



# Banking on IoT Security

## Leveraging Device Data to Manage Risk in Financial Services

ForeScout researchers analyze device deployments to identify and illustrate the cybersecurity risks facing financial organizations today.



# Executive Summary

The financial services industry may be less secure than previously thought. Financial services organizations face diverse and serious cyber risks, and for good reason. Outside of there being so much money involved, the financial services have incredibly complex, sprawling and ever-changing corporate networks. In order to stay one step ahead of innovative cyberthreats, the entire financial services industry has had to continuously adapt and invest in new technology.

There is no question that the average financial services firm has become IP-enabled, capitalizing on the innovations in mobile banking, point of sale (POS) technologies and other connected end devices. Many of these innovations in connectivity have made transactions more fluid, rapid and numerous—but are they secure? More importantly, are cybersecurity and risk management leaders in the financial services industry empowered to respond to a cyber event?

## Methodology

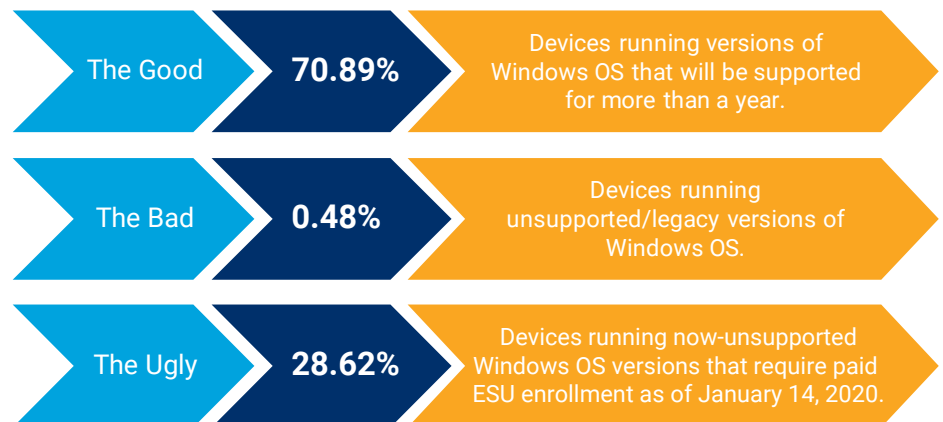
In this report, we will address the aforementioned questions using data that Forescout Technologies has carefully gathered, tested and validated from all forms of device networks and the applications they support. This report presents data from a cross-sectional analysis of the Forescout Device Cloud, which is a repository of host and network information for more than 11 million devices (provided anonymously by Forescout customers). With Forescout Device Cloud, we analyze device fingerprints to identify device function, vendor/model, operating system and version to provide granular auto-classification for a wide range of devices. For this study, researchers limited Device Cloud analysis to 100 large financial services deployments with over 8,500 virtual local area networks (VLANs) and nearly 900,000 devices.

**29% of Windows devices are still running old operating systems that must enter the paid Microsoft Extended Security Updates program after January 14, 2020.**

## Key Findings

- Financial services networks are remarkably flat. Lack of comprehensive network segmentation strategy increases exposure to cyber risk, especially when Internet of Things (IoT) and operational technology (OT) devices that exist outside of the core network are left largely unchecked.<sup>[1]</sup>
- These non-enterprise IoT devices within the financial services industry commonly support applications including hard-to-patch security surveillance systems.
- Nearly half of financial service POS systems (45%) are neighbored by printers. Overall, 63% of POS systems have printer or non-financial IoT device neighbors, highlighting the flat nature of the typical POS network and areas where risk is most prevalent.
- Of all managed Windows devices within financial services, 70.89% are running up-to-date versions of Windows, while 28.62% are now running unsupported OSes and must enter the Microsoft Extended Security Updates (ESU) program starting January 14th, 2020. Known legacy Windows—predominantly XP and Windows Server 2003—are fragile systems that still comprise 0.48% of the managed Windows devices on financial networks today.

**Figure 1:** Windows Operating Systems - The Good, the Bad and the Ugly



## Taxonomy and Definitions

**Financial Services:** Our study focused on “financial institutions” as defined by the Federal Financial Institutions Examination Council (FFIEC): “The term ‘financial institution’ includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.”<sup>[2]</sup>

**IT devices:** Includes traditional computing, Voice over Internet Protocol (VoIP), mobile devices, personal computers (PCs), workstations, laptops, servers, routers, switches, firewalls and wireless access points. Common suppliers of such devices include Dell, HP, Lenovo, Cisco and others.

**IoT devices:** Within the context of financial services networks, IoT devices include banking and retail devices, connected buildings, physical security, access control and video surveillance systems. Other kinds of IoT devices include general sensors, beacons, smart clocks, asset-tracking systems, tag and inventory scanners, kiosks, digital signage, smart TVs, projectors, parking kiosks, and the Forescout research all-time favorite—pneumatic tube systems. In terms of actual device tallies, it can be easier to think of financial services IoT as those IP-enabled devices that are not in the data center and are not computers, servers, networking gear, storage devices, VoIP or mobile. As a rule, IoT devices contain embedded technologies and come with distinct hardware security issues, including hard-to-update firmware, unknown components and customized operating systems.

**OT devices:** OT devices include industrial control systems (ICS), programmable logic controllers (PLC), uninterruptible power supplies (UPS), human machine interfaces (HMI) and other industrial devices. Many of these devices are related to energy and power management in both the data center and campus.

