VEDERE LABS

The Riskiest Connected Devices in Enterprise Networks

October 12, 2022

Contents

1. Executive Summary

The growing number and diversity of connected devices in every industry presents new challenges for organizations to understand and manage the risks to which they are exposed. Most organizations now host a combination of interconnected IT, OT and IoT devices in their networks that has increased their attack surface.

According to a recent report by the Ponemon Institute, 65% of responding organizations say that IoT/OT devices are one of the least secured parts of their networks, while 50% say that attacks against these devices have increased. IT and IT security practitioners in 88% of those organizations have IoT devices connected to the internet, 56% have OT devices connected to the internet and 51% have the OT network connected to the IT network.

Threat actors are well aware of these trends. We recently reported on how ransomware groups have started massively targeting devices such as NAS, VoIP and hypervisors. Not surprisingly, most of these devices were among the riskiest we identified in the 2020 Enterprise of Things Security Report.

In this report, we update our findings about the riskiest devices in enterprise networks in 2022. We take a data-driven approach by analyzing millions of devices in Forescout's Device Cloud using the Forescout Continuum Platform's new multifactor risk scoring methodology, described in Section 2. Section 3 presents the results per device category (IT, IoT, OT and IoMT). Sections 4 and 5 discuss the risk distribution per industry and geography, respectively. Section 6 presents the main takeaways and mitigation recommendations.

Key findings of this report include:

- Many of the device types observed among the riskiest in 2020 remain on the list, such as networking equipment, VoIP, IP cameras and programmable logic controllers (PLCs). However, there are some new entries, such as hypervisors and human machine interfaces (HMIs), that are representative of trends such as critical vulnerabilities and increased OT connectivity.
- The riskiest devices appear in the ranking mostly because they are often exposed on the internet (in the case of IT and IoT) or because they are very critical to business (in the case of OT and IoMT). Vulnerabilities are present across all device categories.
- Manufacturing has the highest percentage of devices with high risk (11%), while government and financial have the top combinations of medium and high risk (43% for government and 37% for financial). The ranking of riskiest devices does not change considerably per industry, which shows that almost every organization currently relies on a combination of IT, IoT and OT (as well as IoMT for healthcare) to deliver their business. It also means that almost every organization is affected by a growing attack surface.
- The riskiest IT and OT devices remain nearly constant across different regions, while the riskiest IoT devices change slightly, and the riskiest IoMT devices change considerably.
- Risk assessment becomes even more important for organizations as their attack surface increases with the addition of new connected devices. Implementing automated controls that do not rely only on security agents and that apply to the whole enterprise can help reduce risk across an organization.

2. 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, 2022, 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.

3. Riskiest Connected Devices in 2022

Using the dataset and scoring methodology described in Section 2, we identified the five riskiest devices in four device categories: IT, IoT, OT and IoMT as shown in Table 1.

Table 1 - Riskiest connected devices per category

	IT	IoT	OT	IoMT
1	Router	IP camera	Programmable logic controller (PLC)	DICOM workstation
2	Computer	VoIP	Human machine interface (HMI)	Nuclear medicine system
3	Server	Video conferencing	Uninterruptible power supply (UPS)	Imaging
4	Wireless access point	ATM	Environment monitoring	Picture archiving and communication system (PACS)
5	Hypervisor	Printer	Building automation controller	Patient monitor

3.1. Riskiest IT devices – still a favorite target

IT devices are still the main target of malware, including ransomware, and the main initial access points for malicious actors. These actors exploit vulnerabilities on internet-exposed devices, such as **servers** running unpatched operating systems and business applications or that use social engineering and phishing techniques to dupe employees to run malicious code on their **computers**.

Routers and wireless access points, as well as other network infrastructure devices, are becoming more common entry points for malware and advanced persistent threats. Routers are risky because they are often exposed online, interfacing internal and external networks, have dangerous exposed open ports and have many vulnerabilities that are often quickly exploited by malicious actors. Wireless access points are the typical border between internal and external networks in physical locations. They frequently host both guest and corporate networks, and are used to connect guest devices, including computers and mobile.

Hypervisors, or specialized servers hosting virtual machines (VMs), have become a favorite target for ransomware gangs in 2022 because (i) they allow attackers to encrypt several VMs at once and (ii) ransomware developers are moving toward languages such as Go and Rust that allow for easier cross-compilation and can target both Linux and Windows.

