The Riskiest Connected Devices in 2026

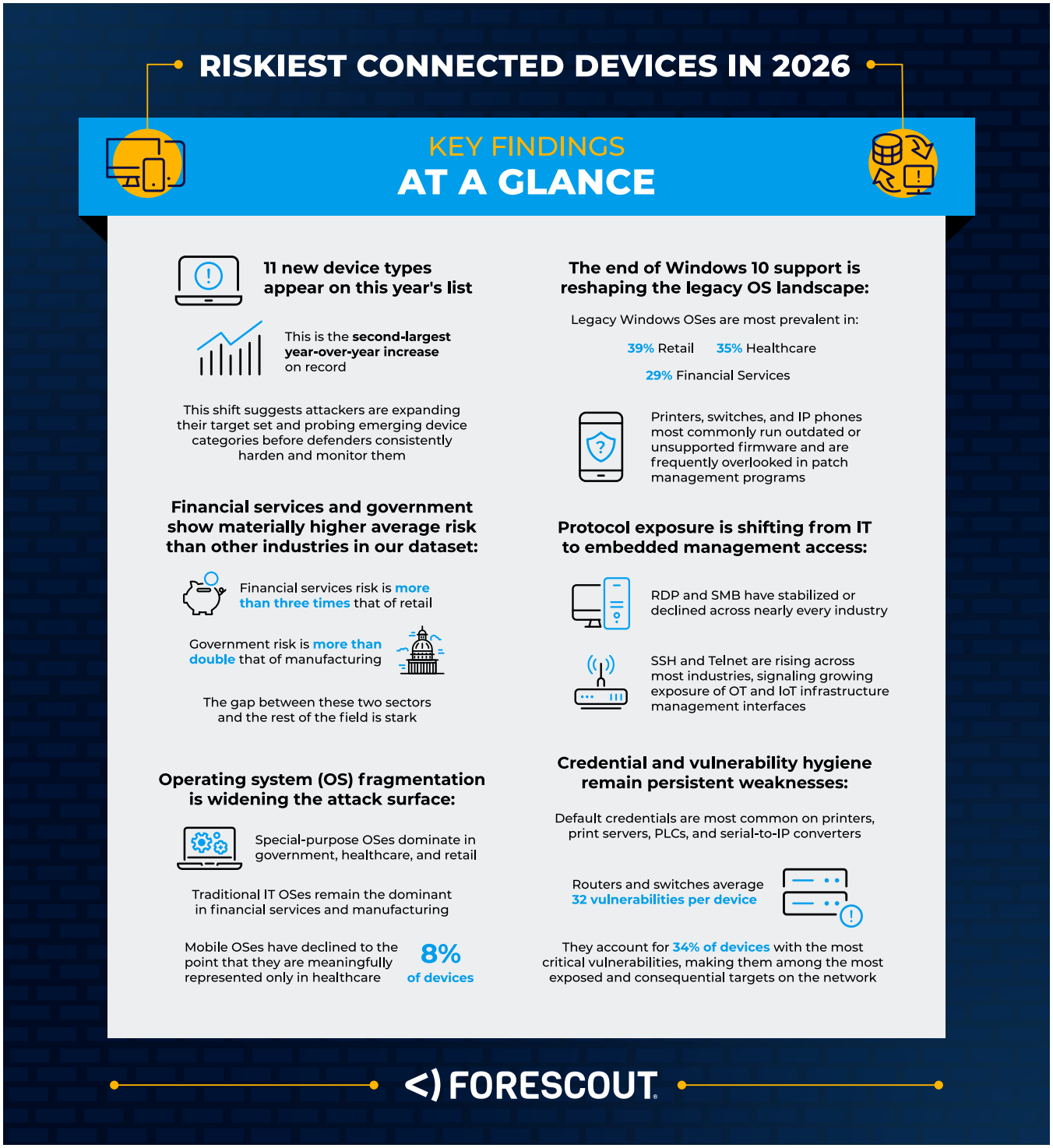
MARCH 23, 2026

FORESCOUT RESEARCH | VEDERE LABS

Contents

1. Executive Summary

Since 2020, Forescout Research – Vedere Labs has monitored the riskiest connected devices in organizational networks using telemetry drawn from assets in the Forescout Device Cloud. For the 2026 edition, we continue our data-driven approach, analyzing millions of devices with our multifactor risk scoring methodology to assess the most at-risk device types in enterprise environments.