**Energy and power:** Includes uninterruptible power supply (UPS) systems, energy device monitoring and energy-specific programmable logic controllers (PLCs). In nearly all cases, these devices and applications will be categorized under the class of operational technology (OT).

**Financial devices:** Includes specific-purpose banking and retail devices like ATMs and POS systems, and more importantly, the fleets of Active Directory (AD)-joined employee PCs used to access critical business applications in a privileged user context. Financial devices also include the often generously permissioned public-facing systems that deliver services such as e-banking, e-commerce, credit scores, insurance quotes, and cardholder data processing and storage. Any device processing these financial data flows is a financial device. In most cases, these devices are categorized under the class of IT.

**Printers:** Multifunctional devices used in the connected office, including printers and copiers. Enterprise printers have evolved significantly and often step over the line from printer-as-accessory to printer-as-IoT. Smart, multifunctional printers—which often include advanced scan and fax functionality—are generally considered IoT. For the purposes of clarity in this report, we separate printers from the IoT umbrella due to findings unique to printers, and risk implications that are unique to the financial services industry.

**VoIP devices:** VoIP phones, video conferencing and related VoIP server infrastructure. VoIP systems have distinct protocols and network behavior that are unlike general-purpose devices. Enterprise VoIP devices are supplied by Cisco, Avaya, Polycom, Mitel/ShoreTel/Aastra, Nortel, Dell, HP, Samsung and a long tail of device manufacturers and private labels. These devices are categorized under the class of IT.

**Mobile devices:** Smartphones, tablets, smartwatches, wearables and personal media devices. Mobile devices are typically represented by employee bring your own device (BYOD) and public access to guest Wi-Fi. Sometimes, mobile devices are a part of customer kiosks and retail vending. These devices are categorized under the class of IT.

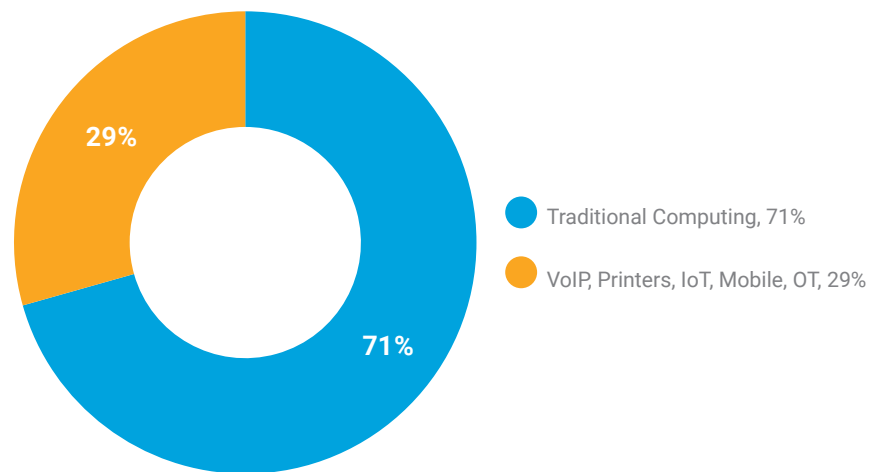
**Building automation systems (BAS):** These include building management systems (BMS), smart lighting, room management, sensors and environment monitoring. BAS also includes management systems for commercial HVAC (heating, ventilation and air conditioning) and thermostats. In most cases, the devices and applications under the BAS umbrella may be categorized under the class of IoT.

# The Risks to Financial Services Networks

The financial services industry may be less secure than previously thought. Security considerations and risk management strategies within the industry seem to have an under-developed device segmentation strategy as it applies to non-traditional computing device networks. Our research suggests that many banking and retail devices are over-exposed to IoT and OT devices which provide elevated opportunities for lateral movement between critical infrastructure and the data center.

For financial services firms, the configuration management database (CMDB) is the pivotal rally point where people and process meet—but the underlying data must be accurate and real-time for this business service desk model to truly work. That’s why defending key data stores within financial services—often referred to as the “crown jewels”—ultimately requires a passive, vendor-agnostic approach to device identification, and by extension, an accurate asset inventory and device segmentation strategy.

**Figure 2:** Breakdown of Devices on Financial Services Networks



Forescout Device Cloud Research 2020

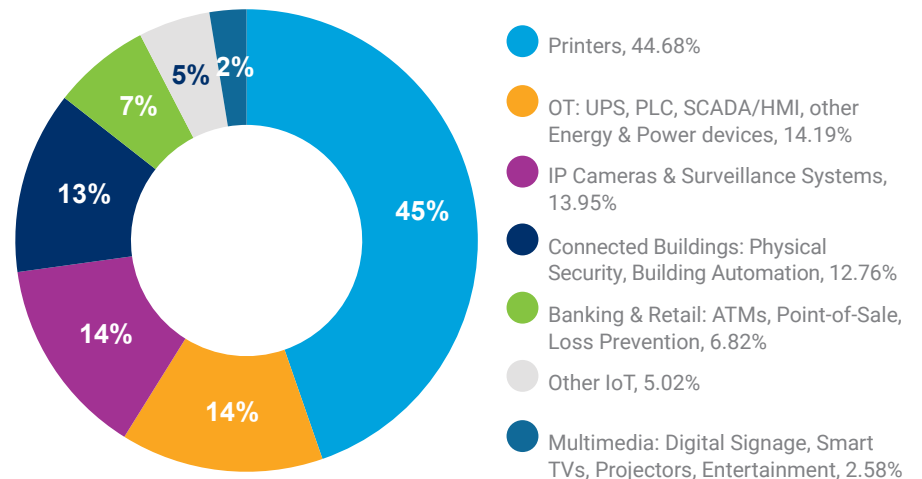
## Printers – The Most Obvious IoT Device Risk

Printers aren’t widely considered to be pivotal devices associated with serious cyber risk. In actuality, they are.

