CLAROTY

TEAM82

STATE OF CPS SECURITY REPORT

HEALTHCARE 2023

An analysis of the cybersecurity trends and events impacting medical device security and the overall healthcare industry

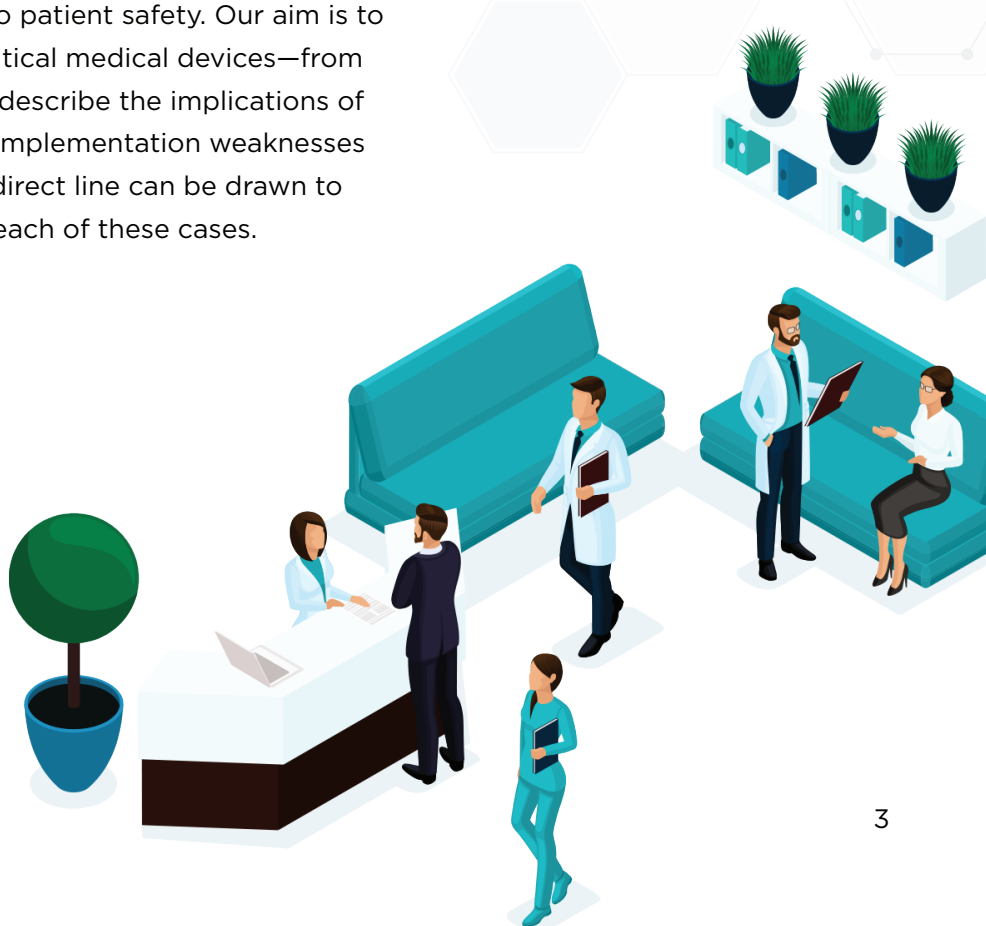
TABLE OF CONTENTS

EXECUTIVE SUMMARY

We have been conditioned as an industry to equate healthcare cybersecurity with data privacy. The Health Insurance Portability and Accountability Act (HIPAA) has been the impetus for this approach for 27 years by zeroing in on the protection of personal patient information and enacting privacy and security rules aimed at keeping such data confidential.

For its time—especially as data breaches ran wild in the early 2000s—that strategy was sufficient as the totem for healthcare-related cybersecurity. Today, disruption to the availability of connected medical devices can severely impact patient care and quality of life. Moving forward, as more connected medical devices and patient systems come online, we expect to see a rising tide of cyberattacks focused on disrupting hospital operations.

In Team82's first "State of CPS Security Report: Healthcare 2023," we examine these cybersecurity challenges to patient safety. Our aim is to demonstrate the broad connectivity of critical medical devices—from imaging systems to infusion pumps—and describe the implications of their exposure online. Vulnerabilities and implementation weaknesses frequently surface in our research, and a direct line can be drawn to potentially negative patient outcomes in each of these cases.



Throughout this report, we demonstrate from our research:

The breadth of medical devices that contain known exploitable vulnerabilities that attackers may leverage and have a clear negative impact on patient safety.

Traditionally, medical devices have replacement schedules based on mean times for component failures, and not on cybersecurity concerns. This has led to the continued use of vulnerable legacy devices, that if exploited could lead to negative patient outcomes.

The proliferation of remotely controlled and monitored devices has introduced architectural weaknesses, such as medical devices bridging networks, and the risk those present. This significantly elevates a hospital's exposure to external threats.

Our provocation is that healthcare delivery organizations (HDOs) are at a pivotal point where cybersecurity can no longer be a reactive exercise. It must be a core business and strategic consideration for HDOs and manufacturers alike, and we hope this report informs decision-makers and policymakers as to where the major cybersecurity issues lie and the risks they must take into account.

Key Findings

The data points and trends in this section represent the key takeaways from our research. They illustrate the exposure of medical devices and implementations to attacks, and demonstrate areas where risk mitigations should be prioritized.

Known Exploited Vulnerabilities in Medical Devices

The Cybersecurity and Infrastructure Security Agency (CISA) maintains a growing catalog of Known Exploited Vulnerabilities (KEVs). KEVs that exist on hospital networks are particularly alarming, because these exposures have exploits written to compromise them, and are therefore easily compromisable. 63% of KEVs tracked by CISA can be found on healthcare networks, while 23% of medical devices—including imaging devices, clinical IoT devices, and surgery devices—have at least one known exploited vulnerability. Complicating matters is that users must contend with 360 medical device manufacturer (MDM) patch certification programs to ensure compliance requirements and verify that products provide reasonable protection against risk.

63%

of KEVs tracked by CISA can be found on healthcare network

360

The number of medical device manufacturer patch certification programs users must contend with.

What are KEVs?

CISA maintains a database of software vulnerabilities and weaknesses that have been used in publicly known attacks. The KEV catalog is updated as public exploits are disclosed for CVEs, and includes the affected vendor, publication date, description of the vulnerability and mitigation or remediation advice. The catalog is available here, and is maintained in machine-readable formats for quick integration into security tools.

Critical Medical Assets Found on Hospital Guest Network

From our research, 4% of devices used in surgeries can be accessible via a hospital's guest network. Of all of the enclaves on a hospital network, clearly the guest network is the least secured and most exposed place for such critical devices to be connected.

MDMs and Patching Challenges

Medical device manufacturers (MDMs) develop on Windows and Linux operating systems, platforms that are regularly patched and updated, yet this capability is not built into medical devices. Instead, vulnerability patching is often an add-on to an already expensive support contract, according to HDOs we spoke to.

Many MDMs also have support contracts for devices that run on unsupported operating systems. This forces HDOs to rely on compensating controls to mitigate vulnerabilities or implementation weaknesses.

MDMs, meanwhile, argue that because of the lengthy device certification process by the FDA, they are concerned about breaking FDA-certified functionality, and therefore are unwilling to invest in complete security testing.

Legacy Systems a Challenge to Patient Safety

Our analysis shows that 14% of connected medical devices are running an unsupported or end-of-life OS. Of the unsupported devices, 32% are imaging devices, including X-Ray and MRI systems that are vital to diagnosis and prescriptive treatment. And unlike infusion pumps and other patient devices that may number hundreds in a hospital setting, there may be only a handful of imaging devices, creating a critical availability issue should one or more be disabled.

4%

of devices used in surgeries can be accessible via a hospital's guest network

14%

of connected medical devices are running an unsupported or end-of-life OS

Clinical IoT devices (23%) and hospital information systems (20%) also are among those running unsupported or EOL OSes. While the vast majority of these unsupported OSes are Windows, they are not limited to the Microsoft OS and range from Linux systems to mobile operating systems, and even outdated Sun Solaris and Sun OS.

The implication of this finding is that legacy OS systems may have critical vulnerabilities that are no longer patchable from the vendors who produced them, leading to critical exposures in medical devices.

Surgical Devices Among Those Running Unsupported OSes

Adding a fine point to the previous finding, 7% of surgical devices—whose failure may endanger patient safety—are running an unsupported or end-of-life OS. These devices include robotic surgery systems, defibrillators and gateways, ventilators, and systems central to anesthesia administration and monitoring.

Medical Devices Predicted to Have Vulnerabilities Rampant in Healthcare Delivery Organizations

11% of patient devices and 10% of surgical devices—critical equipment that if they fail could negatively impact patient care—contain vulnerabilities with high EPSS scores. While these assets don't have a vulnerability today, a high EPSS score is an indicator of a high likelihood to have a vulnerability discovered in this asset in the future.

