Research Report

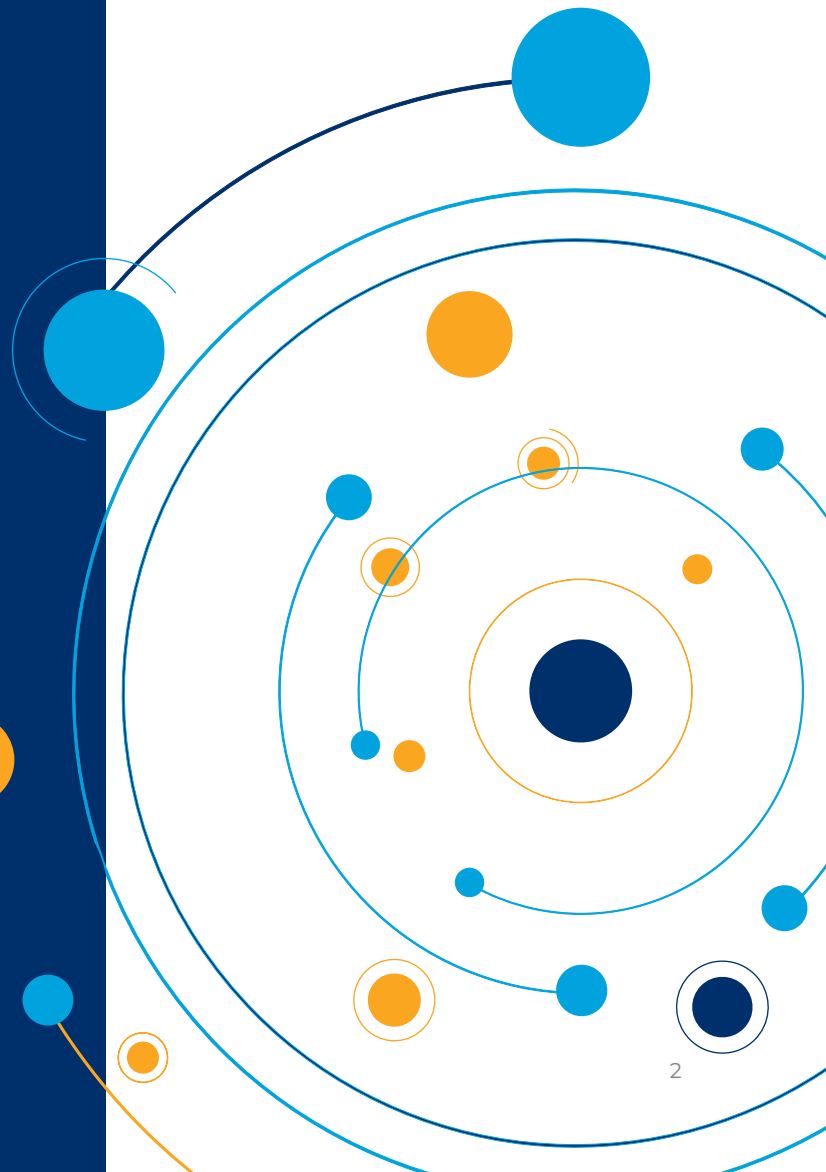
FORESCOUT

The Enterprise of Things Security Report

The State of IoT Security

by Forescout Research Labs

Table of Contents



Executive Summary

In this first edition of The Enterprise of Things Security Report, Forescout Research Labs has undertaken the most comprehensive study of its kind within the greater cybersecurity industry to date to assess the risk posture of **over 8 million devices deployed across 5 verticals: Financial Services, Government, Healthcare, Manufacturing** and **Retail**.

Using carefully defined metrics and data from the Forescout Device Cloud, we identified points of risk inherent to device type, industry sector and cybersecurity policies. Furthermore, we translated these findings into data-informed recommendations to help cybersecurity and risk stakeholders to mitigate and remediate these identified points of risk.

Forescout Device Cloud is one of the world's largest repositories of connected enterprise device data —including IT, OT and IoT device data — and the number of devices it contains grows daily. The anonymous data comes from Forescout customer deployments and, at the time of this report's publication, contains information from approximately **11 million devices** from more than **1,200 global customers**.

Key Findings

- **The riskiest device groups from our Device Cloud data include smart buildings, medical devices, networking equipment and VoIP phones**. IoT devices, which can be hard to monitor and control, exist in every vertical and can present risk to modern organizations, both as entry points into vulnerable networks or as final targets of specialized malware. **The device types posing the highest level of risk are those within physical access control systems**. These devices are ubiquitous and literally open the doors to the physical world, bridging the gap between the cyber and physical realms. According to our data sample, physical access control solutions are the systems at highest risk due to the presence of many critical open ports, a lot of connectivity with risky devices and the presence of known vulnerabilities.
- **Other top-10 riskiest device types include medical devices and networking equipment**. These devices – especially medical devices – have enormous potential impact if compromised, and frequently have critical open ports that expose dangerous services on the network.
- **Windows workstations continue to represent a major risk to organizations. More than 30% of managed Windows devices in manufacturing and over 35% in healthcare are running recently unsupported versions of Windows**. Additionally, almost 30% of managed Windows devices in Financial Services are running operating systems that are not patched against the BlueKeep vulnerability.
- **Commonly exploited network services are spread out across industry verticals. Almost 10% of devices in Government have default Telnet port 23 open, and almost 12% have default FTP ports 20 or 21 open**. In Financial Services, Government and Healthcare, close to 20% of devices have default SMB port 445 and close to 12% have default RDP port 3389 open. These services leave devices open to attacks from automated threats (such as botnets and ransomware) and Advanced Persistent Threats (APTs).

1. Methodology

Defining risk: Risk is classically defined as the likelihood of an incident happening multiplied by the impact of this incident. In cybersecurity, likelihood is usually measured in terms of vulnerabilities and threats, whereas impact is measured in terms of the loss of confidentiality, integrity or availability that usually leads to a negative financial impact.

Measuring risk: Risk is assessed both quantitatively and qualitatively. Good risk metrics should be consistently measured, easy to gather and relevant for decision-makers [1]. Unfortunately, risk assessments are usually based on subjective estimations, since obtaining exact values for likelihood and impact of every possible event is rarely feasible [2]. The main challenges in measuring risk typically include identifying **metrics or factors**, establishing **how to measure** metrics, and defining **how to combine** metrics and measurements in a reasonable risk-scoring formula.

For our exercise, we started by defining a list of **components** that **aggregate** individual **factors** to create a risk score model for IoT devices [1]. In our view, the risk for a device (d) can be calculated as a function of six different components, namely **Vulnerabilities, Security Events, Services, Connectivity, Vendor** and **Potential Impact**.

