FORESCOUT RESEARCH | VEDERE LABS

The Riskiest Connected Devices in 2023

Author: Daniel dos Santos

Date: July 13, 2023

Contents

1. Executive summary

Since 2020, Forescout Research - Vedere Labs has been tracking the riskiest devices on organizations' networks. In 2020, we released the first Enterprise of Things Security Report and followed in 2022 with the Riskiest Connected Devices in Enterprise Networks report.

Our reports are entirely based on data coming directly from connected devices. Throughout the years, we have noticed that although many device types are consistently in these lists – such as IP cameras, VoIP equipment and programmable logic controllers (PLCs) – due either to their inherent criticality or to the persistent lack of attention from security teams, there are other devices whose current risk level reflect developments in the threat landscape.

For instance, in 2022 we reported on hypervisors becoming a major target for ransomware – which is a trend that only grew and continued into 2023. However, the dataset in our 2022 report (January through April) did not include several important later developments, such as the increasing targeting of unmanaged devices by hacktivists, growing numbers of employees returning to their offices after the COVID-19 pandemic and intensified attacks against Western critical infrastructure following the Russian invasion of Ukraine.

Therefore, in this report, we update our findings about the riskiest devices in enterprise networks in 2023. We again take a data-driven approach by analyzing millions of devices in Forescout's Device Cloud using Forescout's multifactor risk scoring methodology. Section 2 presents the results by device category (IT, IoT, OT and IoMT). Section 3 discusses some risk factors in more detail and shows their distribution by industry. Section 4 presents the main takeaways and mitigation recommendations.

Key findings of this report include:

- 13 of the 20 riskiest device types remain on the list since 2022: computers, servers and routers in IT; printers, IP cameras and VoIP in IoT; UPS, PLCs and building automation in OT; healthcare workstations, imaging devices, nuclear medicine and patient monitors in IoMT. Seven device types are new to the list: VPN gateways and security appliances in IT; network attached storage (NAS) and out-of-band management (OOBM) in IoT; engineering workstations and remote terminal units (RTUs) in OT; and blood glucose monitors in IoMT.
- Healthcare is the riskiest industry in 2023, followed by retail, and manufacturing. The highest risk reduction we observed from 2022 to 2023 was in government.
- Traditional operating systems such as Windows and Linux are the majority in every industry, but special purpose operating systems, such as embedded firmware, are particularly strong in retail (14%), healthcare (13%) and government (12%). Special purpose operating systems are more common than mobile OSes in all industries.
- Retail and healthcare have the most legacy Windows (6% of all devices), followed by manufacturing (4%). 63% of OT and 35% of IoMT devices running Windows have legacy versions of the OS.
- More than 4,000 vulnerabilities affect the devices in our dataset. Out of those, 78% affect IT devices, 14% affect IoT, 6% affect OT and 2% affect IoMT. Although most vulnerabilities affect IT devices, almost 80% of those have only high severity. On the other end, IoMT devices have fewer vulnerabilities, but 80% of them are critical, which typically allows for complete takeover of a device. Similarly, more than half of the vulnerabilities affecting OT and IoT devices are critical.
- In all industries, at least 10% of devices that have endpoint protection installed have it disabled. This figure is highest in government, financial services (both with almost 24%) and healthcare (21%).
- Devices in healthcare are more likely to have dangerous ports, such as Telnet, SSH and RDP open. Almost 10% of devices in that vertical still have Telnet ports open, whereas it is only present in around 3-4% of devices in other verticals. The Windows SMB protocol is most popular in financial services.
- Indicators of compromise (IoCs), such as known malicious IPs and domains, were detected most often in government (63% of IoCs), healthcare (19%) and financial services (8%).

- IT network infrastructure and security appliances are the most exposed devices on the internet. They are followed by IoT devices such as IP cameras (an overwhelming majority of IoT at 23%), NAS (7%) and VoIP (3%). There are also large numbers of exposed office equipment such as printers and NAS in government (19%) and OT in financial services (6%, mostly UPS).