Vulnerable Medical Devices by CVE Count

Imaging workstations and PACS servers (picture archiving and communications systems) are far and away the top two medical device categories with published CVEs with 18,000 and 12,000 respectively. Diagnostic workstations, surgical safety devices, and EEG equipment are also among the top 10. Many of these devices run on legacy Windows systems, complicating not only patching, but also identification and segmentation.

7%

of surgical devices—whose failure may endanger patient safety—are running an unsupported or end-of-life OS

Exploit Prediction Scoring System (EPSS):

Developed by the Forum of Incident Response and Security Teams (FIRST), EPSS scores (0-to-100) represent the probability that a software vulnerability will be exploited in the wild. Current threat information from CVEs and actual exploits are used to determine an EPSS score.

Inside the State of CPS Security: Healthcare Report

At Claroty, we place the highest value on public safety, striving to create the most secure environment possible for the operation of medical devices. To ensure our findings are described in industry standards, we have chosen to use The Joint Commission's framework for device classification in analyzing the consequences of failure of a medical device due to the exploitation of a vulnerability.

We believe that the Joint Commission's approach is the most comprehensive and holistic, focusing on the broader healthcare environment. The Joint Commission's framework places greater emphasis on the potential impact on patient care and safety, taking into account not just the likelihood of a device failure but also the severity of the potential harm to patients.

By adopting The Joint Commission's framework, we aim to reinforce the security measures around medical devices, and the environments in which they operate. This approach helps us to better prioritize the cybersecurity measures that we recommend, based on the potential impact of a security failure, and enables us to provide a more robust and resilient solution to our users.

The State of CPS Security Report: Healthcare 2023 is a snapshot of healthcare cybersecurity trends, medical device vulnerabilities, and incidents observed and analyzed by Team82, Claroty's threat research team, and our data scientists. Information and insights from trusted open sources, including the National Vulnerability Database (NVD), the Cybersecurity and Infrastructure Security Agency (CISA), the Healthcare Sector Coordinating Council Working Group, and others, also were used to bring invaluable context to our findings.

MEDICAL DEVICE CYBERSECURITY LANDSCAPE

Here's a look at some of the key events that shaped this report:

Ransomware is a $10 billion scourge across industries, and healthcare organizations are among the hardest hit. The FBI's Internet Crime Complaint Center (IC3)'s 2022 annual report said the bureau received 210 reports of ransomware attacks in the healthcare sector. That number is double the number of reports attributed to many of the remaining critical infrastructure sectors in the U.S. Ransomware and extortion actors target healthcare because of its intolerance of disruption, leading many victims to meet ransom demands in order to regain access to critical patient systems. A report from Phoenix NAP, an IT consultancy, says that victims in healthcare paid ransoms in 61% of incidents, and the average ransom payment approached $200,000 USD. The number of ransomware attacks aimed at hospitals, meanwhile, increased 50% from 2021 to 2022.

In this section of the report, we'll look at some of the impacts of ransomware and extortion attacks within the healthcare sector, and how the industry and federal government has responded with new mandates to improve the secure design and delivery of medical devices.

Many of the data points and information in this report expose some of the entry points criminal and state actors could leverage to inflict the most pain on HDOs. Already we've seen attacks lock providers out of patient information systems, disrupt access to diagnostic and treatment systems, and cause intolerable disruptions leading to re-routing of patients, unacceptable backlogs, and in one extreme case, the closure of a rural Illinois hospital.

Attack a Factor in Hospital Closings its Doors

St. Margaret's Health in Spring Valley, Ill., announced that a cyberattack was a key factor in the provider's decision to close its doors forever. Computer systems were inaccessible for months, hospital officials said, and it was unable to file insurance claims for reimbursement. With St. Margaret's already buckling under staffing costs, inflation, and supply chain issues wrought by the Covid-19 pandemic, the cyberattack was the last financial blow that led the rural health system's leaders to close its doors in June 2023.

Multifaceted Attacks Include Extortion

The Rhysidia ransomware gang is alleged to have been behind an August 2023 ransomware attack against Prospect Medical Holdings, with the group not only threatening to deploy malware, but also claiming it stole a database containing patient Social Security numbers, driver's license information, and legal and financial documents. The ransomware attack forced the 16-hospital group to postpone elective surgeries, outpatient appointments, and other services.

Journal of the American Medical Association Report

A March 2023 report by the **Journal of the American Medical Association (JAMA)** provided context on the impact of ransomware attacks on emergency departments adjacent to an HDO under a ransomware attack. Based on an analysis of pre-attack phase, attack and recovery phases, and post-attack phases, JAMA reported significant increases in the numbers of patients being cared for by adjacent HDOs, including ambulance arrivals, waiting room times, medical diversions, and stroke care, among others.

"These findings suggest that targeted hospital cyberattacks may be associated with disruptions of healthcare delivery at non-targeted hospitals within a community and should be considered a regional disaster."

— JAMA Report

405(d) Hospital Resiliency Landscape Analysis

The Dept. of Health and Human Services (HHS) partnered with the Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG), and the HHS' Centers for Medicare & Medicaid Services (CMS) to create a landscape analysis of active threats targeting hospitals, and an analysis of HDOs' cybersecurity capabilities.

The report reinforces the need for hospitals to be proactive about locking down external access to medical devices because not only are stolen credentials to these systems coveted by attackers, but they're moving quicker than ever to use them and exploit vulnerabilities on devices to access the corporate network.

According to the report:

TIME TO EXPLOIT:

Citing the Crowdstrike 2023 Global Threat Report, the HHS study shows that attackers move laterally from an initial compromise deeper into the network inside of 90 minutes. Largely, attackers are doing so with stolen credentials and leveraging tools already on the network to avoid detection.

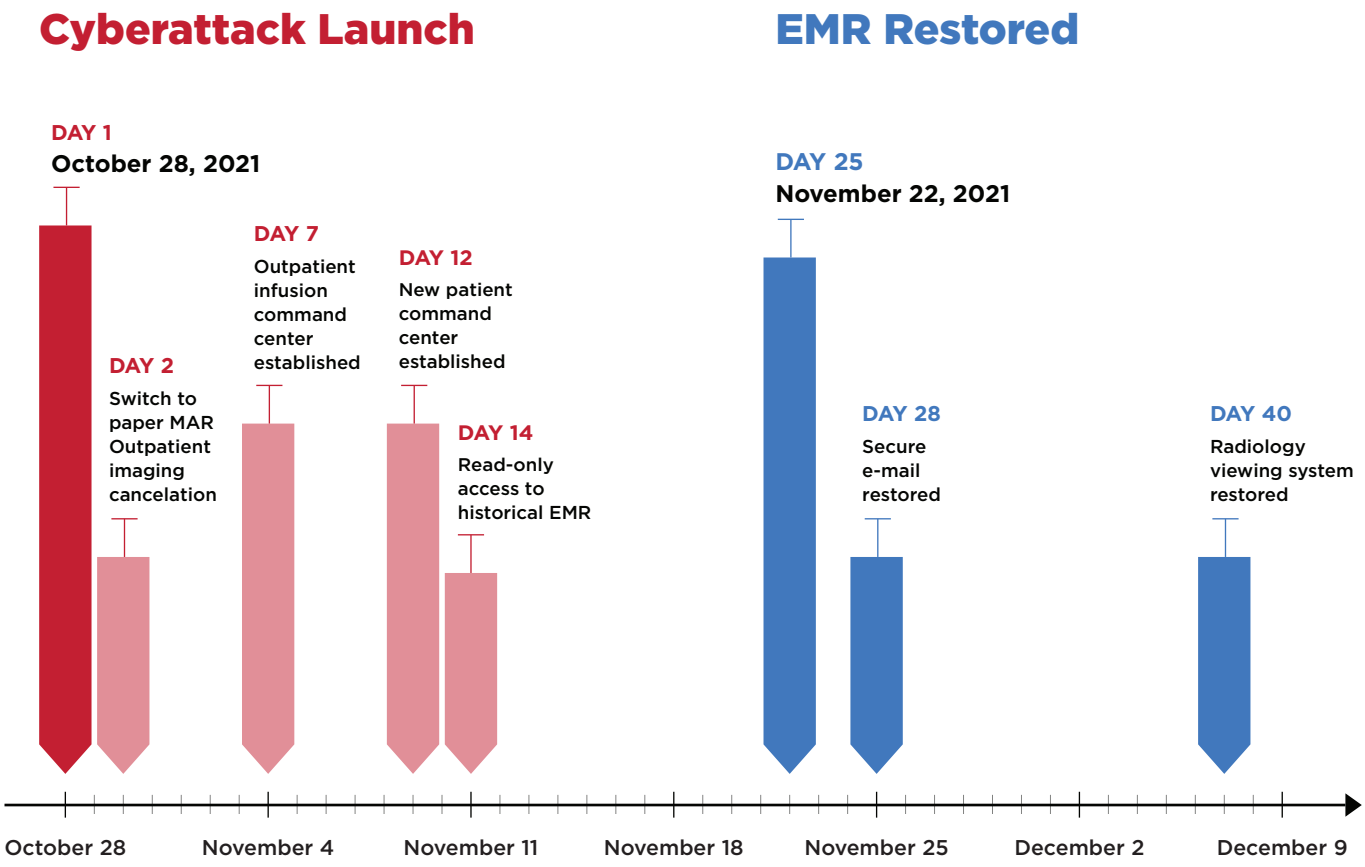
UNDERGROUND ACCESS BROKERS:

Dark web markets profit heavily from selling legitimate access to hospitals and other targets. These so-called access brokers have a significantly higher presence online, growing 112% from 2021 to 2022, and the HHS paper concludes there is enough demand for these brokers to specialize services even further.

