Unveiling the Persistent Risks of Connected Medical Devices

October 29, 2024

FORESCOUT RESEARCH | VEDERE LABS

TABLE OF CONTENTS

EXPOSED IoMT

ACTIONS FOR CISOs

WHAT YOU NEED TO KNOW

Operating System OVERLOAD in HDOs

110 unique OS

300+ unique Vendors

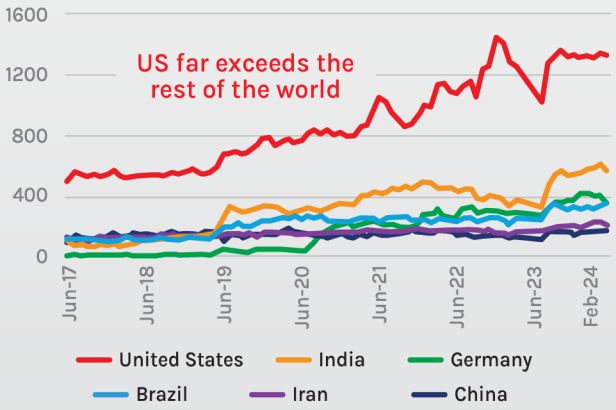
Our Honeypot Captures Attacks

- **1.6M** interactions
- **1** attack every **20** sec avg
- **~23,000** attempted DICOM connection/patient data

Global DICOM Exposure

286% growth since 2017

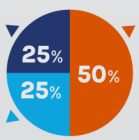
28% growth in <2 years



IoMT Asset Types and Functions

Patient monitors/ infusion pumps

Part of 84 other functions



Comms systems/ healthcare workstations

WHAT YOU NEED TO DO

- Identify and classify every asset
- Perform network flow mapping
- Limit external communications and exposure
- Implement effective segmentation
- Identify devices to segment by:
  - Business context
  - Network flow between device groups
- Monitor network traffic for malicious packets

Key Segmentation Guidance

Devices that cannot be retired or patched should be segmented to restrict access to critical information and services only

Follow Specific Guidance From

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

NIST

FORESCOUT

1. Executive Summary

Hospitals and clinics have faced major cyber attacks over the past several years. Our analysis of public data shows that **hacking incidents are responsible for almost 80% of healthcare data breaches** — with an average of **1.6 data breaches per day**. In 2023, these data breaches affected an average of 200,000 patients. The ability to compromise devices and take control of network assets to demand large ransom payments or monetize patient data is becoming all too common.

When networks at healthcare delivery organizations (HDOs) are shut down, the effects can be life-threatening. Life-saving testing and surgeries are delayed. Patient health monitoring returns to pen and paper – slowing down patient care and the efficiencies of shared patient data. Insurance approvals and billing systems often become unusable, so healthcare overall is stalled.

Because HDOs use and manage an expanding range of internet-connected assets, the challenge to secure these devices is multi-faceted. Our research has been tracking the growth in the volume of medical device types with internet exposure, known vulnerabilities and their respective risk. In this year's Riskiest Devices report, we examined how some HDOs have managed to reduce risk on their networks in the past year by investing in security after a devastating wave of cyberattacks. Here, we focus on a critical part of HDO networks: Connected medical devices, also known as the Internet of Medical Things (IoMT).

KEY FINDINGS

- Our honeypot simulated a medical imaging device for over a year
  - Observed 1.6M interactions
  - **1 attack occurred every 20 seconds on average**
  - **~23,000 interactions attempted a DICOM connection or search for patient data**
- DICOM is one of the most used services by IoMT and one of the most exposed online
  - Since 2017, **DICOM exposure has grown by 246%**
  - In less than 2 years, exposed DICOM has grown by 27.5%
  - Top countries: US, India, Germany, Brazil, Iran, China
- ~50% of assets are traditional managed IT
- ~50% are IoMT, IoT, OT and unmanaged network devices
- 50% of IoMT are communication systems and healthcare workstations
  - 25% are patient monitors and infusion pumps
  - 25% are divided into 84 other functions
- **110 unique operating systems in HDOs**

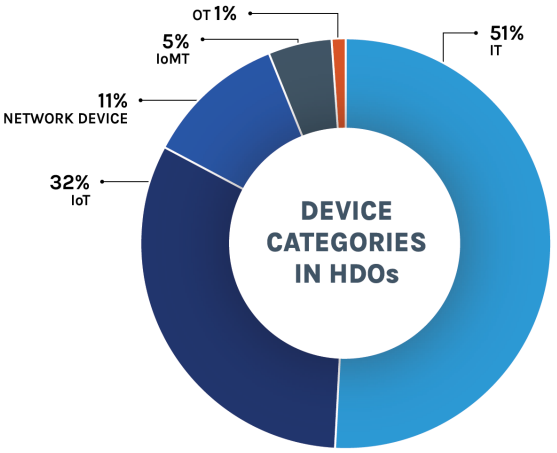
GUIDANCE

- Identify and classify every asset on the network
  - Understand the software and operating systems they run
  - Identify risks and vulnerabilities
- Limit external communications and exposure to prevent use as entry points
- Implement effective segmentation so breaches cannot reach medical devices and patient data
- Monitor all network traffic for signs of intrusion and respond timely

IoMT still presents a significant risk to HDOs. Below, we unveil some of these risks with detailed mitigation guidance.

