The Riskiest Connected Devices of 2025

April 9, 2025

FORESCOUT RESEARCH

VEDERE LABS

TABLE OF CONTENTS

RISKIEST DEVICES

ACTIONS FOR CISOs

WHAT YOU NEED TO KNOW

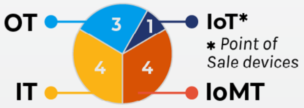
Network devices are the riskiest – especially routers

- **>50%** of devices with the most critical vulnerabilities are routers
- Plenty of risk across IoT, OT and medical devices

Alarming trend in open ports:

- SSH use – which is encrypted – declined across all industries
- Telnet use – which is not encrypted – increased in every industry

12 BRAND NEW device types



Industry Perspective

15% increase in average device risk in all sectors

1. Retail
2. Financial services*
3. Healthcare
4. Government

*Financial services have the most open ports

Top Risk by Country

1. Spain
2. China
3. UK
4. Qatar
5. Singapore

U.S. is tied with three countries for 7th place

New OT Risks

Universal gateways • Data historian servers Physical access control systems

New Medical Device Risks

Blood and urine analyzers • Laboratory Information Systems (LIS) • Healthcare workstations • Infusion pump controllers

WHAT YOU NEED TO DO

APPROACH

- ✓ Use a comprehensive risk and exposure management strategy
- ✓ Identify, prioritize and mitigate risk across all device types
- ✓ Don't treat IT, OT, IoT and IoMT security in silos

AVOID

- ✓ Solutions that only address specific devices
- ✓ OT or IoMT-only solutions cannot effectively assess IT risk
- ✓ IT-focused tools lack visibility into specialized devices

MITIGATION

- ✓ Use automated, proactive controls that extend across the entire enterprise and accelerate response
- ✓ Do not depend solely on security agents
- ✓ Ensure continuous risk reduction across all interconnected systems

⚠ Windows 10 ⚠

Microsoft Windows

Take Note: > 50% of non-legacy Windows devices run Windows 10 (regular support ends in 2025)

- ▶ If on Windows 10, update to Windows 11 as soon as possible
- ▶ In environments where upgrades are challenging, consider extended support and pay close attention to new vulnerabilities.

<) FORESCOUT.

1. Executive Summary

Since 2020, Forescout Research - Vedere Labs has been monitoring the riskiest devices in organizational networks, leveraging data sourced directly from the devices themselves. This marks our fifth report in six years.

For the 2025 edition, we continue our data-driven approach, analyzing millions of devices in Forescout's Device Cloud using our multifactor risk scoring methodology to assess the most vulnerable devices in enterprise networks. Over the years, we have observed some device types consistently appear in these lists due to their inherent criticality or persistent security neglect. Yet, others fluctuate in risk level based on shifts in the threat landscape and attackers' interest in finding new entry points through devices.

Our latest findings confirm a trend first noted last year: **Network equipment – especially routers – has overtaken endpoints as the riskiest category of IT devices.** Driven by increased threat actor focus, adversaries are rapidly exploiting new vulnerabilities in these devices through large-scale attack campaigns. Additionally, **there are 12 new device types in this year's list making it the largest year-over-year change we have observed.** This finding reinforces attackers' continuous pursuit in exploiting new device classes — and the importance for security professionals to stay on top of the latest risks.

KEY FINDINGS

- **Retail has the riskiest devices on average** followed by financial services, government, healthcare, and manufacturing:
  - Industry-wide risk levels have increased by 15%
  - Gaps in risk scores between industry sectors are now minimal
- **The top three countries with the riskiest devices on average are Spain, China and the UK.**
  - Average risk per country rose (by 33%)
  - Differences between individual countries narrowed
- **Special-purpose operating systems (e.g. embedded firmware), are now more prevalent than mobile OSes across all industries**
  - Highest concentrations in healthcare (16%), government (14%) and manufacturing (12%)
  - These OSes grew in these three industries YoY but government had the sharpest rise (from 8.6% to 14%)
- **Legacy Windows versions remain most common in government (2.7%), healthcare (2.2%) and manufacturing (1.8%).**
  - Every industry except government reduced its share of legacy Windows devices
  - Government increased from 1.2% to 2.7%
  - Retail had the biggest reduction (from 4.3% to 0.5%)
- **Across all industries, more than 50% of non-legacy Windows devices still run Windows 10, and**
  - Support for Windows 10 ends in 2025
  - Retail and healthcare have the highest proportion with around 75% of non-legacy Windows devices on Windows 10
- **Encrypted SSH use declined while unencrypted Telnet use increased across every industry.**
  - Government saw the largest growth in Telnet usage (rising from 2% to 10% of devices)
  - Telnet and SSH are now most prevalent in government networks
- **SMB usage increased in financial services and government but declined elsewhere.**
  - RDP usage grew in financial services, healthcare and manufacturing
  - RDP decreased in government and retail
  - Both SMB and RDP are now most prevalent in financial services
- **The most frequently vulnerable device types are computers, routers, and wireless routers/access points.** Over 50% of devices with the most critical vulnerabilities are routers.