PHISHING-AS-A-SERVICE:

The growth of these services is an offshoot of the access broker dynamic. Credentials of particular value are those that bypass multi factor authentication using vishing and OTP (one-time password) smishing techniques.

A stark reminder of the potential disruption to healthcare services and negative impact to patient care came in a 2020 ransomware attack against a U.S. health network resulting in more than $20 million in damages. According to publicly disclosed details, more than 5,000 endpoints were compromised by ransomware, and more than 1,300 servers. The healthcare network operated for more than a month without critical imaging services, and 25 days without secure email.



Courtesy 405(d) Hospital Resiliency Landscape Analysis

"Refuse to Accept"

The U.S. Food and Drug Administration (FDA), meanwhile, has become the statutory authority over medical device cybersecurity after the ratification of Section 3305 of the Consolidated Appropriations Act 2023, which amends the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, "Ensuring Cybersecurity of Devices."

It gives the FDA the ability to issue a refuse-to-accept decision to a medical device manufacturer should there be concerns about missing cybersecurity capabilities of a submission deemed a "cyber device." A cyber device, according to the FDA, is a medical device that can connect to the internet and contains software or other technology that could be vulnerable to cyber threats.

The FDA worked collaboratively with manufacturers on premarket submissions without issuing refuse-to-accept decisions prior to an Oct. 1, 2023 deadline.

This unprecedented authority is one of the most significant steps toward elevating cybersecurity as a patient care and safety priority. Specifically, the FDA now requires new medical device submissions to include:

- A plan to monitor, identify, and address post-market device vulnerabilities; this includes coordinated vulnerability disclosure policies and procedures.
- A plan for processes to assure that devices and systems are secure, and provide post-market updates and security patches to the device and related systems.
- A software bill of materials (SBOM) that lists commercial, open source, and homegrown software components running on a device.

The hope is that this action and authority will inform, and bring rigor to, medical device vulnerability management, and improve transparency between manufacturers and HDOs around potentially vulnerable software components so that they can be addressed in a timely fashion.

A SNAPSHOT OF MEDICAL DEVICE SECURITY

Team82's analysis of medical device security data

Connected medical devices take many forms; a sample of which include:

- Remote patient monitoring systems that track vital signs and inform treatment
- Insulin pumps, pacemakers and other implanted devices that collect and transmit patient information to monitoring systems
- Imaging systems, MRI machines, and CT scanners that are critical diagnostic tools

While all of them share a commonality around improved patient care and treatment efficiency, they are also governed by software and operating systems. Furthermore, the code running on medical devices is not exempt from vulnerabilities, weak configurations, and suspect implementation choices.

In this section of the report, we explain the key factors impacting the cybersecurity posture of medical devices, starting with the scope of vulnerabilities impacting medical devices and their likelihood of being exploited, and the hidden threats lurking on networks labeled "guest networks" by hospitals and how they provide a bridge deeper into other areas of the internal network, and the continued reliance on legacy operating systems.

Vulnerabilities

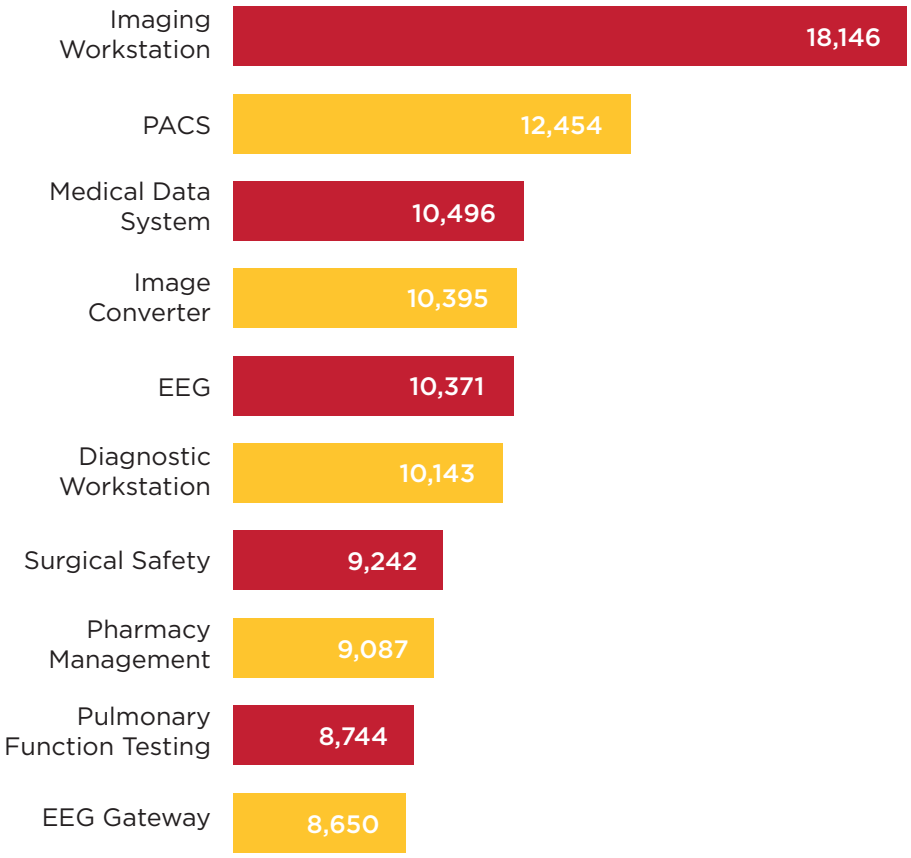
Our research and analysis shows that inherent design and implementation vulnerabilities around connected medical devices are prevalent, and can be leveraged to negatively impact patient care.

To properly understand and make decisions around the medical devices in a hospital IT and IoT environment, you must understand the realities of exploitable vulnerabilities in these critical tools and systems.

In this section, we'll analyze vulnerability information from our research, and do so in context of CISA's Known Exploited Vulnerability Catalog, and also provide some additional analysis in the context of vulnerabilities likely to be exploited in the near future according to their EPSS score.

This is an invaluable perspective for defenders conducting continuous risk assessments, prioritizing remediation activities, and working in concert with manufacturers to address these security shortcomings.

From our research, the following are the top 10 vulnerable medical device types by CVE count.



While there is some value in counting CVEs by medical device type, the real eye-opener comes from a comparison of this information against CISA's KEV catalog.

63%

of KEVs in the CISA catalog apply to medical devices and healthcare networks that we analyzed

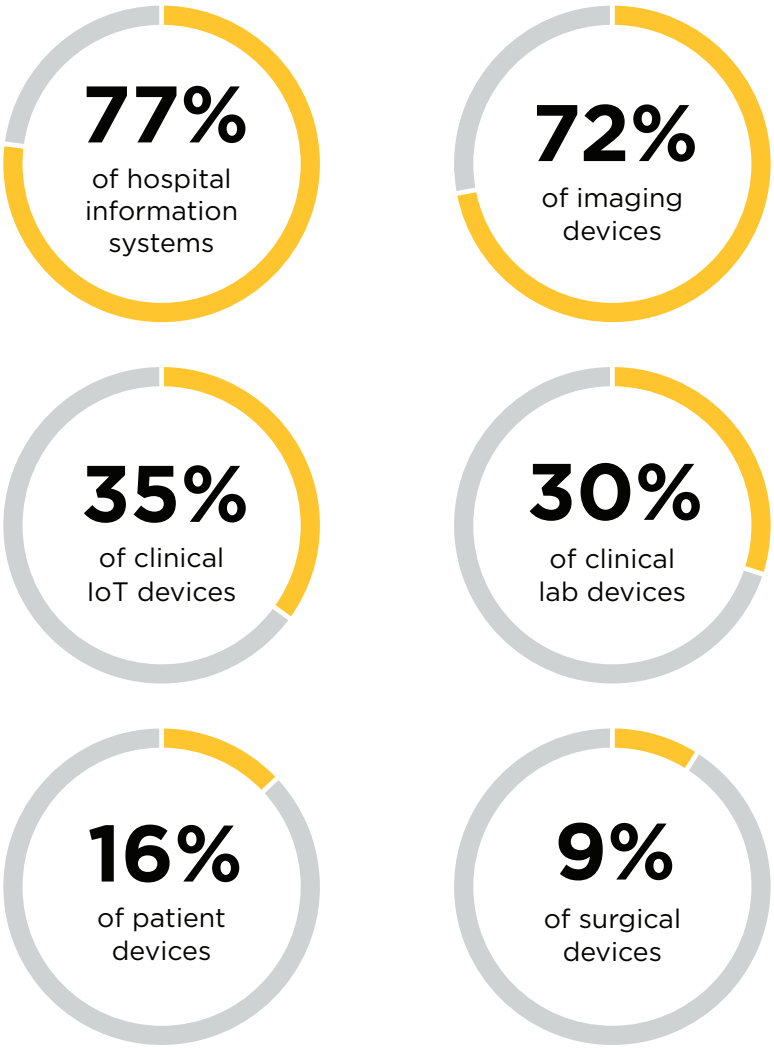
23%

of medical devices that we analyzed contain vulnerabilities present in CISA's KEV catalog