Printed documentation is vital to support customer requests and tort law, so printers are everywhere. Nearly 45% of all IoT devices within financial services are printers, followed by OT devices and IP cameras. It’s also important to understand that printers have a strong association with POS systems. Every time consumers ask for a receipt, some kind of printer technology is utilized. The Payment Card Industry (PCI) Security Standards Council outlines recommendations for segmentation between these scenarios where retail and POS interface with the core network of the financial services organization.<sup>[3]</sup>

Nearly 45% of all IoT devices within financial services are printers, followed by OT devices and IP Cameras.

**Figure 3:** Financial Services IoT Device Breakdown



Forescout Device Cloud Research 2020

Secondly and more importantly, printers expose other financial devices to risk. This is due to the proximity of printers to financial devices and the fact that the innovation of printing security has not kept pace with innovative criminal cyberthreats.

Just as HMIs or ICS applications are connected to various end devices, printers are connected to many mission-critical financial devices supporting central business functions at the average consumer bank. For example, it is observable in our data that printers are commonly connected to the conventional Active Directory workstations with privileged user context. In other words, the average printer may be enabling vulnerable PCs to be used as access points to crown jewels in numerous indirect ways.

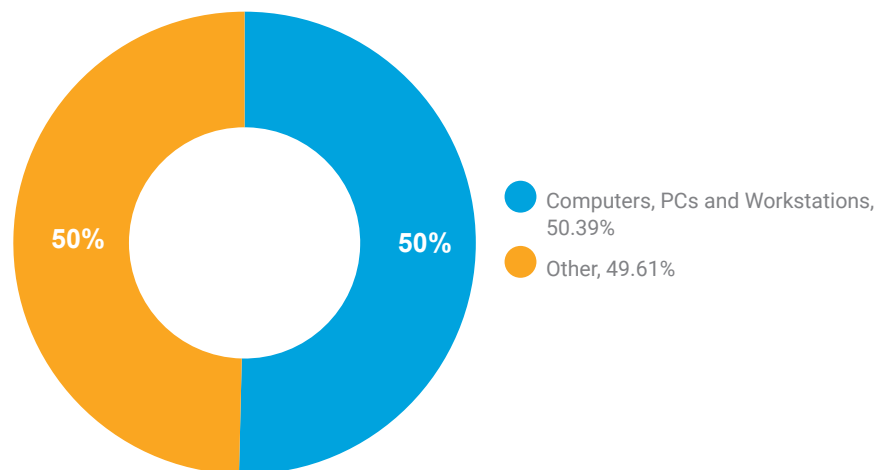
## PCs as Financial Devices

Within financial services, otherwise common PCs are sophisticated instruments that are used by privileged financial employees to access critical business applications. Unfortunately, the users of these fleets of AD-joined PCs also have AD-defined email addresses with corporate naming conventions. These persistently phished employees also have often-vulnerable email clients, browsers and office suites, and their PCs should be considered unsafe simply because they're surrounded by IoT and BYOD ecosystems.

As the FFIEC IT Information Security Booklet elaborates: "Authorized users with elevated or administrator privileges can pose a potential threat to systems and data" while "Unauthorized access to the operating system and system utilities could result in significant financial and operational losses."<sup>[2]</sup>

**More than half of all IT devices within the global financial services campus ecosystem are PCs.**

**Figure 4:** Computers, PCs and Workstations as a Percentage of Devices



Forescout Device Cloud Research 2020

## Other Devices Within the Network

In financial services, there's almost as much electronic "stuff" as computers. For every 100 classified computers, PCs and workstations, there are 99 other devices on financial services networks. In other words, there are a lot of other potential AD-joined devices to account for as a cybersecurity leader. AD-joined devices expose banks to risk because improperly secured financial devices allow state-sponsored criminals and other malicious actors to gain access to critical bank information using adjacent networked devices, such as printers, to mimic permitted bank transfers. This is a real risk today.

Infamous cybercrime syndicates and nation states have orchestrated numerous advanced persistent threats (APT) aimed at financial services with success.<sup>[4]</sup> For example, various reports have estimated that hackers based in North Korea have stolen over \$2 billion from the greater financial services industry by launching cyberattacks on banks and cryptocurrency exchanges. In a specific example from 2016, North Korean cyber actors influenced the Federal Reserve Bank of New York to move over \$81 million

dollars from the Central Bank of Bangladesh to accounts in the Philippines.<sup>[5]</sup> Following this notable cyber heist, it was discovered that cyberthieves had also attacked banks in Vietnam and Ecuador.

To protect against such threats, it is critical to maintain device segmentation controls to prevent lateral movement between financial devices and other AD-joined devices. Of course, this is dependent on cybersecurity stakeholders having the tools to maintain detailed asset inventories of all devices that traverse the IT, OT and IoT realm.

