Remediation

Fixing or patching a root cause to the point that the identified risk is completely expunged.

Mitigation

Implementing controls that significantly reduce the likelihood of risk being realized.

Acceptance

Allowing a risk to go unaddressed based on various factors such as low criticality, remote probability, or prohibitive level of effort required to mitigate or remediate further.

Patching Not Always An Option

In the best-case scenario, a risk can be fully remediated so that it no longer exists; for example, through a patch from a vendor for the vulnerability in question. But this is not always possible, especially in a field as varied as IoT devices that run on hundreds of different operating systems and are manufactured by a plethora of different vendors. Additionally, when it comes to medical devices specifically, long device lifecycles tend to mean that devices will outlast the period when a manufacturer even offers updates to prevent newly discovered vulnerabilities from potential exploitation. That makes mitigation the best available option when remediation is unviable. Mitigating a risk through "virtual patching" is often the best possible security alternative so that vulnerabilities and risks a manufacturer will no longer patch themselves can still be protected against.

Quarantine and Segmentation

There are two types of best practice response actions when it comes to device risks and attacks: the immediate reactive quarantine put it place to shut down a risk or attack that could affect a patient's data, safety, or care, and then the longer-term proactive segmentation meant to pre-empt future attacks before they can be launched. Hospitals should have a way to respond immediately when a threat could imminently affect the hospital and its patients, and they should also have a long-term vision to harden the security around devices so that they can't be leveraged in attacks going forward.

The Importance of Segmentation to Robust Healthcare IoT Cybersecurity

A large, unsegmented network presents a large attack surface that can give adversaries who do manage to gain access free rein to move laterally across critical data and resources. Network segmentation divides a network into multiple parts, which are called segments, with each segment acting as an isolated sliver of the network. In broad terms, more segments mean a more secure network since they make traversing the network without authorization much more difficult for adversaries. Nevertheless, the right amount of segmentation is a balance that won't hinder network connectivity but also won't leave the network open enough to create security risks. Typically, segmentation will be carried out by using Virtual Local Area Networks (VLANs) to break the entire network down into its segments.

Traditional IT security solutions struggle to segment healthcare IoT devices. Common solutions for segmenting IT like firewalls and Network Access Control (NAC) usually can't differentiate between medical devices, accurately assess risk criticality on healthcare IoT, or provide visibility into device connectivity. Because of this, IT security simply cannot provide a high level of confidence that device functionality, and by extension patient safety and care, won't be affected when attempting to segment healthcare IoT with it. Medical-first healthcare IoT solutions that can rigorously test proposed segmentations to ensure no disruption to critical operations are required to effectively contain attacks without negative consequences to patient safety and care.

How Much Critical Risk Does IoT Healthcare Device Segmentation Address?

If a given healthcare IoT risk is critical, or a healthcare IoT device has a critical risk on it, segmentation is hugely beneficial. In fact, effective healthcare IoT segmentation addresses 92% of critical risks detected and reduces the risk for 67% of devices that have a critical risk.

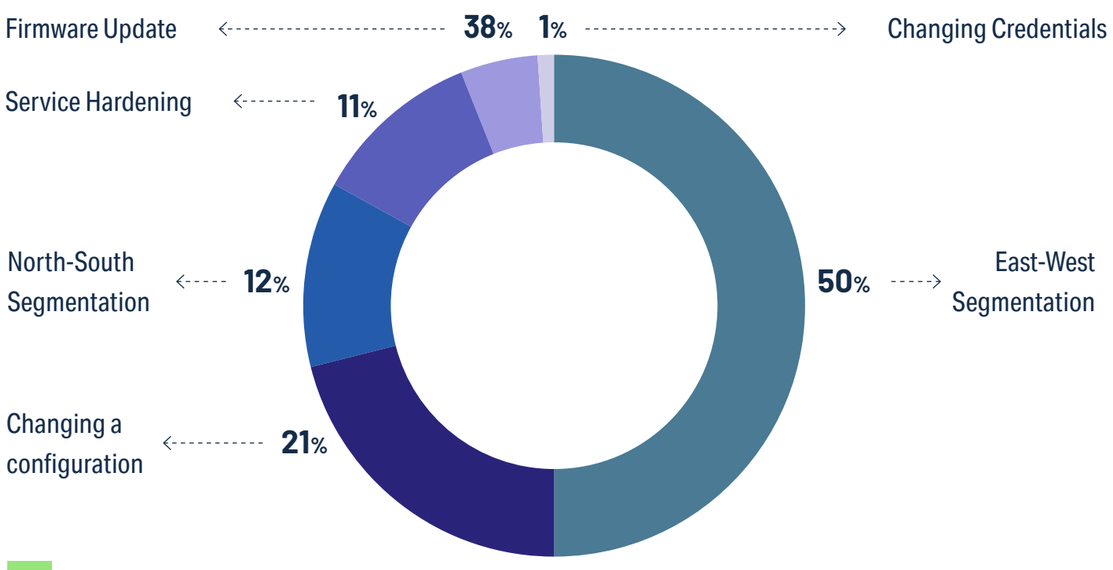
> Effective healthcare IoT segmentation addresses
>
> **92%**
>
> of critical risks detected and reduces the risk for 67% of devices that have a critical risk.