QUANTIFYING DEVICE CYBERSECURITY RISK

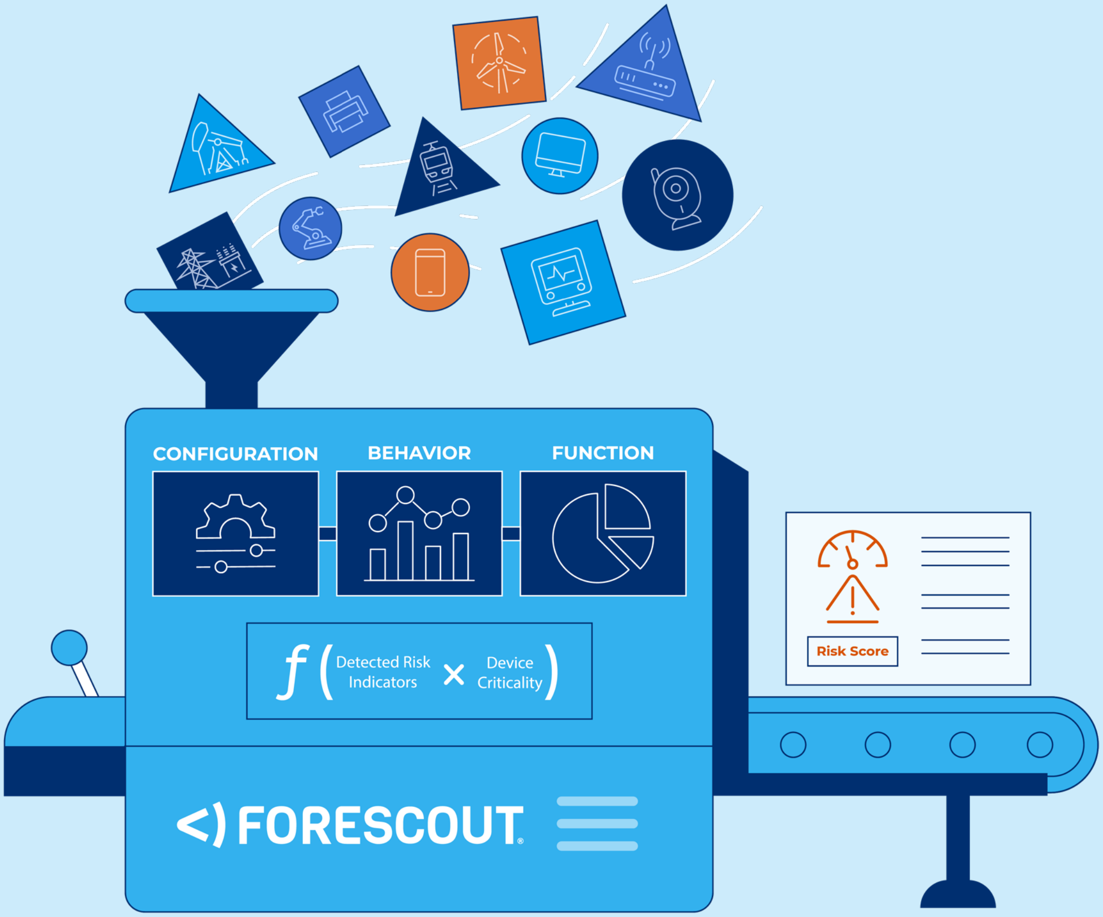
We assess device cybersecurity risk using a multifactor risk scoring methodology based on three key factors:

Configuration evaluates the number and severity of vulnerabilities on the device, as well as the number and criticality of open ports.

Function measures the potential organizational impact if the device is compromised.

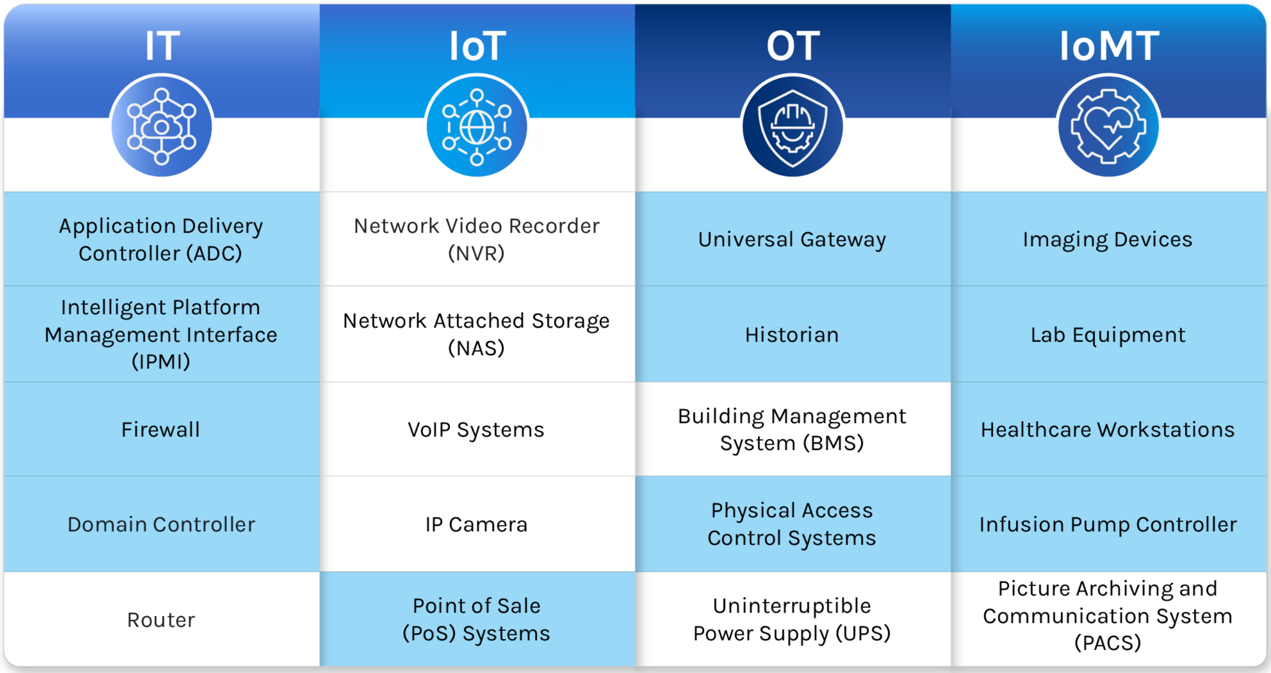
Behavior assesses the device's internet exposure.