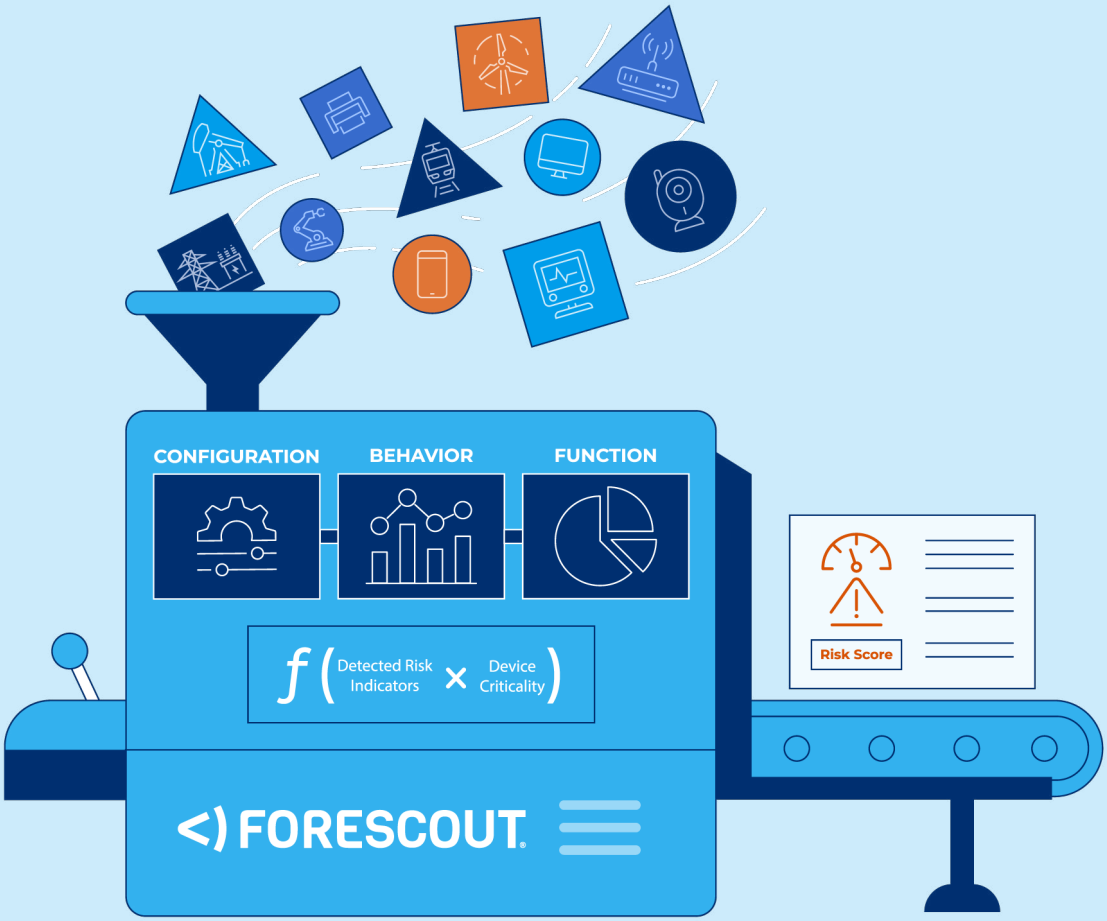
Quantifying Device Cybersecurity Risk

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

- **Configuration:** Evaluates the number and severity of vulnerabilities, the number and criticality of open ports, and other configuration findings such as default credentials or insecure protocol versions.
- **Function:** Measures the potential organizational impact if a device is compromised.
- **Behavior:** Assesses a device's exposure to the internet.

Each device receives a risk score from 1 to 10. After scoring individual devices, we calculate the average risk score per device type to determine which categories pose the greatest risk.

For this report, we analyzed data from Forescout Device Cloud covering the first week of February 2026. Because the analysis window differs from prior editions, year-over-year comparisons in this report focus on relative patterns rather than direct one-to-one equivalence.



2. Riskiest Connected Devices in 2026

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

Table 1 – Riskiest connected devices per category

	IT	IoT	OT	IoMT
1	Router	VoIP System	Power Distribution Unit (PDU)	Medication Dispensing System
2	Serial-to-IP Converter	Printer	Physical Access Control System	Medical Image Printer
3	Workstation	Time Clock	Uninterruptible Power Supply (UPS)	DICOM Gateway
4	Firewall	Network Video Recorder (NVR)	I/O Module	MRI Scanner
5	Domain Controller	RFID Reader	BACnet Router	Healthcare Workstation

Of the 20 riskiest device types identified in 2026, nine also appeared in the 2025 report. In Table 1, these recurring device types are highlighted: red indicates they moved up in the rankings compared with 2025, while green indicates they moved down.

- **Routers, VoIP systems and UPS devices** have appeared consistently since 2022.
  - **Routers moved from fifth (2025) to first (2026) in IT**. They were also the first in 2024 and 2022, and third in 2023.
  - **VoIP systems moved from third (2025) to first (2026) in IoT**. They were second in 2024, fifth in 2023, and second in 2022.
  - **UPS devices moved from fifth (2025) to third (2026) in OT**. They were the first in that category in 2024 and 2023, up from third in 2022.
- **Domain controllers, firewalls and NVRs** first appeared in 2024.
  - Firewalls moved from third (2025) to fourth (2026) in IT.
  - Domain controllers moved from fourth (2025) to fifth (2026) in IT.
  - NVRs moved from first (2025) to fourth (2026) in IoT.
- **Physical access control systems** and **imaging systems** appeared last year, and **healthcare workstations** also appeared in 2025 and 2023.
  - Physical access control systems moved from fourth (2025) to second (2026) in OT.
  - In 2025, **imaging devices** ranked first in IoMT; in 2026, **MRI scanners** appear as a named device type and rank fifth (2026) in IoMT.
  - Healthcare workstations moved from third (2025) to fifth (2026) in IoMT.

