FORESCOUT
Active Defense for the Enterprise of Things™

The Underlying Risks Found in Healthcare Devices

TCP/IP Vulnerabilities Every Healthcare Organization Should Know About

by Forescout Research Labs

Contents

Executive summary

- In this report, Forescout Research Labs shows how TCP/IP stack vulnerabilities affect healthcare organizations analyzing data from the Forescout Device Cloud.
- Sixty-seven percent of organizations across all verticals are affected by these vulnerabilities. That number jumps to 75% for healthcare organizations, which have, on average per organization, the highest number of vulnerable devices (almost 500), the highest diversity of vulnerable devices (8 device types) and the highest diversity of vulnerable vendors (12) on their networks.
- Healthcare organizations are roughly five times more affected by TCP/IP vulnerabilities than any other vertical. There are in total 79 vulnerable types of devices and 259 vulnerable vendors on all healthcare organizations analyzed.
- The most common vulnerable device types in healthcare organizations are printers, VoIP, infusion pumps, networking equipment and building automation devices. The most common vulnerable medical device types are infusion pumps, patient monitors and point-of-care diagnostic systems.
- These and other vulnerable devices often share the same segments of an organization's network, which increases the potential likelihood and impact of cyberattacks.
- The combination of new vulnerable devices, difficult-to-patch vulnerabilities and lack of segmentation exposes healthcare networks to new threat scenarios that can have a big business impact.

Recent TCP/IP stack vulnerabilities. Recently, Forescout Research Labs found and disclosed several critical vulnerabilities on TCP/IP stacks that affect millions of IT, OT, IoT and IoMT devices: AMNESIA:33, NUMBER:JACK and NAME:WRECK. This research – collectively called Project Memoria – has the mission to uncover threats arising from this new class of vulnerabilities and to support the community in addressing them. Table 1 lists the TCP/IP stacks that have been analyzed under different studies and the number of vulnerabilities the researchers found. **A total of 81 vulnerabilities have been found in these studies.**

Table 1 – The vulnerable TCP/IP stacks

Stack	URGENT/11 (2019)	Ripple20 (2020)	AMNESIA:33 (2020)	NUMBER:JACK (2021)	NAME:WRECK (2021)
IPnet	11				1
Treck		19			
uIP			13	1	
PicoTCP			10	1	
FNET			5	1	
Nut/Net			5	1	

Table 1 – The vulnerable TCP/IP stacks - Cont.

Stack	URGENT/11 (2019)	Ripple20 (2020)	AMNESIA:33 (2020)	NUMBER:JACK (2021)	NAME:WRECK (2021)
uC/TCP-IP				1	
cycloneTCP				1	
NDKTCPIP				1	
MPLAB Net				1	
Nucleus NET				1	6
NetX					1
FreeBSD					1

Why these vulnerabilities matter. Vulnerabilities in TCP/IP stacks represent an emerging threat, which may allow attackers to crash or take control of devices with a single network packet. They are also known to spread across many device types and vendors, which makes them difficult to patch. This understanding has certainly shifted the threat and risk landscape for the different industry verticals that Forescout Research Labs monitors.

This report. In this report, we show the penetration of these vulnerabilities specifically within healthcare organizations. We analyzed data from the Forescout Device Cloud, which contains anonymized information from approximately 13 million devices from more than 1,800 global customers to identify devices running vulnerable TCP/IP stacks via application-layer banners (such as HTTP, FTP, Telnet and SSH). We eliminated the following stacks from the analysis because we could not obtain reliable numbers about them: PicoTCP, FNET, NDKTCPIP and MPLAB Net. We considered vulnerable any device running one of the stacks mentioned in Table 1, regardless of version, since the device would have been vulnerable at the time of disclosure.

The facts

Fact 1 – TCP/IP Stack Vulnerabilities Are Widespread.

Forescout Research Labs identified **a quarter of a million devices** affected by TCP/IP stack vulnerabilities. Figure 1 shows a breakdown of the number of vulnerable devices in a subset of selected verticals (government, healthcare, manufacturing, retail and financial) that we used for our study. Government and healthcare have the highest number of vulnerable devices, followed by manufacturing and retail. Our data also shows that **67% of organizations are affected by these vulnerabilities,** which gives a sense of the proliferation of these vulnerabilities and the effort organizations require to secure their networks.

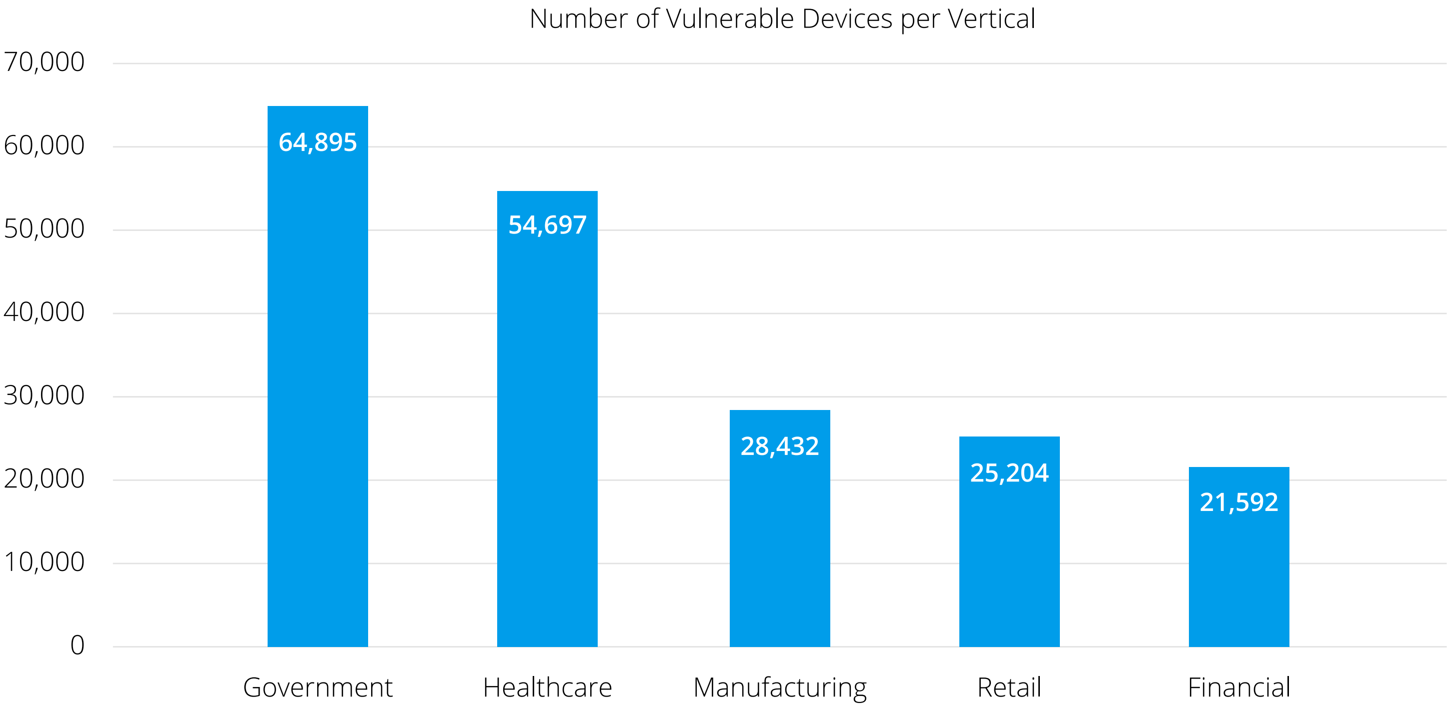

Figure 1 – Number of vulnerable devices per vertical. Government and healthcare have more than double the number of vulnerable devices as compared to the manufacturing, retail and financial sectors.