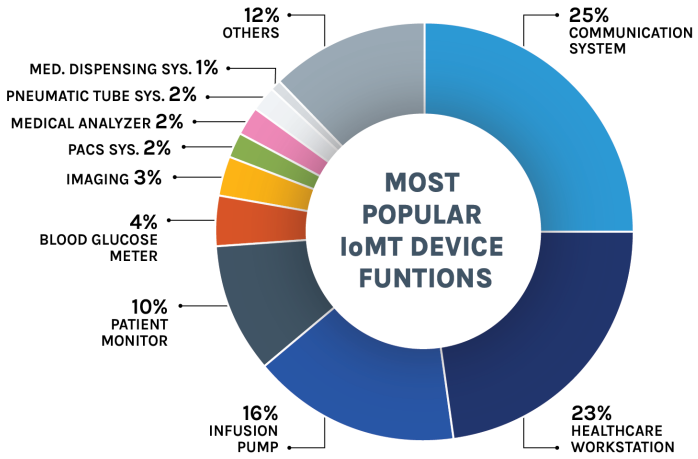
2. Which Connected Medical Devices Are Found on HDO Networks?

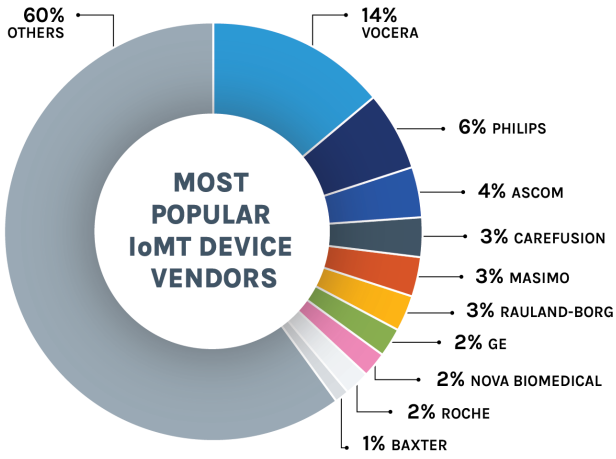
We examined a dataset containing more than 2 million devices across 45 HDO customer networks during the last week of May 2024. These devices are divided into five categories as shown below.



Only about half are traditional managed IT, such as general-purpose workstations. IoT devices represent one third of the attack surface, while IoMT devices account for a further 5%. This gives a total of around 115,000 IoMT devices in our sample, an average of over 2,500 IoMT devices per HDO.

To understand what kind of IoMT devices are most often seen on these networks, we broke down this sample by device function and vendor. We observed 88 distinct IoMT device functions and 306 distinct medical device vendors. The top 10 functions and vendors are shown below.

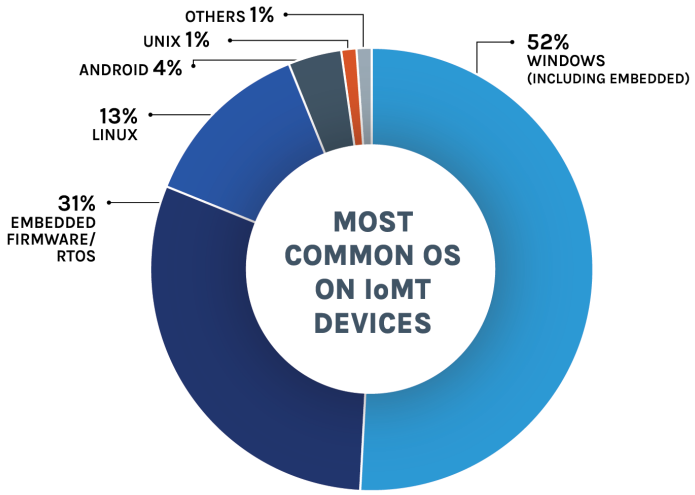




The two most popular device functions – communication systems and healthcare workstations – are not directly connected to patients, but they still provide critical healthcare functions, such as emergency alerts, communication, processing, and storing of patient data. These functions together account for almost 50% of IoMT in healthcare organizations.

Patient monitors and infusion pumps – which are connected directly to patients – represent 25% of devices. The remaining 25% is divided into the 84 other functions identified, including a multitude of imaging systems, lab equipment and other specialized equipment, such as pneumatic tube systems.

The vendor landscape is even more fragmented. Well-known names, such as Philips, GE, Roche and Baxter are among the top 10 most popular vendors. Yet, the ‘Others’ category comprises a staggering 60% of vendors.



These devices run 110 distinct operating system (OS) versions, with the top 5 types shown below. Note that Windows is used not only on workstations but also on some embedded medical devices running Windows CE.