Meanwhile, 11 new device types, highlighted in blue, appear on the 2026 list for the first time. This represents the second-largest year-over-year change to date, following last year's change of 12 device types. This continues to underscore attackers' growing interest in targeting emerging device types.

The riskiest IT device category changed from 2025, with two new device types entering the top five: **serial-to-IP-converters** and **workstations**.

Routers and Firewalls

This continues the trend first noted in 2024 and reaffirmed in 2025: network infrastructure devices have overtaken endpoints as the riskiest category of IT devices. Our 2025 threat roundup report also identified network infrastructure devices as a rapid-growth exploitation category: 19% in 2025, up from 14% in 2024 (and 3% in 2022 and 11% in 2023). They are now the second most exploited device category we observe.

Routers direct network traffic between internal and external networks, including the internet. Firewalls enforce security rules by allowing or blocking traffic based on policy. Because these devices often sit at the network perimeter, they can expose administrative services. In our dataset, they commonly combine exposed management ports, exploitable vulnerabilities (including zero-days), and older weaknesses that persist due to outdated firmware.

As shown in Section 3.4, routers account for roughly a third of the most dangerous vulnerabilities in organizational networks (critical severity with extreme exploitability scores), and firewalls also contribute a significant share. This mirrors last year's pattern: computers lead in total vulnerabilities, but network infrastructure devices concentrate the most dangerous ones.

Another common attack vector against routers and firewalls is weak or reused credentials for management interfaces that are often targeted in brute-force attempts.

Serial-to-IP Converters

Serial-to-IP converters bridge legacy serial interfaces (for example, RS-232) to IP networks, enabling remote monitoring and management of equipment across industrial control systems, building automation, medical networks, and other environments. They are risky for several reasons: they often run with default credentials (see Section 3.3), they are rarely patched, and can become pivot points between IT and OT or medical networks.

Workstations and Domain Controllers

Even as network infrastructure devices accrue more frequently exploited vulnerabilities, endpoints remain a primary target for malware, including ransomware, and a common initial access vector through phishing. Examples include workstations and domain controllers.

Domain controllers are particularly consequential: they store credentials and security policy and govern access to domain resources. As a result, **they are attractive targets for ransomware operators** and other threat actors after initial access, including for credential access, privilege escalation and lateral movement.

The riskiest IoT device types include persistent risks from previous years (VoIP systems and NVRs) along with three device types that appear on the list this year: printers, time clocks, and RFID readers.

VoIP Systems and NVRs

These devices are frequently exposed to the internet, misconfigured with unnecessary open ports, protected by weak credentials, and run outdated, vulnerable firmware. IP phones, in particular, commonly appear among device types running outdated firmware (see Section 3.2) and among the most vulnerable device types (see Section 3.4).

NVRs also remain common targets for botnets. Our 2025 Threat Roundup report showed that a vulnerability affecting Hikvision NVRs has been the third most exploited both in 2024 and 2025.

Printers

Printers include traditional multifunction office devices as well as specialized devices for receipts, labels, tickets, wristbands, and other items. They are used in hospitals, warehouses, retail, financial institutions, and many other organizations. In our dataset, printers appear among device types most commonly running outdated firmware (see Section 3.2) and most commonly configured with default credentials (see Section 3.3). Printers are also frequently connected to sensitive environments, including point-of-sale systems and privileged workstations.

Time Clocks and RFID readers

Time clocks track working hours using PINs, badges, or biometrics. RFID readers identify and track people and goods for uses such as access control and inventory management. These "hidden" IoT devices are often deployed and configured by system integrators and then overlooked by security teams. Because they integrate with business systems (for example, HR/payroll for time clocks, and ERP for RFID), misconfiguration, direct exposure to the internet, or weak segmentation can make them inconspicuous entry points – especially in guest-accessible environments, such as hospitals and retail locations.

The riskiest OT device types include three new entries in 2026: PDUs, I/O modules, and BACnet routers.

PDUs and UPS devices

These are critical OT devices used in every data center. PDUs distribute electrical power to servers, network devices, storage systems, and other infrastructure. Modern PDUs are network-connected and often provide monitoring and remote outlet control. UPS devices provide backup power and are also network-connected. These devices can create high-consequence risk if exposed, weakly managed, or reachable from less trusted network segments. CISA has warned about threat actors targeting UPS devices with default credentials, enabling attackers to disrupt critical infrastructure by shutting off power in a critical location or tampering with voltage settings, potentially damaging sensitive equipment. Similar scenarios are possible by targeting PDUs.

Physical Access Control Systems and BACnet Routers

These systems are both used in smart buildings and facilities in nearly every industry.

Physical access control systems manage doors and locks across facilities ranging from offices to stadiums and retail spaces. In our dataset, they are frequently configured with exposed management services (including Telnet) and can carry vulnerabilities with documented exploitation history (see our Threat Roundup report for real world references).