Risk *(d)* = f (*Vulnerabilities, Security Events, Services, Connectivity, Vendor, Potential Impact*)

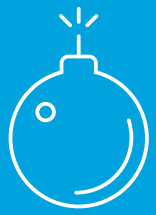
VULNERABILITIES

SECURITY EVENTS

SERVICES

CONNECTIVITY

VENDOR



POTENTIAL IMPACT

The different components of risk that we identified are discussed below. In addition, every risk component can be broken down into multiple quantifiable risk factors:

Table 1: Breakdown of Risk Components into Risk Factors

Risk Component	Risk Factor	Why It Matters
Vulnerabilities	Known Vulnerabilities	Known vulnerabilities can be exploited by threat actors to compromise a device.
	Exploitability	Available exploits make it easier to leverage vulnerabilities.
	Active Exploitability	Vulnerabilities that have been used in known attacks are more likely to be exploited again.
	Remediation Effort	The remediation effort correlates with the probability that the vulnerability will be remediated. In the worst case, a vulnerability may require a patch that cannot be applied to a critical system because it cannot be taken offline.
	Matching Confidence	How certain are we that the device has a vulnerability? This can be influenced by available information about the device or about the vulnerability itself, such as the affected firmware versions.
Security Events	Security Events	Events raised by cybersecurity tools are correlated with the possibility that the device has been or is being targeted in an attack.
Services	Open Ports	Open ports expose network services that can have known or unknown vulnerabilities.
	Interfaces	Available interfaces increase the attack surface. For instance, a device with only an Ethernet port has a more limited attack surface than a device with an Ethernet port, a Wi-Fi antenna and a Bluetooth antenna.
Connectivity	Potential Communications	Devices that reside on the same network segment can be reached by threat actors, even if they have not communicated in the past.
	Observed Communications	Devices that have communicated directly with others may be leveraged in attacks that are more difficult to detect.
	Internet Connectivity	Devices directly connected to the Internet can be exploited remotely.

Risk Component	Risk Factor	Why it matters
Vendor	Security Maturity	The security maturity level of a vendor is directly associated with the presence of vulnerabilities on a device and the likelihood they can be fixed.
	Supply Chain Trustworthiness	This accounts for nation-specific policies around supply chains, such as the well-known restrictions that the U.S. Government imposes on hardware produced in some countries.
	Proximity to EoL	Devices that are either close to or have passed their end-of-life date have the potential to contain unfixable vulnerabilities.
Potential Impact	Business Criticality	Devices that are business-critical have a greater potential impact when compromised.
	Is Managed?	Managed devices are better monitored and controlled by organizations than unmanaged devices (e.g., IoT and OT).

Since our **goal in this study is to measure risk values** for all the devices in our Device Cloud **in an automated and continuous fashion**, we must compute a risk score based on a limited number of risk factors, as presented in **Table 2**. For each factor in Table 2, we also provide information on the external data source that was used to enrich our data.

Table 2: Risk Factors Used in This Report

Category	Factor	How we get the data
Vulnerabilities	Known Vulnerabilities	Data extracted from NVD
	Exploitability	Data extracted from ExploitDB
	Remediation Effort	Data extracted from MITRE CWE
	Matching Confidence	Data manually defined based on the available information
Services	Open ports	Data available in Device Cloud

Category	Factor	How we get the data
Connectivity	Potential Communications	Data available in Device Cloud
Potential Impact	Business Criticality	Data manually defined by domain experts
	Is Managed?	Data available in Device Cloud

2. The Results

In this section, we analyze the data sample from the Device Cloud by applying the methodology and metrics defined for each business vertical individually, and in comparison, to one another.

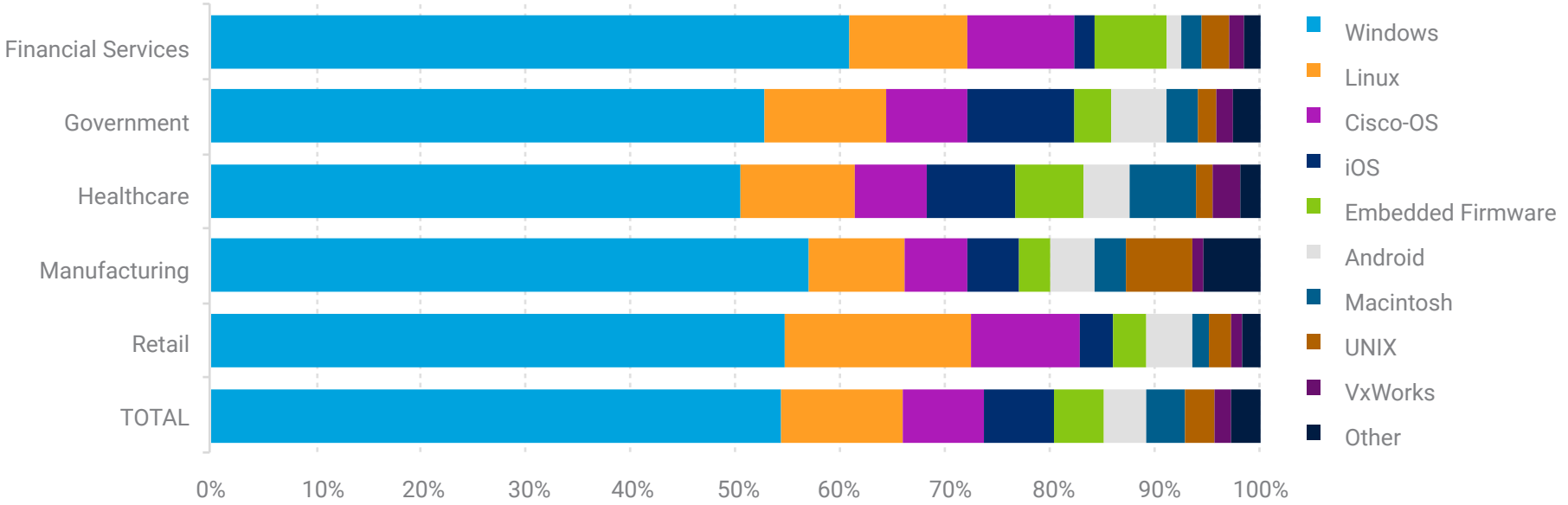
2.1. Risk Exposure

Devices and their risk must be analyzed according to each device's use and role within a vertical application. In this section we illustrate how specific threats and risk factors to some devices manifest and then define the riskiest devices ranked by their risk score. Looking at the device risk allows security teams to focus on key areas according to threat. The threats we selected for analysis are:

- Operating system variants and vulnerabilities
- Unsupported and legacy Windows versions
- Windows machines vulnerable to BlueKeep or CurveBall
- Commonly exploited network services

We selected these specific threats not only because they were prevalent issues in 2019 (and early 2020), but also because they are representative of common network security issues. The need for patching and upgrading common operating systems, limiting access to network services and keeping IoT-specific operating systems under control will not disappear anytime soon.

2.1.1. Operating System Distribution



	Windows	Linux	Cisco-OS	iOS	Emb. Firm.	Android	Macintosh	UNIX	VxWorks	Other
Financial Services	60.96%	11.18%	10.13%	2.06%	6.74%	1.44%	1.98%	2.63%	1.44%	1.46%
Government	52.72%	11.64%	7.78%	10.19%	3.43%	5.35%	3.02%	1.70%	1.61%	2.55%
Healthcare	50.46%	10.98%	6.77%	8.53%	6.51%	4.24%	6.37%	1.67%	2.52%	1.95%
Manufacturing	56.99%	9.20%	5.90%	4.88%	3.10%	4.21%	2.97%	6.32%	0.98%	5.43%
Retail	54.66%	17.77%	10.46%	3.12%	3.23%	4.25%	1.68%	2.08%	1.01%	1.75%
TOTAL	**54.42%**	**11.57%**	**7.77%**	**6.60%**	**4.73%**	**4.08%**	**3.66%**	**2.82%**	**1.65%**	**2.71%**

Figure 1: Distribution of operating system categories according to industry vertical

Windows and Linux dominate the operating system categories seen across all industry verticals, with Windows alone representing more than 50% of the total. These OSes are used in most workstations, servers and even some embedded devices, so their widespread presence is not a surprise. As for Macintosh and UNIX OSes, they are less popular, with Macintosh appearing mostly in laptops and workstations and UNIX variants still representing a considerable slice of IT servers, especially in manufacturing.