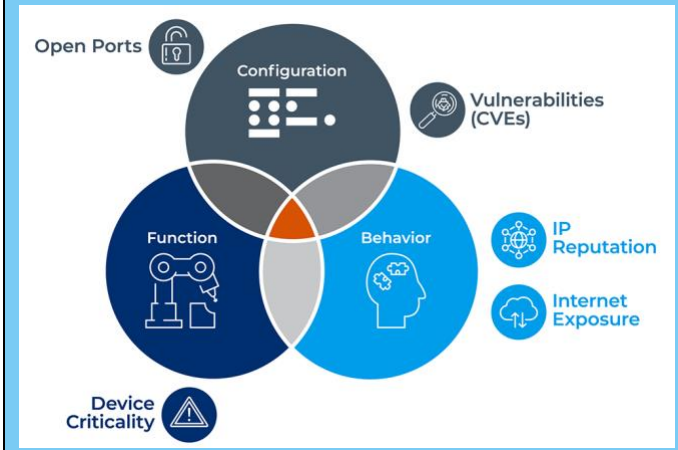
Quantifying Device Cybersecurity Risk

To get a dataset representative of the current device landscape in enterprise networks, we analyzed device data between January 1 and April 30 in Forescout's Device Cloud. Device Cloud is one of the world's largest repositories of connected enterprise device data, including IT, OT, IoT and IoMT device data. The number of devices feeding data to the cloud grows daily. The anonymized data comes from Forescout customer deployments and contains information about almost 19 million devices.

To measure risk on that dataset, we rely on Forescout's multifactor risk scoring methodology, where the risk of a device is calculated based on three factors: configuration, function and behavior.

- *Configuration* considers the number and severity of vulnerabilities on the device as well as the number and criticality of open ports.
- *Function* considers the potential impact to the organization if the device is compromised.
- *Behavior* considers the reputation of inbound connections to and outbound connections from the device, along with its internet exposure.

After measuring the risk of each individual device, we calculate averages per type of device to understand which types are the riskiest.



2. Riskiest connected devices in 2023

Using the dataset and scoring methodology described above, we identified the five riskiest device types in four device categories: IT, IoT, OT and IoMT

	IT	IoT	OT	IoMT
1	Computer	Network attached storage (NAS)	Uninterruptible power supply (UPS)	Healthcare workstation

2	Server	Printer	Programmable logic controller (PLC)	Imaging
3	Router	IP camera	Engineering workstation	Nuclear medicine system
4	VPN gateway	Out of Band Management (OOBM)	Building Automation	Blood glucose monitor
5	Security appliance	VoIP	Remote terminal unit (RTU)	Patient monitor

Out of these 20 device types, 13 were already discussed in the 2022 report and remain on the list, while seven device types are new: VPN gateway, security appliance, NAS, OOBM, engineering workstation, RTU and blood glucose monitor.

- **The riskiest IT devices** continue to be roughly divided into two main groups. First, endpoints – computer and servers – remain risky for being the entry points for phishing or because of unpatched systems and applications. Second, network infrastrutcture devices – routers, VPN gateways and security appliances – are often exposed online and have dangerous open ports. Security appliances are firewalls, proxy servers, intrusion detection systems and other devices used to protect a network, while VPN gateways are appliances used to bridge the connection between separate networks in a VPN infrastructure. Several exploits observed in the second half of 2022 targeted security appliances from major security vendors. Similarly, state-sponsored actors have been exploiting unpatched routers or VPN gateways for initial access.

- **The riskiest IoT devices** include the most persistent suspects – IP cameras, printers and VoIP – which are commonly exposed on the internet and which been historically targeted by APTs, as well as two new entries: NAS and OOBM. NAS devices have been a growing target for ransomware actors, with several ransomware families designed specifically to run on them, due to the valuable data they store and their numerous vulnerabilities. Out-of-band management allow for remote management of equipment via alternative interfaces. Examples include “lights-out management” integrated into the main board of computers and servers as well as dedicated external OOBM console servers. The first variety of OOBM is plagued with critical vulnerabilities, some of which have had public exploits for years and have been exploited by sophisticated malware, others which have been found as recently as late 2022. Devices of the second variety are often found online and sometimes misconfigured, allowing attackers to ultimately access the devices being remotely managed.

- **The riskiest OT devices** include the critical and insecure-by-design PLCs, the UPSs present in many data centers with default credentials and the ubiquitous but often invisible building automation controllers that were present last year, while also for the first time engineering workstations and RTUs. Engineering workstations typically run a traditional operating system such as Windows and allow engineers to manage PLCs, RTUs and other OT equipment on the network. According to SANS, 35% of attacks into OT/ICS in 2022 used engineering workstations as initial access vector, doubling what they reported in 2021. RTUs are used to connect field devices to a distributed control system or SCADA by exchanging data and commands. Vulnerabilities in RTUs are common and some were found in Project Memoria and OT:ICEFALL. In early 2023, the GhostSec hacktivist group claimed to encrypt an RTU as part of their politically-motivated attack campaign.