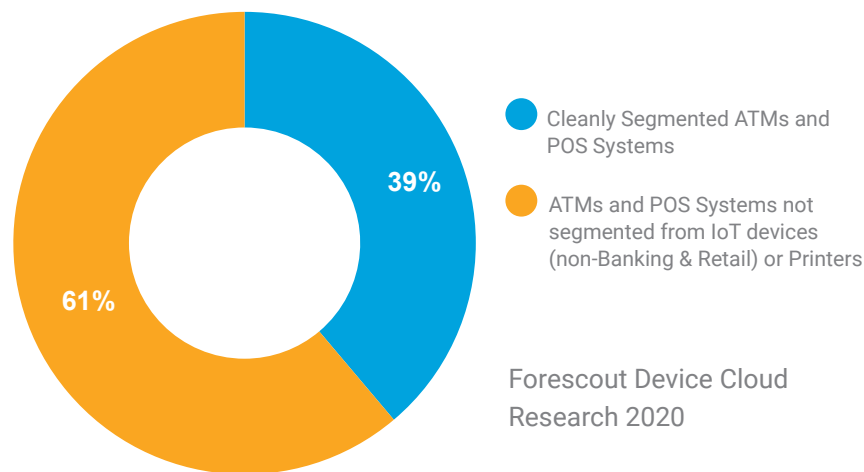


## ATM and POS Devices

The risk posed by unsecured AD-joined devices underscores the growing importance of PCI standards. Specifically, since the creation of the PCI Data Security Standard (DSS) in 2004, the handling and processing of consumer cardholder data has come into greater focus for many reasons, including the growing number of ATMs and other critical endpoints being added to the network.

First, it must be stated that many ATMs are located in ATM-only VLANs or are otherwise micro-segmented from other devices. Beyond that, many ATMs are relatively well-segmented on networks that have significant portions of other ATMs. Our Device Cloud data validates this. However, our data indicates that many ATMs are adjacent to other IoT devices such as security cameras and physical security systems that may not be as rigorously controlled.

**Figure 5:** Segmentation of ATMs and POS Systems



More than half (54%) of ATMs and POS systems are exposed to non-financial IoT devices on their respective network segments. When printers are included, the percentage of ATMs and POS systems exposed to non-financial IoT devices rises to 61%.

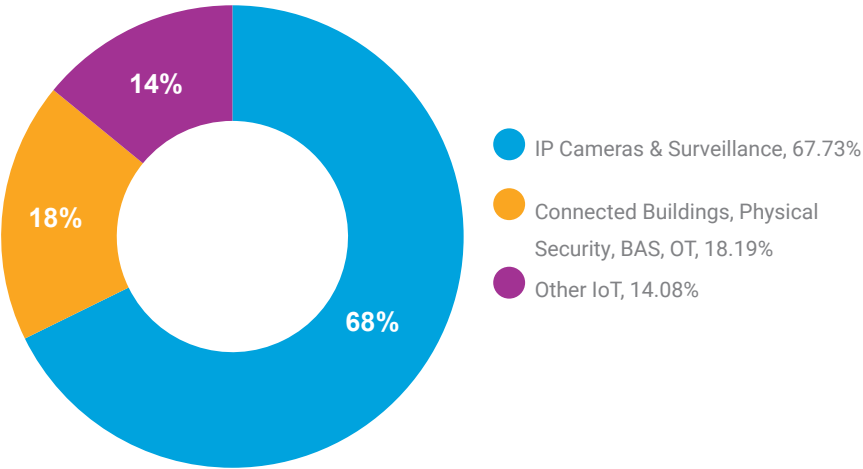
## IP Cameras & Surveillance Systems

PCI ATM security guidelines clearly state that, “where possible and allowed by law, the ATM should be equipped with a security camera.”<sup>[6]</sup> This has made IP cameras the most common neighbor to ATMs.

Unfortunately, that guidance didn’t go so far as to state that security cameras should be segmented from financial devices on the network. One might assume that IP cameras are segmented from central network functions within the financial services industry, but that’s not always the case.

It’s noteworthy that it’s often difficult to provide security updates for surveillance equipment in general, as well as for physical security and access control equipment, and that all of these systems are prone to man-in-the-middle (MitM) attacks.<sup>[7]</sup> Extra precautions should be taken, and additional security controls put in place, to help prevent these devices from becoming compromised.

Figure 6: ATM IoT Device Neighbors on Financial Networks



Forescout Device Cloud Research 2020

In summary, cybersecurity stakeholders within financial services interested in mitigating lateral movement of cyberthreats throughout their greater network infrastructure should be mindful of adjacent and peripheral IoT, OT and mobile devices. The interconnectivity of these devices provides a potential entry point for an attacker to compromise key business functions. While these threats are addressable by investing in technology and adhering to PCI best practices, unsecured AD-joined devices still pose additional risks because they allow threats to traverse physical domains.