Networking equipment with Cisco-OS (a group that encompasses several variants of OS used in Cisco equipment, such as IOS) **is the third largest overall category**, which highlights the vendor homogeneity of networking environments. It is also interesting that these networking-specific OSes appear in more than 10% of devices in the Financial Services and Healthcare verticals, the two industries with the highest percentages of networking equipment. With an average of more than 37 vulnerabilities found per year in the last decade only on versions of Cisco IOS and previous reports of targeted malware in routers, this is one category of OS that security teams should pay close attention to.

These are **followed by mobile operating systems** (iOS and Android), which is an indicator of the commonality of mobile devices in modern enterprise environments, especially in Government where iOS and Android devices together account for more than 15% of devices. Mobile threats are rapidly evolving and, although many security teams still think of mobile threats as targeting personal devices and end users, 33% of organizations suffered a compromise involving mobile devices in 2018 with 60% of those classifying the incident as major [2].

Then we have the large category of **Embedded Firmware**, which is used by many OT and IoT devices. This category encompasses a myriad of different firmware versions and vendors, which makes it difficult to provide a security assessment for each. The main message in this category is that the sheer number and variety of embedded firmware devices 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 [3].

Finally, among other embedded and **Real-Time Operating Systems** (RTOS), we single out Wind River VxWorks in our analysis because of its market share in this category and because of the URGENT/11 vulnerabilities disclosed in 2019, which allow unauthenticated remote code execution in some versions of this OS. Notice that, although this threat is severe and there have been a huge number of device models reported vulnerable (with many more potentially being vulnerable without vendors or users being aware), VxWorks accounts for less than 2% of devices in most industry verticals, with the notable exception of Healthcare, where many smart clocks and medical devices rely on this OS. Healthcare has the highest penetration of real-time operating systems, including VxWorks, ThreadX RTOS, eCos and Nucleus RTOS. Most of the devices found in Device Cloud that run the Robot Operating System (ROS) are deployed within Manufacturing.

2.1.2. Legacy Windows Threat

Since Windows is the most popular operating system across all industry verticals, we analyze its versions in more detail along with two important recent vulnerabilities affecting the OS. Notice that for the vulnerability discussion we only consider managed devices from which we can obtain precise information about currently applied patches.

Figure 2 below illustrates the percentage of devices in each vertical running completely unsupported versions of Windows (i.e., all versions prior to Windows 7, such as Vista and XP) and those running versions that are only supported via the Extended Security Updates (ESU) program (i.e., all versions of Windows 7 as of January 14, 2020).

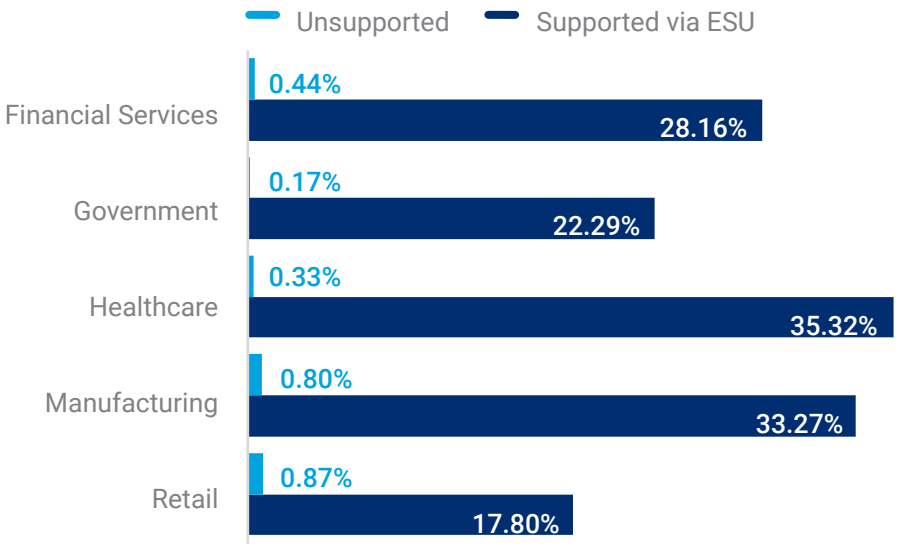


Figure 2: Distribution of Legacy Windows Devices

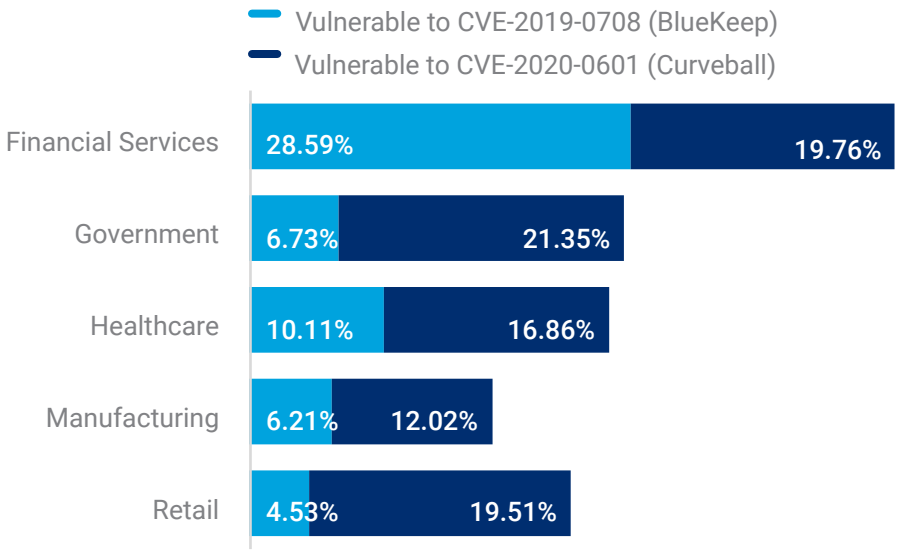


Figure 3: Distribution of Windows Devices Vulnerable to BlueKeep or CurveBall

Although the **truly legacy and unsupported versions account for less than 1%** of devices in each vertical (with Retail in the lead and Government far behind), the percentage of **versions supported via ESU is worrisome in most vertical industries. This is especially true in Healthcare, where more than 35%** of Windows devices are in that category. The ESU program should be a last resort for organizations that cannot upgrade their devices, and it is not a cheap one. For instance, the German government will have to pay at least €800,000 in 2020 to keep more than 33,000 workstations updated.

The existence of a support program for a specific OS is not enough to guarantee that devices will be patched. As an example, **Figure 3** illustrates the percentage of managed Windows devices that are vulnerable to BlueKeep (CVE-2019-0708) or CurveBall (CVE-2020-0601). Those are two serious examples of vulnerabilities disclosed in 2019 and 2020, respectively. BlueKeep allows remote code execution and can be used to create malware that spreads automatically, while CurveBall is a cryptographic vulnerability that may allow attackers to trick users into believing that malicious code is legitimate.

It is noteworthy that even though **BlueKeep** was reported in May 2019, there was an available Metasploit exploit in September 2019 and active attacks confirmed in November 2019. **Almost 30% of managed Windows devices in Financial Services are still running potentially vulnerable OSes**. That figure is much higher than any other industry vertical, where the figures are between 4%-7%, with the exception of Healthcare. Interestingly, the ranking for both vulnerabilities is not correlated since the OS versions affected by each issue are mutually exclusive. For **CurveBall**, a vulnerability reported more recently that impacts modern Windows versions (Windows 10 and Windows 2016), the numbers are generally **higher (12%-22%)**, except in Financial Services where CurveBall is less prevalent than BlueKeep.