BACnet routers connect and route traffic between BACnet networks (for example, BACnet/IP over Ethernet and MS/TP field networks). Because these devices sit at the intersection of building automation networks and broader enterprise connectivity, poor segmentation and weak management controls can increase risk. **BACnet is a very common protocol and the third most attacked OT protocol**, as shown in our Threat Roundup report.

Beyond cyber risk, such as providing an entry point into corporate networks or being recruited into botnets, these devices can also introduce physical risk if compromised. Our prior research has shown that vulnerabilities in access control and building automation components can enable unauthorized changes that affect physical access and building functions (for example, HVAC, lighting, badge access, and fire safety) depending on the deployment.

I/O Modules

I/O modules bridge digital control systems and physical processes connecting sensors (inputs such as temperature) to actuators (outputs such as relays, valves, and fans). They may be integrated into PLCs or deployed as separate modules in modular racks. Like PLCs, they can be insecure-by-design and may lack modern security controls, increasing risk when poorly segmented.

The riskiest IoMT device types changed significantly from 2025, with multiple new entries in the top five. Medication dispensing systems, medical image printers, DICOM gateways, and MRI scanners appear alongside healthcare workstations.

Medication Dispensing Systems

Medication dispensing systems have been known to be vulnerable for nearly a decade, since Billy Rios documented 1,418 vulnerabilities on seven third-party components of a popular device in this category. In our dataset, medication dispensing systems also appear among device types commonly running outdated firmware (see Section 3.2), allowing older weaknesses to persist.

MRI Scanners, DICOM Gateways and Medical Image Printers

Imaging-related systems have been a recurring theme in the Riskiest Connected Devices report. In 2025 and 2023 “imaging devices” appeared on the list as the riskiest, and in 2022 and 2024, both DICOM workstations and PACS were present. In 2026, this category appears as three related device types: MRI scanners, DICOM gateways and medical image printers.

These devices are often connected to Picture archiving and communication systems (PACS) for storage and retrieval of medical images. They frequently run on legacy hardware and software, including vulnerable operating systems, and require extensive network connectivity to support image-sharing workflows. **Medical image printers and DICOM gateways are also among the most common devices running outdated firmware** (see section 3.2)

These systems rely on the DICOM standard (Digital Imaging and Communications in Medicine) to exchange medical imaging files; DICOM defines both image formats and communication protocols. In past reports, we examined real-world activity, such as internet-wide scanning for exposed medical systems (including honeypots) searching for patient data and campaigns that targeted healthcare organizations by abusing weaknesses in DICOM applications to infect patient devices and compromise healthcare organizations.

Healthcare Workstations

These are used to access and manage clinical data and to interface with medical systems and equipment, including imaging workflows (for example, DICOM workstations), treatment planning systems, and diagnostic terminals. They handle sensitive clinical information and commonly integrate with electronic health records (EHR) and billing systems using standards, such as HL7 (Health Level 7).

Because these devices provide access to high-value patient and clinical workflows, they are valuable and frequently targeted by ransomware gangs. They also appear among the most vulnerable device types in our dataset (see Section 3.4).

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 2026, financial services has the highest average device risk, followed by government and healthcare. The gap between the top two industries and the rest is significant: average device risk in financial services is more than three times that of retail, and average device risk in government is more than double that of manufacturing.

We do not compare these risk scores to last year's findings because the risk scoring methodology now includes several new configuration findings.

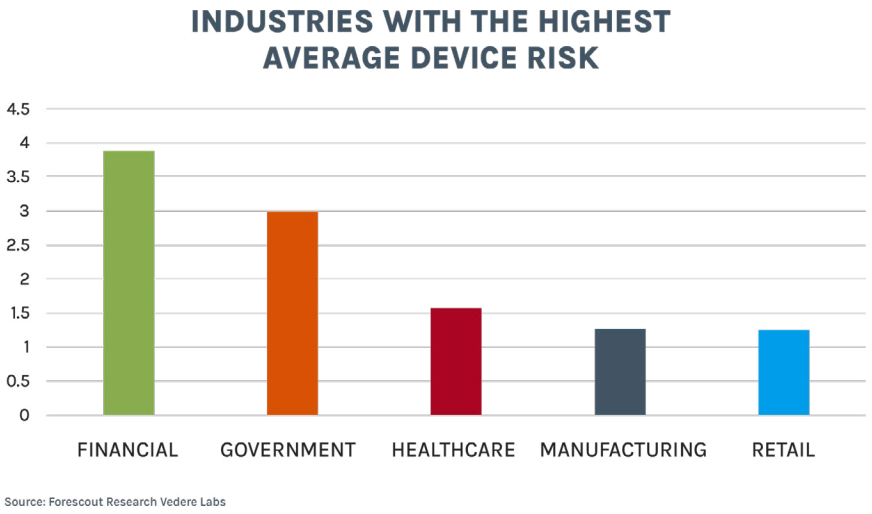


Figure 1 – Industries with the highest average device risk

3.2. Operating Systems

Devices across the five industries in our dataset run a variety of operating systems, as shown in Figure 2.