Each device receives a risk score ranging from 1 to 10. After scoring individual devices, we calculate average risk score per device type to determine which categories pose the greatest risk. For this report, we analyzed device data from Forescout's Device Cloud covering the period January 1 to February 28, 2025.



2. Riskiest Connected Devices of 2025

Using our dataset and multifactor risk-scoring methodology, we identified the five riskiest device types across four major categories: Information Technology (IT), Internet of Things (IoT), Operational Technology (OT) and Internet of Medical Things (IoMT).



IT	IoT	OT	IoMT
Application Delivery Controller (ADC)	Network Video Recorder (NVR)	Universal Gateway	Imaging Devices
Intelligent Platform Management Interface (IPMI)	Network Attached Storage (NAS)	Historian	Lab Equipment
Firewall	VoIP Systems	Building Management System (BMS)	Healthcare Workstations
Domain Controller	IP Camera	Physical Access Control Systems	Infusion Pump Controller
Router	Point of Sale (PoS) Systems	Uninterruptible Power Supply (UPS)	Picture Archiving and Communication System (PACS)

Source: Forescout Research Vedere Labs

Table 1 – Riskiest connected devices per category

Of the 20 riskiest device types identified in 2025, only eight were also featured in the 2024 report. Remaining on the list are:

- Routers, VoIP systems, IP cameras and UPS devices which have consistently appeared since 2022
- NAS and BMS which have remained since 2023
- NVR and PACS which first appeared in 2024

Meanwhile, 12 new device types (marked in blue) are making a first “riskiest device” appearance. This represents the largest year-over-year change observed to date, underscoring attackers’ growing interest in targeting emerging device types.

IT Devices

The riskiest IT device category saw considerable changes from 2024 as four new device types enter the list.

ADCs, Firewalls, and Routers

In 2023, endpoints were considered riskier than network infrastructure. However, this trend reversed last year. In 2025, network infrastructure remains the riskiest category — since these devices are often exposed at the network perimeter with open administrative ports.

While routers remain on the list from last year, ADCs and firewalls are new additions. ADC devices typically sit in data centers between firewalls and internal application servers to provide web acceleration and load balancing.

Firewalls and routers are essential for securing and enabling communications with external networks. However, all three device types are now routinely affected by high-severity vulnerabilities — many which are actively exploited as zero day threats.

IPMI

IPMI is a hardware-based, out-of-band server management specification that relies on a Baseboard Management Controller (BMC) chip. Often referred to as "lights-out management," IPMI allows for remote server management even when systems are powered off. Unfortunately, IPMI devices are riddled with critical vulnerabilities, including some with public exploits available for years and others that were recently discovered in 2024. Attackers, including those deploying sophisticated malware, have actively exploited these flaws.

Domain Controllers

These are dedicated servers responsible for authentication within a network domain. They determine whether a host can access domain resources and store user credentials and security policies – essentially holding the "keys to the kingdom." As a result, domain controllers are among the most critical assets in internal networks, making them a prime target for ransomware attacks. Threat actors frequently compromise them post-initial access using them as pivot points for lateral movement within a network.

IoT Devices

The riskiest IoT devices include several persistent threats from previous years along with the new addition of PoS systems.

NVRs, VoIP Systems and IP Cameras

These remain high-risk because they are often exposed to the internet, contain easily exploitable vulnerabilities and have a long history of being targeted by both cybercriminal botnets and Advanced Persistent Threats (APTs).

NAS Systems

These network-attached storage systems share the same risks as other IoT devices – internet exposure, vulnerabilities, and frequent exploitation. However, they face an additional threat from ransomware actors. Since 2021, with the advent of QLocker, ransomware groups have increasingly targeted NAS systems. Today, multiple ransomware families are specifically designed to infect NAS devices, exploiting the valuable data they store and their security weaknesses.

Point of Sale Devices

PoS devices process customer transactions, such as sales in retail stores. They may run traditional IT operating systems (e.g. Windows) or dedicated embedded OSes. These devices have long been prime targets for cybercriminals, who deploy keyloggers and infostealers to capture sensitive data. Additionally, RAM scrapers scan the system's memory for credit card numbers and payment data before encryption. Certain PoS devices also contain specific vulnerabilities that attackers can exploit to gain deeper system access.

OT Devices

The riskiest OT devices saw several changes this year, with Universal Gateways and Historians appearing on the list for the first time.