2.1.3. Risk from Enabled Services

As discussed in the motivation for the risk metrics, known vulnerabilities are among the riskiest factors for a device, but exposed services are what leave devices open to attacks, both because of known vulnerabilities and unknowns such as Zero-day vulnerabilities.

Figure 4 illustrates the percentage of devices in each vertical that have **enabled services commonly exploited by threat actors**. Each color in the bar graph represents a networking service; the **default ports** they use are noted in parentheses.

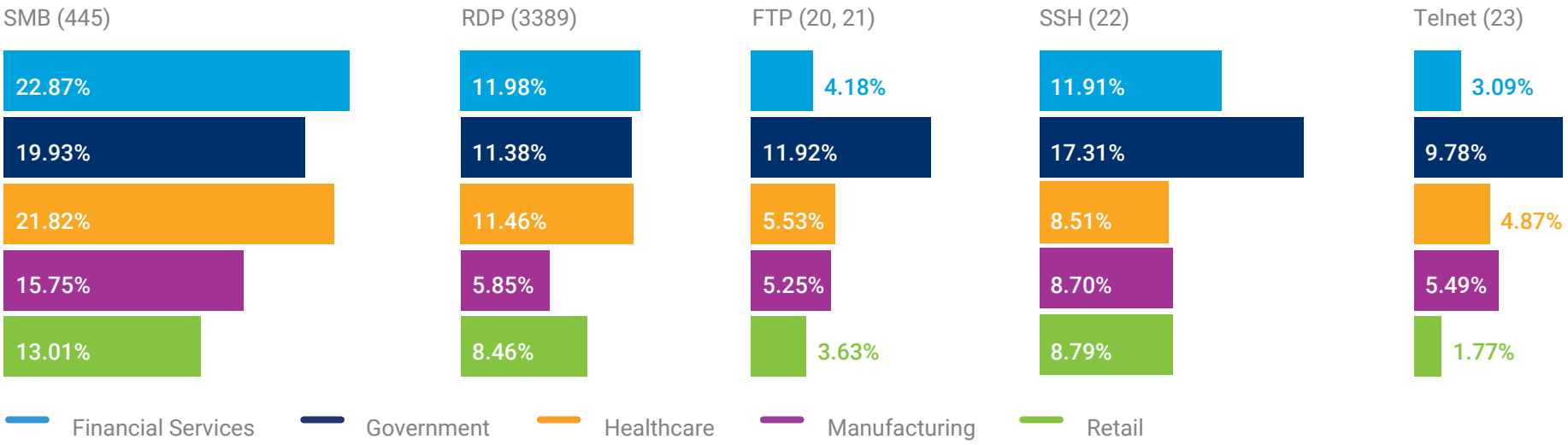


Figure 4: Distribution of Enabled Services

Server Message Block Protocol **(SMB)** is used by Windows machines for file sharing, printer sharing and access to remote services. WannaCry and NotPetya are two examples of ransomware that exploited the EternalBlue vulnerabilities in SMB. Remote Desktop Protocol **(RDP)** provides remote access to manage devices using a graphical interface and is also commonly exploited by modern automated threats, including brute-force attacks and the recent Ryuk ransomware. Secure Shell **(SSH)** provides remote management capabilities, especially to Linux/UNIX servers, and, although it is cryptographically secure, it may be abused by leveraging brute-force attacks and other vulnerabilities to log remotely onto machines. Recently, the TrickBot data exfiltration malware was updated to collect SSH keys in infected networks. **Telnet** and File Transfer Protocol **(FTP)** are often-exploited vectors. These protocols do not secure or encrypt network sessions, allowing credentials or sensitive data to be sniffed in the network. The Mirai and SYSCON botnets, for instance, relied heavily on exploiting Telnet and FTP, respectively.

Financial Services leads in instances of **SMB and RDP**, which are usually present in Windows workstations and among the most common exploitation vectors in 2019. In second place for those same protocols comes **Healthcare. These percentages are in line with breach statistics that show that Financial Services and Healthcare are the most targeted verticals and leading in ransomware infections** [4]. Of course, the presence of open ports does not fully explain why these industry verticals are targeted, since threat actors are mostly interested in return on investment and these industry verticals are rife with personal sensitive information that can be sold on black markets [5].

One of the most interesting facts from Figure 4 is the number of devices with **FTP and Telnet enabled in Government**. It is scary to see that roughly 12% and 10% of devices have FTP or Telnet enabled, respectively, and that these devices may be exchanging unencrypted sensitive information. Besides the **data leakage** opportunities, these protocols open devices up to exploitation attempts from automated malware, such as the Mirai and SYSCON botnets previously mentioned, as well as Advanced Persistent Threats (APTs) [6].

2.2 Riskiest Devices

To determine the riskiest device functions, we first computed the individual risk score for each device. Next, we aggregated this score by taking the average risk per device function. We filtered out devices that had a function classification considered not granular enough (such as devices classified simply as “Operational Technology”).

As mentioned earlier, the risk that a device poses to an organization is measured by aggregating Vulnerabilities, Exploitability, Remediation Effort, Matching Confidence, Open Ports, Potential Communications, Business Criticality and whether the device is Managed. Note that the number of devices of a certain type or vendor does not impact the risk score since we are not looking for popular devices that are risky, but rather devices that are either inherently risky or risky because of their connectivity.

Our analyses in this section adhere to the Forescout model classification, which assigns a single vendor/model per device when searching for vulnerabilities in third-party sources. This is advantageous for devices that have low fragmentation of their software and hardware supply chains, with both software and hardware delivered by the same vendor (e.g., most IoT devices and some networking equipment). For other devices, it is very difficult to reliably map the knowledge base on publicly reported vulnerabilities to a specific hardware/software combination used by a vendor. Therefore, we may miss some vulnerabilities in the search, and the final risk score must be adjusted accordingly.

2.2.1. Riskiest Devices by Vertical

Smart Building devices | Healthcare devices | Networking and VoIP devices | Operational Technology | Other IoT Devices

	Financial Services	Government	Healthcare	Manufacturing	Retail
1	Uninterruptible Power Supply	Physical Access Control	Pneumatic Tube System	Uninterruptible Power Supply	Physical Access Control
2	HVAC	HVAC	Uninterruptible Power Supply	Physical Access Control	HVAC
3	IP Camera	Emergency Communication System	HL7 Gateway	Programmable Logic Controller	IP Camera
4	Programmable Logic Controller	IP Camera	PACS Archive	IP Camera	Programmable Logic Controller
5	Network Management	Programmable Logic Controller	Radiotherapy System	HVAC	Firewall
6	Firewall	Serial-to-IP Converter	Sterilization	Point of Sale	Out of Band Controller
7	Out of Band Controller	Lighting	Physical Access Control	Network Management	Wireless Access Point
8	Router or Switch	Out of Band Controller	Radiology Workstation	Out of Band Controller	Video Conferencing
9	VoIP Server	Video Conferencing	HVAC	Video Conferencing	Router or Switch
10	Printer	Network Management	Programmable Logic Controller	Robots	Network Attached Storage

Figure 5: Riskiest Device Functions Per Vertical

Figure 5 illustrates the ten riskiest device types in each vertical and highlights the types of devices that security staff in each vertical should look at more carefully.

In Figure 5, granular device functions are grouped to facilitate the discussion, as follows: **Smart Building devices** include HVAC systems, IP Cameras, Physical Access Control, Emergency Communication Systems and Lighting.

Healthcare devices include HL7 Gateways, Picture Archiving and Communication System (PACS) Archives, Radiotherapy Systems, Radiology Workstations and Sterilization.