14%

of electronic health record systems that we analyzed contain vulnerabilities present in CISA's KEV catalog

Looking closer at the vulnerable medical devices by CVE count, you'll see many of those device types contain at least one known exploited vulnerability.



9% of surgery devices and 16% of patient devices that we analyzed with a high impact on patient safety are affected by a known exploited vulnerability

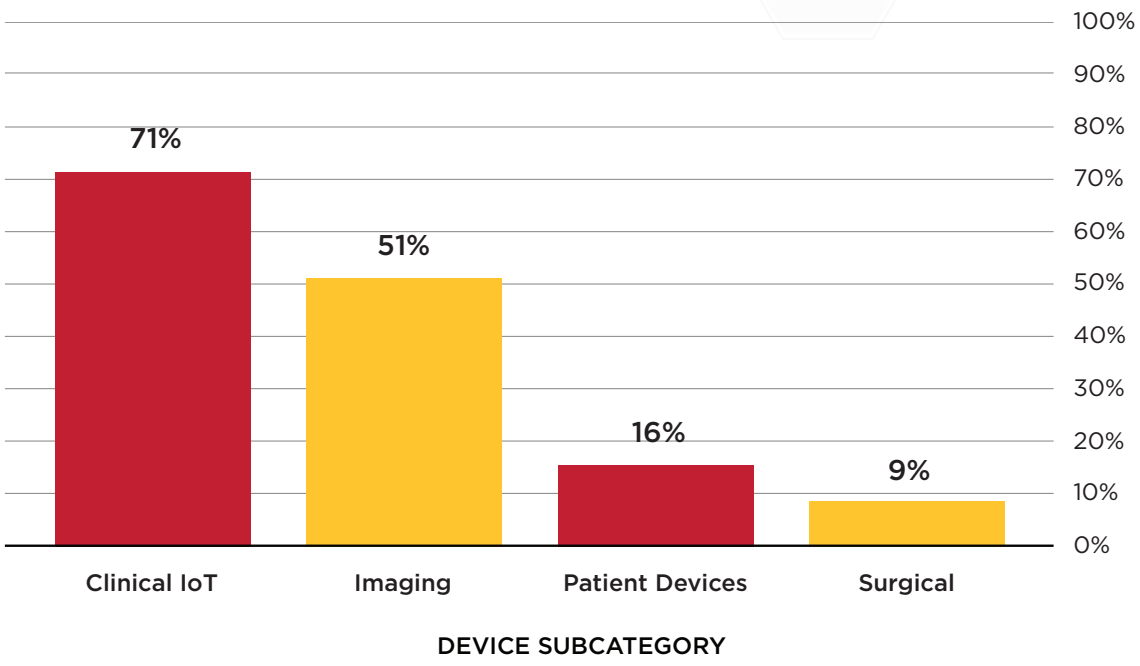
93%

of critical Known Exploited Vulnerabilities in the CISA catalog can be remediated via an OS update or patch from the vendor, such as Microsoft for Windows-based devices. Often, it takes months for MDMs to certify a patch before it may be applied to the individual device.

6%

of critical Known Exploited Vulnerabilities in the CISA catalog impact unsupported, end-of-life software products

HIGH CONSEQUENCE OF FAILURE DEVICES WITH KEVs



While the KEV catalog represents public exploits in the wild for known vulnerabilities, the EPSS score represents a measure of threats and likelihood of exploitability within the next 30 days of issuance, according to FIRST.

"EPSS is only estimating the probability that a vulnerability will be exploited. EPSS does not account for any specific environmental, nor compensating controls, nor does it make any attempt to estimate the **impact** of a vulnerability being exploited. **EPSS is not, and should not be treated as a complete picture of risk**, but it can be used as one of the inputs into risk analyses."

— FIRST EPSS User Guide

0% to 100%

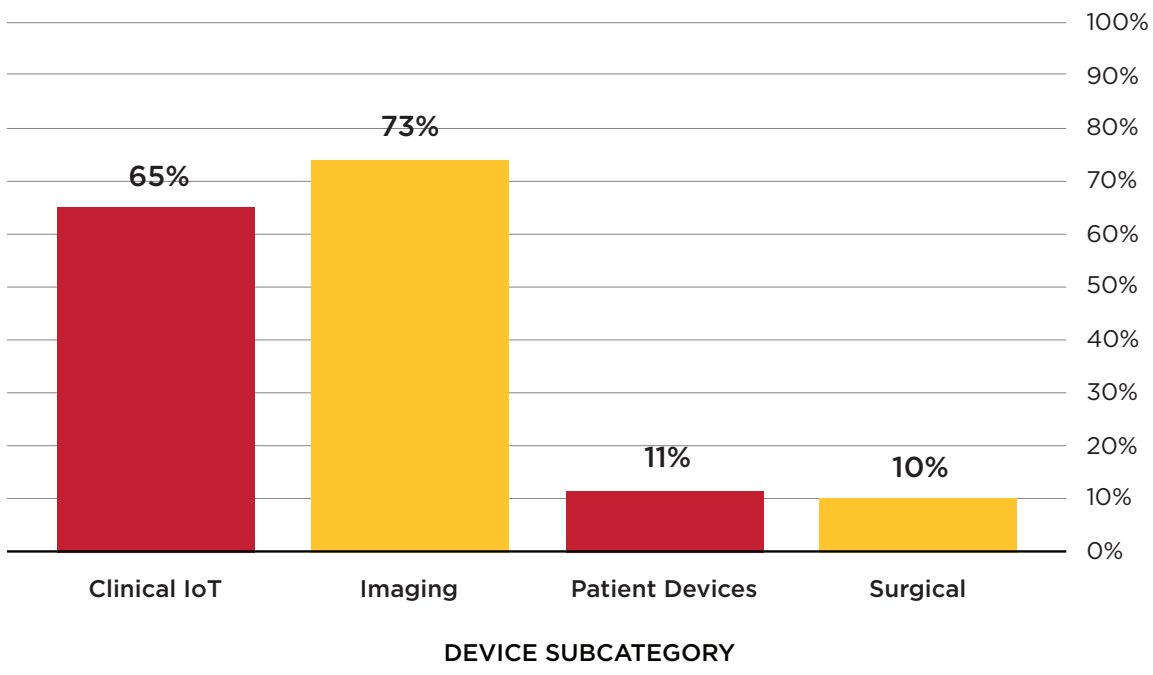
A higher score indicates the likelihood that a vulnerability will be exploited within the next 30 days

An EPSS score, which is built using data from, among others, the MITRE CVE list, data about CVEs such as days since publication, and observations from exploitation-in-the-wild activity from security vendors, can be used in concert with the more familiar CVSS v3 score, which is used to assess a criticality rating to disclosed vulnerabilities.

Unlike CVSS, EPSS produces a probability that a vulnerability will be exploited, and should be a consideration along with other factors in building a vulnerability management strategy.