Universal Gateways

These facilitate communication between systems using different protocols (e.g. Modbus and EtherNet/IP) and are commonly at Purdue levels 1 and 2. Their risk stems from interconnecting disparate systems, sometimes bridging both Ethernet and serial communications. This introduces the potential for lateral movement within OT networks and enables threats from the Ethernet network to impact serially connected devices – a concern highlighted in our Deep Lateral Movement research.

Historians

These servers store operational process data, typically deployed at Purdue level 3. Because they exchange data with enterprise IT systems they sit at the high-risk junction between IT and OT networks. According to SANS, 10% of OT incidents in 2024 involved data historians as an initial access vector. That same report also identified remote storage and processing of historian data as the second and fourth most common OT cloud adoption use cases, potentially expanding OT networks' attack surface.

BMSs and Physical Access Control Systems

These are critical for facilities management across many industries. There have been multiple instances of smart buildings exploited by threat actors to disable controllers and render them unusable, recruit vulnerable physical access control devices into botnets, or compromise management workstations for initial access into enterprise networks. These devices combine the insecure-by-design nature of OT with IoT's internet connectivity, making them highly susceptible to online exposure - even in critical facilities.

UPS

Uninterruptible power supplies play a crucial role in power monitoring and data center power management. CISA has warned about threat actors targeting UPSs with default credentials, enabling attackers to disrupt critical infrastructure by shutting off power in a critical location or tamper with voltage settings, potentially damaging sensitive equipment.

IoMT Devices

The riskiest medical devices saw significant changes from 2024, with four new device types entering the list – similar to the IT category.

Imaging Devices

These includes CT scanners, PET-CT scanners and X-ray machines, which generate medical images and are often connected to **PACS systems** for storage and retrieval. They frequently run legacy, vulnerable IT operating systems and require extensive network connectivity to facilitate image sharing. They rely on the DICOM standard (Digital Imaging and Communications in Medicine) for sharing these files, which defines both image formats and communication protocols. In a recent report, we examined real-world attacks searching for patient data in medical honeypots and threat campaigns leveraging DICOM applications to infect patients and healthcare institutions.

Lab Equipment

These devices, such as blood and urine analyzers, are essential for diagnostic laboratories to process biological samples and provide critical health data. These devices typically run specialized operating systems and are connected to Laboratory Information Systems (LIS). A major concern is that data transmission between lab equipment and LIS is often unencrypted, leaving It vulnerable to data exfiltration and data tampering attacks.

Healthcare Workstations

These are used to interface with various medical data and equipment, including DICOM workstations, treatment planning systems, and diagnostic terminals. These systems handle clinical data using standardized formats such as HL7 (Health Level 7) to integrate with, electronic health records (EHR) and billing systems. These devices provide access to highly sensitive medical information, which is valuable on the dark web and frequently targeted by ransomware gangs.

Infusion Pump Controllers

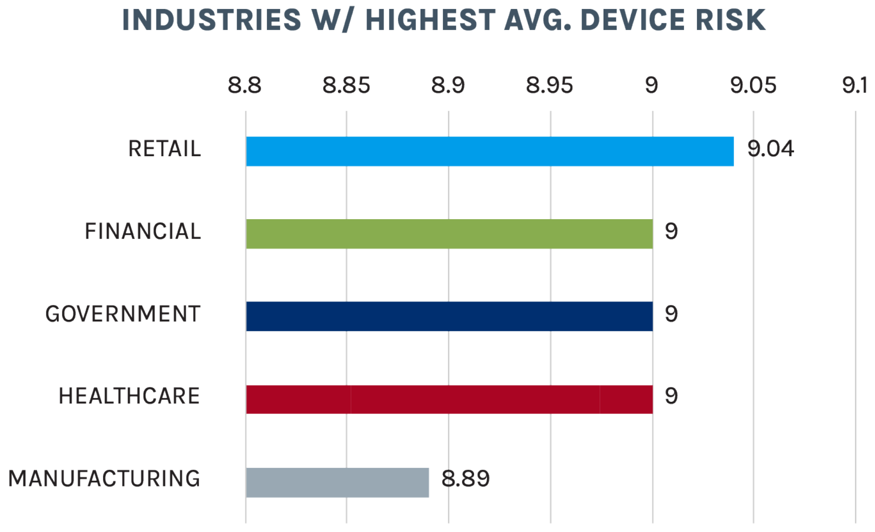
These manage modular infusion pump systems, regulating medication dosage and infusion duration for patients. As the "brains" of modular infusion systems, they are among the most common and critical devices in hospitals. A successful compromise could allow an attacker to tamper with drug delivery settings, posing serious risks to patient safety.

3. Detailed Analysis

3.1. Risk by Industry

Figure 1 illustrates the distribution of average device risk by industry in our dataset. For this analysis – and the discussions in the following sections - we selected the five industries with the largest number of connected devices.

In 2025, retail has the highest average device risk followed by financial services, government, and healthcare. Manufacturing ranks fifth. The gap in risk scores between industries has narrowed — with an overall average risk score of 8.98. This marks a significant 15% increase from 2024's average of 7.73 — highlighting a growing cybersecurity threat across all sectors.