Fact 2 – Healthcare has the highest average numberof vulnerable devices per organization.

On average, **every organization has 200 vulnerable devices.** Figure 2 shows that **healthcare has by far the largest average of vulnerable devices – almost 500 – per organization. On average, healthcare organizations are roughly five times more affected by vulnerabilities in TCP/IP stacks than financial organizations.**

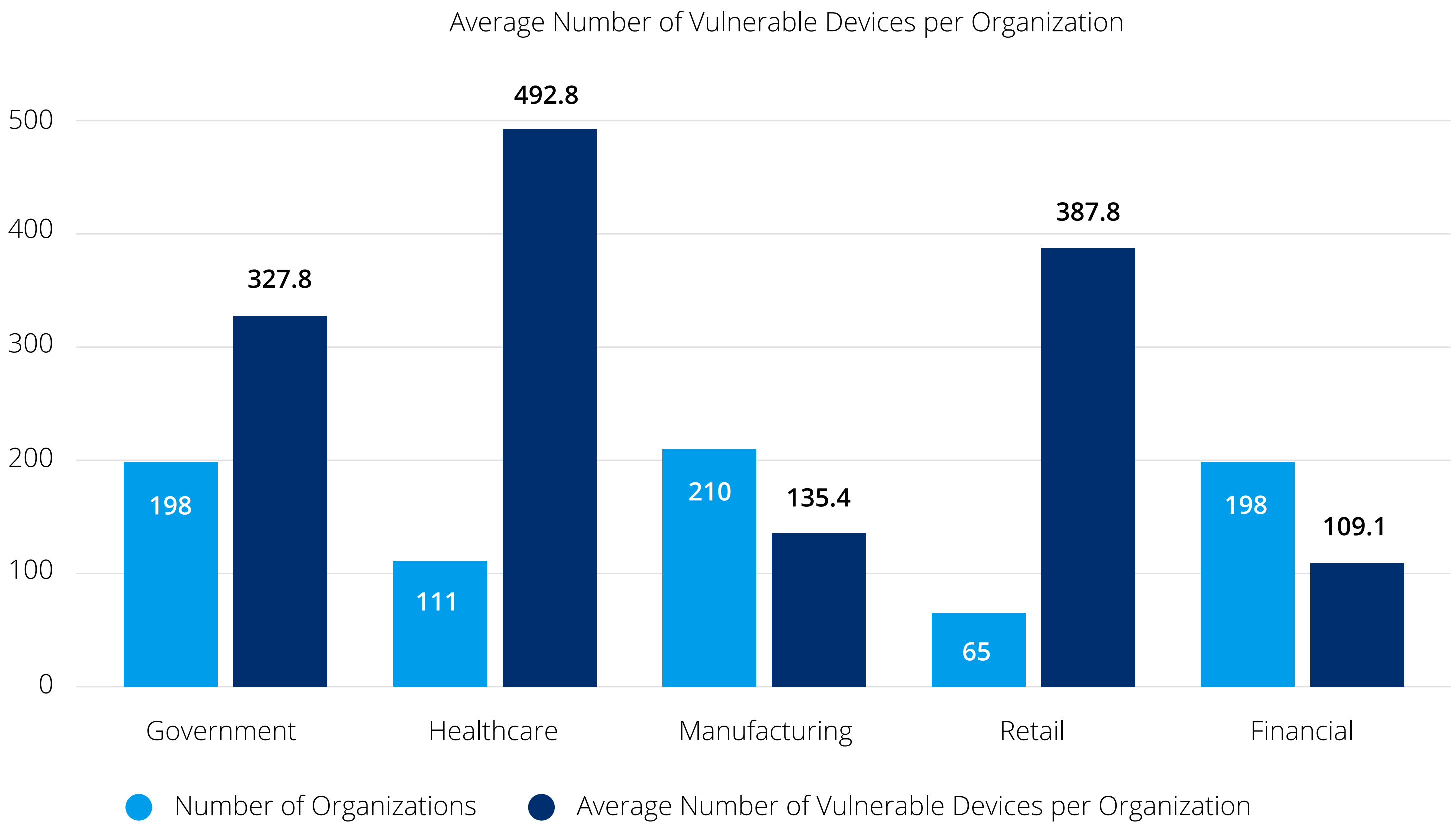

Figure 2 – Average number of vulnerable devices per organization. The healthcare sector has by far the highest number, followed by retail, government, manufacturing and financial.

Fact 3 – Healthcare organizations have the highest vulnerable device diversity.

Figure 3 shows a breakdown of distinct vulnerable device types per vertical, something that we call device diversity. The implication of high device diversity within an organization is that patching vulnerabilities will be more time consuming. In our analysis, **healthcare has the highest number of distinct vulnerable device types (79) and the highest average per organization (about 8).** In networks with high device diversity, security operators must spend a considerable amount of time to identify and patch vulnerable devices. This is because (1) the tools able to identify IT devices might differ from those able to identify medical or IoT devices, and (2) because with different device types come different vendors and, hence, patches available with different timelines and applicable with different procedures, as highlighted in the following section.