- **The riskiest IoMT devices** are healthcare workstations, which include the DICOM workstations we discussed last year but also specialized workstations for radiology, for instance. Imaging devices, including nuclear imaging, and patient monitors were also on last year’s list. Those are all among the most vulnerable and at the same time most connected IoMT devices in hospitals. The new device type on the list is blood glucose monitors. Blood glucose monitors are often used together with insulin pumps ,and there is a history of vulnerabilities affecting these devices and their communication protocols, which may

allow attackers to capture, replay, inject or modify traffic between devices. More recent versions of these devices are often paired with patients' personal mobile devices, which means that they may be connected first to an insecure home network and later to a supposedly more secure clinical network used by much more critical medical devices.

3. Detailed analysis

3.1. Overall risk by industry

Figure 1 shows the distribution of device risk levels (low, medium and high) by industry in our dataset. We have selected the same five industry verticals we analyzed in 2022. Overall, we saw a reduction in the risk levels of devices in every industry, except for healthcare. In 2022, healthcare organizations had 8% of devices with high risk and 12% with medium risk. In 2023, healthcare is the riskiest industry, having 9% of devices with high risk and 13% with medium risk. Healthcare is followed by retail, which now has 17% of devices with medium or high risk (down from 18% in 2022) and manufacturing, which has 15% of devices in the same condition (down from 26% in 2022). On the other hand, the highest risk reduction we observed was in government, where the combination of devices with medium and high risk decreased from 43% to 10%.

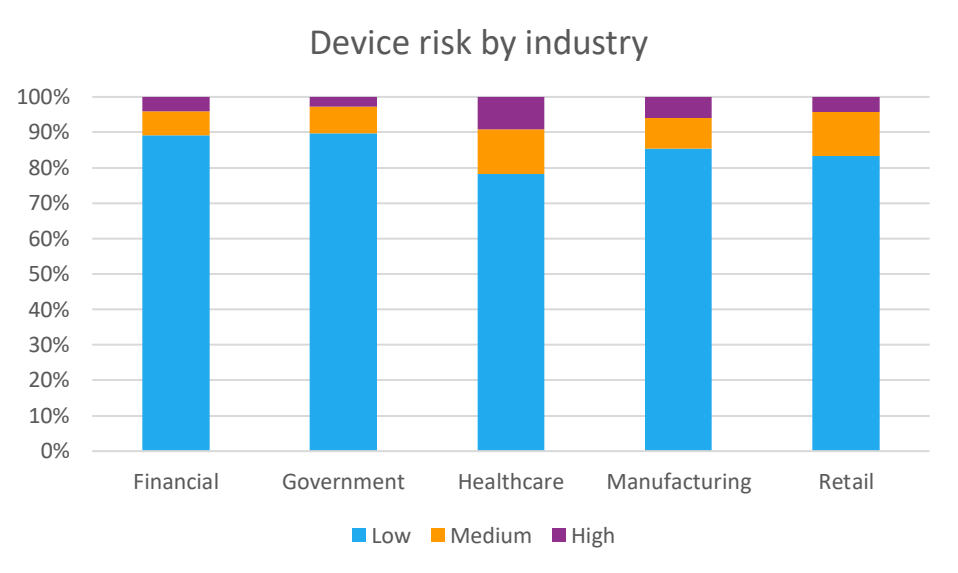


Figure 1 – Device risk distribution by industry

3.2. Operating systems

The devices in these five industries run the operating systems shown in Figure 2. Most devices in every industry run "traditional" operating systems such as Windows, Linux, Mac and UNIX. This includes several specialized IoT/OT/IoMT devices that run Linux or Windows. However, the category of special purpose operating systems, which includes embedded firmware, networking operating systems and others, is particularly strong in retail (14%), healthcare (13%) and government (12%). Special purpose operating systems are more common than mobile OSes in all industries.

The variety of special purpose OSes (we observe more than 2,500 unique versions on Device Cloud) is a nightmare for security teams to keep track of and is one of the main reasons for the need for visibility into networked devices. Embedded firmware is also well known for presenting systematic security issues, such as backdoors, hardcoded credentials and keys and memory corruption vulnerabilities.