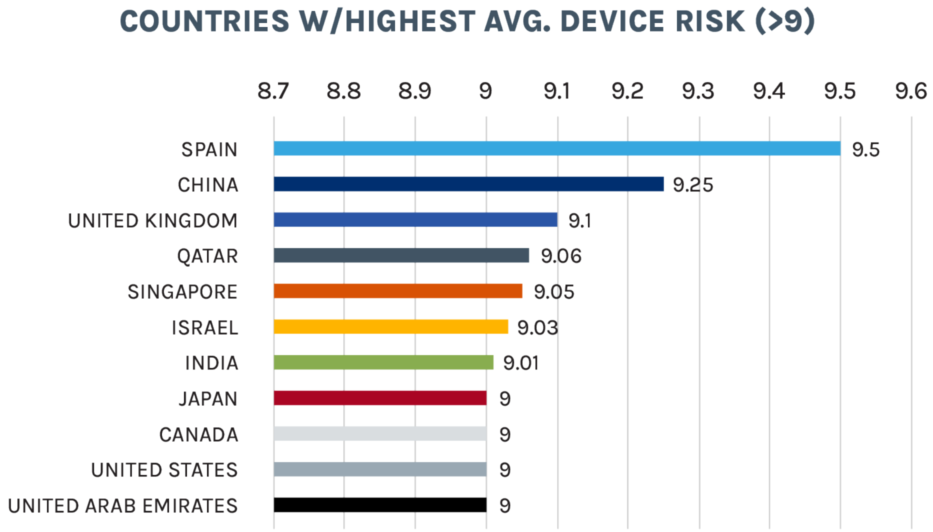


Source: Forescout Research Vedere Labs

Figure 1 – Industries with the highest average device risk

3.2. Risk by Country

Figure 2 presents the distribution of average device risk by country in our dataset. For this analysis, we selected the 11 countries where the average device risk was 9.0 or higher. The top three countries with the riskiest devices are Spain, China and the UK. As with industries, the average risk per country has also increased significantly this year. In 2024, the average risk for the top 10 countries was 6.53, whereas in 2025 it has risen to 9.1 – a 33% increase, highlighting a sharp escalation in cybersecurity risk worldwide.



Source: Forescout Research Vedere Labs

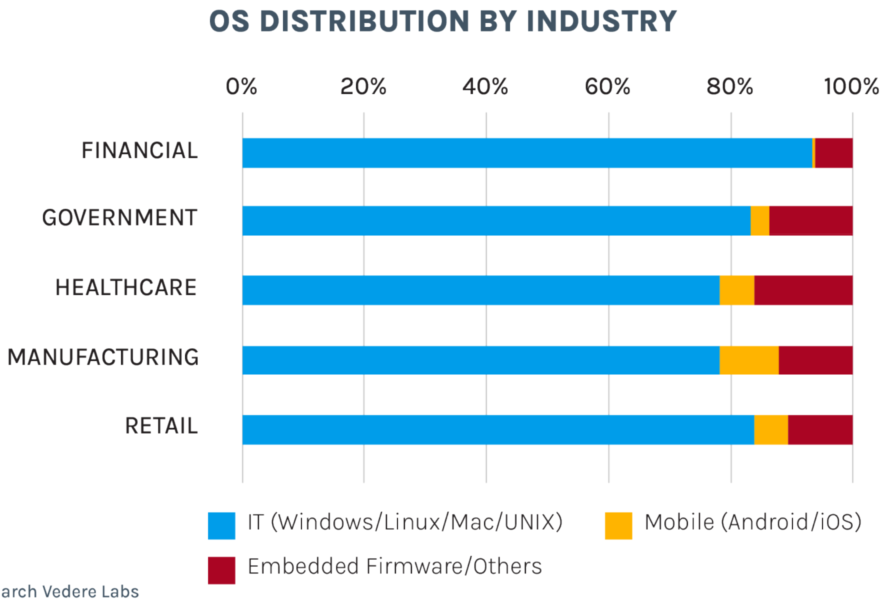
Figure 2 – Countries with the highest average device risk

3.3. Operating Systems

The devices across the five industries in our dataset run a variety of operating systems, as shown in Figure 3. In every industry, traditional IT operating systems – such as Windows, Linux, macOS, and UNIX – remain dominant. This includes many specialized IoT, OT, and IoMT devices that operate on Linux or Windows.

The financial services sector has the highest proportion of IT devices — with 93% running IT operating systems. However, special purpose operating systems, including embedded firmware and networking Oses, are prevalent in healthcare (16%), government (14%) and manufacturing (12%). These specialized OSes now outnumber mobile operating systems across all industries — which continues a trend we first observed in 2024. The presence of embedded OSes grew in government, healthcare and manufacturing. Government is experiencing the largest increase (from 8.6% in 2024 to 14% in 2025). Conversely, financial services and retail experienced a slight decline in embedded OS adoption.

The sheer variety of special-purpose OSes – with over 2,500 unique versions observed in Forescout's Device Cloud – poses a significant challenge for security teams. Tracking and managing these systems is a major visibility issue for organizations. Moreover, embedded firmware is notorious for systematic security flaws including, backdoors, hardcoded credentials and cryptographic keys, and memory corruption vulnerabilities. These risks underscore the critical need for continuous network visibility and security monitoring across all industries.

