Putting Healthcare Security Under the Microscope

Forescout analyzes deployment data to better understand the cybersecurity risks facing healthcare organizations today.

FORESCOUT®

Executive Summary

The Internet of Medical Things (IoMT) continues to offer exciting possibilities for healthcare organizations to improve patient care. However, this digital transformation and increase in connectivity is also introducing new privacy and security risks. The device landscape is growing exponentially, adding to the complexity of networks and making it difficult to manage and improve their security posture.

The objective of this report is to provide healthcare organization security and risk management leaders with insight into the types of devices connecting to networks and their associated risks. In addition, this report recommends a holistic security approach that goes beyond just securing medical devices.

Source data for this report came from the Forescout Device Cloud, a repository of host and network information for more than 8 million devices, making it one of the largest crowdsourced device repositories. For this study, researchers limited Device Cloud analysis to 75 healthcare deployments with over 10,000 virtual local area networks (VLANs) and 1.5 million devices. Since the primary focus of the report is the status of medical devices, many of the results are based on analysis of more than 1,500 medical VLANs with 430,000 devices.

Key findings

- **Today's healthcare environments are increasingly diverse:** Rapid growth and diversity of connected medical devices and operating systems make it increasingly difficult to secure networks.
- **Legacy Windows operating systems are a major vulnerability:** Many networks still use unsupported Microsoft Windows operating systems. A major Windows milestone is soon approaching that will leave many more devices unsupported.
- **Segmentation strategies are lacking:** Network segmentation, a best practice for limiting malicious lateral movement by focusing on data sensitivity, location and criticality, is inconsistently applied on today's diverse networks.
- **Device vendor sprawl needs to be tamed:** The proliferation of device vendors causes major interoperability, security and asset management challenges.
- **Common services left on leave the network vulnerable:** Common protocols left open provide uncontrolled access to attackers.

The State of Cybersecurity for Healthcare Organizations

The IoMT continues to become a strategic priority due to its ability to improve patient care, provide better clinical data, increase efficiency and reduce healthcare costs. It's understandable why healthcare organizations are rapidly adopting the IoMT—a connected infrastructure of medical devices, software applications, healthcare systems and services. However, this rapid adoption of connected devices is creating a serious side effect: It distracts from the broader need to address overall security for today's converged environments, beyond connected medical devices, creating significant cybersecurity gaps.

> The Internet of Medical Things is a connected infrastructure of medical devices, software applications, healthcare systems and services. For the purpose of this study, IoMT falls into the categories of Internet of Things (IoT) and operational technology (OT).

Explosion of connected IT and OT devices in healthcare

The number of connected devices is growing at hyperspeed, expanding the attack surface and making it difficult to scale security. These devices include healthcare devices like patient tracking and identification systems, infusion pumps and imaging systems. It also includes infrastructure devices such as building automation systems, physical security systems, uninterrupted power supplies, backup generators and other OT systems and devices that are increasingly joining IT networks. Consequently, the responsibility for OT is moving under the purview of IT. According to Gartner, "By 2021, 70% of OT security will be managed by the CIO, CISO or CSO department, up from 35% today."[1]

Understanding and prioritizing risk

The convergence of these two previously disparate networks can create a new class of security risks. Cybercriminals can now move laterally across your interconnected IT and OT networks. The increase in mergers and acquisitions, which are prevalent in the healthcare sector, further amplifies these security challenges.

Much like clinical diagnosis and treatment, CISOs must detect risks early and prioritize the best course of action. Security and risk management teams that attempt to mitigate every risk will realize marginal results. By fully understanding threats on the network and pinpointing the devices that are harboring the most risk, it's possible to maximize productivity, increase ROI and reduce risk across the network.