The most common OS in embedded firmware is Linux, followed by: The real-time operating systems (RTOS) VxWorks, KADAK AMX RTOS, NutOS, ThreadX, and Digi Net+OS.

Although 52% of these medical devices run Windows, we only see active anti-malware running on 10% of all IoMT.

3. How Are These Devices Vulnerable?

The most common vulnerabilities affecting IoMT devices are the following:

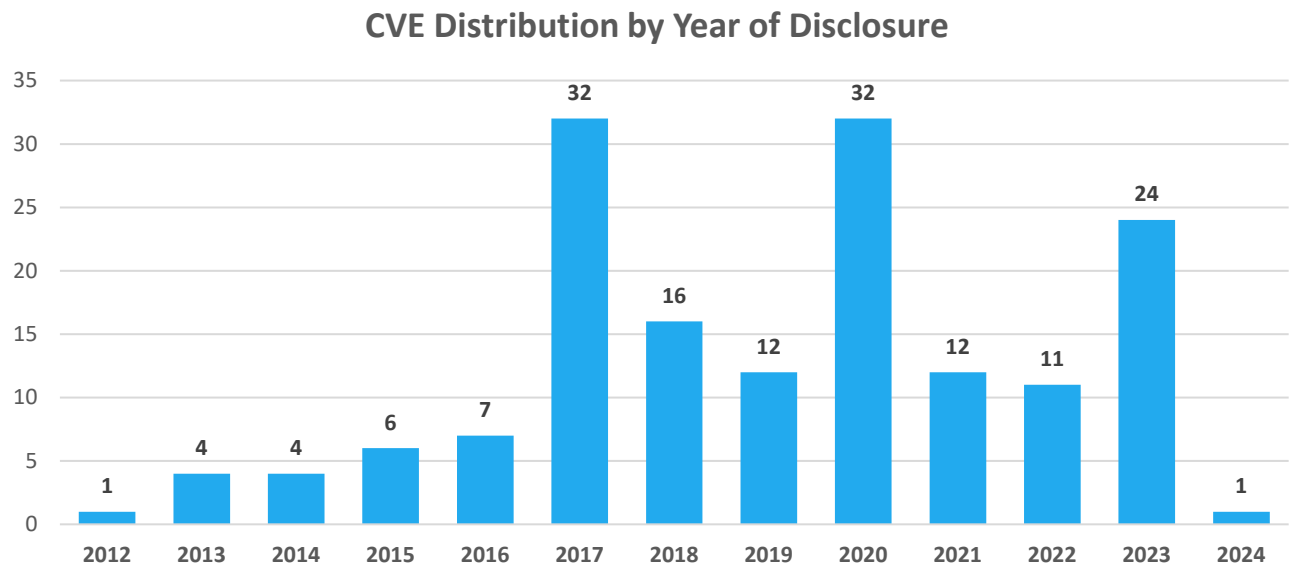
#	PRODUCT	VULNERABILITY DESCRIPTION
1	Microsoft Windows	CVE-2019-0708 – Microsoft Windows Remote Desktop Services (RDP) code execution (a.k.a. BlueKeep)
2	Wi-Fi Protected Access	CVE-2017-13077 until CVE-2017-13088 – WPA handshake traffic can be manipulated to induce nonce and session key reuse (aka KRACK)
3	BD Pyxis	CVE-2022-22766 (Information disclosure) and CVE-2022-22767 (Default account)
4	Philips PageWriter	CVE-2018-14799 (Buffer overflow) and CVE-2018-14801 (Default account)
5	Microsoft Windows	CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, CVE-2019-1226 – Microsoft Windows Remote Desktop Services (RDP) code execution
6	Baxter Sigma Spectrum	Several, including information disclosure, code execution, security bypass and default account – see ICSA-15-181-01, ICSMA-20-170-04 and ICSMA-22-251-01
7	Microsoft Windows	CVE-2022-26809 – Microsoft Windows RPC Runtime Library code execution
8	Siemens Biograph	CVE-2022-29875 – Siemens Biograph Horizon PET/CT Systems code execution
9	Microsoft Windows	CVE-2017-0143 until CVE-2017-0148 – Microsoft Server Message Block (SMB) code execution (a.k.a. EternalBlue)
10	Microsoft Windows	CVE-2021-26414 – Microsoft Windows DCOM Server security bypass

Half of these are serious vulnerabilities on Windows OS, affecting healthcare workstations (which as shown above are the second most common type of medical device) and embedded devices running Windows CE. These vulnerabilities can lead to full takeover of a device via remote code execution and may be automatically exploited by malware if there are medical devices exposed on the internet or connected on the same network as other compromised machines. This is what happened, for instance, with WannaCry exploiting CVE-2017-0143 (still the ninth most popular vulnerability on medical devices.)

The second row in the table is set of vulnerabilities, known as KRACK, that affects several medical devices using Wi-Fi and allows attackers to decrypt sensitive communications.