3.2. Riskiest IoT devices – harder to patch and manage

A growing number of IoT devices on enterprise networks are being actively exploited because they are harder to patch and manage than IT devices. IoT devices are compromised due to weak credentials or unpatched vulnerabilities primarily to become part of distributed denial-of-service (DDoS) botnets. Beyond DDoS, several threat actors have been using IoT devices for other phases of attacks, as listed below.

IP cameras, VoIP and **video conferencing systems** are the riskiest IoT devices because they are commonly exposed on the internet, and there is a long history of threat actor activity targeting them. For instance, in 2019 APT28 compromised VoIP phones for initial access to multiple networks, in 2021 Conti targeted cameras to move internally in affected organizations and, in 2022, both UNC3524 and TAG-38 have targeted video conferencing and cameras for use as command and control infrastructure.

ATMs appear in the ranking because of their obvious business criticality in financial organizations and also because our data indicates that many ATMs are adjacent to other IoT devices such as security cameras and physical security systems that are often exposed.

Printers include not only multifunctional printing and copying devices used in the connected office but also specialized devices for printing receipts, labels, tickets, wristbands and other uses. Although printers are not widely associated with cyber risk, they should be. Like IP cameras, they have been exploited in intrusions by threat actors such as APT28 and spammed by hacktivists on multiple occasions. And just like ATMs, printers are often connected to sensitive devices, such as point of sale systems in the case of receipt printers and conventional workstations with privileged users in the case of office printers.

3.3. Riskiest OT devices – mission critical yet insecure by design

In the past decade, state-sponsored attacks against OT systems and devices have become commonplace. Examples include Russian actors targeting the energy sector, Chinese actors targeting gas pipelines and specialized malware targeting PLCs and other OT equipment in several sectors. Even more troubling is the rise in cybercriminal and hacktivist activity targeting these devices. Recently, ransomware groups gained access to the SCADA systems of water utilities on several occasions and hacktivists gained access to the HMI of a water treatment facility in Florida.

PLCs and HMIs are the riskiest OT devices because they are very critical, allowing for full control of industrial processes, and are known to be insecure by design. Although PLCs are not often connected to the internet, many HMIs are connected to the internet to enable remote operation or management. These devices are not only common in critical infrastructure sectors, such as manufacturing, but also in sectors such as retail, where they drive logistics and warehouse automation.

OT devices are typically associated with manufacturing and critical infrastructure. However, other observed risky OT devices are much more widespread than PLCs and HMIs. For instance, **uninterruptible power supplies (UPSs)** are present in many corporate and data center networks next to computers, servers and IoT devices. UPSs play a critical role in power monitoring and data center power management. CISA has alerted about threat actors targeting UPSs with default credentials. Attacks on these devices can have physical effects, such as switching off the power in a critical location or tampering with voltage to damage sensitive equipment.

Environment monitoring and **building automation systems** are critical for facilities management, which is a common need in most organizations. Smart buildings perfectly exemplify a cross-industry domain where IT, IoT and OT are converging on the same network. There are several examples of smart buildings exploited by threat actors to render controllers unusable, recruit vulnerable physical access control devices for botnets or leverage engineering workstations for initial access. These devices dangerously mix the insecure-by-design nature of OT with the internet connectivity of IoT and are often found exposed online even in critical locations.

3.4. Riskiest IoMT devices

Connected medical devices are obviously risky because of their potential impact on healthcare delivery and patient safety. There have been many ransomware attacks on health system corporate IT networks that spilled over to medical devices, rendering them unusable, such as WannaCry in 2017, the attack on a hospital in Alabama affecting fetal monitors in 2019 and several attacks affecting radiation information systems in the United States and Ireland since 2020. The effect of these attacks is typically delayed or canceled patient treatment.

The actual type of medical device in our ranking is less important than the fact that they reflect the ongoing trend toward digitalization in healthcare, where medical devices are connected to the IT network and can generate and exchange patient data with other systems.

DICOM workstations, nuclear medicine systems, imaging devices and PACS are all devices related to medical imaging. They have a few things in common: They often run legacy vulnerable IT operating systems, have extensive network connectivity to allow for sharing imaging files and use the DICOM standard for sharing these files.