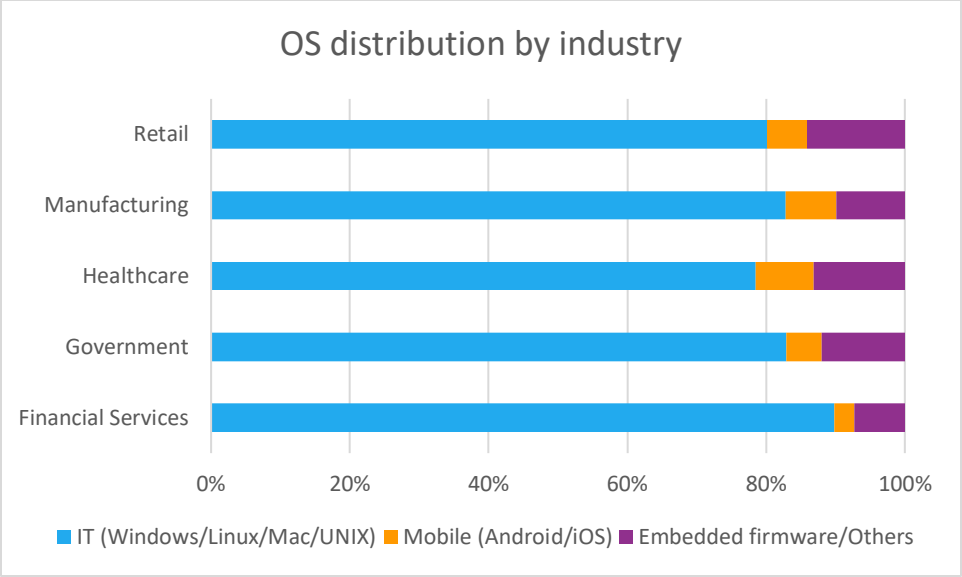


Figure 2 – Operating system distribution by industry

Since Windows is by far the most common OS across every industry, we drill down into the versions used in each industry. We divide Windows versions into two categories: currently supported – such as Windows 10 and 11 – and legacy, which includes versions such as Windows 8, 7, XP and CE.

Figure 3 shows the percentage of devices running legacy Windows versions in each industry and for each device category. Retail and healthcare have the most legacy Windows with 6% of devices, manufacturing is third with 4%. When we look at device categories, it is obvious that specialized devices run legacy Windows much more frequently than general purpose IT devices. Sixty-three percent of OT devices running Windows have legacy versions of the OS, whereas 35% of the IoMT devices run legacy Windows. These specialized devices run older versions of the OS because of their long lifespans, the legacy applications they run and the need for vendors to certify that they can be safely upgraded to newer OSes.

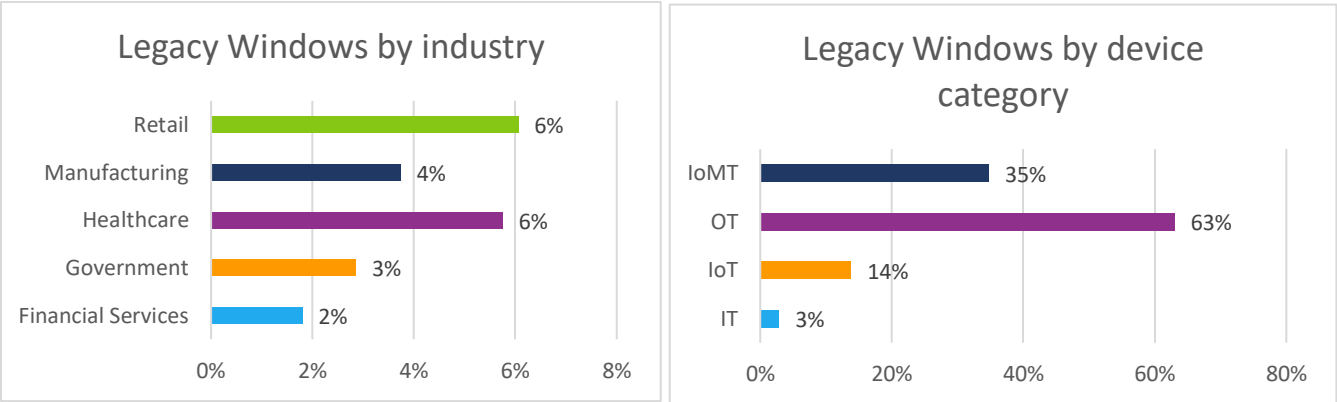


Figure 3 – Legacy Windows OS distribution by industry and device category

3.3. Vulnerabilities

More than 4,000 vulnerabilities affect the devices in our dataset. Out of those, 78% affect IT devices, 14% affect IoT, 6% affect OT and 2% affect IoMT. Figure 4 shows the distribution of these vulnerabilities according to the severity of their CVSS v3 scores: 96% have either a high or critical severity. The figure also shows the distribution of vulnerability severity per device type. Although most vulnerabilities affect IT devices, almost 80% of those have only high severity. On the other end, IoMT devices have fewer vulnerabilities, but 80% of them are critical, which typically allows for a complete takeover of a device. Similarly, more than half of the vulnerabilities affecting OT

and IoT devices are critical. Since these specialized devices are harder to upgrade and patch (as discussed above), this means that these most severe vulnerabilities tend to linger for longer in critical networks.