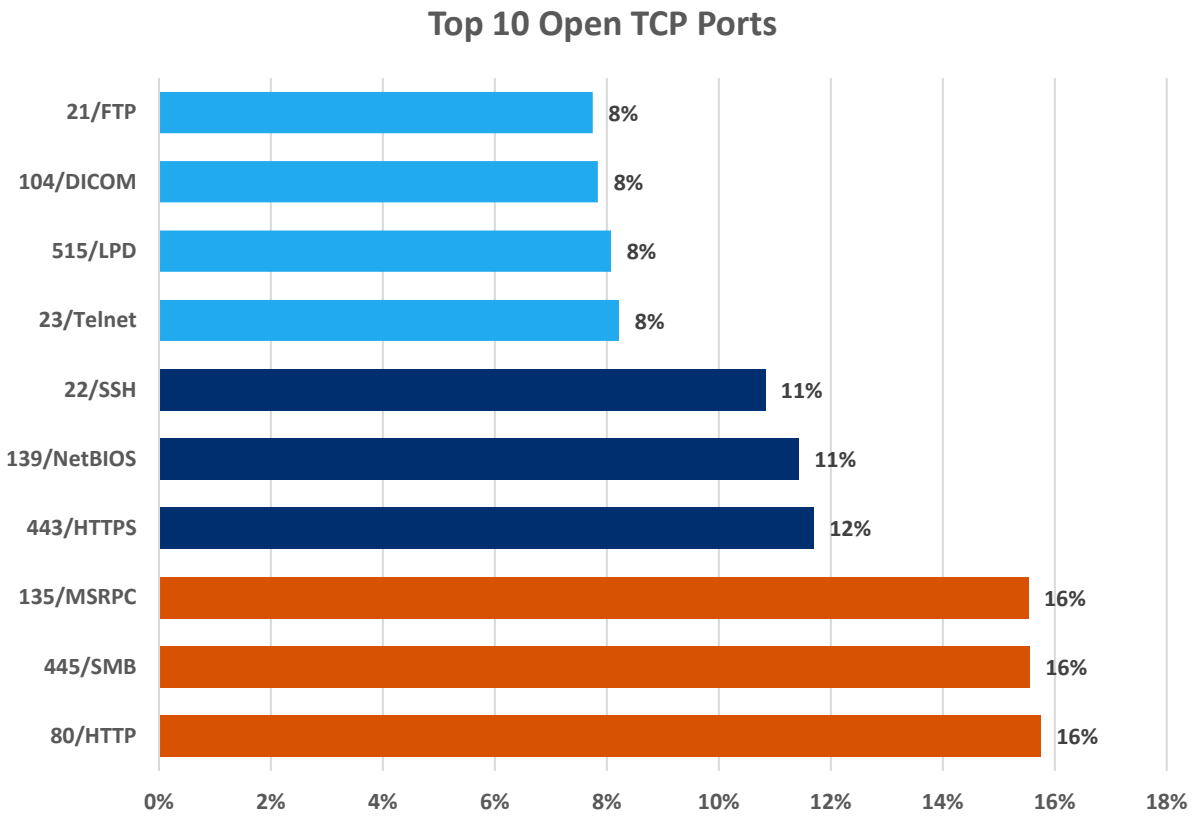
The remaining four sets of vulnerabilities affect specific medical devices that are popular on HDO networks: BD Pyxis medication dispensing systems, Philips PageWriter electrocardiographs, Baxter Sigma Spectrum infusion pumps and Siemens Biograph Horizon PET/CT scanners. It is interesting to note that three of these four arise from the use of default accounts on medical devices.

Beyond this top 10, we identified a total of 162 vulnerabilities affecting IoMT devices in our dataset. Most of these vulnerabilities were disclosed after 2017. The peak in 2017 is because of KRACK and the EternalBlue issues shown in the table above. The peak in 2020 is because of Ripple20.



4. Open Ports and Internet Exposure: Why DICOM is Still Relevant

The figure below shows the most commonly open ports on IoMT devices (sorted by the percentage of IoMT devices in the dataset that have the port open). Not surprisingly, they are mostly related to web services (HTTP and HTTPS), Windows services (SMB, MSRPC and NetBIOS) as well as embedded device management and communication (SSH, Telnet, LPD, FTP). There is one port that is interesting to explore further: 104, which is used for DICOM communications.