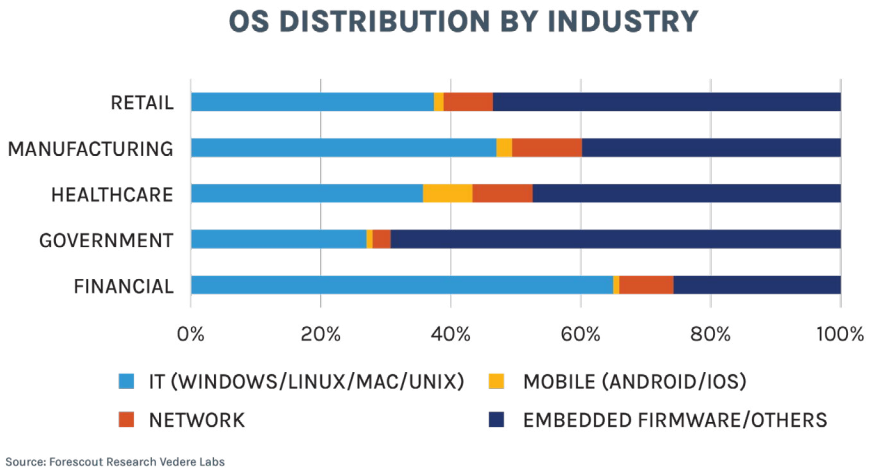


Figure 2 – OS distribution by industry

Traditional IT operating systems – such as Windows, Linux, macOS and UNIX – remain dominant in financial services and manufacturing. This marks a shift from 2025, when traditional IT operating systems were dominant across all five industries. Financial services has the highest proportion of traditional IT operating systems at 65%, while government has the lowest at 27%.

Within the traditional IT category, Windows remains the most widely used operating system. Windows 10 reached end of support on October 14, 2025, and Windows 11 is the primary supported desktop version (excluding Windows server versions). Figure 3 illustrates the percentage of devices running legacy Windows versions by industry.

Retail has the highest percentage of legacy Windows at 39%, followed by healthcare at 35%, and financial services at 29%. These percentages increased across industries following the end of support for Windows 10. In all five industries, more than half of non-legacy Windows devices previously operated on Windows 10; organizations can enroll in the Extended Security Updates (ESU) program but we cannot know which Windows 10 devices are covered.

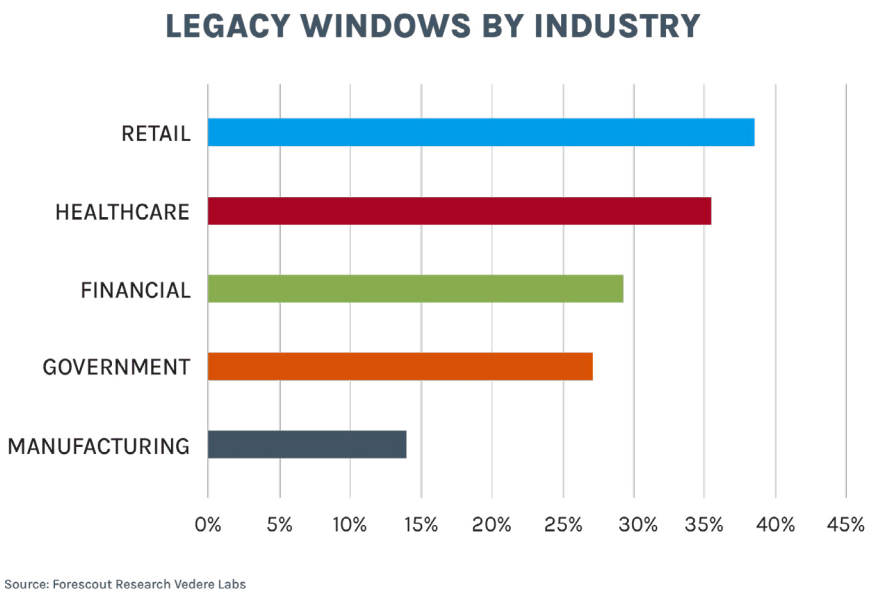
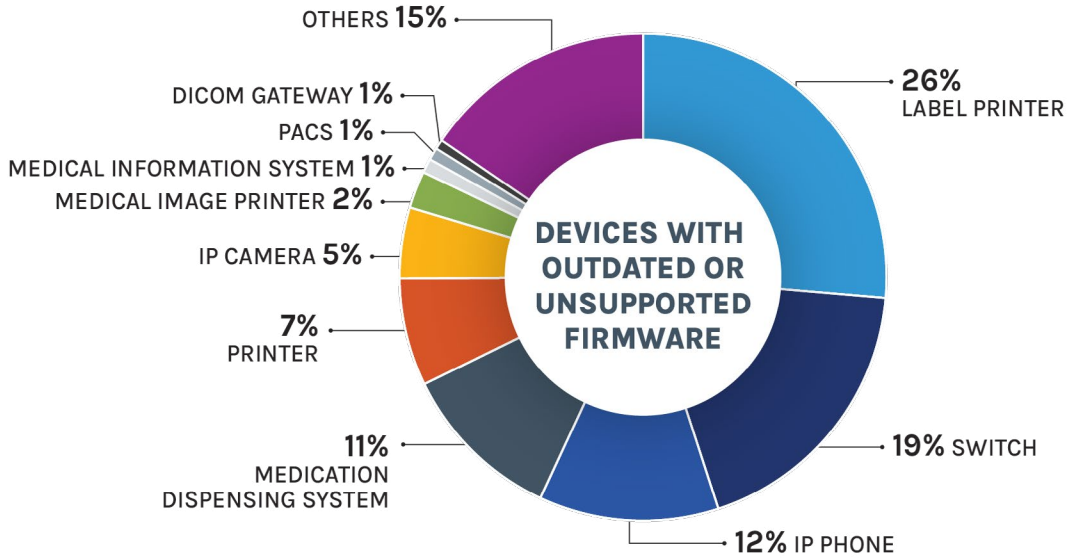