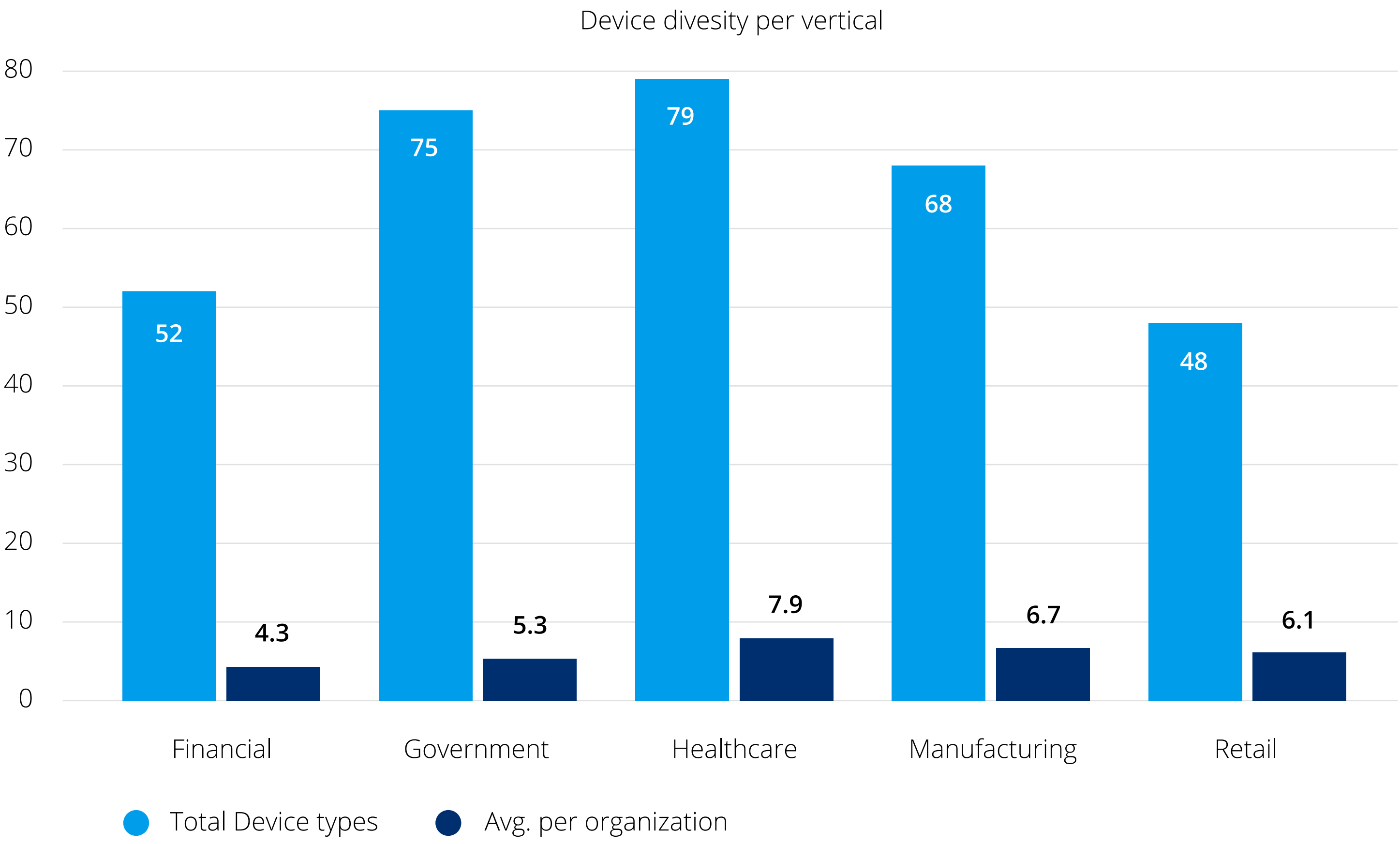

Figure 3 – Device diversity per vertical

Fact 4 – Healthcare organizations have to wait on average for 12 vendors to issue patches.

Figure 4 shows the average number of distinct vendors affected by TCP/IP vulnerabilities, something we call **vendor diversity.** As for device diversity, a high vendor diversity is directly connected to more time needed to apply patches. According to the data in Figure 4 (dark blue bars), **healthcare has the highest average diversity per organization (12), followed by manufacturing and retail (about 10).** By looking at each vertical as a whole (light blue bars), **manufacturing has the absolute highest number of vendor diversity** (293 vulnerable vendors over 210 organizations), **followed by healthcare** (259 vulnerable vendors over 111 organizations). Since patches for TCP/IP stack vulnerabilities must trickle down the supply chain, several of those vendors either do not issue patches or take months to do so, which means the affected devices remain vulnerable for a long period of time.

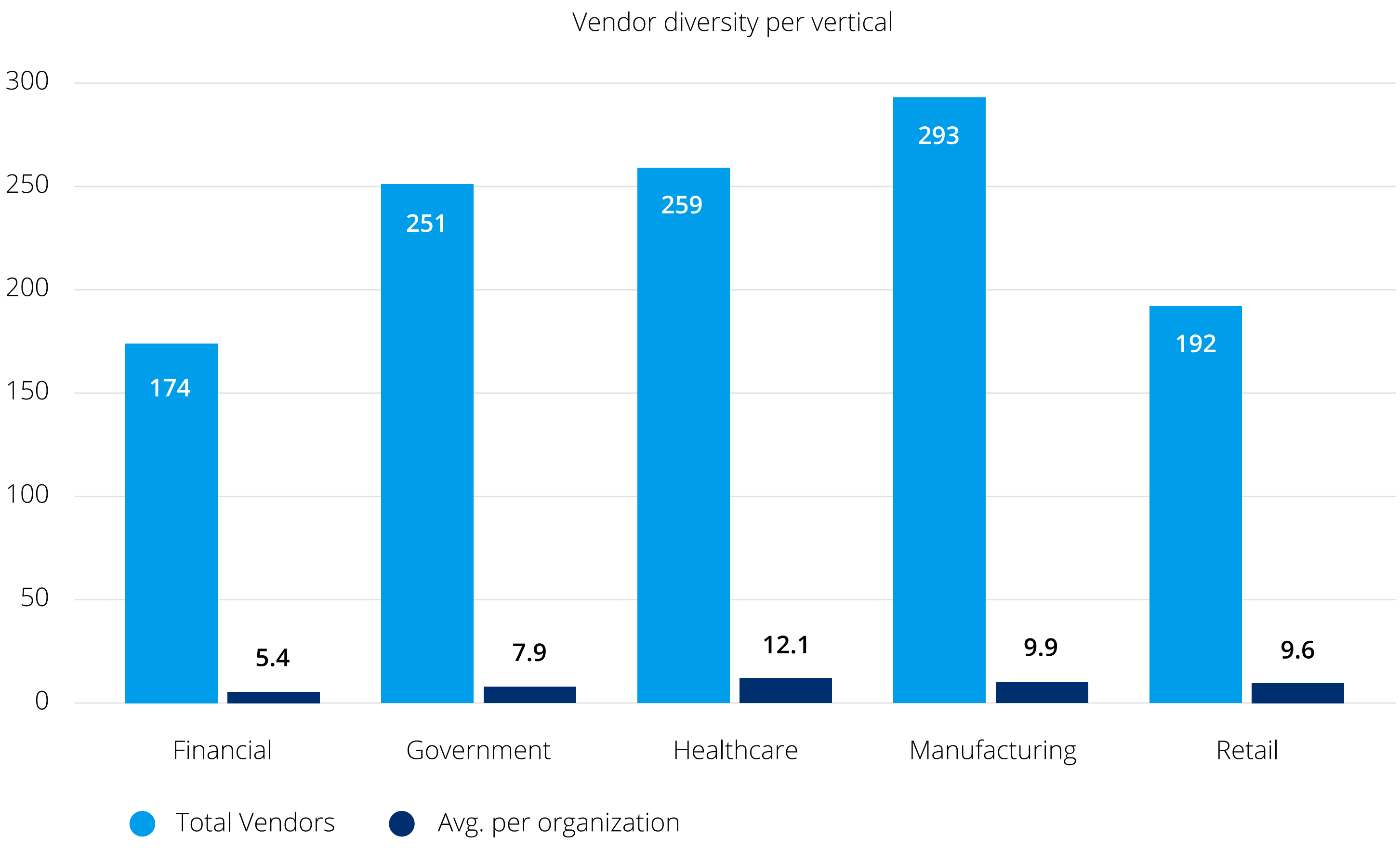

Figure 4 – Vendor diversity per vertical

Fact 5 – Printers, IP phones, networking devices, building automation and infusion pumps are the most vulnerable device types.