The real costs of deferring risk containment

Once again, the fields of cybersecurity and healthcare share a common trait: early detection and treatment yields superior outcomes and dramatically reduces overall costs. Consider these statistics: According to *HIPAA (Health Insurance Portability and Accountability Act) Journal*, the average healthcare breach in 2018 involved 17,974 records.[2] Ponemon calculated the average resolution cost per capita/per personal health information (PHI) record in healthcare in 2018 at $408.[3] This puts the average cost of *containment, investigation, disclosure and notification* at $7.3 million per breach. Of course, the financial carnage doesn't end there as healthcare organizations must also deal with significant brand and reputational damage that negatively affects patient loyalty for years, especially in the U.S. Moreover, they can plan on a cycle of continual and ongoing audits going forward. The axiom of pay now or pay later has never been more appropriate.

[1] "Strategic Roadmap for Integrated IT and OT Security," Gartner, Inc., May 2018, www.gartner.com/doc/3873972/-strategic-roadmap-integrated-it

[2] "Analysis of 2018 Healthcare Data Breaches," HIPAA Journal, January 2019, www.hipaajournal.com/analysis-of-healthcare-data-breaches/

[3] "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute, July 2018, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

Healthcare is a prime target for cyberattacks

The attack surface in the healthcare sector expands every day as more medical devices connect to networks and hackers continue to target healthcare organizations to access personal health information, which ranks among the most sensitive type of consumer information. Cybercriminals covet PHI as it fetches a handsome reward due to an abundance of valuable personal data that can include date and place of birth, credit card details, social security number, physical address and email address.

Common cyberattacks impacting healthcare organizations

- **Ransomware such as the WannaCry and NotPetya Trojans:** This malware encrypts files, preventing healthcare staff from using systems or accessing electronic health records (EHRs) to provide care until a ransom is paid and systems are restored. *The May, 2018 WannaCry attacks disrupted patient care across the UK's National Health Service and forced the cancellation of more than 19,000 medical appointments. The Department of Health calculated the financial cost of WannaCry attacks at £92m.*[4] *Similar attacks in 2016 took Hollywood Presbyterian Medical Center's computers offline for a week, crippling their ability to deliver medical services until the medical center paid a $17,000 ransom.*[5]

- **Denial of access and dedicated denial of service:** An attacker floods the network and internet-connected servers with packets, preventing the flow of normal traffic and slowing system and application performance to a virtual halt. These attacks are also sometimes used to divert the security team's attention while a data theft breach is underway. *In 2014, hacktivist group Anonymous targeted the Boston's Children's Hospital with a DDoS attack. According to the Center for Internet Security, the hospital spent more than $300,000 responding to and mitigating the damage from this attack.*[6]

- **Device impersonation:** A device connects to the network and behaves like an authorized device but is actually a rogue device that collects data. Attackers use this technique to either steal PHI or penetrate backend systems. *Concerns about MedJacking, a common form of medical device impersonation, first surfaced when U.S. Vice President Dick Cheney ordered changes to his pacemaker to better protect it from hackers. According to Wired, MedJack attackers are now intentionally using old malware to target their assaults at medical devices running outdated operating systems like Windows XP and Windows Server 2003.*[7]

- **Man-in-the-middle attack:** An attacker inserts himself in the middle of two parties' communications (typically through a phishing scam) to eavesdrop or impersonate. *In April, 2017, the U.S. Department of Health and Human Services' office for Civil Rights advised covered entities and their business associates to use the Secure Hypertext Transport Protocol (HTTPS) to ensure protected health information is not left unsecured.*[8]

- **Fileless malware:** Attackers have learned to circumvent traditional antimalware tools with a new type of malware that resides only in the host computer's dynamic memory. The Ponemon Institute predicts that in 2019, fileless malware will represent 38% of attacks.[9] In addition to being pushed down through out-of-date or unpatched browsers, these in-memory attacks often exploit weak points in Microsoft Windows such as PowerShell and Remote Desktop Protocol (RDP).