Figure 3 – Legacy Windows by industry

Mobile operating systems continued to decline across the industries we analyzed, hovering between 1% and 2%, except in healthcare, where they run on 8% of devices. In healthcare, mobile operating systems extend beyond smartphones and tablets to support specialized clinical workflows and devices such as mobile barcode scanners.

Special-purpose operating systems – including embedded firmware and networking operating systems – are prevalent in government (72%), retail (61%), and healthcare (56%). Across all industries, special-purpose operating systems outnumber mobile operating systems. The variety of special-purpose operating systems creates operational security challenges: tracking versions is a visibility issue, patches are rarely applied automatically, and outdated or unsupported firmware is common. Figure 4 shows the devices with special-purpose operating systems that most often run outdated or unsupported firmware.



Source: Forescout Research Vedere Labs

Figure 4 - Devices with outdated or unsupported firmware

3.3. 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. Figure 5 illustrates the percentage of devices in each industry with an open instance of these protocols:

- **Server Message Block (SMB)** is used by Windows machines for file sharing, printer sharing and remote service access. SMB remains widely used across all industries, but its usage declined everywhere except government. Financial services, government and healthcare have the highest SMB exposure.
- **Remote Desktop Protocol (RDP)** provides graphical remote management for Windows devices. RDP use remained mostly stable with decreases in financial services and manufacturing, and an increase in government.
- **Secure Shell (SSH)** enables command-line remote management primarily for Linux/UNIX servers and embedded devices, including IoT and OT. In 2026, SSH is the second most common protocol across the industries we analyzed. Every industry except retail increased its SSH exposure; SSH is most common in financial services, government, and manufacturing.
- **Telnet** is an unencrypted remote management protocol still used by legacy and specialized devices. **Telnet is the most concerning finding in this analysis: its usage increased in financial services, healthcare, and manufacturing**, and decreased slightly in government and retail. This follows last year's increase across all five industries. The biggest increase was in financial services where Telnet exposure rose from 3% to 12%. Manufacturing exposure increased from 5% to 12% and healthcare from 6% to 8%.