Figure 5 shows that printers (34%), IP phones (20%), networking devices (8%), building automation (8%) and infusion pumps (4%) are the most common device types vulnerable to TCP/IP stack vulnerabilities. Table 2 shows the top 5 most common vulnerable device types in each vertical. This confirms some of our earlier findings discussed in the 2020 Enterprise of Things Security Report, namely that the **previously known riskiest devices are even riskier when we consider the presence of new critical vulnerabilities.**

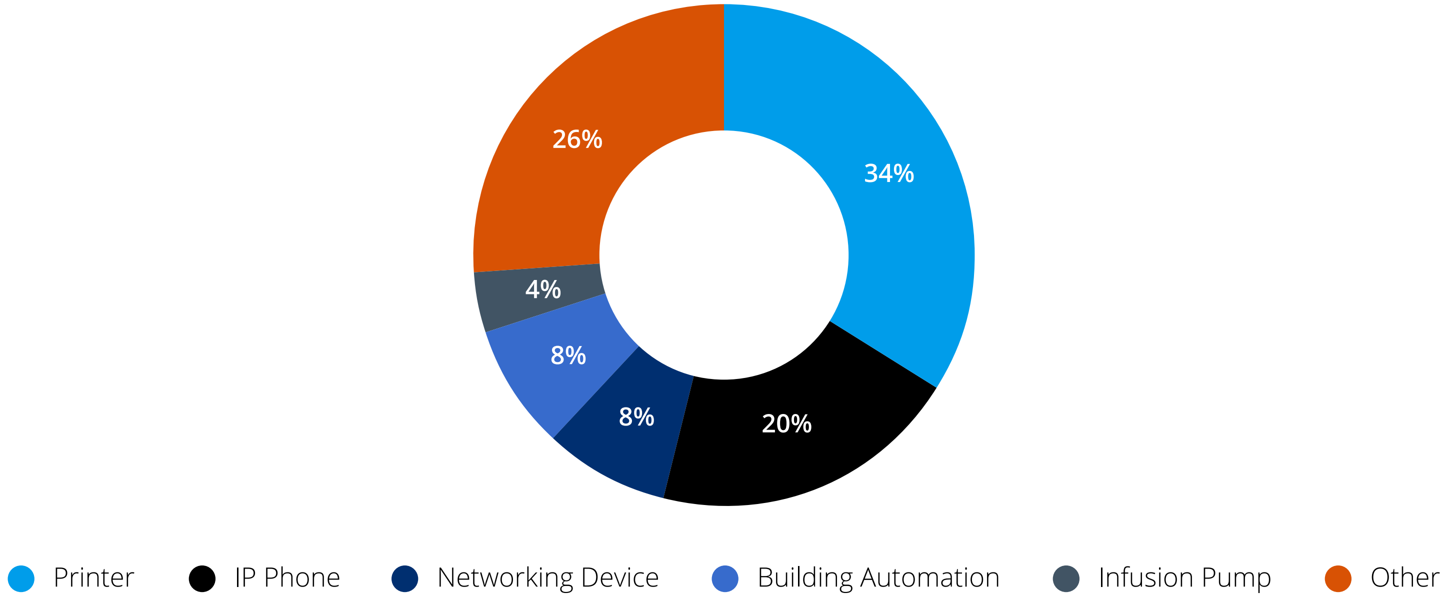

Figure 5 – Top 5 vulnerable device types across all verticals

Table 2 – Top 5 vulnerable device types in each vertical

	Financial Services	Government	Healthcare	Manufacturing	Retail
1	Printer	VoIP	Printer	Printer	Printer
2	VoIP	Printer	VoIP	Networking	Networking
3	UPS	Networking	Infusion pump	PLC	Clock
4	Networking	Storage	Networking	VoIP	PLC
5	Out-of-band controller	Thin client	Building automation	Storage	VoIP

The next facts provide a more detailed analysis into healthcare, which has shown to have the highest average number of vulnerable devices, device type diversity and vendor diversity. In the following, we look more closely at the **almost 55,000 vulnerable devices in 111 healthcare organizations** from the initial dataset.

Fact 6 – 75% of healthcare organizations are affected by TCP/IP vulnerabilities.

In Forescout Device Cloud, we collect data from 149 healthcare organizations. The data shows that 111 of those (almost 75%) are affected by these vulnerabilities.

Fact 7 – 35% of healthcare organizations have hundreds of vulnerable devices.

Figure 6 shows the number of vulnerable devices per healthcare organization divided into buckets. **Thirty-five percent of the monitored healthcare organizations have at least 100 vulnerable devices – and up to 1000!**

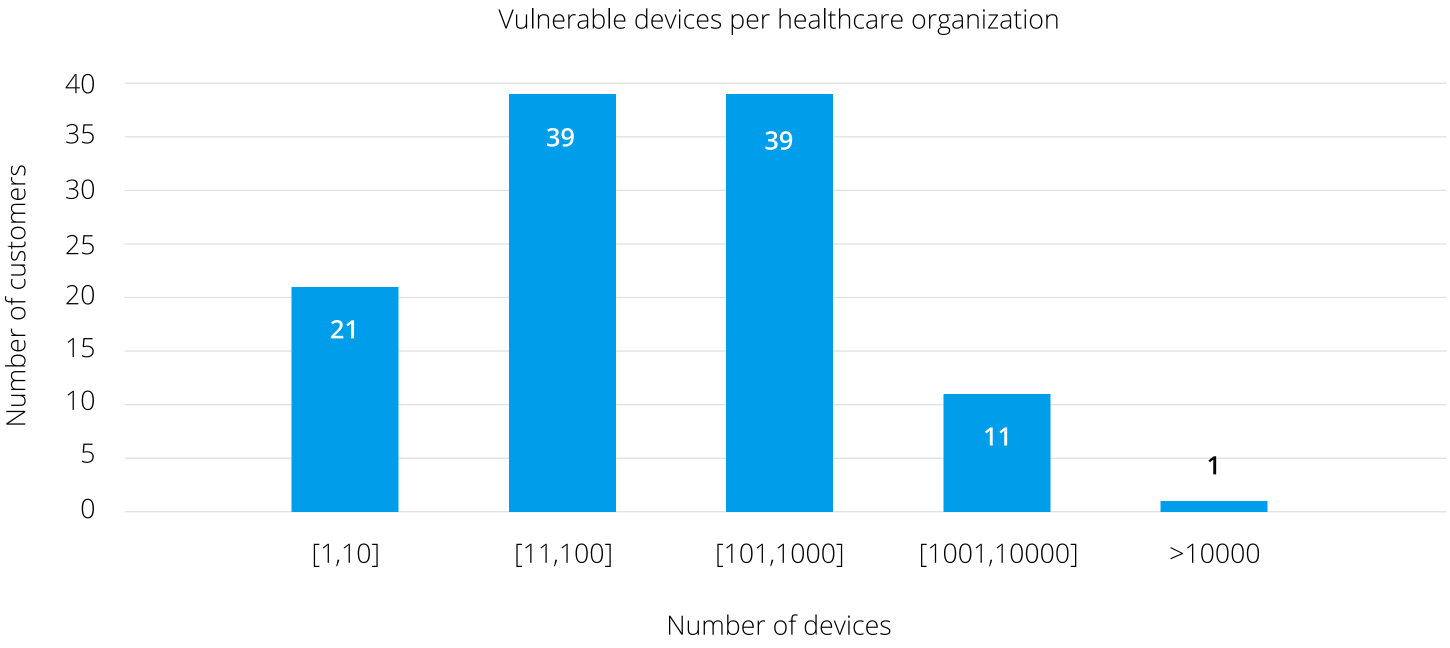

Figure 6 – Vulnerable devices per healthcare organization

Fact 8 – About 25% of healthcare organizations have a vulnerable device diversity higher than 10.