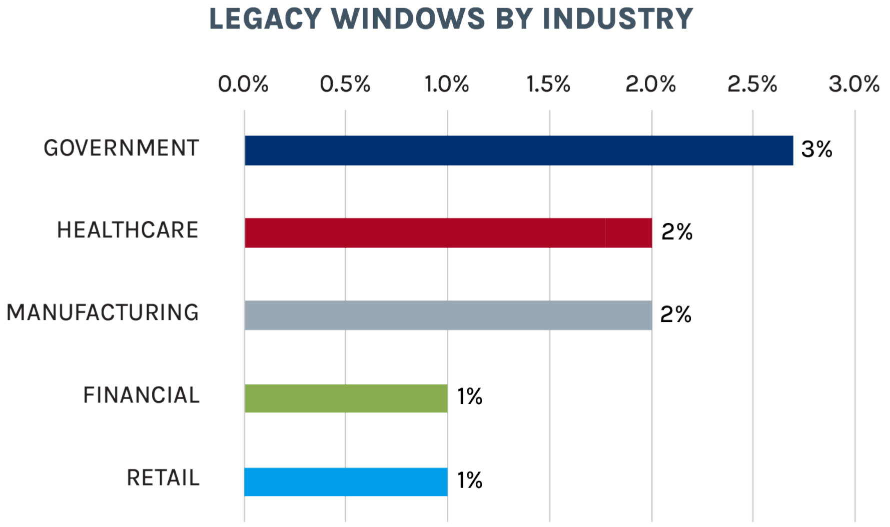


Source: Forescout Research Vedere Labs

Figure 3 – OS distribution by industry

Since Windows remains the most widely used operating system across all industries, we analyze the versions in use. We categorize Windows versions into two groups: Currently supported – Windows 10 and 11 – and legacy including, Windows 8, 7, XP, CE, and older unsupported versions.

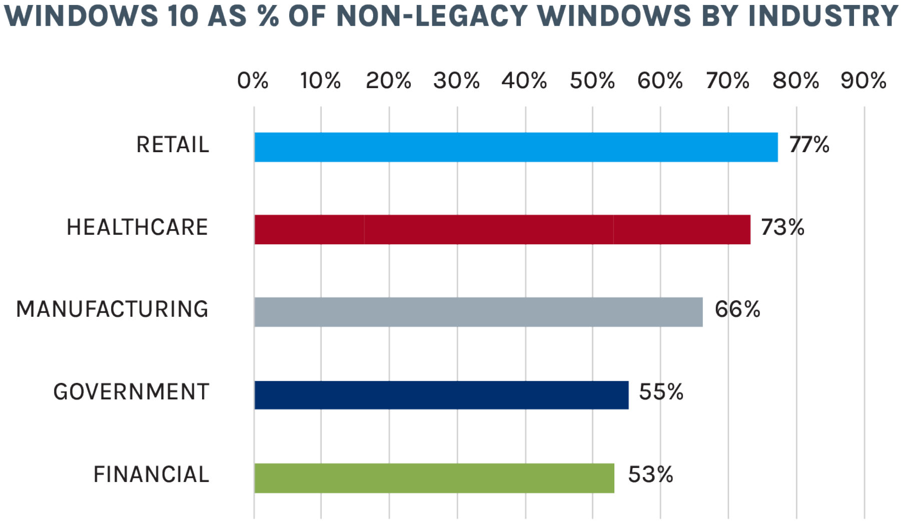
Figure 4 illustrates the percentage of devices running legacy Windows versions by industry. Government has the highest percentage of legacy devices (2.7%), then healthcare with 2.2%, and manufacturing at 1.8%. Every industry except government reduced its share of legacy Windows devices compared to 2024. Government's percentage increased from 1.2% to 2.7%. Retail saw the highest reduction, dropping from 4.3% in 2024 to just 0.5% in 2025.



Source: Forescout Research Vedere Labs

Figure 4 – Legacy Windows by industry

Although it is not considered a legacy version yet, Windows 10 will reach end of support by October 14, 2025. As with previous versions, Microsoft will offer an extended security updates (ESU) program priced at $61 per device for the first year with the cost doubling annually for up to three years. For organizations with thousands or even hundreds of thousands of devices, this expense could become substantial. Given this, we analyzed which industries have the highest percentage of non-legacy Windows devices still running Windows 10. Alarmingly, in all five industries more than 50% of non-legacy Windows devices still operate on Windows 10. Retail and healthcare have the highest percentages of non-legacy devices still running Windows 10 — both are over 70%. Although we expect to see organizations transition to Windows 11 over time, there will likely be a period of delayed upgrades, so the number of legacy devices will increase in 2026 as Windows 10 support ends.