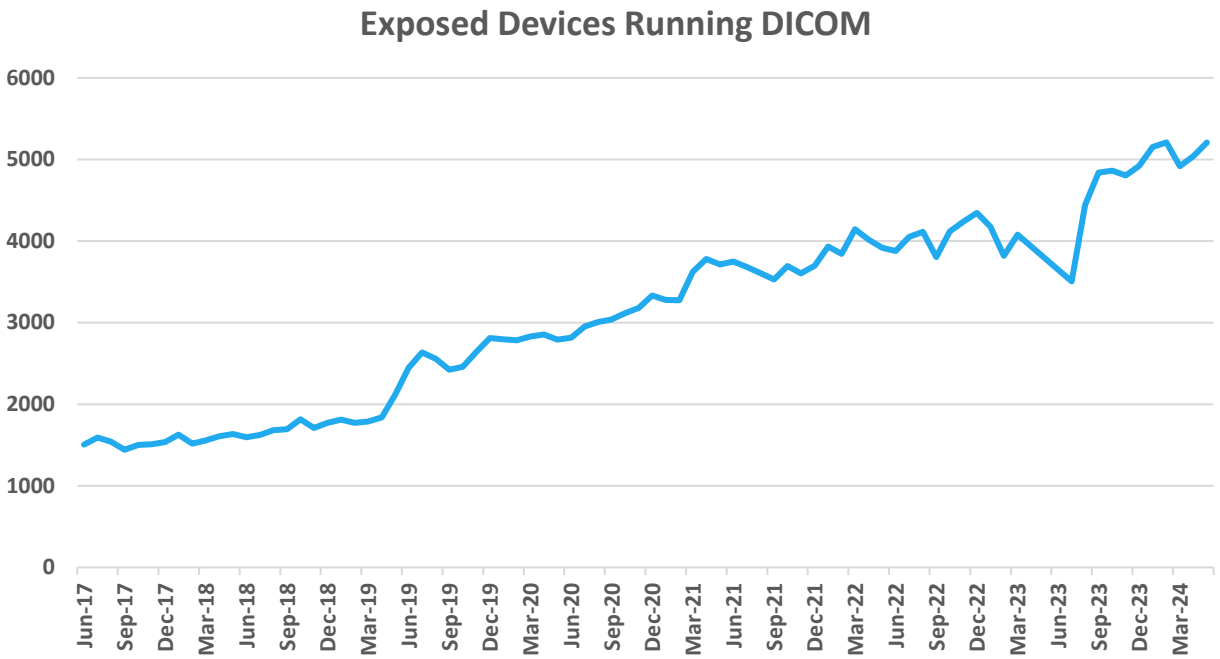


Digital Imaging and Communications in Medicine (DICOM) defines both the format for storing medical images and the communication protocols used to exchange them. As a de facto standard, DICOM is implemented by all major vendors of devices involved in medical imaging processes, such as diagnostic workstations, storage servers and medical printers.

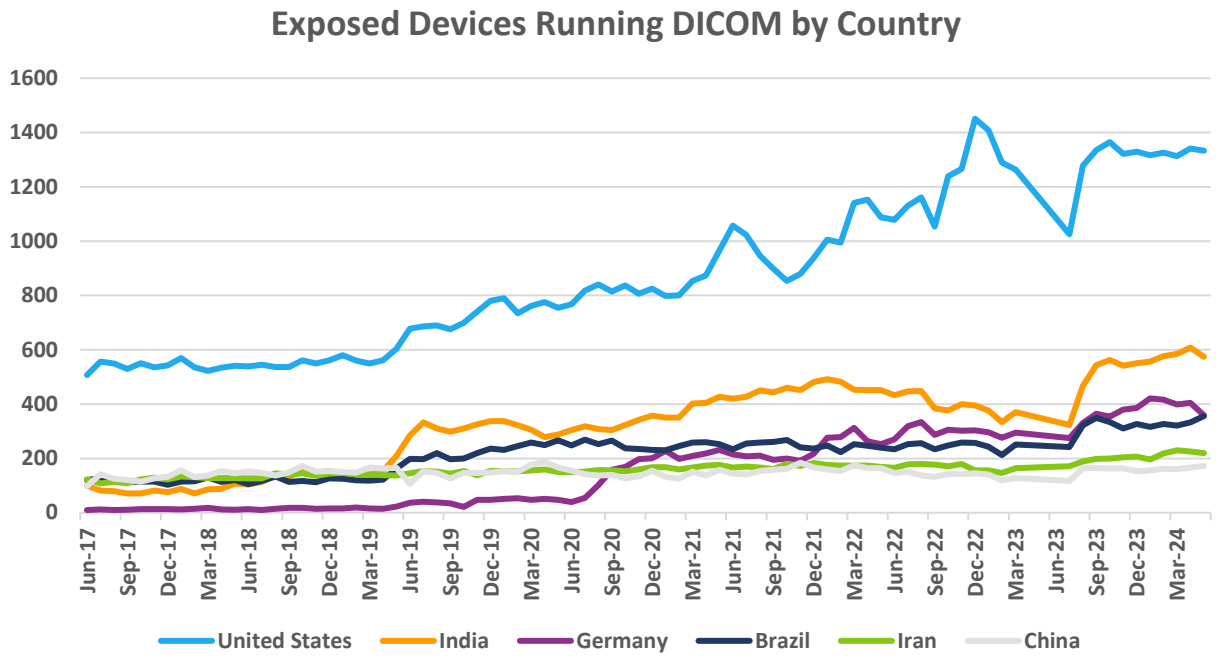
In the recent Riskiest Devices report, we showed that the IoMT devices most exposed to the internet are Picture Archiving and Communication Systems (PACS) running DICOM. We also published a dedicated study about internet exposure of medical devices in 2022 that reached the same conclusion.