Figure 7 shows the distribution of affected device types per healthcare organization. **Most organizations (65 or 58%) have between 1 and 6 device types (13 organizations have only 1 type), but 26 organizations (23%) have more than 10 of those.**

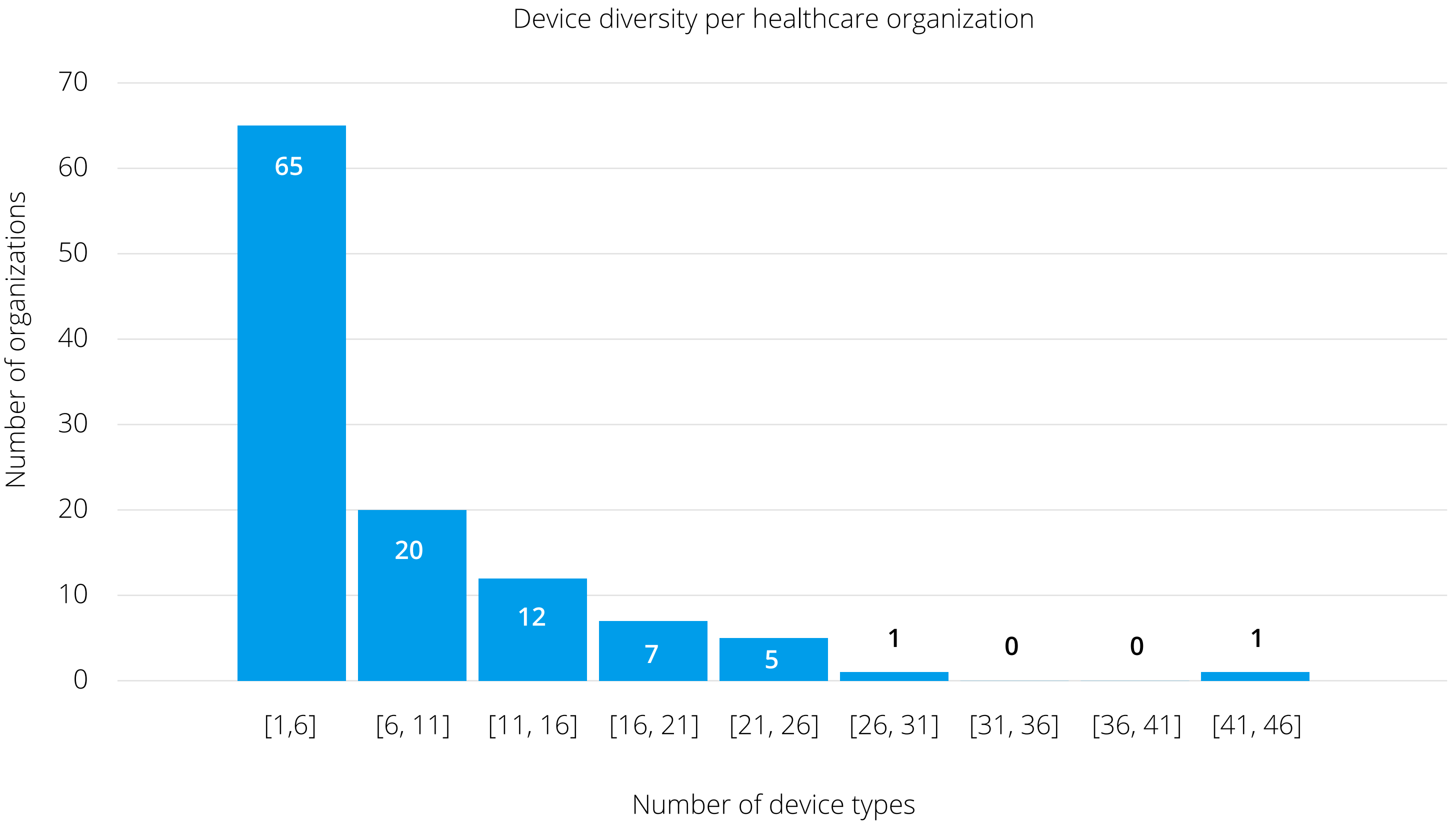

Figure 7 – Device diversity per healthcare organization

Fact 9 – 36% of healthcare organizations have a vulnerable vendor diversity higher than 10.

Figure 8 shows the vendor diversity per healthcare organization. **Few organizations (10%) have a single vulnerable vendor on their network** ("easier" to patch), **most organizations (46%) have between 3 and 10 vulnerable vendors, while the remaining organizations (36%) have more than 10 vulnerable vendors in their network (which is more time consuming to patch). That shows it is not just a single bad vendor selection that makes an organization vulnerable, since vulnerabilities are widespread among vendors.**