[4] "Securing Cyber Resilience in Health and Care," October, 2018, www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

[5] "Los Angeles Times Article," February 18, 2016, www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[6] "DDOS Attacks: In the Healthcare Sector," Center for Intenet Security, www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/

[7] "Medical Devices are the Next Security Nightmare," WIRED, March 2017, www.wired.com/2017/03/medical-devices-next-security-nightmare/

[8] "Healthcare Organizations Warned of Risk of Man-In-The-Middle Attacks," HIPPA Journal, April 2017, www.hipaajournal.com/healthcare-organizations-warned-risk-man-middle-attacks-8757/

[9] "State of Endpoint Security Risk," Ponemon Institute, October 2018, https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

Understanding Connected Devices and Associated Risks

Methodology

This report is a cross-sectional analysis of the Forescout Device Cloud, a repository of host and network information for more than 8 million device fingerprints, making it one of the largest crowd-sourced device repositories. The Device Cloud data contains thousands of different types of devices from more than 1,000 Forescout customers that share de-identified device insight. Forescout analyzes the device fingerprints from its Device Cloud to identify device function, vendor and model, and operating system and version to provide granular and extensive auto-classification for a wide range of devices.

For this study, researchers limited Device Cloud analysis to 75 healthcare deployments with over 10,000 virtual local area networks (VLANs) and 1.5 million devices. Since the primary focus of the report is the status of medical devices, many of the results are based on analysis of more than 1,500 medical VLANs with 430,000 devices.

Classes of devices on medical VLANs

Many networks still operate in organizational silos, leaving gaps in security. Clinical engineers often focus on securing connected medical devices while facilities and operations teams concentrate on securing building automation systems. Given these siloed priorities, who is responsible for looking at security holistically?

At the most basic level, healthcare organizations need to be aware of the IT, IoT and OT devices connecting to their networks. This awareness helps to break down security silos, brings the right groups together to discuss security strategies, and provides the foundation for a holistic approach to security.

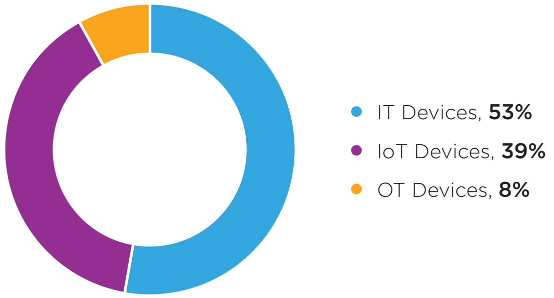
The classes of devices will likely shift in size as more medical devices connect to networks, making it critical to regularly review and adapt security strategies.

Figure 1: **Classes of Devices on Medical VLANs**

IT devices: Personal computers, laptops, purpose-built workstations, servers, thick and thin clients, virtualization hypervisors and enterprise networking gear.

OT devices: Medical devices, critical care systems, building automation/HVAC systems, power generators, badging and other facilities-related devices as well as IP-enabled security cameras and physical security systems.

IoT devices: VoIP phones, network printers, mobile devices, tablets, controllers and converters, video conferencing devices, presentation systems, smart TVs, entertainment consoles, various accessories.