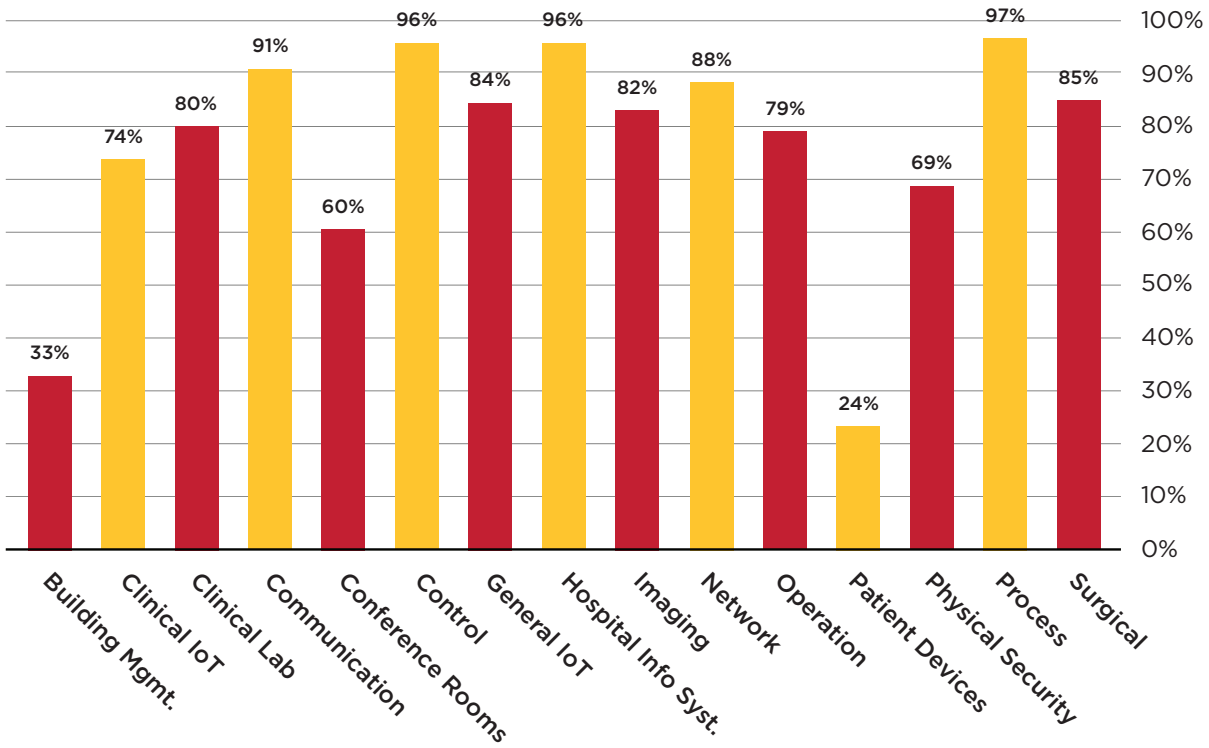
Our research shows that a not-so-insignificant number of patient and surgical devices, including ventilators, anesthesia monitors, heart-lung machines, robotic surgery systems, and others contain vulnerabilities with a high EPSS score.

PATIENT AND SURGICAL DEVICES WITH HIGH EPSS SCORES



We see similar trends around the percentage of devices running end-of-life, unsupported OSes that contain vulnerabilities with high EPSS scores.

UNSUPPORTED OSes WITH HIGH EPSS SCORES



HIGH EPSS SCORES ABOUND

96%

of healthcare information systems with unsupported OSes have high EPSS vulnerabilities

85%

of surgical devices with unsupported OSes have high EPSS vulnerabilities

82%

of imaging devices with unsupported OSes have high EPSS vulnerabilities

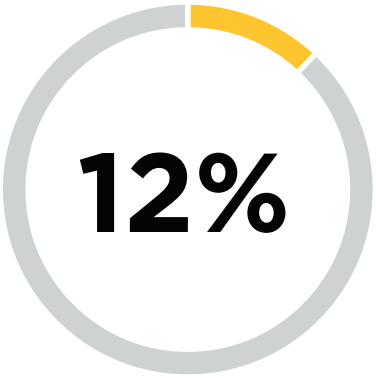
99%

of electronic health record systems with unsupported OSes have high EPSS vulnerabilities

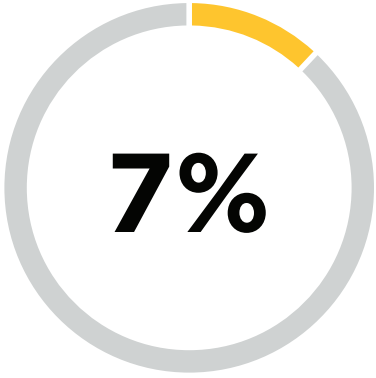
Note: These percentages reflect devices from our research.

Unsupported OSes

The consequences of potential failures caused by cybersecurity incidents that affect end-of-life patient devices—including infusion pumps, network modules, gateways, incubators, cardiac rhythm management systems, mobility monitors, and others—can impact patient safety.



of medical devices whose failure could endanger patient safety run on unsupported OSes



of surgical devices whose failure could endanger patient safety run on unsupported OSes

14%

of medical devices in our research run an end-of-life or unsupported OS*

Device Types Running Unsupported OSes

Imaging (32%)

Clinical IoT Devices (23%)

Hospital Information Systems (20%)

Clinical Lab Devices (13%)

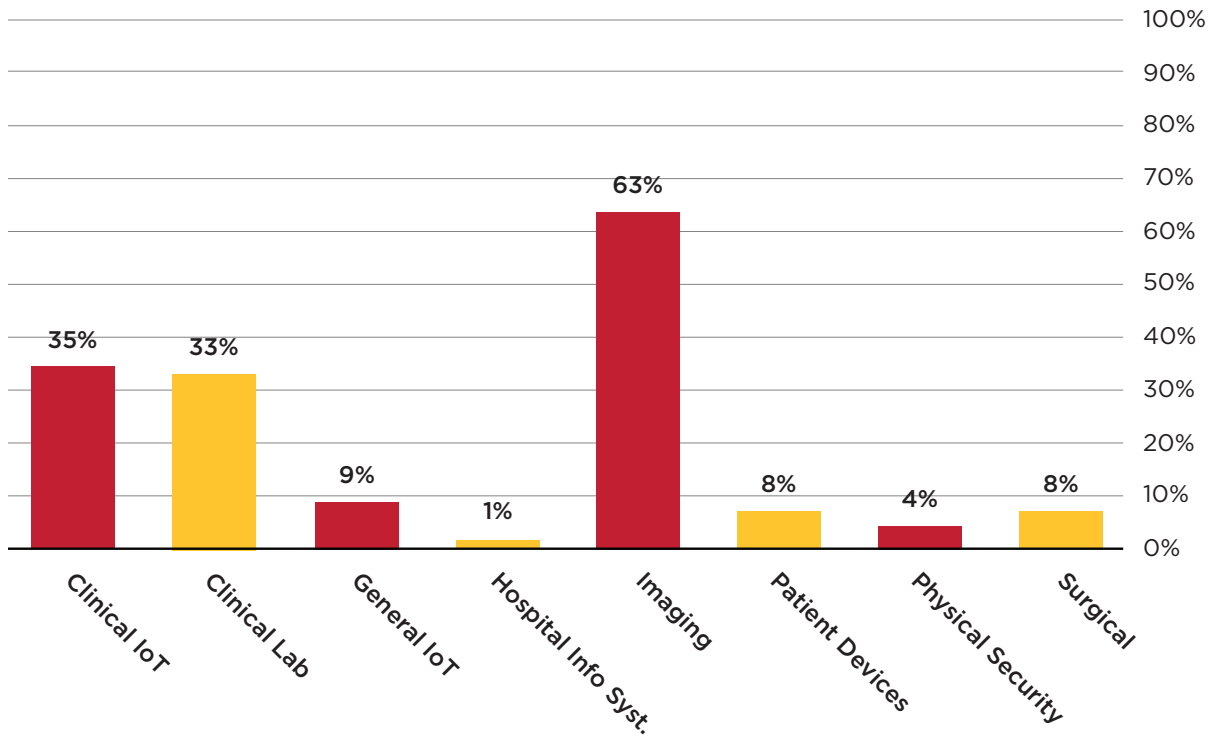
Surgical Devices (12%)

Patient Devices (10%)

* Windows OSes dominate, but the list is not exclusively Microsoft. Linux, mobile OSes, Sun Solaris, and SunOS, among others, are also on the list.

Unsupported operating systems are considered end-of-life by their respective vendors, and no longer receive security or feature updates. Furthermore, many of the Windows devices in our research are unmanaged, meaning they are not part of an Active Directory domain. This adds complexity for defenders who cannot use domain management, for example, to push any updates, new security policies, enforcement of Access Control Lists (ACLs), enforcement of password granularity, or updates for locally installed endpoint protection.