To understand how things have changed in these almost two years, we again examined exposed DICOM servers on the internet using the Shodan search engine.

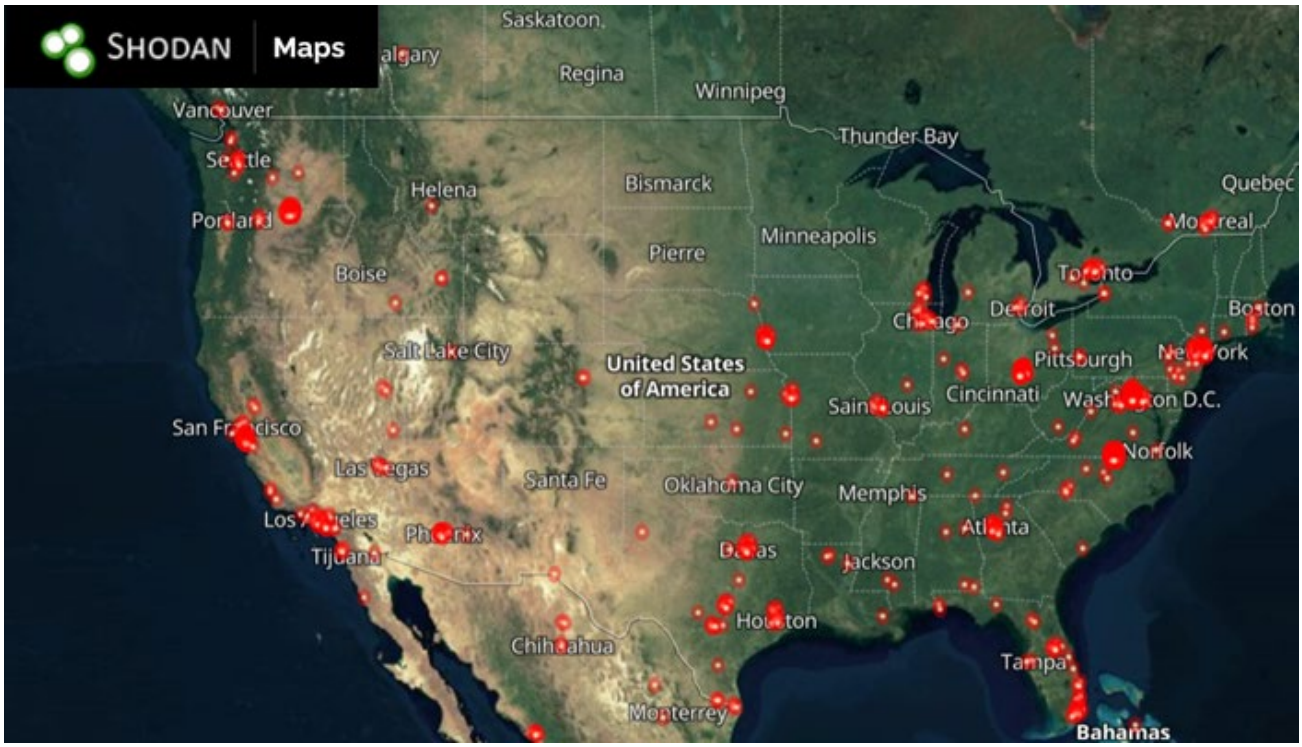
In August 2022, we reported 4,114 exposed DICOM servers with 825 of those being honeypot simulations, for a total of 3,289 real devices. In May 2024, we observe 5,207 servers with 1,013 honeypots, for a total of 4,194 real devices. That is a growth of 27.5% in less than 2 years. That is almost twice the rate of growth (15.4%) we observed for medical systems in general – such as EMR, integration systems and others – during the same period. It is also much greater than the *decrease* in exposed industrial control systems in the same period, which we recently reported. Looking back all the way to 2017 we see a growth of 246% in exposed DICOM servers.



The countries hosting the most DICOM servers have not changed much since 2022. The current top countries, in order, are the United States, India, Germany, Brazil, Iran and China, as shown below. They all exhibited a significant increase in exposed DICOM servers since 2017: 480% for India, 197% for Brazil, 163% for the US, 78% for Iran and 76% for China. Germany shows a change of 3,480% but that is due to a very small starting point of 10 servers in 2017, which seems too low and may be due to some quirk in Shodan not identifying these devices.



The figure below illustrates exposed DICOM devices all over the US.



5. Attacks on DICOM: Observed and Potential

The DICOM data model includes a *patient* connected to a series of *studies*, which are individual medical examinations. Each study may contain several *series* of related *images*, such as a set of MRI scans.

DICOM files may include not just patient images but also metadata, such as personally identifiable information (PII), including name, address, date of birth, gender and social security number; as well as protected health information (PHI), including information about the performed examinations.