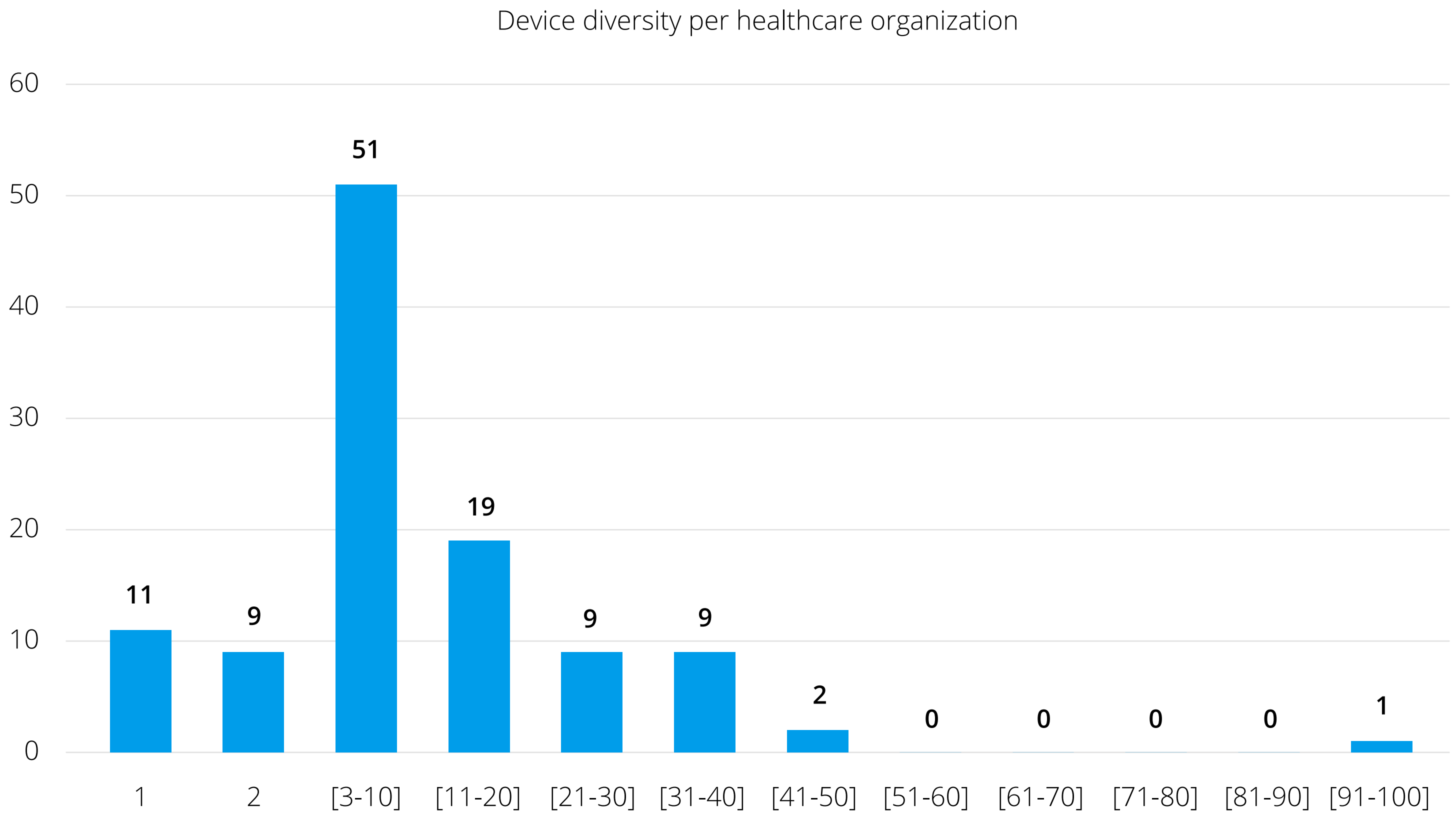

Figure 8 – Vendor diversity per healthcare organization

Fact 10 – There are more than 60 vulnerable medical device models.

The most common vulnerable connected medical device types we saw on Device Cloud are infusion pumps, patient monitors and point-of-care diagnostic systems. To discuss real examples of those (and other devices), Table 3 shows a list of connected medical devices known to have been affected by TCP/IP stack vulnerabilities, including 12 major vendors and more than 60 device models. (The information is taken directly from the latest versions of the advisories released by each vendor.)

Table 3 – Connected medical devices affected by TCP/IP stack vulnerabilities

Vendor	Device Models
Abbott	ACCELERATOR APS, ACCELERATOR a3600, ACCELERATOR p540, Alinity h, Alinity ci-series, Alinity s, Alinity m, ARCHITECT, CELL-DYN Ruby, CELL-DYN Sapphire, m2000, i-STAT Alinity, CELL-DYN Emerald 22 AL
Accuray	Radixact® System Software version 1.x, TomoTherapy® with iDMS® System Software version 1.x, TomoTherapy® HTM Series System Software version 2.x, TomoHDTM System Software version 2.x, TomoTherapy Hi-Art® System Software version 5.x
Baxter	Spectrum Infusion System Wireless Battery Modules
B. Braun	Outlook 400ES infusion pump
BD (URGENT/11 and Ripple20)	Alaris™ PC Unit, BD Kiestra™ Total Lab Automation (TLA) with a System Control Unit (SCU), BD Kiestra™ Work Cell Automation (WCA) with a System Control Unit (SCU), BD Kiestra™ ReadA standalone with a System Control Unit (SCU), BD Rowa™ conveyor technology, BD Rowa™ Label Printer
Boston Scientific / Guidant Medical	Transvenous implantable cardiac devices, as well as the associated device programmers located in physician offices and the LATITUDE™ Remote Patient Management Systems

Table 3 – Connected medical devices affected by TCP/IP stack vulnerabilities - Cont.

Vendor	Device Models
Canon	Infinix systems V6.9 and higher, Aquilion LB TSX-021A/3, Alexion TSX-032A, Alexion TSX-034A, Aquilion Lightning TSX-035A, Aquilion Start TSX-037A
Draeger	Evita V300, Infinity Acute Care System – Workstation Critical Care (Evita Infinity V500), Infinity Acute Care System –Workstation Neonatal Care (Babylog VN500), Babyleo TN500, Perseus A500, Connectivity Converter CC300
GE Healthcare	Affected but does not mention specific products publicly
Philips (URGENT/11 and Ripple20)	Achieva and Achieva 3.0T (R5.3, R5.4 and higher), BrightView SPECT(1.x), BrightView X(2.x), BrightView XCT(2.x), GEOPC (Component of Allura & Azurion), HDI 3500, HDI 3000, HeartStart Intrepid Monitor/ Defibrillator (867172), Ingenia (R4, R5.3, R5.4 and higher), IntelliSpace Breast (v2.1, 2.2, 3.1, 3.2), Multiva (R5.3, R5.4), Multiva/Prodiva (R5.4), Smart-hopping Access Point Controller (for MX40 and Telemetry products), Zenition
Smiths Medical	CADD-Solis Pump Wireless Communication Modules
SpaceLabs	Ultraview UVSL, Xprezzon, Qube, Qube Mini

Fact 11 – Whole classes of devices are vulnerable.

Table 3 shows that **these vulnerabilities are widespread within whole classes of devices and vendors.** There are at least four very popular infusion pump systems affected: Baxter, B. Braun, BD and Smiths Medical. The table also shows that some device manufacturers use more than one stack from different software vendors in their product lines. For instance, BD and Philips are vulnerable to both URGENT/11, which affects the IPnet stack from Wind River, and Ripple20, which affects the stack produced by Treck.

Fact 12 – The medical device supply chain can be long and complex.

These two points – widespread vulnerabilities and the use of software components from multiple vendors – point to the complexity of the supply chain uncovered by TCP/IP stack vulnerabilities. Connected medical devices are built up from several hardware and software components, including TCP/IP stacks, real-time operating systems and connectivity modules, that are produced and maintained by separate vendors. Figure 9 shows the Ripple20 vulnerabilities affecting two infusion pump models that share the same OS in different modules, but **this example involves *six* vendors.**

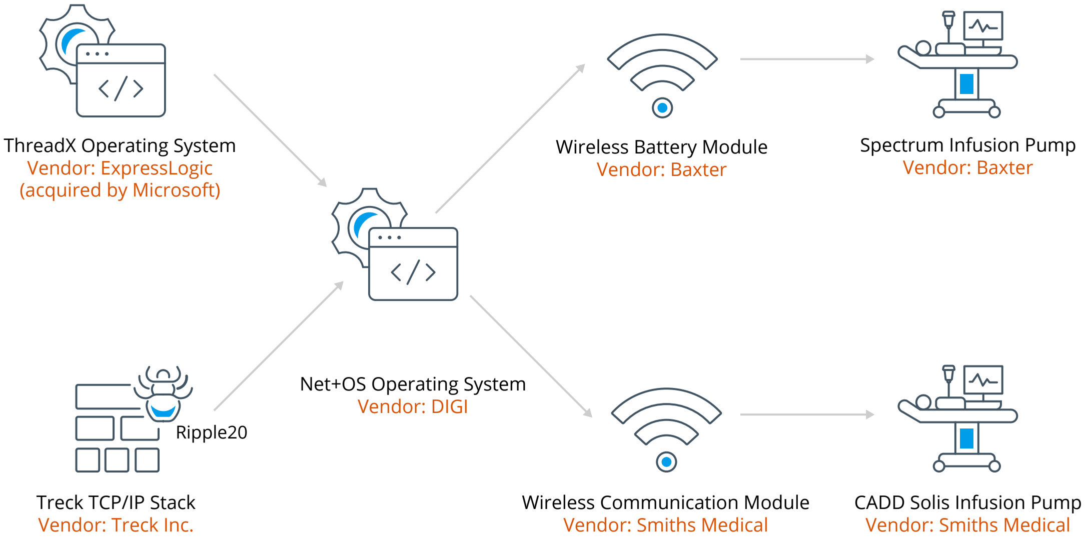

Figure 9 – An example of a long supply chain in a medical device

Fact 13 – Supply chain complexity makes patching difficult.