Networking and VoIP devices include Network Management, Firewalls, Out of Band Controllers, Routers or Switches, VoIP servers, Serial-to-IP converters and Wireless Access Points.

Operational Technology devices include UPS, PLCs and Robots.

Other IoT devices include Printers, Video Conferencing, Pneumatic Tube Systems, Point of Sale (POS) and Network-Attached Storages.

Below, we discuss each device group in detail. Most of these device functions score highly because of their potential impact coupled with many open ports, connections and vulnerabilities. All except the networking equipment functions are also typically unmanaged devices. Although general-purpose **IT workstations** do not appear in the Figure due to **hardware/software fragmentation**, note that they are still the main entry points into enterprise networks. Attacks leveraging these workstations usually start with phishing, malicious e-mails or infected websites and are followed by lateral movement within the Active Directory domain [7].

- **Smart building devices:** Devices in this group are the **top 1 or 2 in every vertical, except Healthcare** (where medical devices are the riskiest). These devices are especially important in **Government** and **Retail**, where they show up as the three riskiest. Both these industry verticals are known for having many facilities, which exacerbates the risk presented by smart building devices. Government has the **largest number of device functions related to smart buildings in the top 10**. Smart buildings perfectly exemplify a cross-industry domain where IT and OT are converging and where IoT devices are proliferating[8]. Our **recent research**[9] [10] has shown how these buildings can be **vulnerable**, how IoT devices can be **leveraged** as an **entry point** to a building's network, and what kinds of **effects** these attacks can have (e.g., **physical authorization bypass** and **data center damage** via HVAC tampering). A real case of a smart building device serving as an entry point into a corporate network is the recent data breach where a casino was hacked via the Internet-connected thermometer in a fish tank[11]. Other examples in which building systems were the final targets of **reported attacks** include a hotel in Austria where people were locked out of their rooms until a ransom was paid[12] and two apartment buildings in Finland in which a DDoS attack targeting the heating system left residents in the cold[13].

- **Healthcare devices:** Connected medical devices are obviously **risky because of their potential impact**, both in terms of **business continuity** and, much more importantly, their **potential** to **harm patients**. The actual type of medical device in the 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 devices such as Electronic Health Records systems. This trend is represented in Figure 5 by **HL7 Gateways** and **PACS Archive**, which use the two most important interoperability standards in Healthcare (HL7 and DICOM, respectively) to interconnect medical devices and medical information systems. Alongside this reliance on new technologies and increased connectivity, we are witnessing an **increase in the number and sophistication of vulnerabilities in medical devices**[14] [15] and **cyberattacks on hospitals**[16], although these rarely target medical devices directly. Targeted attacks against life-supporting and life-saving devices could have devastating consequences for patients and Healthcare organizations alike. Attacks targeting HL7 and DICOM systems have been demonstrated by researchers[17] [18], while attacks already seen in different domains such as the ones against smart buildings described above show that OT and IoT may be targeted by real attackers. The rise of Shodan and other specialized tools for finding exposed OT and IoT devices and potential exploits can aid attackers in launching such attacks. All of this makes it **essential to be prepared for attacks that exploit the complexity of Healthcare ecosystems**.

- **Networking and VoIP devices:** Networking and VoIP are also ubiquitous functions in enterprise networks, so they appear in the top 10 of **all industry verticals except Healthcare** for the same reason as smart building devices. Nevertheless, they are **generally less risky than smart building** devices because their **impact is often restricted to information systems**. One of the main issues with networking equipment (such as routers, switches and firewalls) is that it is **often exposed online**, since it can be the interface between internal and external networks. **Consumer-grade routers are one of the preferred targets for VPNFilter and other botnets** since these devices are rarely updated and often have default credentials[19]. Other potential attacks leveraging networking equipment include **DNS poisoning, man-in-the-middle and VLAN hopping**[20]. The **Wireless Access Points** showing up in Retail are the typical border between internal and external networks. They are frequently used to host both guest and corporate networks and are increasingly used to connect guest mobile devices. **Guest devices** usually have **no access** to **"crown jewels,"** but they are often **connected to many other guest devices**, are potentially infected and are much **more difficult to monitor** than managed devices. Many modern access points also integrate wireless technologies such as Bluetooth Low Energy (BLE) and ZigBee, which may open them up to new types of attacks[21].

VoIP is **pervasive in enterprise networks** and devices such as softphones, adapters and even servers. There is a **long history of VoIP attacks** such as denial-of-service, call snooping, and even call spoofing, using popular protocols such as SIP[22] [23]. However, these devices **can also be used to compromise other hosts** in the network[24]. Interestingly, devices used for internal network management and connectivity also appear on the list, such as **serial-to-IP converters** and **out-of-band controllers**. Serial-to-IP converters are ubiquitous and used to connect devices that utilize serial communications to more modern Ethernet networks. These devices were part of the 2015 attack on the Ukrainian grid that resulted in a power outage for more than 200,000 consumers,[25] and their huge risk to critical infrastructure is well known[26]. 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 allow for the possibility of very hard-to-detect spyware and rootkit penetration[27].

- **Operational Technology devices:** Devices in this group are more specialized, so we only see three examples in the Figure 5: UPS, PLCs and robots. Surprisingly, OT devices are present in all verticals, which again indicates the effects of IT-OT convergence. In Retail, OT devices are related to the **logistics** side of the vertical, whereas in **Manufacturing** they show up as two of the three **most critical** devices, since they are fundamental to drive (in the case of PLCs) and execute (in the case of robots) manufacturing processes. In the other verticals, they are mostly related to data centers, especially in the case of UPS. The **potential impact** of OT devices in Manufacturing is very high, somewhat comparable to that of medical devices in Healthcare. One important difference, however, is that destructive attacks to industrial processes are becoming more common[28].

- **Other IoT devices:** The **most common risky device in this category is video conferencing**, which appears in Government, Manufacturing and Retail. Recently, researchers at Forescout Labs disclosed vulnerabilities in a sophisticated whiteboard/video conferencing solution that allows threat actors to breach organizations or to use the platform as a spying device. In Healthcare, there are **pneumatic tube systems**, which although they sound like an ancient solution, are still widespread in hospitals and carry thousands of sensitive lab samples and prescription medicine every day[29]. Other interesting devices appearing in the list are **Printers** and **Point of Sale systems**. Printers are often connected to mission-critical financial devices supporting central business functions in consumer banks, while POS systems have been frequently targeted by specialized RAM-scraping malware to steal credit and debit card data[30].

2.2.2 The 10 Riskiest IoT Devices of 2020

Aside from analyzing the risk levels of device groups, as well as device-group distribution within industry verticals, Forescout Research Labs also measured the risk associated with specific device function and type from our dataset. To identify device risk, we first computed the individual risk score for each device, then we aggregated this score by taking the average risk per device model. We filtered out of the results devices that had a model classification considered not granular enough (e.g., devices classified simply by device function). Vendor names and model numbers have been anonymized.