UNMANAGED WINDOWS-BASED MEDICAL DEVICES

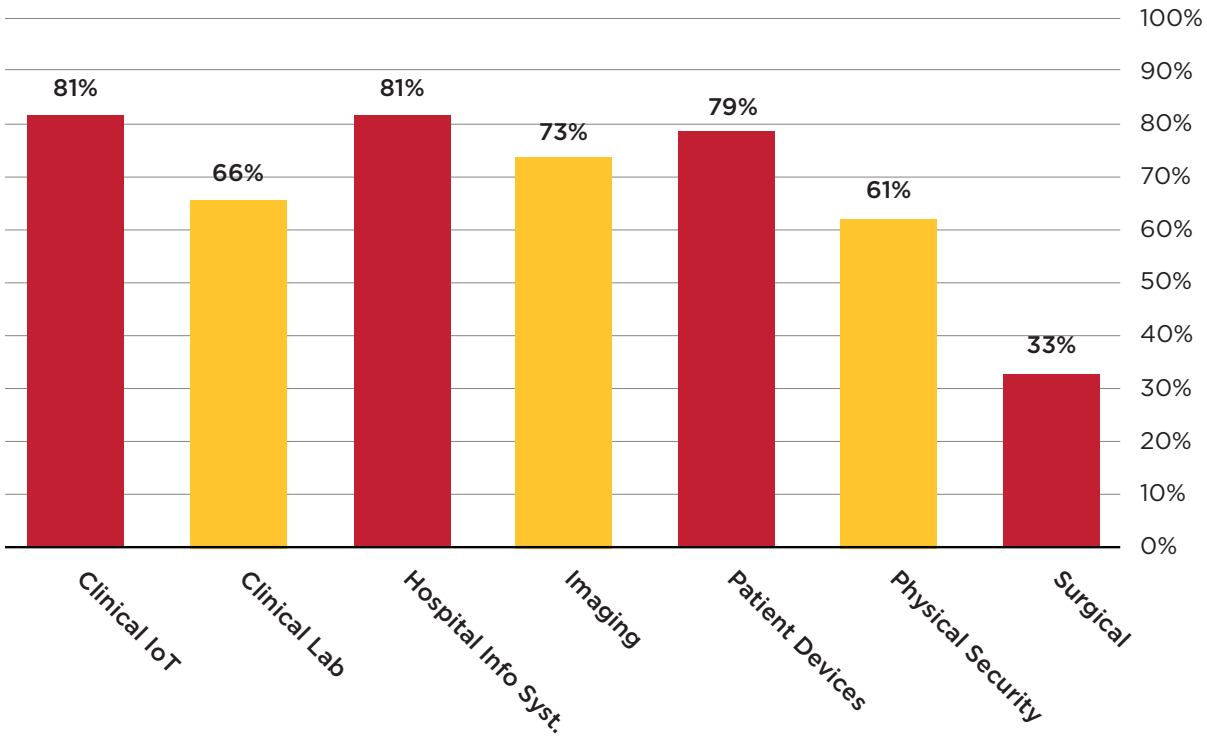


DEVICE SUBCATEGORY

Exploitable vulnerabilities in legacy systems or unmanaged devices, can be considered forever-day vulnerabilities. In our research, we see considerable percentages of connected medical devices running on unpatched Windows systems falling into this category.

Furthermore, many of these Windows-based systems are capable of communicating online.

PERCENTAGE OF WINDOWS-BASED MEDICAL SYSTEMS COMMUNICATING ONLINE



DEVICE SUBCATEGORY

Forever-day vulnerabilities are highly attractive flaws to threat actors because they won't be fixed, and in the case of healthcare, are found in devices that support indispensable services vital to patient care. HDOs facing budgetary strains brought on by the pandemic and other factors are unlikely to rip-and-replace these systems, thereby exponentially widening their exposure to attackers.

These exist in stark contrast to vulnerabilities in current versions of Windows, for example, that are disclosed and patched on regular update cycles. The same goes for Apple, Adobe, and other technology giants who push patches to users on a reliable cadence.

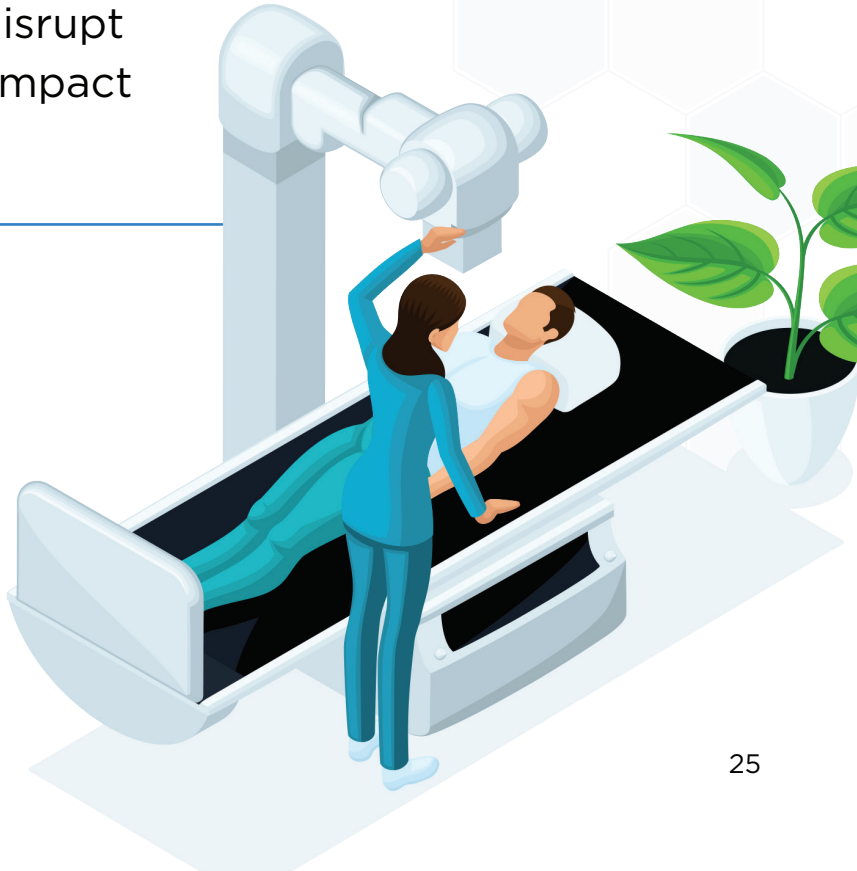
Forever-Day Vulnerability:

A known software vulnerability that a medical device manufacturer or software provider will not patch or update because it no longer supports the product. There are extreme cases when an out-of-band patch will be released for an unsupported OS, but these are rare.

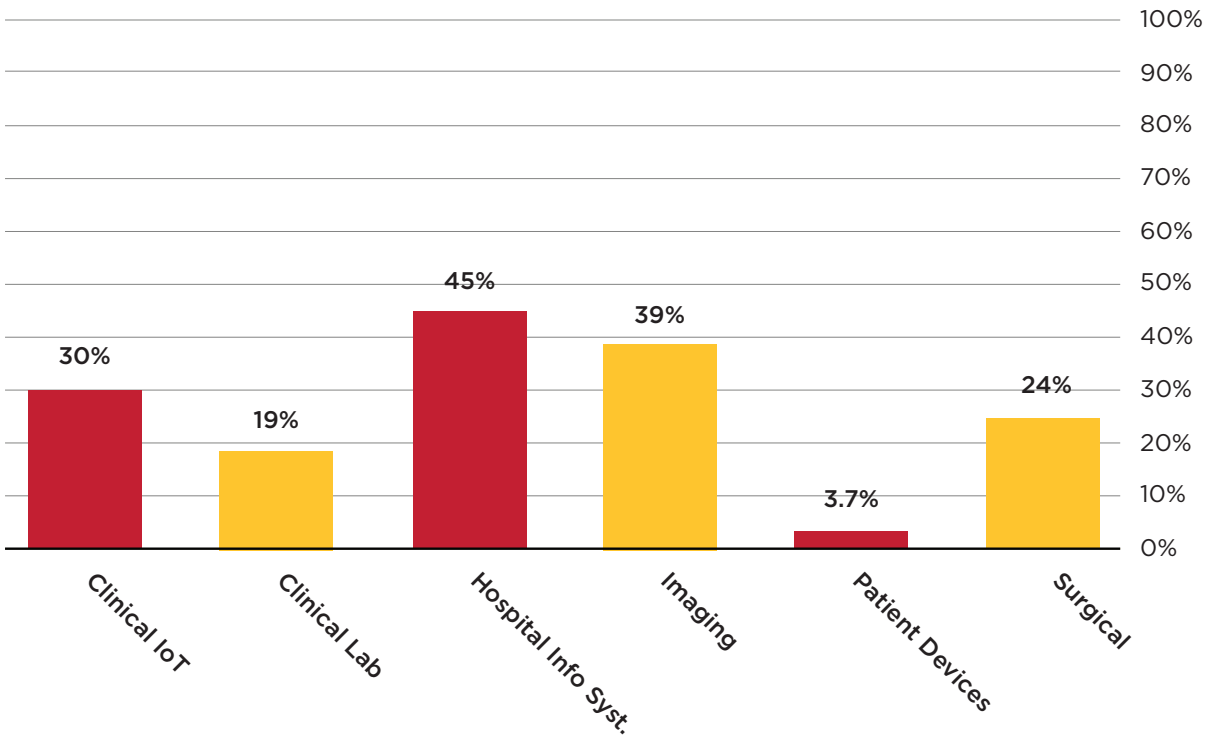
Network and Endpoint Security

Connectivity has spurred big changes in hospital networks, creating dramatic improvements in patient care with doctors able to remotely diagnose, prescribe, and treat with a never-before-seen efficiency. In parallel, this requires proper network architecture and an understanding of the exposure to attackers that it introduces. Systems that were once offline and essentially air-gapped are now increasingly capable of communicating online, or are reachable remotely, see chart below.