Both Baxter and Smiths Medical released security advisories detailing the impact of the vulnerabilities on their products (on June 16, 2020 and July 2, 2020, respectively), but this type of vulnerability often takes a long time to be recognized and patched by vendors because of long supply chains or the difficulty in identifying affected components. For instance, Dell released an URGENT/11 advisory for PowerConnect switches in May 2020 (more than six months after the original disclosure) and updates until February 2021. In some cases, vendors somewhere along the supply chain may be out of business, which means that patches will not make it to the end user (as in the UPS example we described in the AMNESIA:33 report).

Fact 14 – Not all vulnerable devices are medical devices.

Although connected medical devices are currently (and rightly so) the focus of much security discussion, Table 2 shows that other types of IoT figure prominently among the most affected by widespread TCP/IP stack vulnerabilities in healthcare organizations. This applies, for instance, to a variety of building automation devices and a multitude of specific printers, such as those for patient labels and PoS receipts.

Fact 15 – Segmentation is crucial to avoid spreading risk.

A security recommendation in many advisories from medical device manufacturers (as well as from the NIST) is to ensure that these devices operate in well-segmented networks such that they can only communicate with other devices they are supposed to. Network segmentation is fundamental to limit the attack surface in healthcare networks and is often achieved via VLANs. If a segment mixes sensitive and vulnerable devices, a vulnerable device may be used to reach a sensitive one. In a previous healthcare report, we have shown several examples of network segments mixing devices of different criticality in healthcare organizations. Below, we show that this also happens with IoT devices with vulnerable TCP/IP stacks.

Fact 16 – Security teams in HDOs should not lose their sleep over Medical Devices (only!).

Two interesting device examples that we picked from our dataset are label printers running Nut OS, thus vulnerable to AMNESIA:33, and building automation controllers running Nucleus NET, thus vulnerable to NUMBER:JACK and NAME:WRECK. In the case of the label printers, there are devices from three different vendors. In the case of the controllers, there are devices from five different vendors. Figure 10 shows a VLAN containing a mix of vulnerable IoT and medical devices of different criticalities seen on Device Cloud. The medication dispensing system indicates that this VLAN is for a hospital's pharmacy. Connected to the same VLAN, there are a building automation controller vulnerable to NAME:WRECK and NUMBER:JACK, and a printer vulnerable to AMNESIA:33. This means that each of those devices can represent an entry point to the medical network, and attackers have a wide selection of targets on the menu.

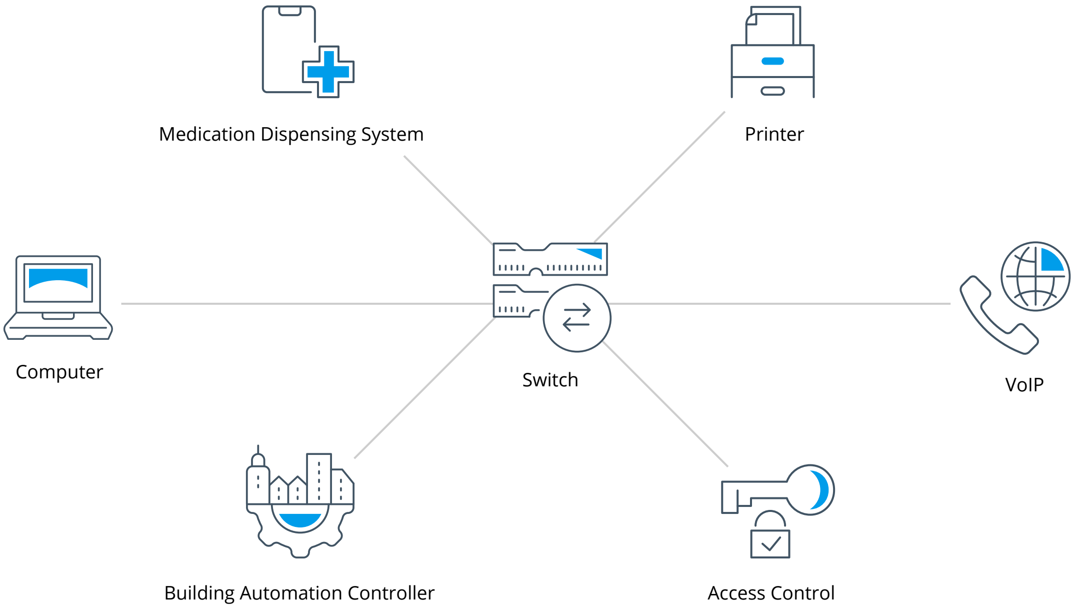

Figure 10 – Example of vulnerable VLAN

We also see much worse examples of almost completely flat networks where similar vulnerable printers and building automation controllers share the same segments with ultrasound machines, point-of-care diagnostic systems, DICOM workstations, patient monitors and many other types of medical devices. Security teams in healthcare organizations must realize that if they focus only on medical devices, they are missing other weak links in their networks.

Fact 17 – TCP/IP vulnerabilities increase risk.

Risk is the likelihood of a cyberattack multiplied by its potential impact. Because TCP/IP stack vulnerabilities are widespread and difficult to patch, they increase the likelihood of attacks. Because they affect several critical devices, including medical and many other types, they increase potential impact. Both likelihood and impact are amplified by the increased attack surface seen on poorly segmented networks.

Fact 18 – We have seen this before.

This combination of hard-to-patch devices, critical impact and poor segmentation allows for the most traditional attacks in healthcare organizations currently: data breaches and ransomware. But these traditional attacks are mostly limited to Windows-based IT equipment. They typically enter the network via vulnerable IT equipment, such as PCs, and allow the attacker to either (i) steal sensitive personal information and profit from its trade, or (ii) cripple devices via ransomware, including workstations and other Windows-based medical equipment, then demand payment to stop the attack. (Curently, combining both attacks in the same campaign allows attackers to profit doubly.)