The protocol used to operate on these files includes commands such as:

- C-FIND, used to search for objects on a server.
- C-GET, used to fetch objects from a server.
- C-STORE, used to stores objects on a server.

DICOM insecurity is not a new research topic. We discussed several possible attacks on DICOM in a past report, which itself cited other prior research. To update our previous research, below we describe some attacks that are possible leveraging these data and commands:

Data Breaches

Researchers recently showed that 45% of internet-exposed DICOM servers accept connections used to retrieve patient data (C-FIND and C-GET) with no authentication required. This situation has been known since at least 2018 but has not changed in more than half a decade. Another research at the end of 2023 showed that these exposed servers contain 59.5 million sensitive records: 16 million contain PII and 43.5 million contain PHI.

Data Tampering

Many of these servers also accept C-STORE commands that can be used to tamper with existing images, including injecting signs of conditions that will require medical treatment.

Vulnerability Exploits

When an attacker can send data or images to a server (for instance, using C-STORE), they may also exploit vulnerabilities on DICOM implementations that may lead to denial of service, information disclosure or even remote code execution. Our dataset had 641 different versions of DICOM implementations running on 5,300 devices. Among the most popular was OFFIS DCMTK, a library which was found to have serious vulnerabilities in 2022. The second most popular was an open-source project used by several vendors and we saw four more open-source implementations in the dataset. The security implications of the use of open source in medical applications and devices was recently reviewed by the HHS.

To understand which of these attacks are being perpetrated in the wild, we deployed a honeypot simulating a medical imaging device running a web server on port 80 and a DICOM server on port 11112 (a known alternative to the port 104 we saw in our dataset previously). The web server displayed the image of a known PACS server and the DICOM server supported commands such as C-FIND, C-GET (serving a set of open-source example DICOM images) and C-STORE.

We observed 1.6 million attacks on this honeypot in the past one year (May 2023 until May 2024), which is an average of one attack every 20 seconds. 88.6% of these attacks targeted port 80 (HTTP) with generic attempted exploits, such as log4shell. 10% of attacks were port scans or connection attempts on ports not running any significant service. However, 1.4% of requests – about 23,000 – targeted the DICOM server on port 11112.

Out of those 23,000, there were 8,633 valid DICOM interactions. Almost all of those were establishing connections, but 61 were relevant C-FIND commands searching for patient information.

In conclusion, exposed DICOM devices *are* being targeted by opportunistic attackers. Although most interactions are scans and automated attempts to exploit standard services such as HTTP, **there are attacks in the wild attempting to retrieve sensitive patient data**. We did not see evidence of attempts to tamper with images or to exploit specific DICOM vulnerabilities.

The fact that attackers are going after patient data should not be surprising, as we discuss below.

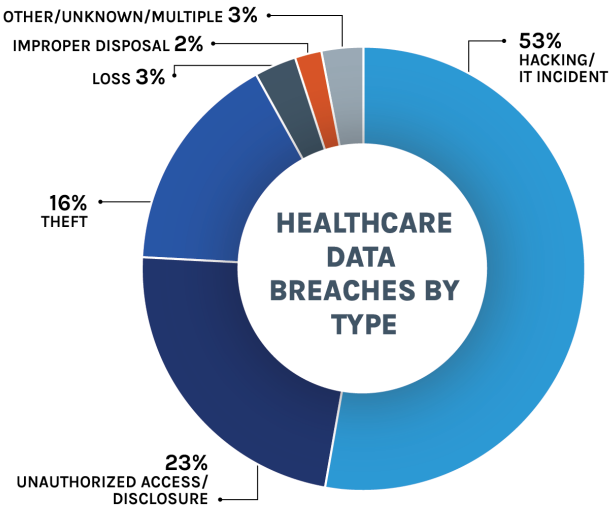
6. The Effects of Healthcare Vulnerabilities: Data Breaches

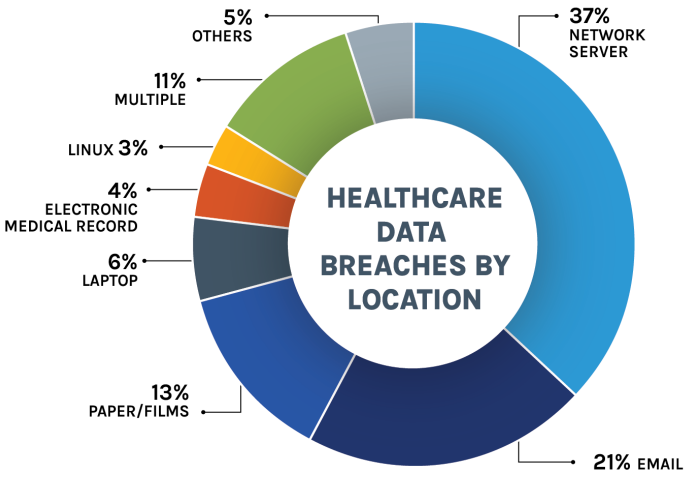
Although there is much discussion in the cybersecurity community about the possible physical impact of attacks on medical devices, as we showed above attackers are mostly after patient data that can be exfiltrated and later sold on underground markets or used to extort an HDO.