What Are the Most Common Ways to Segment Critical Risks on Bedside Devices?

Not all IoT healthcare network segmentations are created equal; they need to be crafted according to the potential threat vectors they are addressing as well as the potential vulnerabilities that could be exploited and the clinical context of each device in the segment.

It is also worth highlighting the two main forms of segmentation – east-west and north-south. East-west segmentation blocks all essential device-to-device communication across the LAN, while north-south segmentation blocks all non-essential communication to prevent malicious entities within the network from exfiltrating data. Of course, devices can have more than one risk factor present at the same time and require multiple segmentation actions.

Most Effective Strategy for Segmenting Bedside Device



The Future of Healthcare IoT Security

Where do we go from here? The trend is already clear – it's too late to merely start an IoT asset inventory count as a baseline project to start getting control of medical device security at a hospital. Attackers are already leveraging any vulnerability they can find on hospital networks and using them to launch ransomware attacks and steal protected health data. Even so, most IoT healthcare cybersecurity is still focused on providing a comprehensive inventory of connected devices, perhaps with some data related to their potential risk. But these solutions don't provide a way to fight back against threats, and you can't protect against what you can't remediate. Hospitals don't need more data – they need to be able to act decisively when attacked.

Identifying and addressing risk vectors that are already being leveraged in the wild is a good first step towards implementing healthcare IoT security that will make a hospital's connected device footprint more resilient. We expect that there will be a broader acceptance of such mitigating controls for healthcare IoT as the footprint of these devices quintuples in the next decade. But hospitals also need solutions in place to respond to live attacks when "the wild" is suddenly at their doorstep. Attackers motivated by money and indifferent to the care they may be adversely impacting will look for the lowest-hanging fruit to attack, and hospitals will need to speed up their time to attack detection as more hospitals increase their healthcare IoT security fortification. As IT security moves to an XDR (Extended Detection and Response) model to automate incident identification and remediation, healthcare IoT will need to move towards an attack detection and response model as attacks continue to evolve and target the healthcare sector more than any other.

About Cynerio

Cynerio is the one-stop shop Healthcare IoT security platform. With solutions that cater to healthcare's every IoT need – from Enterprise IoT to OT and IoMT – we promote cross- organizational alignment and provide hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We empower healthcare organizations to stay compliant and proactively manage every connection on their own terms with real-time IoT attack detection and response and rapid risk reduction tools, so that they can focus on healthcare's top priority: delivering quality patient care.

The Cynerio Platform consists of three solutions that go beyond healthcare IoT asset management to defend IoT and connected medical devices from ransomware and other live attacks from day one, while also identifying and remediating the most critical device risks in under a month.

Attack Detection and Response (ADR)

Cynerio's Attack Detection and Response for Healthcare IoT empowers hospitals to identify, contain and mitigate threats on devices exhibiting malicious or suspicious behavior so that patient health and service provision won't be impacted. Thorough remediation, including the collection of actionable forensics, can then be performed when the device is not in use to accelerate rapid attack recovery.

Rapid Risk Reduction (RRR)

Cynerio enables hospitals and healthcare facilities to get unparalleled visibility into their IoT, OT and connected medical devices, reduce their vulnerability and risk, and immediately respond to ransomware, breaches and other threats aimed at them. Don't just identify connected devices using asset management – secure them to ensure that they are an integral part of protecting patient safety, care, and data.

Technical Account Manager (TAM)

To help effectively address IoT security challenges in hospital environments, Cynerio provides its leading healthcare IoT security platform with long-term Technical Account Managers (TAMs) that handle deployment and optimization of the solution with minimal resources required. TAMs work with your IT, Security, Network, BioMed and other team members to integrate Cynerio with existing technology stacks while also providing the valuable guidance needed when addressing risks and attacks on Medical IoT devices.

For more information, visit cynerio.com and follow us on Twitter @Cynerio.

Cynerio

Secure. Faster

Healthcare IoT Cybersecurity