DICOM defines both the format for storing medical images and the communication protocol used to exchange them. The protocol supports message encryption, but its usage is configured by individual healthcare organizations. We observe unencrypted communications in many organizations, which could allow attackers to obtain or tamper with medical images, including to spread malware.

Patient monitors are among the most common medical devices in healthcare organizations and also among the most vulnerable. Like medical imaging devices, they often communicate with unencrypted protocols, which means attackers can tamper with their readings.

4. Industry Discussion

Figure 1 shows the distribution of device risk levels (low, medium and high) per industry in our dataset. We have selected the same five verticals we analyzed in the 2020 report. Manufacturing has the highest percentage of devices with high risk (11%), while government and financial have the top combinations of medium and high risk (43% for government and 37% for financial). Healthcare and retail have the lowest risk overall, with 20% of devices having medium or high risk in healthcare and 18% in retail.

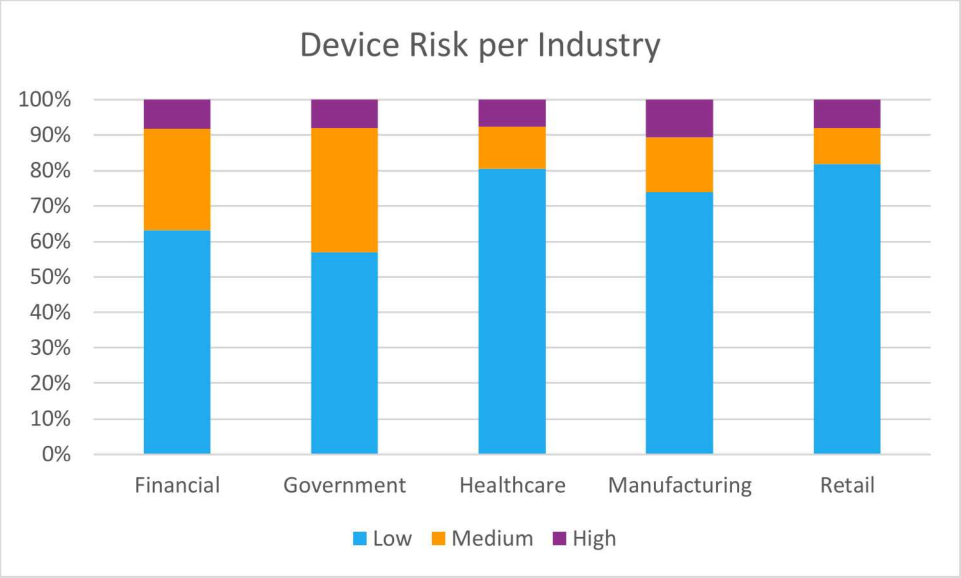

Figure 1 - Device risk per industry

The ranking of riskiest devices does not change considerably per industry, which shows that almost every organization currently relies on a combination of IT, IoT and OT (as well as IoMT for healthcare) to deliver their business. It also means that almost every organization is affected by a growing attack surface. One specific observation is interesting: When we look exclusively at the financial sector, ATMs jump to the first position of riskiest IoT, while customer self-service kiosks appear as a new fifth riskiest IoT.

5. Geography Discussion

The devices in our dataset are distributed geographically as shown in Figure 2, where APJ stands for Asia-Pacific and Japan, and META stands for Middle East, Turkey and Africa.