Implementation errors are magnified, and like exploitable vulnerabilities, these mistakes can open the door to attacks from outside the network that disrupt critical services and negatively impact patient care.



DEVICES CAPABLE OF INTERNET COMMUNICATION



Securing networked medical devices requires a complex strategy of mitigation efforts, starting with installing endpoint protection agents on devices that support it. This, however, is a relatively small number; Team82 research reveals that only 13% of medical devices support endpoint protection agents. Meanwhile, our research shows that 72% of medical devices are connected and communicating with the internet. Given the lack of support for endpoint agents, this puts the onus on defenders to accurately identify connected assets, and implement network security strategies such as segmentation to mitigate risk.

Segmentation allows HDOs to isolate certain devices and functions from one another, generally on virtual LANs (VLANs), for example, segmenting connected medical devices from the corporate network and guest networks (as we'll see later on in this report, guest networks pose a major problem, according to the information in our research).

None of this is achievable without first having as complete an asset inventory as possible. However, asset visibility is a weak spot across the healthcare industry. A recent American Health Association and KLAS Research Cybersecurity Benchmarking Study shows that HDOs and other types of healthcare organizations struggle to identify connected assets. Asset management was identified as one area with particularly low coverage by organizations who took part in the study. Claroty's 2023 Global Healthcare Cybersecurity Study has asset inventory management ranked as the second biggest gap in organizations globally, behind only patching vulnerabilities in medical devices.

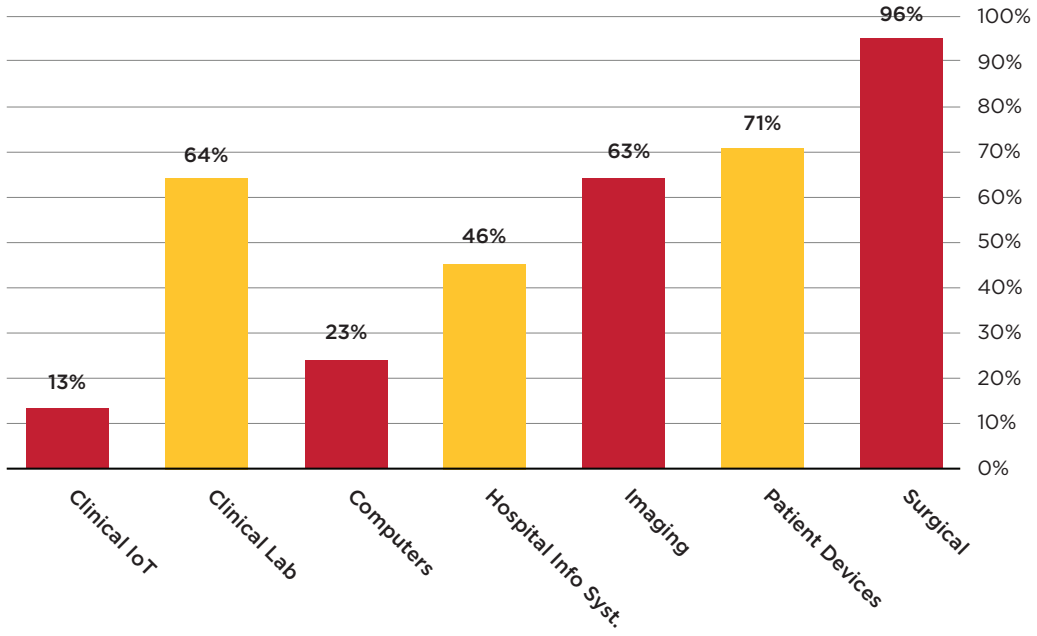
Without proper asset inventory, defenders inside HDOs cannot adequately protect devices they are blind to, and therefore cannot assess which devices are critical and most vulnerable, or take steps to mitigate threats in order to lower risk.

In addition, attackers can leverage exposed endpoints or poor configurations to gain a foothold on networks. Interesting paths will be scanned for, and an attacker will look to move laterally in order to steal patient data or business information. They may also use this stolen cache of information to extort money from HDOs by threatening them with either a public leak of the stolen information or a ransomware attack.

Endpoint Security

As we mentioned earlier, the FDA requires manufacturers to validate and approve software design changes around patches. HDOs must often instead resort to a mitigating control such as network segmentation or endpoint protection if a device supports such an agent. All the while, the vulnerability remains present in the device software or firmware, exposed to attackers. Also, HDOs are limited to where they can add endpoint protection based on manufacturing support and SLA contracts.

PERCENTAGE OF DEVICES WITHOUT ENDPOINT PROTECTION



The HHS' Hospital Cyber Resiliency Initiative's Landscape Analysis, released in April 2023, charts out a list of threat actions, impacts, and recommends over and over the use of endpoint detection and remediation as a potential mitigation action, alongside controls that manage devices accessing the network. This includes an inventory of medical devices, non-medical devices, mobile devices authorized to access the network.

Let's dive into our research and understand some of the real-world problems that HDOs and other healthcare providers are struggling with.

Guest Networks

Guest networks, labeled as such by hospitals in our research, provide patients and visitors with WiFi access, yet these publicly accessible services are apparently a bridge to other internal networks, our research shows.

For example, 22% of hospitals in our research have connected devices that bridge the guest and internal networks. Whether these are purposeful choices, or misconfigurations, this situation exposes devices with vulnerabilities, including those with critical CVSSv3 scores or high EPSS scores.

The types of connected medical devices that communicate over the guest network, meanwhile, are alarming—and surprising. We found clinical IoT devices and surgical devices accessible on public, guest networks; should these devices suffer any disruption, there would be a direct impact on patient treatment and quality of care. While there are relatively small percentages of devices on the guest network, in reality, there should be zero such exposure.

As a result, many HDOs and providers find themselves with attack vectors on two networks. This is especially distressing when looking at these percentages and possibilities combined with our data on EPSS scores and CVE counts. Clinical IoT devices, imaging systems, EEG scanning equipment, robotic surgical tools, pulmonary function testing, and general patient monitoring systems are among the devices with the highest CVE counts in our data. Couple that with our percentages of surgical and imaging devices—for example, running on end-of-life OSes and also contain not only unpatched vulnerabilities, but also security flaws with high EPSS scores—and there are numerous paths and outcomes an attacker could force that would negatively impact patient care.

Whether missing or improper segmentation, or less-than-desirable architecture is to blame matters little; **an attacker can quickly find and target assets on the public WiFi, and leverage that access as a bridge to the internal network.**

4.5%

of clinical IoT devices communicate on guest networks

4%

of surgical devices communicate on guest networks

2%

of hospital information systems communicate on guest networks

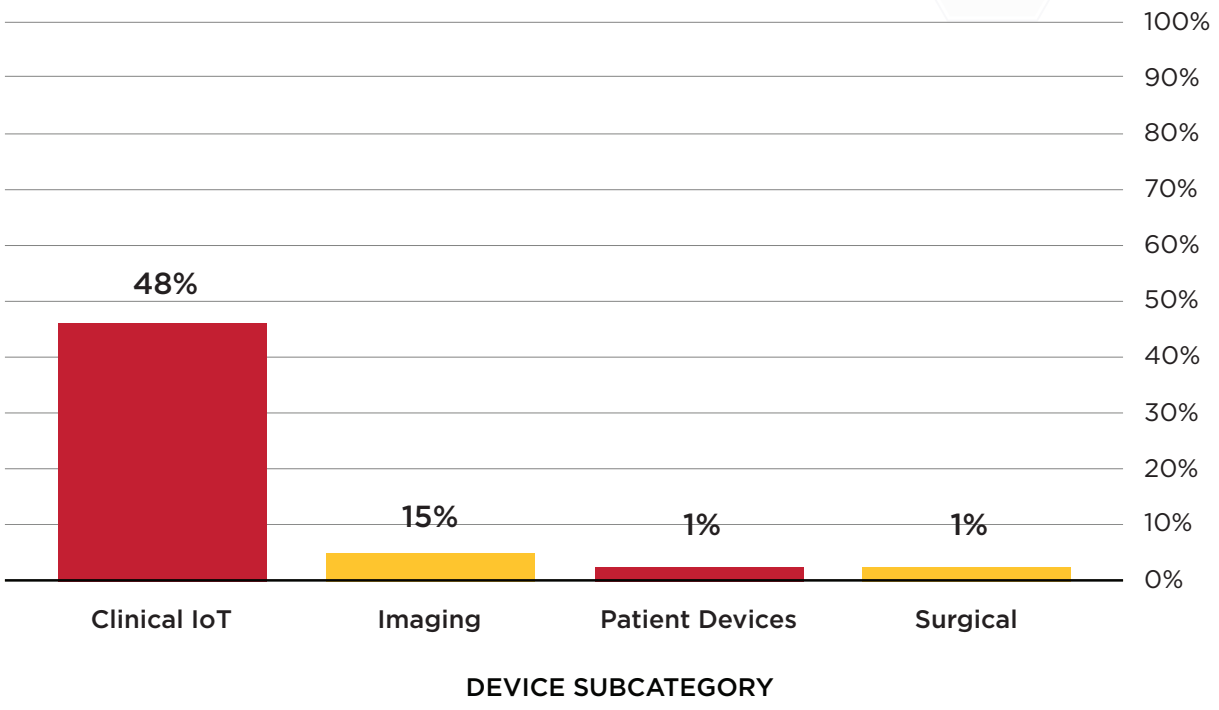
1%

of imaging devices communicate on guest networks

Devices Capable of Being Remotely Accessed

Remotely accessible medical devices in our research with a high consequence of failure include defibrillators, robotic surgery systems, and defibrillator gateways.