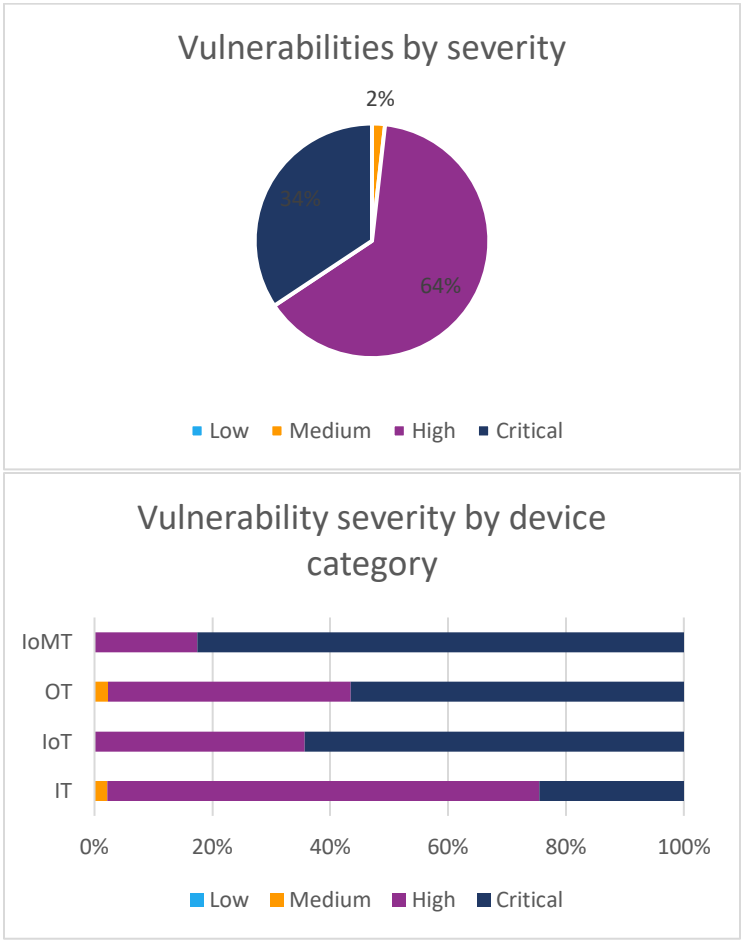


Figure 4 – Vulnerability distribution by severity and severity distribution by device category

Not every vulnerability is exploited or even exploitable. CISA maintains a constantly updated list of vulnerabilities known to be exploited by threat actors. As of May 2023, the list contains 925 vulnerabilities. Six IT software vendors – Microsoft, Adobe, Apple, Google, Oracle and Apache – are responsible for 477 (52%) of these vulnerabilities, which may affect a variety of devices running their software. However, several vulnerabilities affect specific types of devices, including IoT and OT. Figure 5 shows these vulnerabilities distributed by device type. All those device types being targeted by threat actors appear in the 2023 riskiest devices list, except for conferencing systems and hypervisors, which were present in the 2022 list.

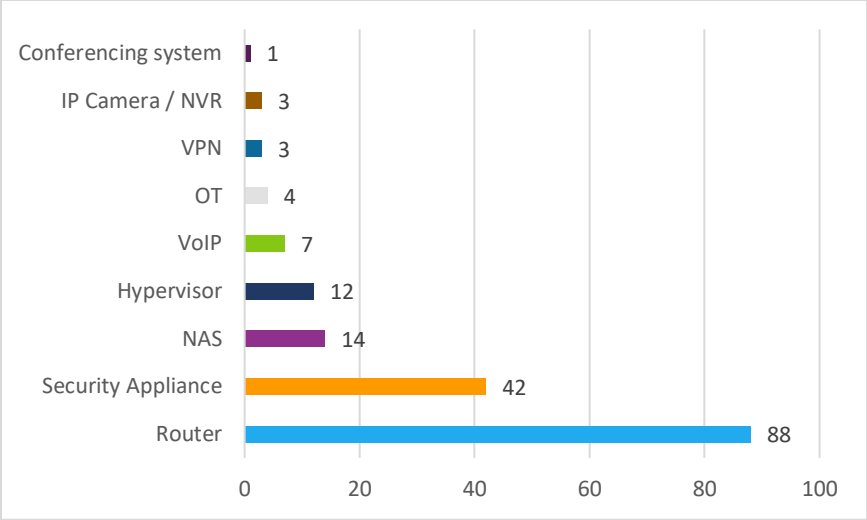


Figure 5 – Exploited vulnerabilities by device type

3.4. Endpoint protection

Besides legacy operating systems and vulnerabilities, a major example of risky misconfiguration is disabled endpoint protection. Only a subset of devices in the network nowadays accept endpoint protection (mostly managed IT devices). However, even when these agents are installed, they are often disabled, leaving devices unprotected. Figure 6 shows that in all industries at least 10% of devices that have endpoint protection installed have it disabled, a figure which is highest in government, financial services (both with almost 24%) and healthcare, with 21% of devices.