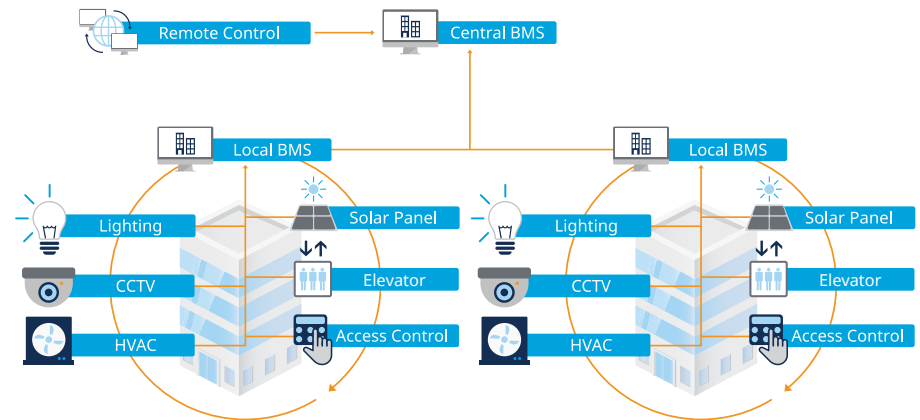




## Connected Buildings

A huge concern for financial services is a breach that affects the data center. As in all industries dependent on the data center, financial services is invariably reliant on energy and power infrastructure, including systems associated with connected buildings and BAS. Therefore, many banks have implemented redundant power supplies in an effort to mitigate risk to their data centers—which is a great first step. However, security stakeholders should consider additional precautions to manage and contain energy and power infrastructure-related vulnerabilities. Our data suggests that there should be greater focus on segmentation strategies when it comes to connected building infrastructures and the OT devices that define them.

**75% of connected building IoT devices in financial services are comprised of physical security systems and BAS technologies such as HVAC, Thermostats and Smart Lighting.**





Devices on the network that are a part of connected buildings and BAS are obviously relevant for financial services because these institutions have many buildings and invest heavily in devices for physical security and surveillance.

**Figure 7:** Financial Services Connected Buildings Device Breakdown

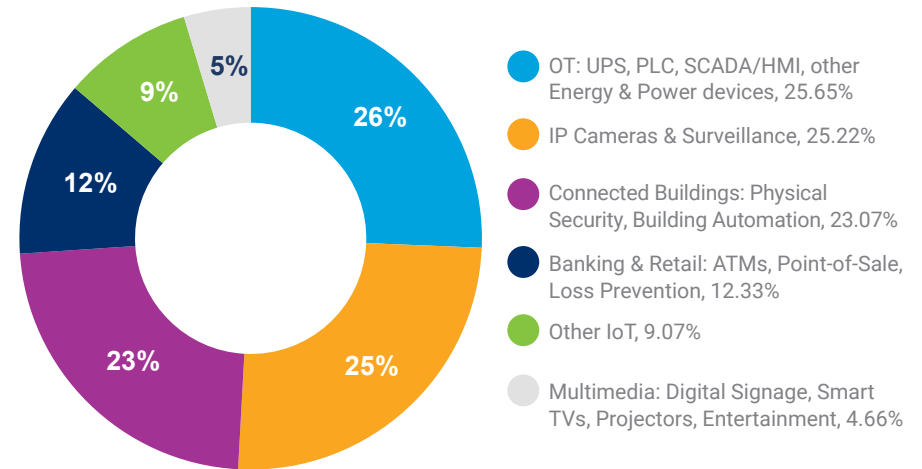
Device Groups	Percentage
Physical Security: Building Security	43%
Building Automation Systems (BAS): HVAC Management, Thermostats, Environment Sensors, Smart Lighting	32%
Physical Security: Building Access Control	19%
Physical Security: Building Safety, Alarms, Emergency Systems	6%

Forescout Device Cloud Research 2020

### BAS and OT

OT devices involved in supporting energy and power infrastructure like UPS, SCADA/HMIs, PLCs and other industrial devices comprise 14.19% of the IoT infrastructure within financial services. These UPS devices are present in both the campus and data center, and have common computer, server, and IoT neighbors. In short, UPS devices are neighbors to many devices within the general IT infrastructure.

**Figure 8:** Financial Services IoT Device Breakdown (Excludes Printers)



Forescout Device Cloud Research 2020

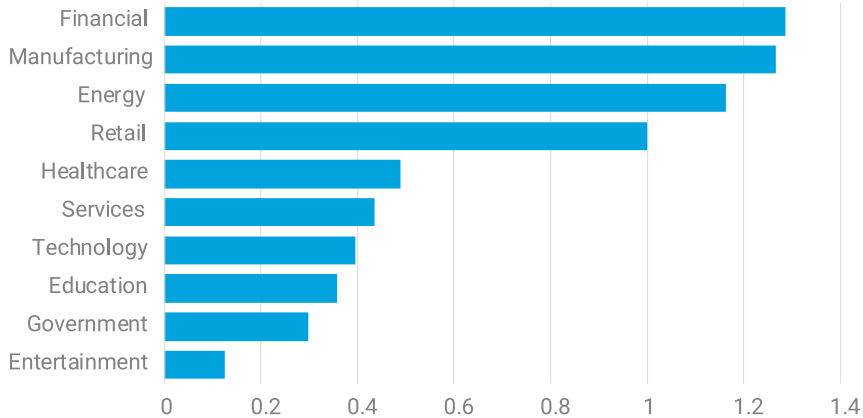
**OT and BAS devices cannot be ignored. UPS, PLCs, SCADA/HMI and IP Cameras account for over 50% of all IoT devices in financial services (excluding printers).**

[Forescout research](#) recently delved into the use of malware to target BAS. In particular, it focused on attackers targeting common surveillance equipment using building-specific malware called siegeware, which can be used to hold entire buildings for ransom.<sup>[7]</sup> While this is just one threat that capitalizes on vulnerabilities only found in IP cameras and surveillance systems, it is representative of the cybercriminal innovations that are targeting industrial infrastructure via BAS and OT devices, with great potential impact on core business functions.