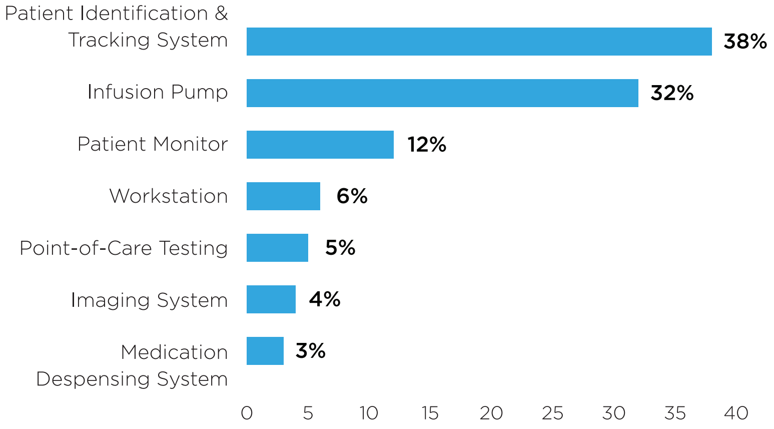


The most common connected medical devices

Inpatient medical facilities tend to see a higher percentage of devices that are "connected" to a patient. Per-patient devices such as patient identification and tracking systems, infusion pumps and patient monitors represent the majority of healthcare devices on clinical networks. This makes sense as they are the devices tracking and monitoring patients on a 1:1 ratio.

Devices such as those used in laboratory diagnostics or medical imaging represent a smaller number because they are shared devices. These more expensive systems tend to become long-lived legacy devices that are challenging to patch and keep updated.

Figure 2: **Most Common Connected Medical Devices**



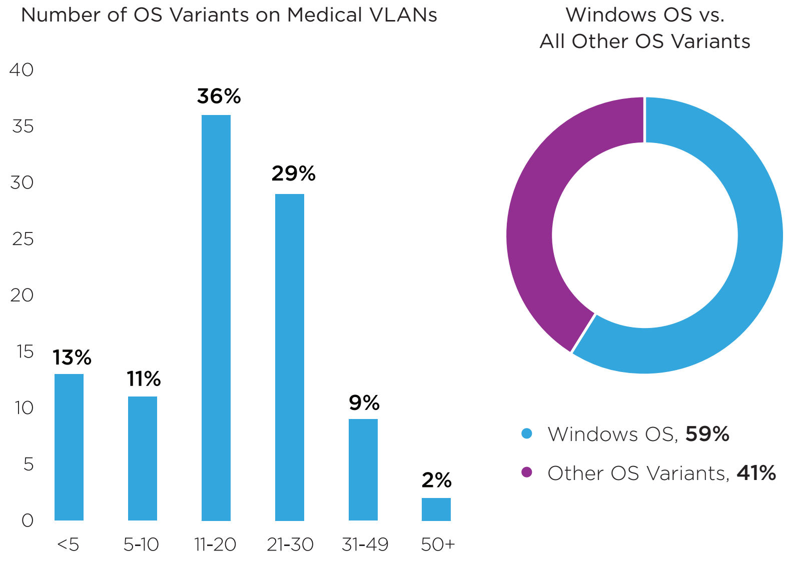
Diversity of device operating systems

The diversity of device operating systems can make managing security increasingly challenging. The study revealed that 40% of deployments had more than 20 different operating systems on their medical VLANs.

When looking at the different types of operating systems found on medical VLANs, more than half (59%) were Windows operating systems and 41% were a mix of other variants, including mobile, embedded firmware and network infrastructure. Patching and updating operating systems in healthcare environments—especially acute care facilities—can be challenging and require devices to remain online and available. Some medical devices cannot be patched, may require vendor approval or need patches to be manually implemented.

> 40% of deployments had more than 20 different operating systems on their medical VLANs.

Figure 3: **Diversity of Operating Systems on Medical VLANs**



The legacy Windows problem

Within our data sample, Microsoft support for more than 70% of devices running Windows, which includes Windows 7, Windows 2008 and Windows Mobile, is planned to expire by January 14, 2020. Running unsupported operating systems poses a risk that negatively impacts compliance with many regulations.

Networks will most likely continue to have medical devices running legacy operating systems since updates are costly. The downtime associated with an operating system update might not be acceptable for critical-care systems. In addition, certain legacy applications simply will not work on more recent versions of Windows due to lack of support, compatibility or license schema issues. The business need to run legacy operating systems on medical devices isn't going away any time soon, so these devices must be segmented appropriately to protect access to critical information and services.

> 71% of devices will be running unsupported Windows operating systems by January 14, 2020.