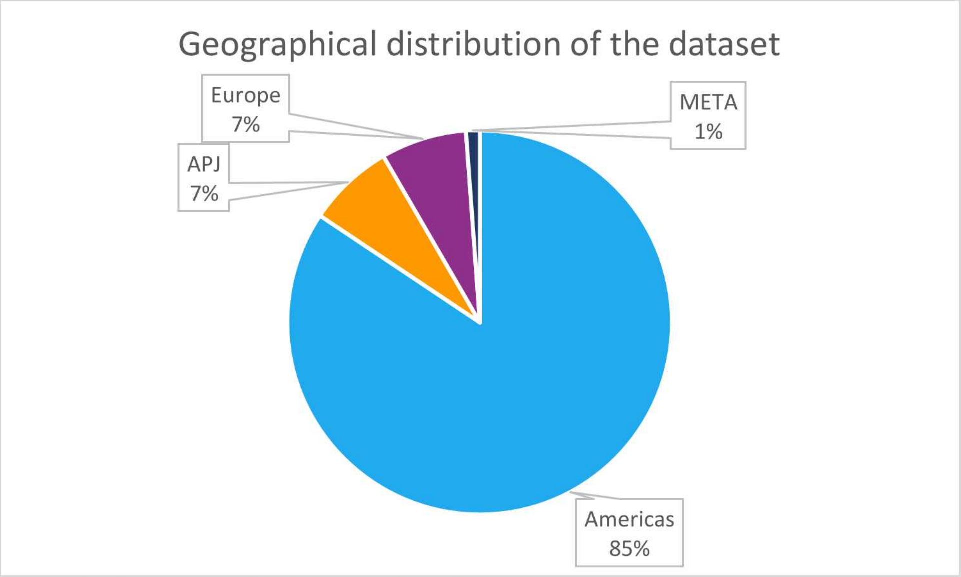

Figure 2 - Geographical distribution of the dataset

The vast majority of devices are in the Americas region, but if we zoom in on the other regions, we observe three interesting facts:

- **The riskiest IT and OT devices remain nearly constant**. There are a few changes in the ranking, but the five riskiest IT and OT devices are the same in every region.
- **The riskiest IoT devices change slightly**. In each region, we see a new IoT device entering the ranking. In APJ, smart home controllers are the fifth riskiest. These devices perform functions similar to OT building automation controllers, but smart home controllers typically have even more connectivity because they rely on remote cloud solutions and mobile apps for management. In Europe, out-of-band controllers are the fourth riskiest. Out-of-band controllers provide dedicated management channels (also called lights-out management) for servers even when they are powered off. These devices increase the attack surface in data centers and have been used to deploy very hard-to-detect malware. In META, network attached storages are the fifth riskiest. Network attached storages often have both easy-to-exploit vulnerabilities and internet connectivity; thus they have been recently targeted by threat actors for ransomware, botnets, crypto mining or simply data destruction.
- **The riskiest IoMT devices change considerably**. Table 2 shows the riskiest IoMT devices in each region. DICOM workstations are the only devices that consistently make the list in every region.

Table 2 - Riskiest IoMT devices per region

	Americas	APJ	Europe	META
1	DICOM workstation	Electrocardiograph	DICOM workstation	DICOM workstation
2	Nuclear medicine system	CT scanner	Electrocardiograph	PACS
3	PACS	DICOM workstation	Ultrasound	Medication dispensing system
4	Imaging	Imaging	Patient monitor	CT scanner
5	Medical analyzer	Medication dispensing system	Mammography system	Angiography system

6. Takeaways and Mitigation Recommendations

Two recurring themes in the recent research of Vedere Labs have been the growing attack surface due to more devices being connected to enterprise networks and how threat actors leverage these devices to achieve their goals.

The attack surface now encompasses IT, IoT and OT in almost every organization, with the addition of IoMT in healthcare. It is not enough to focus defenses on risky devices in one category since attackers can leverage devices of different categories to carry out attacks. We have demonstrated this with R4IoT, an attack that starts with an IP camera (IoT), moves to a workstation (IT) and disables PLCs (OT).

You need proper risk assessment to understand how your attack surface is growing. However, assessing device risk is not easy. For instance, to determine whether a device is vulnerable or not, granular classification information is needed, such as device type, vendor, model and firmware version.

As an example, take some of the advisories issued by HP in response to the Ripple20 vulnerabilities. First, HP has multiple versions of their Integrated Lights-Out (iLO) out-of-band controllers, at least one confirmed vulnerable (v2) and one confirmed not vulnerable (v5). Simply classifying a device as an "out-of-band controller" (function) or as an "HP iLO" (vendor and model) is not granular enough to determine if that device is vulnerable: We also need the model version. Second, some HP printers are also vulnerable, but they receive automatic firmware updates, so determining if a printer is vulnerable depends on vendor, model and a firmware version that can change automatically with an unscheduled update.

Once you understand your attack surface, you need to mitigate risk with automated controls that do not rely only on security agents and that apply to the whole enterprise instead of silos like the IT network, the OT network or specific types of IoT devices.