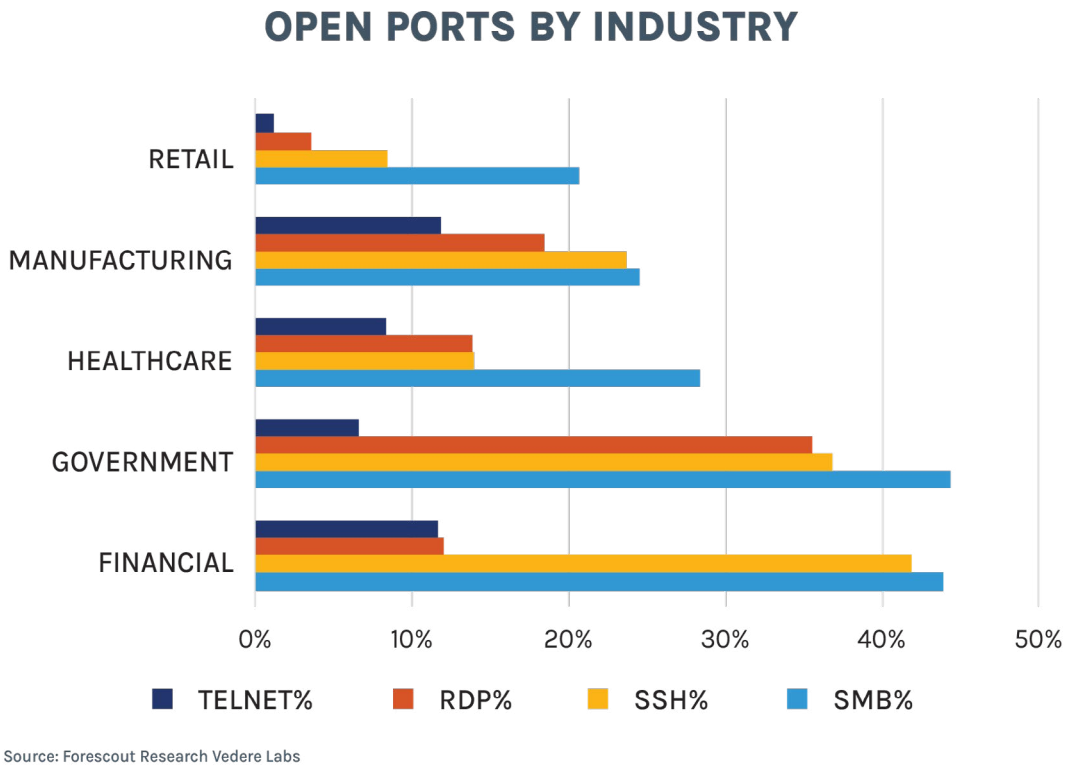
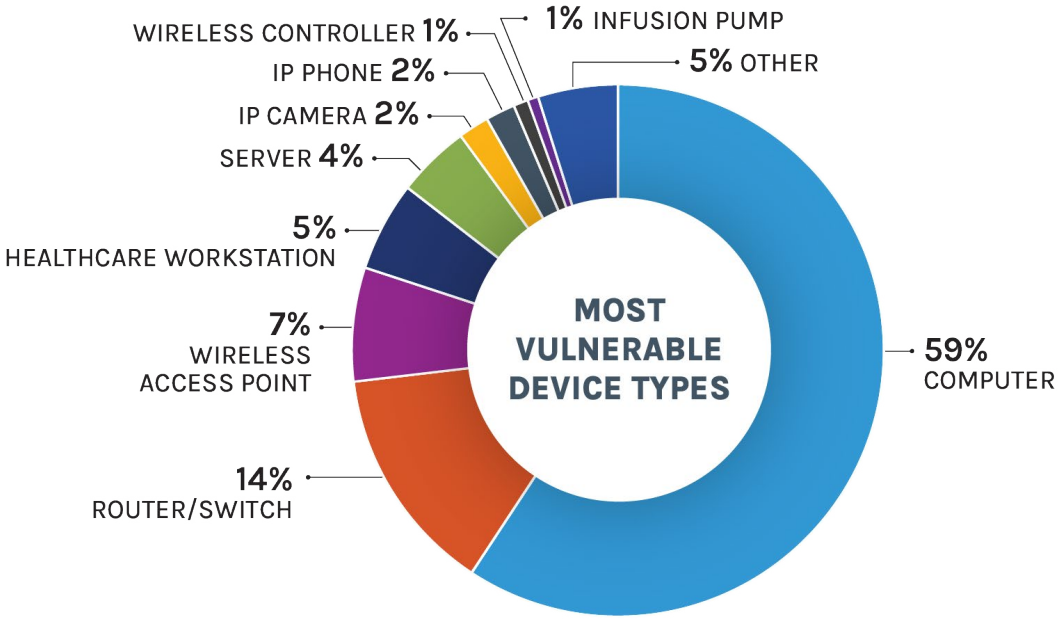


Figure 5 – Open ports by industry

As in prior editions, these trends indicate a shift in protocol exposure toward embedded and legacy device management, including increased reliance on insecure remote management methods. **Default credentials on management interfaces remain a compounding risk and are widely observed on printers, print servers, programmable logic controllers (PLCs), and serial-to-IP converters.**