Figure 4: **Windows Operating Systems - The Good, the Bad and the Ugly**

The Good

29%

Devices running versions of Windows OS that will be supported for more than a year.

The Bad

.4%

Devices running unsupported/legacy versions of Windows OS.

The Ugly

71%

Devices that will be running unsupported Windows OS by January 14, 2020.

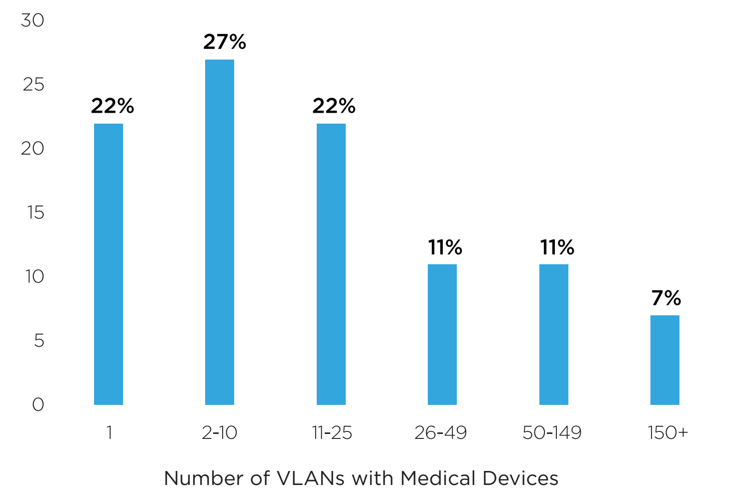
Usage of VLANs to support segmentation

Segmentation significantly reduces system attack surfaces. Users only "see" the servers and other devices necessary to perform their daily tasks. Segments are created by grouping common user types and limiting network access to those resources that users require to do their jobs.

Segmentation can be accomplished in a variety of ways. At the most basic level, VLANs can be employed to segment the network based on organization needs and priorities, effectively isolating critical data, segregating similar devices by function or limiting access to data, systems and other assets based on user credentials. The data in this study depicts a low number of VLANs with medical devices, suggesting that some healthcare organizations have yet to sufficiently invest in segmentation.

> 49% of deployments have medical devices across 10 VLANs or less, suggesting an immature segmentation implementation.

Figure 5: **Number of VLANs with Medical Devices**



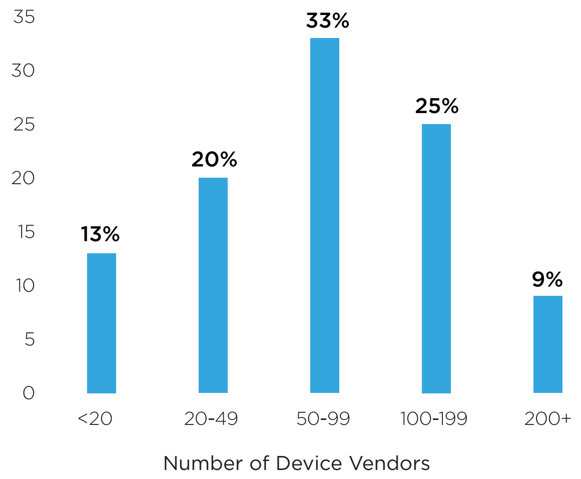
Device vendor complexity on the rise

Today's healthcare organizations are technology-saturated environments. Device vendors have historically not designed products with security as a top priority, making it more challenging to manage and secure them. In addition, vendors approach clinicians with devices that end up connected to the network, bypassing security and risk protocols. IT and security teams may detect these unauthorized connected devices, but typically are unable to classify or easily locate them.

Multi-site healthcare campuses are not technically homogeneous by any means—more than 30% of organizations' medical VLANs support more than a hundred distinct device vendors—and that diversity doesn't include the vendor tally from the other functional networks, such as back office, front office, and more. In many instances, the vendors themselves are responsible for patching and maintaining specialized clinical systems.