Source: Forescout Research Vedere Labs

Figure 5 – Windows 10 as percentage of non-legacy Windows by industry

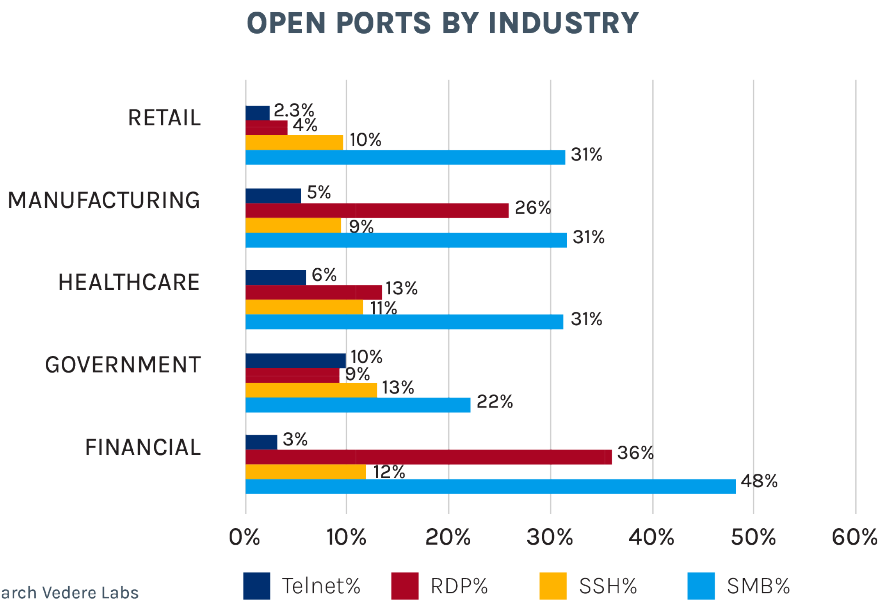
3.4. Open Ports

Open ports expose devices to attacks by enabling both known vulnerabilities and potential zero-day exploits. For this analysis, we examined four commonly exploited ports selected from those most targeted in 2024. **Server Message Block Protocol (SMB)** is used by Windows machines for file sharing, printer sharing and remote service access. **Remote Desktop Protocol (RDP)** provides graphical remote management for Windows devices. **Secure Shell (SSH)** enables command-line remote management primarily for Linux/UNIX servers and IoT devices. **Telnet** also provides an unencrypted remote management protocol still used in legacy and specialized devices.

Figure 6 illustrates the percentage of devices in each industry with an open instance of these protocols. **SMB remains the most widely-used protocol across all industries.** SSH is the second most common in all industries except financial services and manufacturing, where RDP takes second.

We did notice a concerning trend: The use of SSH – which is encrypted – declined across all industries but the use of Telnet – which is not encrypted – increased in every industry. The largest rise in Telnet usage occurred in government networks – growing from 2% to 10% of devices – which correlates with the rise in embedded operating systems. SMB usage increased in financial services and government but declined in other industries. RDP usage increased in financial services, healthcare, and manufacturing, but declined in government and retail. Telnet and SSH are now most prevalent in government. SMB and RDP remain dominant in financial services.

These trends indicate a shift in protocol exposure across industries, with an increasing number of legacy and embedded devices relying on insecure remote management methods — raising significant cybersecurity concerns.



Source: Forescout Research Vedere Labs

Figure 6 – Open ports by industry

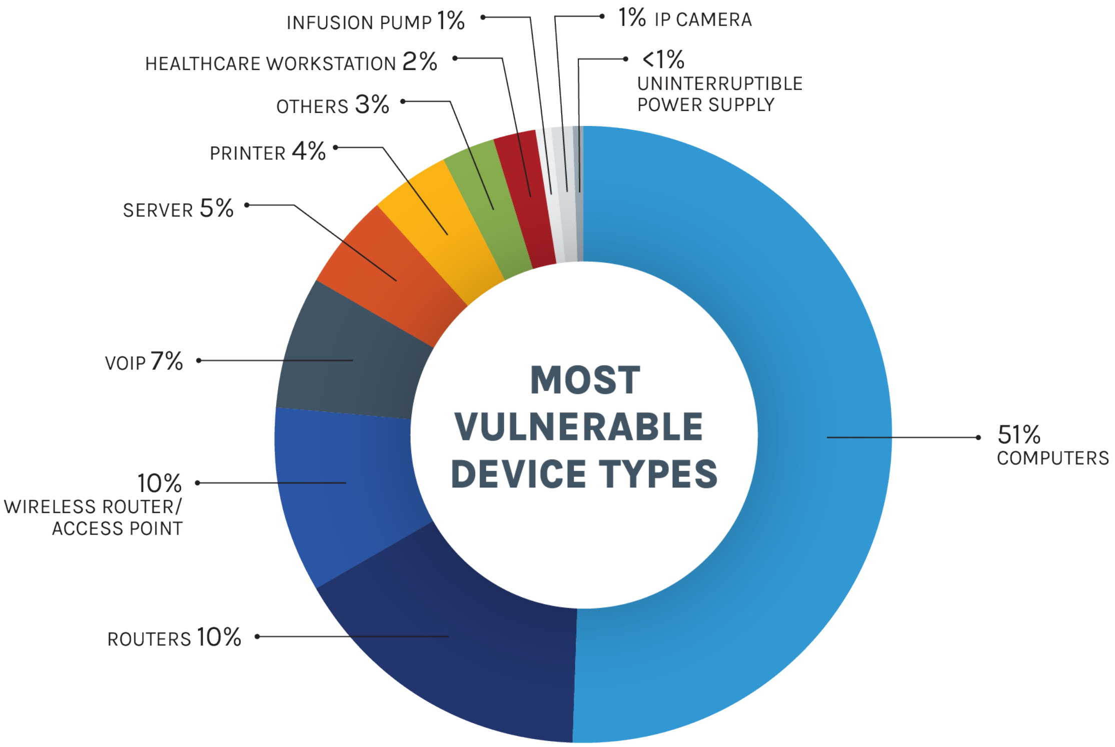
3.5. Vulnerabilities

Figure 7 highlights the most frequently vulnerable device types. Notably, five of the top 10 device types also appear among the riskiest devices listed in Table 1. This emphasizes that vulnerabilities are a major risk factor for connected devices.