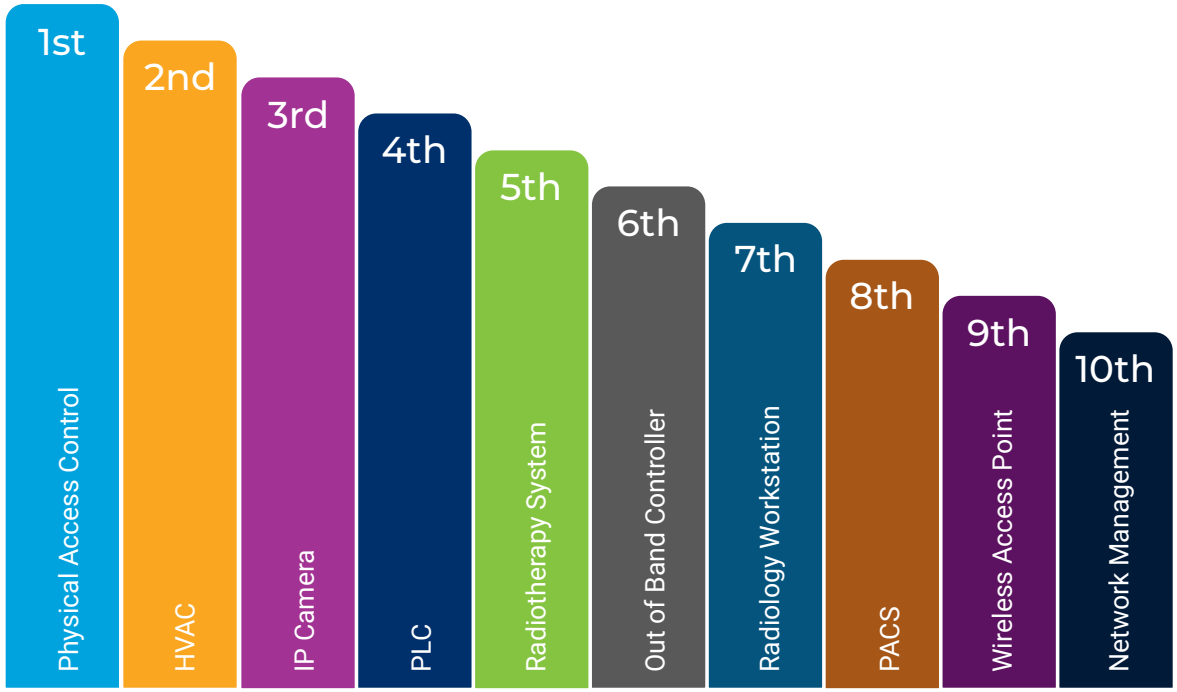


Figure 6: Riskiest Device Functions Across Verticals

Figure 6 illustrates the ten riskiest device functions over the whole data sample. These device functions are representative of the risky functions presented above and provide examples of concrete vulnerabilities of typical network configurations (e.g., open ports and connectivity). They are by no means the only functions that should be monitored by security teams. Notice that all those devices are typically unmanaged.

1. **Physical Access Control Solution:** These devices are used to open or close door locks in the presence of authorized badges. In our research, they were often found configured with open ports (including Telnet port 23), connected to other risky devices and containing serious reported vulnerabilities[31] [32].

2. **HVAC Systems:** These devices were also found configured with critical open ports (including Telnet), connected to other risky devices and containing a couple of critical vulnerabilities that allow complete takeover of a device (CVE-2015-2867 and CVE-2015-2868).

3. **Network Cameras:** These IP cameras have dozens of serious vulnerabilities associated with them (e.g., CVE-2018-10660), they are usually configured with critical ports such as SSH port 22 and FTP port 21 enabled, and they are connected to risky devices. For more about this device risk, read our past research on the topic: https://www.forescout.com/securing-building-automation-systems-bas/

4. **PLC:** The PLCs identified here have serious vulnerabilities associated with them (e.g., CVE-2018-16561) and their potential impact is very high, since PLCs control critical industrial processes. (The infamous Stuxnet malware, for instance, targeted S7 systems used for uranium enrichment[33].) Still, these devices are ranked lower than the first three since, in our sample, they have fewer ports open and reduced connectivity.

5. **Radiotherapy Systems:** There are no vulnerabilities reported for these devices, but they were found configured with many critical ports open (including Telnet) and connectivity to other risky medical devices. The impact of exploitation of these devices is inherently high.

6. **Out-of-Band Controllers:** This refers to an out-of-band controller for servers that are integrated into the main board, which provides an interface to manage and monitor server hardware. It contains its own processor, memory, network connection and access to the system bus. Relevant vulnerabilities have been found in these devices, such as CVE-2015-7272, which can be exploited via SSH (port 22 was open in all of these devices found in our dataset) to achieve a denial-of-service attack and CVE-2019-13131, which can be exploited via SNMP (port 161 was open in most iDRAC devices found in our dataset) to achieve remote code execution.

7. **Radiology Workstations:** This workstation is commonly connected to many peripheral systems in healthcare delivery organizations, such as Radiology Information Systems, PACS, Electronic Heath Records systems and so on. As in the case of radiotherapy systems, there are no reported vulnerabilities. However, these devices were found configured with many critical ports open and connectivity to risky devices. The exploitation impact is also very high, since it is a workstation where common attacker tools can be easily adapted to achieve persistence or to pivot within a healthcare network.

8. **Picture Archiving and Communication Systems (PACS):** PACS are medical imaging systems that provide storage, retrieval, management, distribution and presentation of medical images. Our research found vulnerabilities associated with these systems (e.g., CVE-2017-14008 and CVE-2018-14789). They have a similar risk profile to other medical devices in our research sample due to their place in the network and their use context.

9. **Wireless Access Points:** These contain many critical vulnerabilities, including CVE-2017-3831 and CVE-2019-15261, and are often connected to multiple risky guest devices.

10. **Network Management Cards:** These cards are used to remotely monitor and control individual UPS devices. Besides the presence of known vulnerabilities (e.g., CVE-2018-7820), high connectivity and open ports, these devices have the interesting capability of supporting the BACnet/IP and Modbus/TCP protocols, which again highlights the convergence of smart building technology with IT infrastructure.

3. Conclusions and Recommendations

Forescout Research Labs analyzed more than 8 million devices deployed in the networks of organizations across five industry verticals, making the first Enterprise of Things Security Report the most comprehensive cybersecurity research endeavor of its kind to date. By leveraging the data in the Device Cloud, Forescout Research Labs was able to provide the global cybersecurity community with detailed information about what type of devices are present in enterprise networks and potential risks they can introduce to an organization.

The number and diversity of connected devices in virtually every industry vertical has presented new challenges for all organizations and indirectly made every business leader a cybersecurity stakeholder. According to a recent report by the Ponemon Institute [34], respondents from more than half of the organizations they surveyed are most worried about attacks involving OT and IoT assets. At the same time, that report identifies that new approaches for measuring risk are needed. Cyber risk is an interdisciplinary problem and there are many ways to reduce cyber risk in an organization [35]. Getting and sharing threat intelligence (e.g., by joining an Information Sharing and Analysis Center) is one of them. Applying security controls can also help reduce cyber risk [36], with the advantage that technical controls can be automated by security tools. The **Forescout platform** is one such tool that reduces risks and increases the overall resilience of networks across the extended enterprise in the following ways:

- **eyeSight** can dramatically increase visibility by continuously discovering, classifying and assessing devices without agents or active techniques that could compromise business operations.
- **eyeSegment** can accelerate the design, planning and deployment of dynamic network segmentation across the extended enterprise, reducing the attack surface and regulatory risk.
- **eyeManage** enhances endpoint manageability with a single pane of glass for every network-connected device and unified asset, enabling compliance and risk reporting across the extended enterprise.
- **eyeControl** automates and enforces policy-based control by enabling countermeasures to mitigate threats, incidents and compliance gaps.
- **SilentDefense** highlights OT and IoT exposure by continuously and passively discovering, classifying and monitoring network-connected OT and IoT devices, thus providing real-time risk management.

3.1. Notes on the Analysis and Methodology

At Forescout Research Labs, we leveraged an anonymous data sample from our Device Cloud, which is unique not only because of the number of devices, but also because of the attributes of each device.