We have also demonstrated in the past an attack that could disrupt IoMT and other connected devices in a hospital, but we are yet to see this kind of complex targeted attack in a real HDO – a sort of “Stuxnet moment” for IoMT. What we do observe constantly is the rise in data breach incidents.

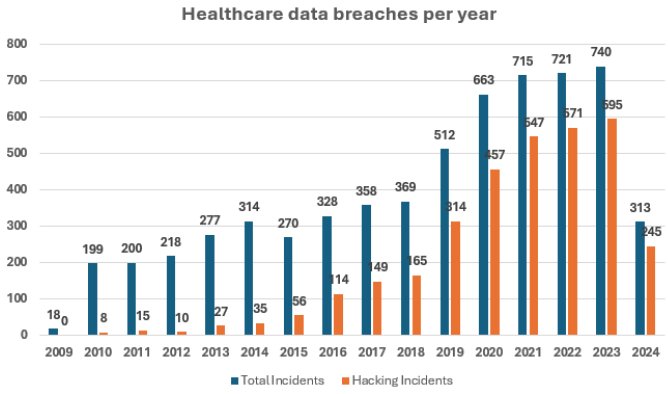
As of June 3, 2024 there were 6,215 incidents on the breach portal of the U.S. Department of Health and Human Services (HHS), which is required to report breaches affecting more than 500 patients dating all the way back to 2009.

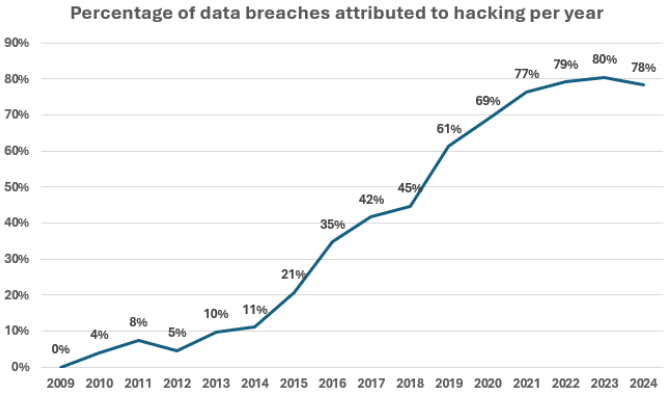
The 6,215 incidents are categorized by type of breach and location of breached information as follows:





Clearly most of these incidents were due to hacking and targeted network servers or e-mails. The figure above does not, however, give the real dimension of the *growth* in hacking incidents. **Hacking incidents went from 0% of data breaches to close to 80% in 15 years.** Taking the last full year of data (2023) as a basis, the 595 hacking incidents in 365 days represent an average of 1.6 data breaches per day on healthcare institutions. Keep in mind that this only includes incidents with 500 or more affected patients. Taking into account all the incidents in the database, the average data breach affected around 93,100 individuals. However, that number is also growing. In 2023, the average incident affected almost 200,000 people.





Not all those breaches leverage medical devices, but that type of device can provide attackers with a plethora of sensitive information, as we have shown in the DICOM case, which means that HDOs should pay special attention to securing these devices.

7. Mitigation Recommendations

Although healthcare organizations have been making progress in reducing cybersecurity risk after a series of devastating attacks, IoMT devices remain critical. We recommend HDOs prioritize the following best practices to reduce security risk in their networks.

Identify and Classify Every Asset

HDOs will have to contend with medical devices running legacy or non-standard operating systems for the foreseeable future. Hence, it is imperative to first identify and classify these devices to understand how to mitigate this risk. Devices that cannot be retired or patched should be segmented appropriately to restrict access to critical information and services only.

Limit External Communications and Exposure

Network flow mapping of existing communications is not just a prerequisite for designing effective segmentation zones. It also provides a baseline understanding of external and internet-facing communication paths. This can help identify unintended external communications and prevent medical data from being exposed publicly.

Implement Effective Segmentation

Segmentation is a foundational control for risk mitigation in networks with a diversity of IT, IoT, OT and IoMT devices. However, segmentation requires well-defined trust zones based on device identity, risk profile, and compliance requirements for it to be effective in reducing the attack surface and minimizing blast radius.

While there is increasing awareness of the benefits of segmentation, examples of poorly designed segmentation zones abound. Start by accurately identifying devices you want to segment by business context and understanding existing network flows between device groups. Then design appropriate zones and access policies to gain the positive security outcomes of segmentation.

Monitor All Network Traffic for Malicious Packets

These packets may try to exploit known vulnerabilities or possible zero-days on medical devices. Anomalous and malformed traffic should be blocked – or at minimum – alert its presence to network operators.

Other resources include:

- NIST has a series of guides for securing specific healthcare devices, such as infusion pumps and PACS systems
- CISA released a comprehensive mitigation guide for the healthcare sector in 2023