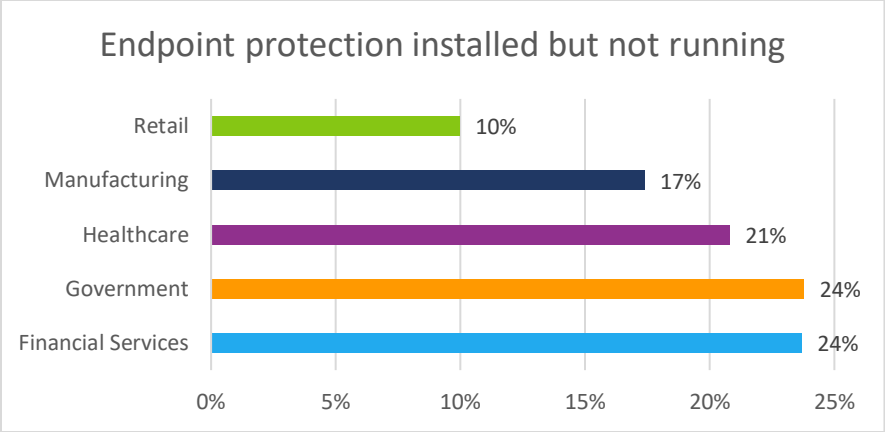


Figure 6 – Devices with endpoint protection installed but not running

3.5. Open ports

Vulnerabilities are among the riskiest factors for a device, but open ports are what leave devices open to attacks, both because of known vulnerabilities and unknowns such as zero-days. We selected four common ports to analyze out of the ones we observed as most exploited in 2022. Server Message Block Protocol (SMB) is used by Windows machines for file sharing, printer sharing and access to remote services. Remote Desktop Protocol (RDP) provides remote management for devices using a graphical interface. Secure Shell (SSH) provides remote management using a command-line interface especially to Linux/UNIX servers and IoT devices, while Telnet also provides remote management mainly for legacy specialized devices.

Figure 7 shows the percentage of devices in each industry with a given open port. Healthcare leads in every protocol except for SMB. Almost 10% of devices in that vertical still have Telnet ports open, whereas it is only

present in around 3-4% of devices in other verticals. SMB is most popular in financial services (29%), but other industries have a similar level of exposure (27%), except for manufacturing, which is much less exposed at 24%.