> 34% of organizations' medical VLANs support more than 100 distinct device vendors.

Figure 6: **Number of Device Vendors on Medical VLANs**



Common services left on leave the network vulnerable

A surprising number of devices on medical VLANs had high-risk services turned on, allowing uncontrolled access for attackers to get beyond the perimeter and move laterally. The access requirements of medical vendors and outsourced suppliers often require devices to have services like Microsoft's Remote Desktop Protocol enabled. Other times, the network ports are left open by default without the knowledge of IT and security staff.

- **Server Message Block Protocol (SMB):** SMB is the transport protocol used by Windows machines for a variety of purposes such as file sharing, printer sharing and access to remote Windows services. WannaCry and NotPetya are two examples of ransomware that exploited vulnerabilities in SMB.
- **Remote Desktop Protocol (RDP):** RDP is another common protocol exploited by modern automated threats, including fileless malware.
- **File Transfer Protocol (FTP), Secure Shell (SSH), Telnet and Digital Imaging and Communications in Medicine (DICOM) imaging protocol:** Less common but often-exploited vectors, these protocols do not secure or encrypt network sessions. Security models mix poorly with a legacy reality where too many devices rely on unencrypted basic services.

> 85% of devices running Windows OS had Server Message Block Protocol (SMB) turned on.

Windows Service	Percentage Running
SMB	85%
RDP	32%
FTP*	1%
SSH	<1%
Telnet Protocol*	<1%
DICOM Imaging Protocol	<1%

* Unencrypted

Recommendations

It's inevitable: The number of devices connecting to healthcare networks will continue to rise, and the environment will become more complex. The time to begin developing and implementing a proactive and enterprise-wide security and risk-management strategy is now.

Enable agentless discovery of all devices

Although devices with software agents make it easier for security and IT management to communicate with devices and monitor their activity, most medical devices do not support agents. Agentless detection of all IP-connected devices across the extended network is critical.

Identify and auto-classify devices

It's not sufficient to simply detect a device's IP address. Rapid and granular auto-classification is essential for extracting contextual insights from each device on the network and determining its purpose, owner and security posture. This information must feed into a real-time asset inventory to drive access control policies and help security teams quickly respond to targeted attacks on specific operating systems or devices.

Continuously monitor devices

Medical devices must be continuously monitored to detect any change in device posture. A point-in-time analysis can result in a set-it-and-forget-it mentality whereby compliance fatigue sets in and risk propagates. Nonstop network monitoring using passive and/or active techniques in clinical and OT environments provides security teams with real-time situational awareness to continuously track asset information and behavior while increasing the efficiency of security teams and saving their valuable time.

Enforce segmentation

Network segmentation is a known best practice, but it isn't easy to manage or enforce throughout the network. High-risk devices such as known-to-be-vulnerable legacy systems should be segmented to contain a potential breach and limit risk.

Conclusion

It's critical for healthcare organization security and risk management leaders to look at securing all devices across the extended enterprise. Solely focusing on securing medical devices rather than securing all device classes can cause significant gaps in your security posture. A holistic approach to security requires continuous visibility and control over the entire connected-device ecosystem—including understanding the role a device visibility and control platform can play in orchestrating actions among heterogeneous security and IT management tools.

As stated previously, the costs of inaction can be staggering. Every second that a device remains noncompliant extends your window of vulnerability and increases your risk factor—exposing your healthcare organization to significant patient safety, financial and business consequences. Healthcare organizations have a choice: invest in proactive risk planning and mitigation efforts now or pay later and face the wrath of security-conscious regulatory agencies, patients and legislators.

About Forescout Technologies

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment. As of December 31, 2018, 3,300 customers in over 80 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity. Learn how at www.forescout.com.

Forescout researchers constrained the scope and data sample for consistency and the convenience of issuing a one-time brief. We have 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.

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