## Energy and Power

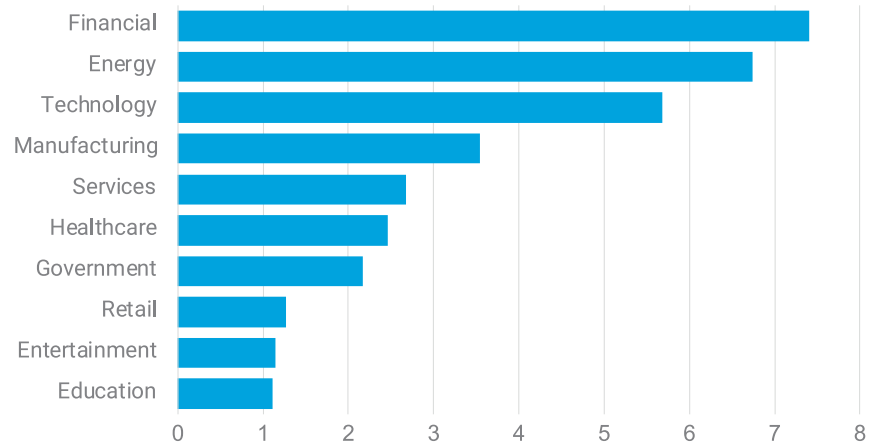
Nothing says on-premises data center like a slew of OT devices supporting energy and power applications. This of course includes UPS systems, PLCs and HMIs used to interact with and control all aspects of building and data center power, server backup and electricity distribution. The prevalence of the on-premises data center is why financial services has the leading rates of UPS and OT energy device distribution compared to other verticals.

**Figure 9:** Percentage of Total Observed OT (UPS, PLC, HMI and other Energy devices) Devices Observed in Forescout Device Cloud



Forescout Device Cloud Research 2020

**Figure 10:** Percentage of UPS Devices of Deployed IoT Across Industries



Forescout Device Cloud Research 2020

The financial services requirements for energy, power and high availability go even beyond that of the energy-dependent manufacturing industry.

Although the UPS system is most frequently sold into and found in the financial data center, it's also embedded in the buildings across the financial campus and the high-availability IT environments inside. That's where UPS systems are deployed alongside the high-availability workstations used to access business-critical applications within the highest zones of trust.

The risk that UPS devices pose to both the data center and campus are real. UPS devices from major vendors like APC by Schneider Electric, Vertiv/Emerson and Eaton are periodically reported as vulnerable, thanks to embedded web servers with open source components, exposed services and varying default configuration settings. As recently as 2018, UPS systems have been found critically vulnerable with a 10/10 CVSS score.<sup>[8]</sup>

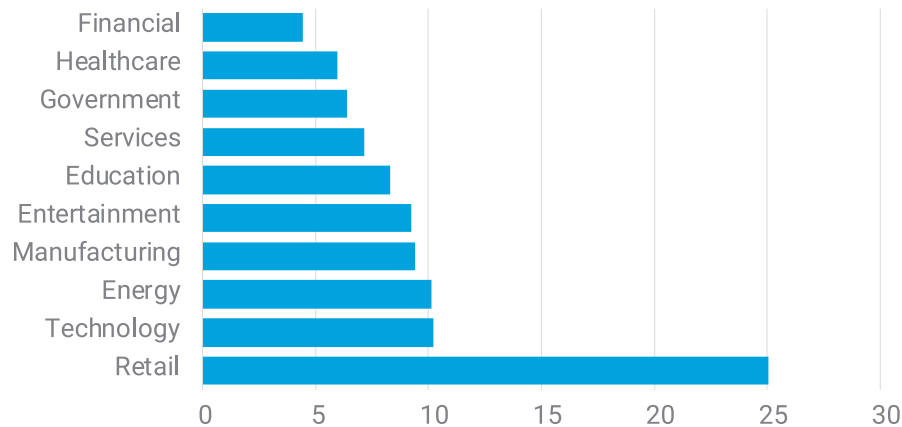
# The Benefits of a Compliance-Driven Environment

## How Virtualization Has Helped Cybersecurity

In financial services, virtualization brings countless security, patching and maintenance benefits, and at its core is all about enforcing control in a highly regulated, compliance-driven environment with a vast spread of devices.

Other industry benchmarks also indicate that the intensive regulation within financial services appears to be working well. When compared to other verticals, financial services maintains the lowest ratios of both unclassified and unmanaged devices. This can be used to loosely validate the claim that financial cybersecurity leaders have achieved the highest benchmark when it comes to device control capabilities.