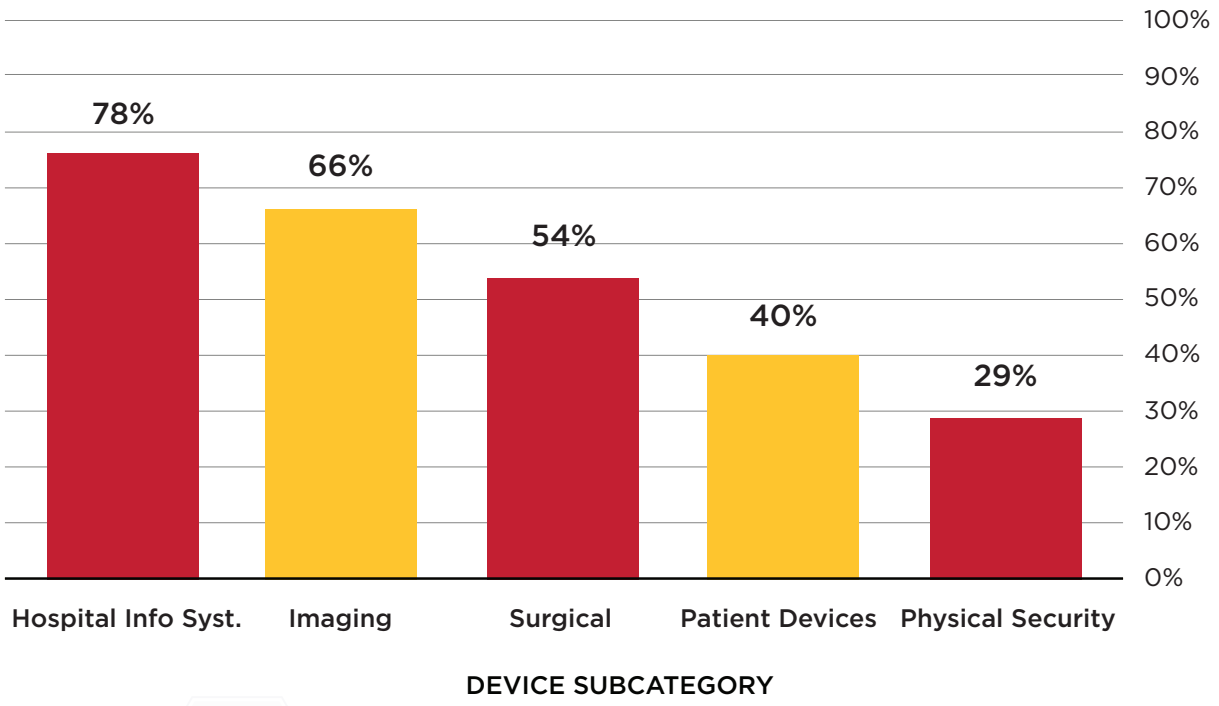
REMOTELY ACCESSIBLE, AND HIGH CONSEQUENCE OF FAILURE



Digging further, we see other critical healthcare systems that either have internet capabilities or are remotely accessible. Close to 80% of hospital information systems that process personal health information (PHI), insurance, and billing data, leads the list of devices in our research in this category, followed by 66% of imaging devices.

There can be devastating consequences to attacks against these internet-facing HDO enterprise systems and medical devices capable of communicating over the internet. A remote attacker successfully accessing a reachable system could disrupt operations in myriad ways; for an HIS system, data theft or alteration is a possibility that could impact patient care.

INTERNET CAPABLE AND REMOTELY ACCESSIBLE MEDICAL SYSTEMS



RECOMMENDATIONS

In order to truly prioritize cybersecurity as a patient safety mandate in healthcare, we believe there needs to be a two-pronged approach, one that starts with leadership from the U.S. Federal Government that is complemented by stark improvements from medical device manufacturers and defenders on policy, practice, and technology.

Federal Government

The FDA must continue to lead in promoting healthcare cybersecurity. Enforce the provisions of the PATCH Act that mandate:

- Minimum cybersecurity requirements for new medical device submissions after Oct. 1, 2023
- Submit plans to address post-market vulnerabilities in devices and associated systems.
- A software bill of materials (SBOM) detailing commercial, open source, and off-the-shelf software running on a device

Industry

Develop cybersecurity policies and strategies that stress the need for resilient medical devices and systems that can withstand intrusions. The Health Sector Coordinating Council's Cybersecurity Working Group has been tasked with analyzing which basic cybersecurity practices would be most impactful toward this goal. These include:

- Limiting remote access to endpoints (medical devices), i.e., do not connect them directly to the internet.
- Secure remote access through proper provisioning of credentials, require multifactor authentication, especially for interactive sessions such as VPNs, virtual desktops, and terminal sessions.
- Restrict third-party connections from vendors and contractors via segmentation, ACLs, and other techniques.
- Properly inventory medical devices and other assets that are internet-facing, prioritizing those assets most likely to be targeted by attackers.

Provide funding for under-resourced hospitals and HDOs, especially smaller facilities in rural areas, and cybersecurity training for staff and new hires. Fill open cybersecurity roles.

Develop a system to incentivize hospitals and HDOs to move away from legacy, unsupported software packages in medical devices. This could include tax incentives, or a potential shift in Medicare payment policies to include cybersecurity expenses into practice expenses.

Ensure world-class vulnerability management.

- Begin with an accurate inventory of assets, especially those that are reachable online.
- Be vigilant about patching connected devices and systems, especially those that bridge enterprise and medical networks
- Conduct regular, continuous vulnerability scanning of assets directly exposed to the internet, prioritize mitigation and remediation efforts around those devices
- Prioritize risk management efforts based on metrics such as EPSS scores and known exploited vulnerabilities; this effort minimizes existing risk around vulnerabilities likely to be exploited within 30 days, according to the EPSS score.

Segmentation is a paramount strategy.

- Isolate connected medical devices—patient and surgical—from corporate networks.
- Determine whether devices that have a high consequence of failure, including patient and surgical devices—are not reachable from the guest network. Prioritize segmenting and isolating these devices from public networks.
- Ensure that devices and other assets that do not support an endpoint protection agent are segmented and monitored.

Evaluate additional opportunities from collecting device cybersecurity data to drive measurable business value for health systems.

- Leverage device and lifecycle management data to drive well-informed procurement decisions
- Improve operational and staff efficiencies
- Consider the downstream improvements to patient experience and satisfaction
- Right-size fleet of devices to meet actual utilization demands
- Reduce maintenance and procurement costs through improved asset management

ABOUT CLAROTY

Claroty empowers organizations to secure cyber-physical systems across industrial, healthcare, public sector, and commercial environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit Claroty.com.

ABOUT TEAM82

Team82, the research arm of XIoT cybersecurity company Claroty, is an award-winning group of researchers known for its development of proprietary threat signatures, OT protocol analysis, and discovery and disclosure of industrial, healthcare, and commercial vulnerabilities.

Fiercely committed to strengthening XIoT cybersecurity and equipped with the industry's most extensive testing lab, the team works closely with leading vendors to evaluate the security of their products. As of October 2023, Team82 has discovered and disclosed more than 500 vulnerabilities.

For more information, visit: Claroty.com/Team82.

ACKNOWLEDGEMENTS

The primary author of this report is Chen Fradkin, full stack data scientist at Claroty.

Contributors include: Ty Greenhalgh, industry principal healthcare, Yuval Halaban, risk team lead, Rotem Mesika, threat and risk group lead, Nadav Erez, vice president of data and Amir Preminger, vice president of research. Special thanks to the entirety of Team82 and the data department for providing exceptional support to various aspects of this report and research efforts that fueled it.