The Device Cloud contains a combination of device attributes obtained from passive network traffic monitoring and active querying of switches, managed workstations and other devices, as well as classified attributes based on our continuously updated automatic classification engine. This data, obtained with the consent of our users, is first anonymized and then used by researchers to constantly improve the device classification engine.

Our methodology to collect and analyze data is detailed in Section 3.2. Our goal was to provide a comprehensive summary of the state of enterprise IoT network security within and across industry verticals by looking at enterprise network threat and **risk exposure**, including the riskiest devices observed across industry verticals.

3.2. Data Collection and Analysis

The methodology used by Forescout Research Labs has three main steps: Data Collection, Data Cleaning and Enrichment, and Data Analysis.

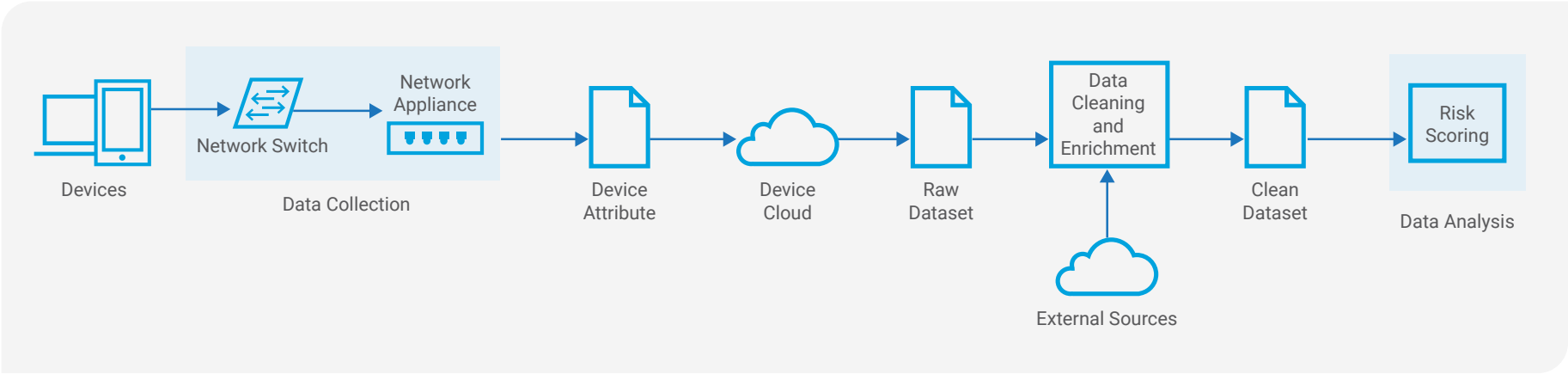


Figure 7: Overview of Data Collection and Analysis

In Figure 7 above, the appliance collects data by passively listening to traffic from devices on the network, actively interacting with the devices on the network by running Nmap and other network scanning tools, and querying third parties to learn more about a device.

3.3 Data Sample

The dataset used for this study contains a total of **8,007,430 devices from 506 deployments**. The deployments are divided according to industry vertical and geography as shown in Table 3.

Table 3: Distribution of Deployments in Verticals and Geography

Vertical	Number of Deployments	Number of Devices	Geography		
			Americas	EMEA	APJ
Financial Services	135	1,239,740	71.85%	16.30%	11.85%
Government	119	1,918,183	78.99%	12.61%	8.40%
Healthcare	88	2,309,639	72.73%	20.45%	6.82%
Manufacturing	125	1,509,498	48.80%	27.20%	24.00%
Retail	39	1,030,370	56.41%	28.21%	15.38%
TOTAL	**506**	**8,007,430**	**66.80%**	**19.76%**	**13.44%**

An example of a device from this dataset is shown below. Notice that the example is simplified, containing only 11 basic attributes, while devices can have more than 200 attributes depending on the plugins that are active in a network. The last attribute – "Is Managed?" – indicates whether a device has a network management agent, meaning a process running in the device that allows a managing entity to take local actions (see [37] for a definition of network management and managed devices).

Table 4: Example of Device in Our Dataset

Type	Attribute	Value
Customer attributes	Customer ID	1234abcd
	Customer Vertical	Financial
	Geography	Americas
Device attributes	IP Address	192.168.0.1
	MAC Address	01-23-45-67-89-AB
	Open Ports	22/TCP, 23/TCP, 80/TCP, 443/TCP
	OS	Cisco IOS-XE 03.06
	Vendor / Model	Cisco Switch 3000 Series
	Function	Switch
	VLAN	vlan1
	Is Managed?	True

To understand the diversity of devices and networks in the Device Cloud, consider that our dataset contains a total of **5,412 unique vendor/model combinations, running 603 unique operating system versions and classified in 251 unique functions**. There are also **62,287 total Virtual Local Area Networks (VLANs)**.

3.4 Open Questions for Your Consideration

The following points are some notes on the methodology adopted in this study, which highlight **open research questions that we invite the security research community to collaborate** with us in addressing.

1. **Real-world, enterprise-scale networks are not easy to monitor.** We may not observe all possible devices nor all possible attributes for a specific device because of the conditions of our deployments, such as some passive-only implementations, monitoring sensors placed in restricted network segments, data from some sensors not being uploaded to the cloud and so on. These deployments are tailored for customer needs, and we can only analyze the data that our sensors capture and that is shared with us. In any case, this is the largest data-driven study of connected devices in enterprise networks.

2. **Device classification is an actively studied research problem** [39] [40] [41]. Our device classification engine is based on a set of heuristics that can contain errors or be incomplete, but which is continually improved day by day. The purpose of Device Cloud is to use customer data to deliver better products back to our customers, while enhanced classification is one of the most important use cases for analyzing data from the Device Cloud.

3. **Risk is difficult to measure and dependent on context.** Our risk analysis in this report did not consider mitigation measures in specific network deployments of a device and other contextual information because we do not have access to this information. Besides, not all risk metrics are easily quantifiable or quantifiable at the same time because they depend on observed attributes and metrics which may have an associated degree of certainty. Nevertheless, we provided a transparent and documented methodology that can be used to quantify risk and – with some limitations based on data availability – we quantified risk for millions of devices in the Device Cloud.

4. **Our risk analyses that define the riskiest device functions and models rely on our classification engine, which can contain errors** (as described in point 2). In the case of device models this limitation is even more impactful since the classification per device model has lower coverage than the classification per function (i.e., there exist many more device models than possible functions), and model classification is a harder problem to solve than function classification.

5. **Relying on third-party sources for threat intelligence data may introduce errors.** In our risk analysis, we use the NVD and ExploitDB databases, which are well known in the security community. However, even if they are standard tools, the information in those sources may be outdated or incomplete, while their search functions may produce errors in matching vulnerabilities and exploits to devices.

Working within these bounds, Forescout researchers have done their best to ensure consistent, reliable and high-integrity reporting.

References

[1] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley Professional, 2007.

[2] P. Burnap, "The Cyber Security Body Of Knowledge - Risk Management & Governance Knowledge Area," 2019. [Online]. Available: https://www.cybok.org/media/downloads/Risk_Management__Governance_issue_1.0.pdf.

[3] A. Costin, J. Zaddach, A. Francillon and D. Balzarotti, "A Large-Scale Analysis of the Security of Embedded Firmwares," in 23rd USENIX Security Symposium, 2014.

[4] Beazley, "2019 Breach Briefing," 2019. [Online]. Available: https://www.beazley.com/Documents/2019/beazley-breach-briefing-2019.pdf.