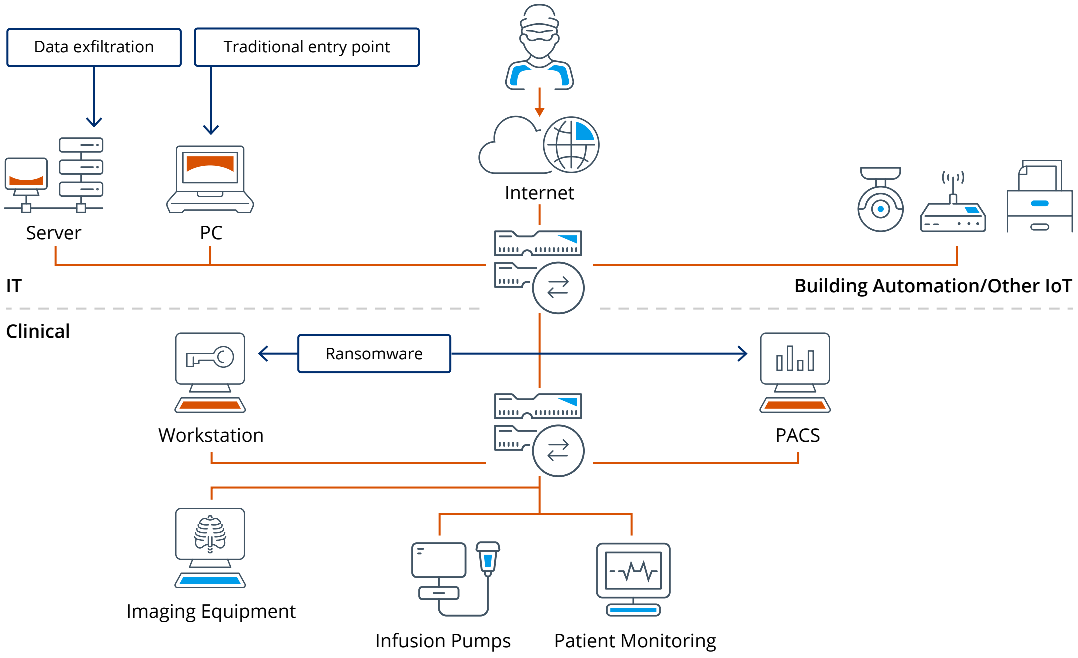

Figure 11 – The current threat scenario: data exfiltration and ransomware – devices in red are part of the attacks

Fact 19 – There are new threat scenarios on the rise.

TCP/IP stack vulnerabilities open new potential attack venues for malicious actors. They affect a much wider set of embedded devices, which includes many new IoT and building automation devices that are internet-connected and can serve as either entry points or final targets of attacks, as well as many medical devices that are not Windows-based and are directly connected to patients.

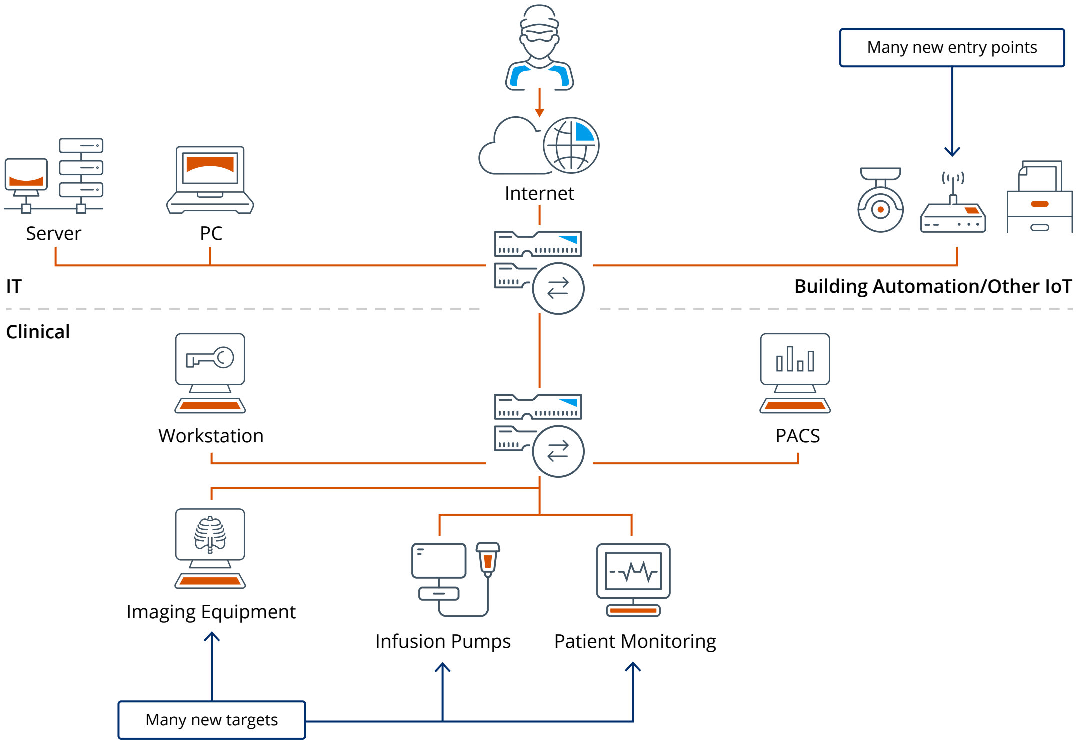

Figure 12 – Emerging threat scenarios: the IoT threat

Fact 20 – TCP/IP vulnerabilities open the door to threat scenarios with a potentially huge business impact.

The combination of traditional vulnerabilities (which we have explored in last year's report) with a host of new vulnerable devices that we explored in this report means that attackers can now enter and move more freely in the networks of impacted organizations. This emerging threat scenarios have the following business implications:

- **Increased exposure to attacks –** Since more devices and less-monitored device types are now vulnerable, organizations are more susceptible than ever to cyberattacks. Such attacks may affect the confidentiality and availability of sensitive data such as patients' Protected Health Information or personally identifiable information. This comes at a time of rising costs associated with healthcare data breaches. These breaches cost an average of $7.13 million in 2020, including lost business because of customer turnover, damaged reputation or system downtime.

- **Increased downtime of affected devices –** Ransomware can take big parts of an organization offline, but it is now something that the industry has learned to deal with by following standard guidelines. Downtime caused by exploiting vulnerabilities in embedded devices can be much higher because it may affect different device types in a completely different way (e.g., network disconnection, intermittent downtime, persistent denial of service), is mostly unknown to cybersecurity personnel and may demand specialized maintenance from the vendor or, in the worst case, equipment replacement. At a cost of thousands of dollars per scan, plus idle staff, plus delayed patient care, each hour that an MRI scanner is down can easily cost tens of thousands in lost revenue.

- **Denial of healthcare delivery –** Previous attacks lead to reputational damage (due to data breaches) or a decrease in healthcare delivery capacity (due to ransomware), which translate into lost revenue. However, attacks targeting directly medical devices such as patient monitors and infusion pumps can completely stop an HDO's ability to provide patient care and, in the worst case, harm patients.

Conclusions and recommendations

This report shows that TCP/IP stack vulnerabilities affect 75% of healthcare organizations, that they affect at the same time several vendors and device types in the same organization, and that they open the doors to potentially devastating attacks.

The widespread nature of these vulnerabilities in IoT and OT devices and the difficulty in patching those means that every organization, particularly in the healthcare sector, needs a proactive and holistic approach to cybersecurity that prioritizes the following steps:

- **Discover and inventory devices running the vulnerable stacks and assess their business risk.** Forescout Research Labs has released an open-source script that uses active fingerprinting to detect devices running the affected stacks. The script is updated constantly with new signatures to follow the latest development of our research.
- **Enforce segmentation controls and proper network hygiene** to mitigate the risk from vulnerable devices. Restrict external communication paths and isolate or contain vulnerable devices in zones as a mitigating control if they cannot be patched or until they can be patched.
- **Monitor progressive patches released by affected device vendors** and devise a remediation plan for your vulnerable asset inventory, balancing business risk and business continuity requirements.
- **Monitor all network traffic for malicious packets** that try to exploit known vulnerabilities or possible zero-day threats affecting TCP/IP stacks. Anomalous and malformed traffic should be blocked or at least alert its presence to network operators.

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

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

Learn more at Forescout.com