**Figure 11:** Percentage of Unknown / Unclassified Devices Across Industries

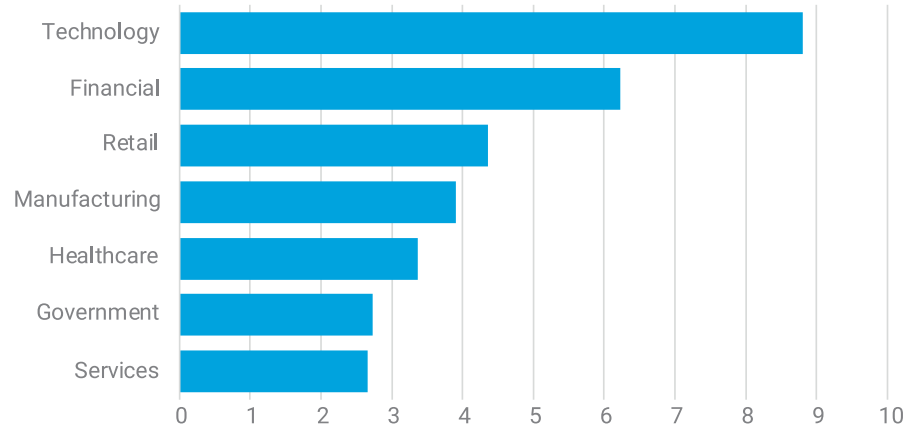


Forescout Device Cloud Research 2020

Financial services has proven to be a leader in virtualization, or Virtual Desktop Infrastructure (VDI). While virtualization and VDI alone are not antidotes for achieving cyber resilience and risk mitigation, they definitely represent huge steps in the right direction. With VDI, cybersecurity leaders are better equipped to implement comprehensive device procurement and ongoing compliance tasks.

**Financial Services is second only to the Technology industry in the use of VDI.**

**Figure 12:** Percentage of Virtual Desktop Infrastructure (VDI) Devices Across Industries



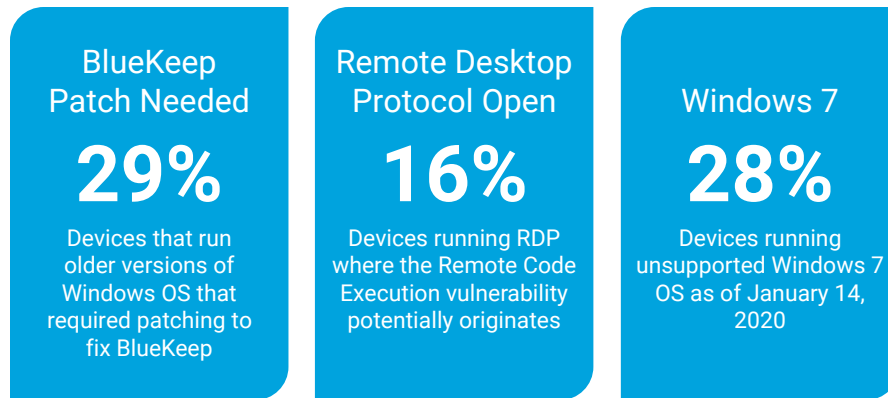
Forescout Device Cloud Research 2020

**Financial Services is a leader among industry peers when it comes to device classification.**

## BlueKeep Risk in Financial Services

However, while the financial services sector may be more secure than some other industries due to its wide adoption of VDI, many organizations are still exposed to vulnerabilities from BlueKeep. Our data suggests that 29% of Windows OS devices required patching to address BlueKeep, 16% of devices are running RDP services where the BlueKeep vulnerability may originate, and 27.55% of Windows devices run Windows 7, which is now unsupported by Microsoft. As noted in Figure 1, a looming procurement challenge remains on the horizon, with 28.62% of the financial services Windows device fleet losing support and requiring paid maintenance in Microsoft's ESU program.

**Figure 13:** Propensity for BlueKeep in Financial Services (managed Windows devices)



Forescout Device Cloud Research 2020

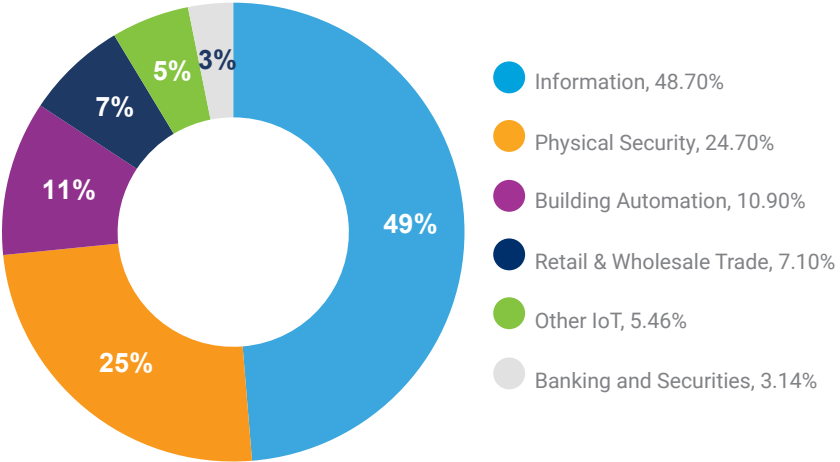
**Propensity for BlueKeep vulnerabilities and remotely accessible Windows devices in financial services still pose serious risks.**



# Conclusion

According to Gartner analysts, the Internet of Things is “the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.”<sup>[9]</sup> Given this perspective, cybersecurity in the context of the financial services industry is largely about risks posed by IoT devices. Financial services cybersecurity leaders must recognize that while they have achieved a higher degree of virtualization and device visibility than many other industries, they must still come to grips with the large numbers of hard-to-secure IoT and OT devices that widely exist to this day in the industry—devices that represent a high degree of unmitigated cyber risk.