While Figure 7 considers all vulnerabilities, Figure 8 focuses exclusively on the most dangerous ones that are classified with critical severity and extreme exploitability scores. The difference is very clear: **Computers have the highest number of vulnerabilities overall but not the most dangerous ones.** When considering only the most dangerous vulnerabilities, **routers surpass computers, accounting for half of the most critical vulnerabilities in organizational networks.**

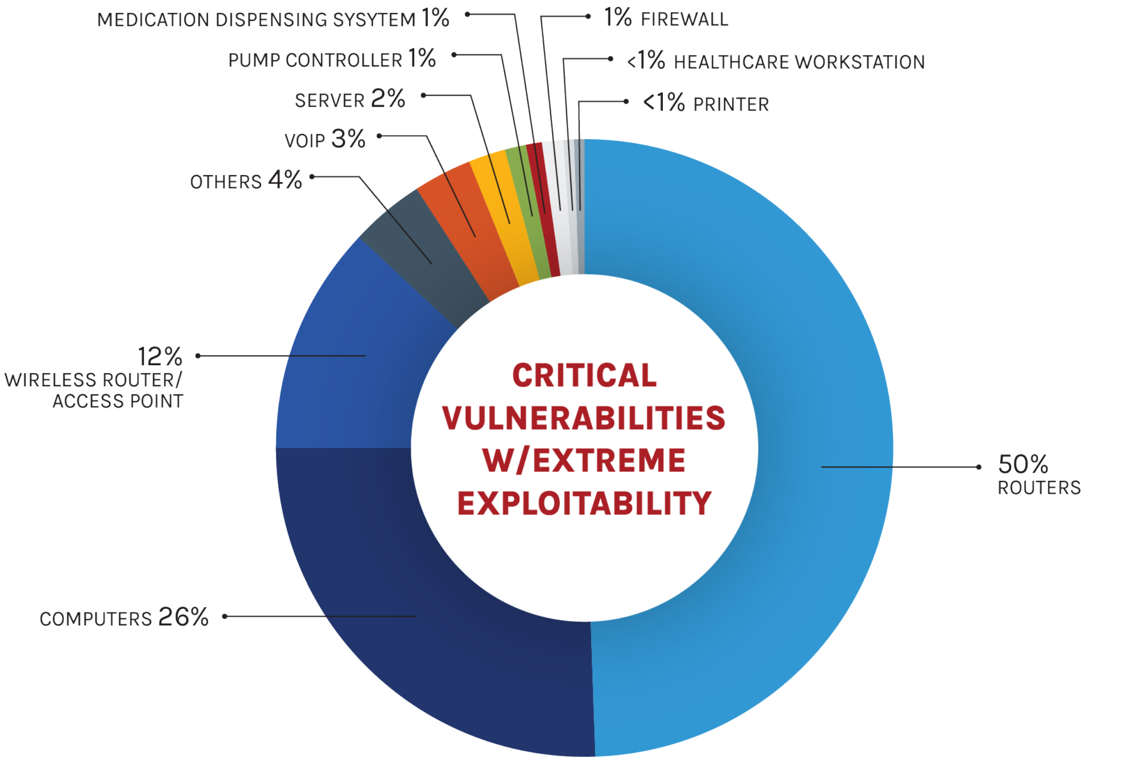
Several IoMT devices, including pump controllers, medication dispensing systems and healthcare workstations, appear among the devices with the most dangerous vulnerabilities — highlighting the increasing cybersecurity risks in healthcare environments.

This distinction between total vulnerabilities and highly exploitable ones reinforces why network infrastructure and medical devices are prime attack targets in 2025.



Source: Forescout Research Vedere Labs

Figure 7 – Most vulnerable device types



Source: Forescout Research Vedere Labs

Figure 8 - Most vulnerable device types with critical vulnerabilities w/ extreme exploitability

4. Conclusion

The attack surface in modern organizations now spans IT, IoT and OT, with IoMT adding another layer of complexity in healthcare. Focusing security efforts on a single category is no longer sufficient, as attackers exploit devices across different domains to execute attacks. We previously demonstrated this with R4IoT, an attack that begins with an IP camera (IoT), moves to a workstation (IT) and disables PLCs (OT) – illustrating the interconnected nature of today's cyber threats.

This report has analyzed the current risk levels across this expanded attack surface, identifying the most vulnerable devices that demand immediate attention from security teams.

To effectively defend this evolving attack surface, organizations must adopt modern security strategies that address risk across all device categories. As threat actors continue shifting their focus away from traditional endpoints, they increasingly target less-protected devices that offer easier initial access. A comprehensive risk and exposure management strategy must identify, prioritize and mitigate risk across IT, OT, IoT and IoMT – rather than treating them in silos. Avoid solutions that only address specific devices, since these fail to provide a complete picture of risk. For example, OT or IoMT-only solutions cannot effectively assess IT risk, just as IT-focused tools lack visibility into specialized devices.

Beyond risk assessment, mitigation should leverage automated controls that extend across the entire enterprise – not just isolated environments like IT, OT, or specific IoT networks. Moreover, these controls should not depend solely on security agents, ensuring that organizations maintain continuous risk reduction across all interconnected systems.