[5] C. Czeschik, "Black Market Value of Patient Data," in Digital Marketplaces Unleashed, Springer, 2018.

[6] N. Virvilis and D. Gritzalis, "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?," in International Conference on Availability, Reliability and Security (ARES), 2013.

[7] P. Kim, The Hacker Playbook 2, SecurePlanet LLC, 2015.

[8] Memoori, "The Collision of IT & OT is Shaping the Future of Buildings in the IoT Age," 2018. [Online]. Available: https://www.memoori.com/collision-ot-shaping-future-buildings-iot-age/.

[9] Forescout, "Cybersecurity in Building Automation Systems," 2019. [Online]. Available: https://www.forescout.com/securing-building-automation-systems-bas/.

[10] Forescout, "Rise of the Machines: Transforming Cybersecurity Strategy for the Age of IoT," 2019. [Online]. Available: https://www.forescout.com/places-in-network/building-automation-system-bas/transforming-cybersecurity-strategy-for-the-iot/.

[11] W. Wei, "Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer," 2018. [Online]. Available: https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

[12] M. Burgess, "Could hackers really take over a hotel? WIRED explains," 2017. [Online]. Available: http://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers.

[13] I. Ashok, "Hackers leave Finnish residents cold after DDoS attack knocks out heating systems," [Online]. Available: http://www.ibtimes.co.uk/hackers-leave-finnish-residents-cold-after-ddos-attack-knocks-out-heating-systems-1590639.

[14] Y. Xu, D. Tran, Y. Tian and H. Alemzadeh, "Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices," in IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2019.

[15] CISA, "ICS-CERT Advisories," [Online]. Available: https://www.us-cert.gov/ics/advisories.

[16] HIMSS, "2019 HIMSS Cybersecurity Survey," 2019. [Online]. Available: https://www.himss.org/2019-himss-cybersecurity-survey.

[17] J. Tully, C. Dameff and M. Bland, "Pestilential Protocol: How Unsecure HL7 Messages Threaten Patient Lives," 2018. [Online]. Available: https://www.blackhat.com/us-18/briefings/schedule/index.html#pestilential-protocol-how-unsecure-hl-messages-threaten-patient-lives-11726.

[18] Y. Mirsky, T. Mahler, I. Shelef and Y. Elovici, "CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning," in USENIX Security, 2019.

[19] D. Palmer, "Hacking attacks on your router: Why the worst is yet to come," 2019. [Online]. Available: https://www.zdnet.com/article/hacking-attacks-on-your-router-why-the-worst-is-yet-to-come/.

[20] H. Mokadem, “Switch Attacks and Countermeasures,” [Online]. Available: https://www.cisco.com/c/dam/en_us/training-events/le31/le46/cln/promo/share_the_wealth_contest/finalists/Hany_EL_Mokadem_Switch_Attacks_and_Countermeasures.pdf.

[21] M. Garbelini, S. Chattopadhyay and C. Wang, “SweynTooth: Unleashing Mayhem over Bluetooth Low Energy,” 2020. [Online]. Available: https://asset-group.github.io/disclosures/sweyntooth/sweyntooth.pdf.

[22] D. Plamer, “This mysterious hacking campaign snooped on a popular form of VoiP software,” 2019. [Online]. Available: https://www.zdnet.com/article/this-mysterious-hacking-campaign-is-snooping-on-a-popular-form-of-voip-software/.

[23] M. Alvarez, “Hello, You’ve Been Compromised: Upward Attack Trend Targeting VoIP Protocol SIP,” 2016. [Online]. Available: https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip/.

[24] R. Farley and X. Wang, “Exploiting VoIP softphone vulnerabilities to disable host computers: Attacks and mitigation,” International Journal of Critical Infrastructure Protection, vol. 7, no. 3, pp. 141-154, 2014.

[25] A. Shehod, “Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US,” 2016. [Online]. Available: https://cams.mit.edu/wp-content/uploads/2016-22.pdf.

[26] P. Roberts, “Serial To Ethernet Converters are the Huge Critical Infrastructure Risk Nobody Talks About,” 2016. [Online]. Available: https://securityledger.com/2016/04/serial-to-ethernet-converters-the-giant-infrastructure-risk-nobody-talks-about/.

[27] A. Bonkoski, R. Bielawski and J. Halderman, “Illuminating the Security Issues SurroundingLights-Out Server Management,” in Proceedings of the 7thUSENIXWorkshop on Offensive Technologies (WOOT), 2013.

[28] Kaspersky, “Threat landscape for industrial automation systems, H1 2019,” 2019. [Online]. Available: https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/.

[29] Stanford Medicine, “Gone with the wind: Tubes are whisking samples across hospital,” 2010. [Online]. Available: http://med.stanford.edu/news/all-news/2010/01/gone-with-the-wind-tubes-are-whisking-samples-across-hospital.html.

[30] R. Rodriguez, “Evolution and characterization of point-of-sale RAM scraping malware,” Journal of Computer Virology and Hacking Techniques, vol. 13, p. 179–192, 2017.

[31] Zero Day Initiative, “HID VertX/Edge discoveryd Command Injection Remote Code Execution Vulnerability,” 2016. [Online]. Available: https://www.zerodayinitiative.com/advisories/ZDI-16-223/.

[32] N. Andre, “Vulnerabilities in HID iClass RFID Access Control Systems,” 2013. [Online]. Available: http://www.cs.tufts.edu/comp/116/archive/fall2013/nandre.pdf.

[33] R. Langer, “To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve,” 2013. [Online]. Available: https://www.langner.com/to-kill-a-centrifuge/.

[34] Ponemon Institute, “Measuring & Managing the Cyber Risk to Business Operations,” 2019. [Online]. Available: https://www.tenable.com/ponemon-report/cyber-risk.

[35] G. Falco, M. Eling, D. Jablanski, M. Weber, V. Miller, L. Gordon, S. Wang, J. Schmit, R. Thomas, M. M. T. Elvedi, E. Donavan and S. Dejung, “Cyber risk research impeded by disciplinary barriers,” Science, vol. 366, no. 6469, pp. 1066-1069, 2019.

[36] SANS, “CIS Critical Security Controls: Guidelines,” [Online]. Available: https://www.sans.org/critical-security-controls/guidelines.

[37] J. Kurose and K. Ross, Computer Networking: A Top-Down Approach, 6th Edition, Pearson, 2013.

[38] Gartner, “Gartner Glossary,” 2020. [Online]. Available: https://www.gartner.com/en/information-technology/glossary.

[39] Y. Meidan, M. Bohadana, A. Shabtai, J. Guarnizo, M. Ochoa, N. Tippenhauer and Y. Elovici, “ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis,” in Symposium on Applied Computing (SAC), 2017.

[40] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi and S. Tarkoma, “IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT,” in IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017.

[41] L. Bai, L. Yao, S. Kanhere, X. Wang and Z. Yang, “Automatic Device Classification from Network Traffic Streams of Internet of Things,” in IEEE 43rd Conference on Local Computer Networks (LCN), 2018.

About Forescout Technologies

Forescout is the leader in Enterprise of Things security, offering a holistic platform that continuously identifies, segments and enforces compliance of every connected thing across any heterogeneous network. The Forescout platform is the most widely deployed, scalable, enterprise-class solution for agentless device visibility and control. It deploys quickly on your existing infrastructure – without requiring agents, upgrades or 802.1X authentication. Fortune 1000 companies and government organizations trust Forescout to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

Don't just see it. Secure it. Visit forescout.com to learn how Forescout provides active defense for the Enterprise of Things.
Learn how at www.forescout.com.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com