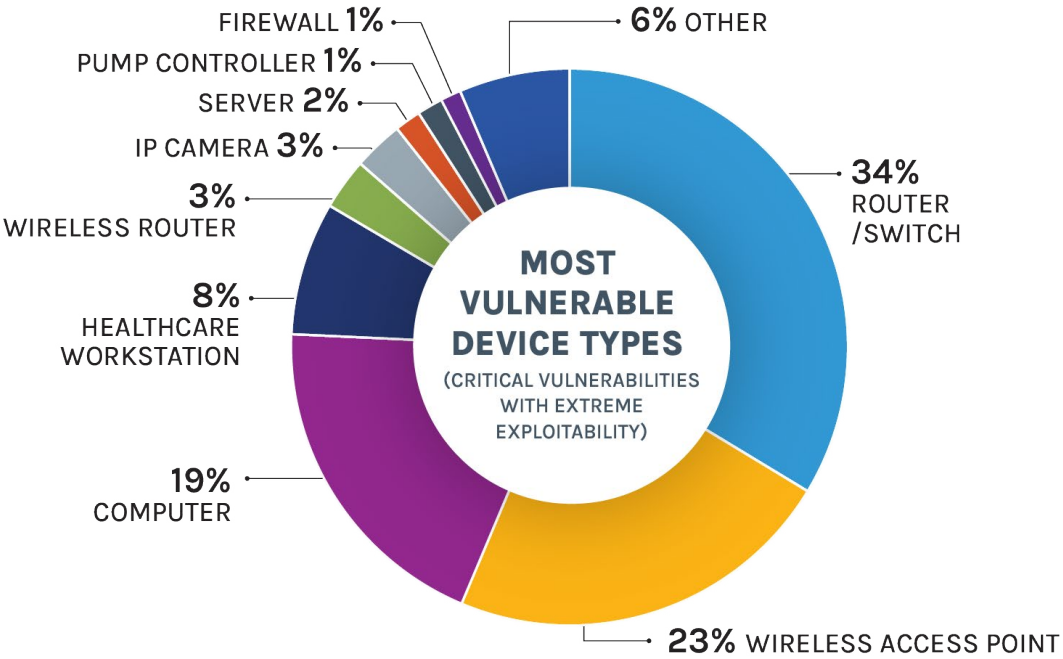
3.4. Vulnerabilities

Figure 6 highlights the device types most often found vulnerable. Figure 6 considers all vulnerabilities, while Figure 7 focuses exclusively on the most dangerous vulnerabilities – those classified as critical severity with extreme exploitability scores. The pattern remains consistent with last year: computers have the highest number of vulnerabilities overall, but not the most dangerous ones. When considering only the most dangerous vulnerabilities, **routers surpass computers and account for roughly a third of the most critical vulnerabilities in organizational networks**. Other network equipment, including **wireless access points, routers, and firewalls also appears prominently among device types with dangerous vulnerabilities**.



Source: Forescout Research Vedere Labs

Figure 6 – Most vulnerable device types



Source: Forescout Research Vedere Labs

Figure 7 - Most vulnerable device types

Another view is the average number of vulnerabilities per device. Routers are at the top with nearly 32 vulnerabilities per device, followed by wireless access points, wireless controllers, and healthcare workstations with 18 each. Computers average 14.

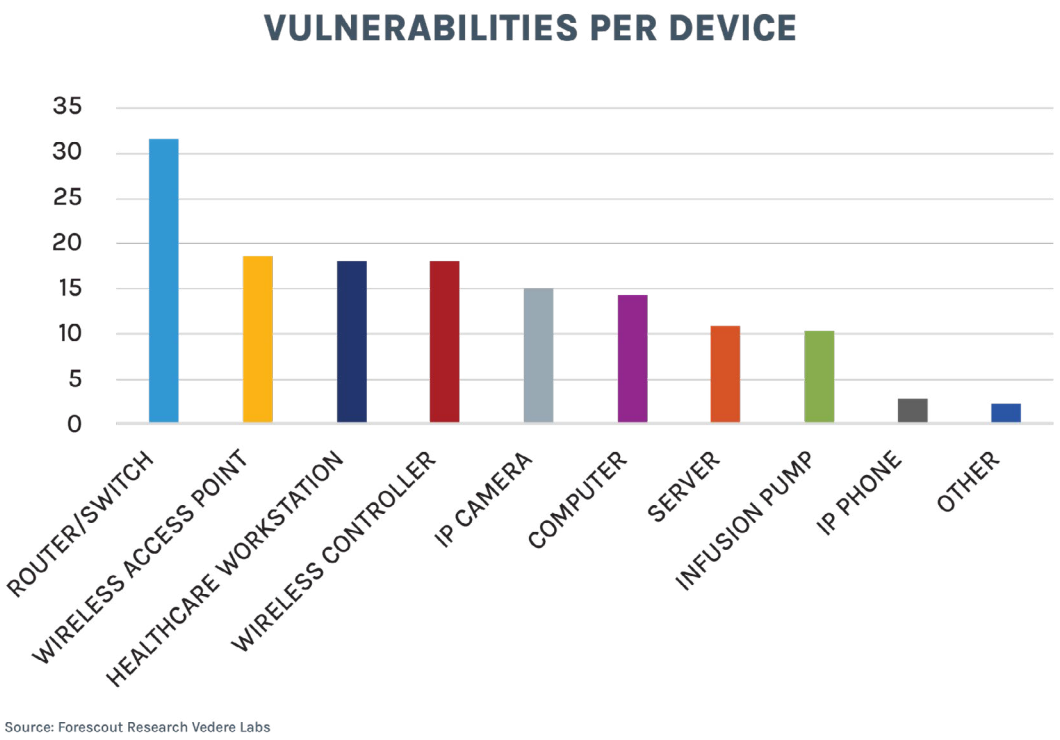


Figure 8 – Average number of vulnerabilities per device

This distinction – total vulnerabilities versus highly exploitable vulnerabilities, as well as vulnerabilities per device – helps explain why network infrastructure devices remain prime attack targets in 2026.

4. Conclusion

The attack surface in modern organizations spans IT, IoT, and OT, with the Internet of Medical Things adding complexity in healthcare. Focusing security efforts on a single domain is no longer sufficient: attackers exploit weaknesses across multiple environments and pivot between them. From ransomware targeting IP cameras and routers to IT malware infecting OT workstations and IoT botnets with credentials for medical systems, the impact is real.

This report assessed the current risk across this expanded attack surface and identified the riskiest connected devices that warrant priority attention. Effective defense requires security strategies that identify, prioritize, and reduce risk across IT, OT, IoT, and IoMT — rather than managing each domain in isolation. As threat actors increasingly target network infrastructure and other less-protected devices alongside traditional endpoints, organizations need a consistent approach to risk and exposure management across all connected devices.

Mitigation should also scale beyond assessment. Organizations benefit from automated controls that operate across the enterprise, not only within isolated IT, OT, or IoT environments, and that do not rely exclusively on endpoint agents. To sustain risk reduction, controls should support continuous risk reduction, enforcement, and verification across interconnected systems.