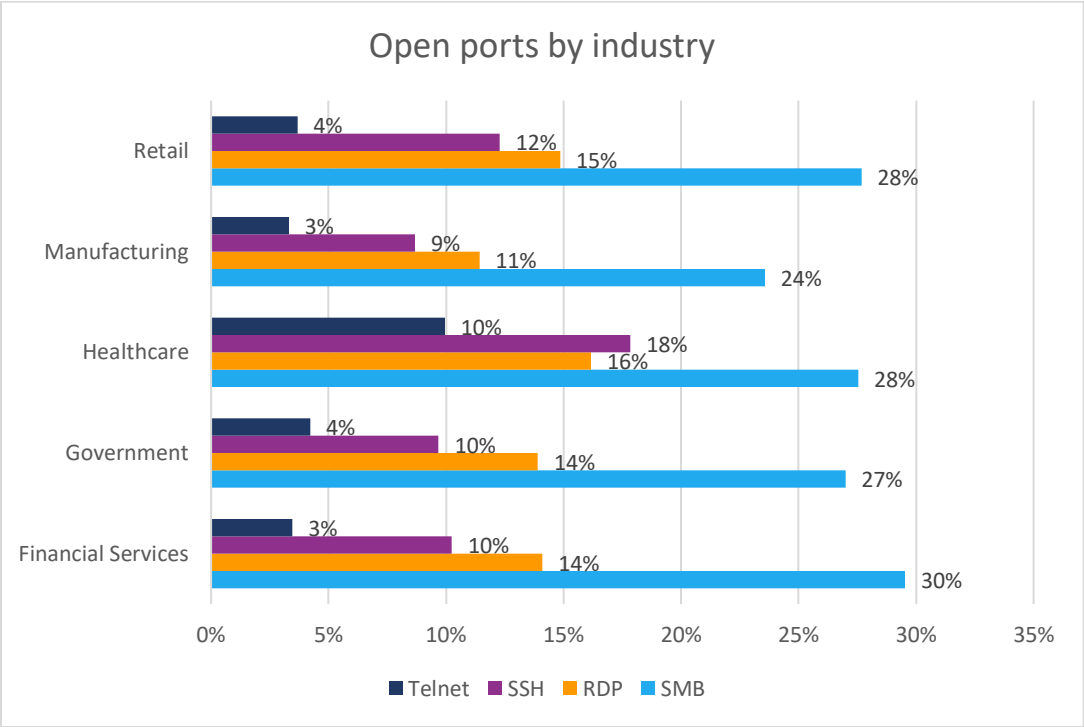


Figure 7 – Percentage of devices with a given open port by industry

3.6. IoCs

We also observe risky behavior of devices, such as communication with known malicious IPs and domains. Figure 8 shows the number of detected indicators of compromise (IoCs) in devices by industry. Government is by far the first, with 63% of IoCs, followed by healthcare (19%) and financial services (8%).

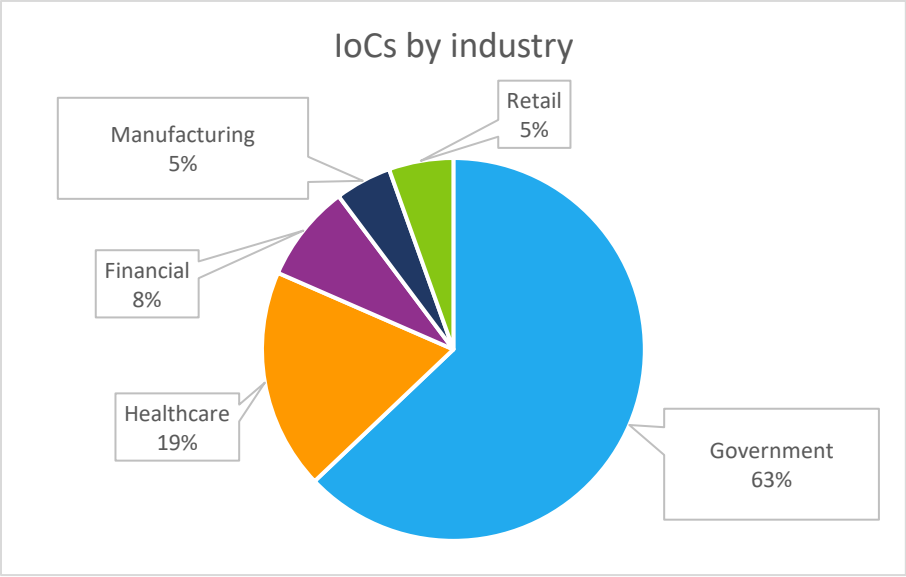


Figure 8 – Detected IoCs by industry

3.7. Internet exposure

To discuss internet exposure, we expand the dataset from the Device Cloud to include results from Shodan searches. First, we looked at the most exposed devices overall, as shown in Figure 9. As expected, IT network infrastructure and security appliances are the most commonly exposed devices, since they work as the perimeter between internal and external networks. Looking at the other types of devices, IP cameras are the next largest percentage at 23%, followed by NAS at 7% and VoIP at 3%.

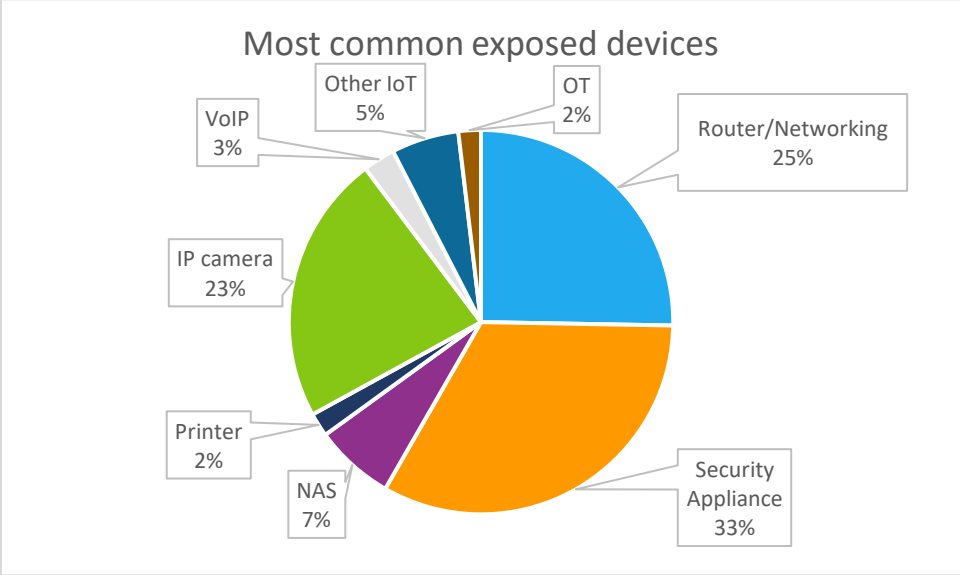


Figure 9 – Most common exposed devices

Second, for each industry, we defined a set of keywords and searched for organizations matching those keywords to understand what devices are most common in each industry, as shown in Figure 10. The results reflect what was seen before, with networking infrastructure and security appliances at the top. However, it is interesting to see the large numbers of IP cameras in retail (8%), office equipment such as printers and NAS in government (19%), and OT in financial services (6%, mostly UPS).