**Figure 14:** Classified Devices on Financial Services Networks (Gartner IoT Definition)



Forescout Device Cloud Research 2020

With the age of IoT, the likelihood of lateral movement of malware has grown—and this is certainly the case for financial services. As earlier discussed, more than half of ATMs in named VLANs have other, non-financial IoT device neighbors. Some of these neighbors, particularly IP cameras, are dubious at best. Similar findings also apply to POS systems. Overall, 63% of POS systems are neighbored by seemingly innocuous devices, like printers, that provide a path for lateral movement of cyberthreats. Furthermore, devices far outside of the financial device realm, such as UPS systems, can provide additional paths of lateral movement for attackers.

Cybersecurity stakeholders within financial services must invest in comprehensive segmentation strategies built upon accurate and up-to-date asset inventories to support ongoing device fleet procurement at scale. Only from a vantage point of complete device visibility, from IT, OT and IoT, can financial services cybersecurity leaders orchestrate device-based controls such as network segmentation, micro-segmentation and advanced network access control. Every IP-enabled asset in the CMDB inventory is a device that should be governed by timely, well-orchestrated security policy.

**IoT encompasses a myriad of connected device types, all of which must be continuously monitored, classified, and secured in order to fully protect financial services networks.**

# Recommendations

- Based on Forescout's extensive work with financial services organizations, control should **start with passive device visibility** that delivers an accurate CMDB asset inventory for hardware, software, IT, OT and IoT—and all the specialty devices within those categories.
- Place a higher level of attention and **stricter segmentation policies on AD-joined devices subject to lateral movement risk from neighboring devices**, such as printers.
- **Extend device visibility from the data center, to the cloud, and across the campus.**
- Implement threat detection tools that **offer a broad array of classification fingerprints** to enhance device control with business context.
- Enable and test the ability to **continuously monitor device status** to help ensure situational awareness and asset status. Avoid tools that only provide snapshots in time and expect real-time assessments of device posture and security status.
- Bring **data center and cloud devices into a unified control plane** so that devices are managed similarly, to make the data center migration easier and contextual analysis fluid for key cybersecurity stakeholders.
- Perform and scale network segmentation actions across campus, data center and cloud. Forescout Device Cloud data shows that classical segmentation is widely deployed in the financial services industry, but cybersecurity leaders need to consider **implementing more segmentation to better protect critical devices** such as ATMs and IoT/OT devices.
- **Automate and enforce policy-based controls where possible** to minimize the time to respond to infractions or threats. Start by automating highly repetitive controls that don't require security personnel expertise or insight to let staff focus more on value-added tasks.
- Finally, **orchestrate interaction between existing security tools** using dedicated modules that can share updates across the entire cybersecurity solutions portfolio based on strengths in the inventory and classification of assets, privileged access control and network segmentation.

Ready to Make Your Network  
Cyber Resilient?

LEARN HOW

## 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](https://forescout.com) to learn how Forescout provides active defense for the Enterprise of Things.

For the purposes of this document, Forescout researchers limited the scope and data sample for consistency and the convenience of issuing a one-time brief. Researchers noted limitations due to study type and time, scope, data de-identification, passive data capture methods and errors in AI-based classification of device functions, operating systems and vendors. The reality of using live, production-environment cloud data means sometimes having imperfections in the data supply.

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

- [1] <https://attack.mitre.org/techniques/T1210/>
- [2] <https://ithandbook.ffiec.gov/it-booklets/information-security.aspx>
- [3] <https://www.pcisecuritystandards.org/merchants/>
- [4] <https://www.forbes.com/sites/kateoflahertyuk/2019/08/07/north-korean-hackers-2-billion-heist-is-funding-wmd-programs/>
- [5] <https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html>
- [6] [https://www.pcisecuritystandards.org/pdfs/PCI\\_ATM\\_Security\\_Guidelines\\_Info\\_Supplement.pdf](https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf)
- [7] <https://www.forescout.com/securing-building-automation-systems-bas/>
- [8] <https://www.schneider-electric.com/en/download/document/SEVD-2018-074-01/>
- [9] <https://www.gartner.com/en/information-technology/glossary/internet-of-things>




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](https://forescout.com)

© 2021 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents are available at [www.forescout.com/company/legal/intellectual-property-patents-trademarks](https://www.forescout.com/company/legal/intellectual-property-patents-trademarks). Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 01\_21**

## Case Studies

A banner for the Rabobank case study. It features a dark blue background with a white line graph showing an upward trend. A white silhouette of a person is positioned above the graph. The text "Rabobank" is in a large, white, sans-serif font, and "Learn more" is in a smaller, white, sans-serif font with a white right-pointing triangle arrow.

Rabobank  
Learn more ▶

A banner for the Meritrust case study. It features a dark blue background with a white line graph showing an upward trend. A white silhouette of a person is positioned above the graph. The text "Meritrust" is in a large, white, sans-serif font, and "Learn more" is in a smaller, white, sans-serif font with a white right-pointing triangle arrow.

Meritrust  
Learn more ▶

A banner for the Credit Human case study. It features a dark blue background with a white line graph showing an upward trend. A white silhouette of a person is positioned above the graph. The text "Credit Human" is in a large, white, sans-serif font, and "Learn more" is in a smaller, white, sans-serif font with a white right-pointing triangle arrow.

Credit Human  
Learn more ▶