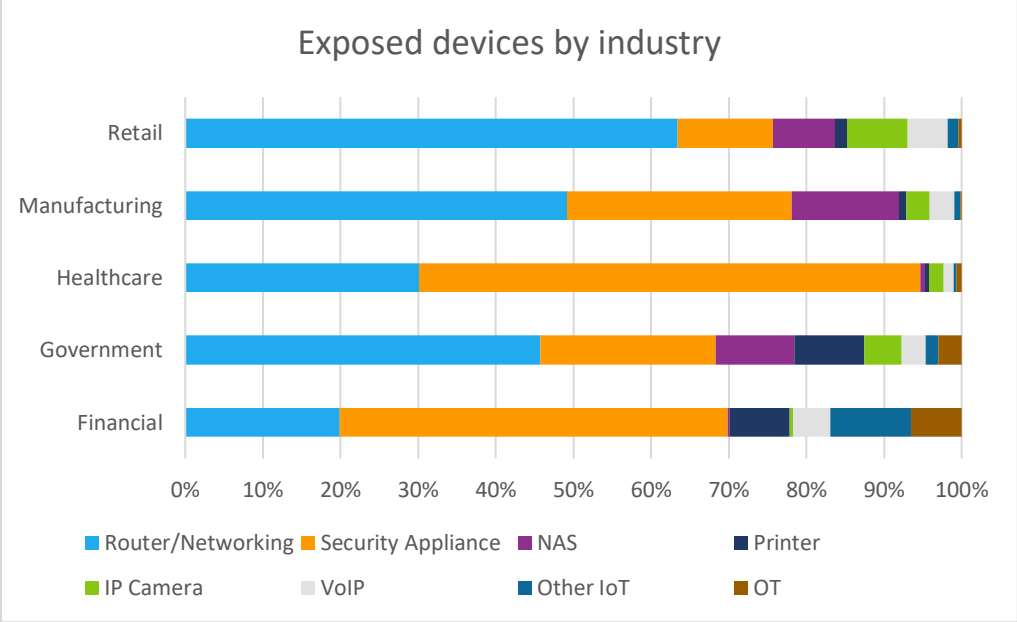


Figure 10 – Exposed devices by industry

Many of these exposed devices have already been compromised. With specific queries, we can observe for instance: 3,600+ NAS encrypted with DeadBolt ransomware, 1,600+ Windows XP running Metasploit, 1,000+ hacked routers, 400+ hacked DVRs and 100+ encrypted Windows RDP.

4. Conclusion

This report explored the current risk associated with the expanded attack surface that now encompasses IT, IoT and OT in almost every organization, with the addition of IoMT in healthcare.

Some of our findings point to specific actions that can be taken by organizations to reduce immediate risk:

- The prevalence of legacy Windows and critical vulnerabilities in OT and IoMT means that organizations need immediate action plans to upgrade, replace or isolate these devices as much as possible.
- The often-disabled endpoint protection solutions in IT devices means that organizations must adopt automated device compliance verification and enforcement, to ensure that non-compliant devices cannot connect to the network.
- The commonly found exposed devices such as IP cameras and dangerous open ports such as Telnet mean that organizations must improve network security efforts, including segmentation.

Beyond these specific recommendations, the increased risk profiles of devices as diverse as security appliances, VPN gateways, NAS, out of band management and blood glucose monitors means that organizations need to embrace the fact that this attack surface requires new, superior security approaches to identify and reduce risk.

To bypass traditional endpoint security approaches, threat actors are consistently moving to devices that offer easier initial access. Modern risk and exposure management must encompass devices in every category to reduce risk across the whole organization. Solutions that work only for specific devices cannot effectively reduce risk because they are blind to other parts of the network being leveraged for an attack. For instance, OT or IoMT-only solutions cannot assess risk for IT devices, while IT-only solutions will miss the nuances of the specialized devices.

Beyond risk assessment, risk mitigation should use automated controls that do not rely only on security agents . Likewise, they must apply to the whole enterprise instead of silos like the IT network, the OT network or specific types of IoT devices.