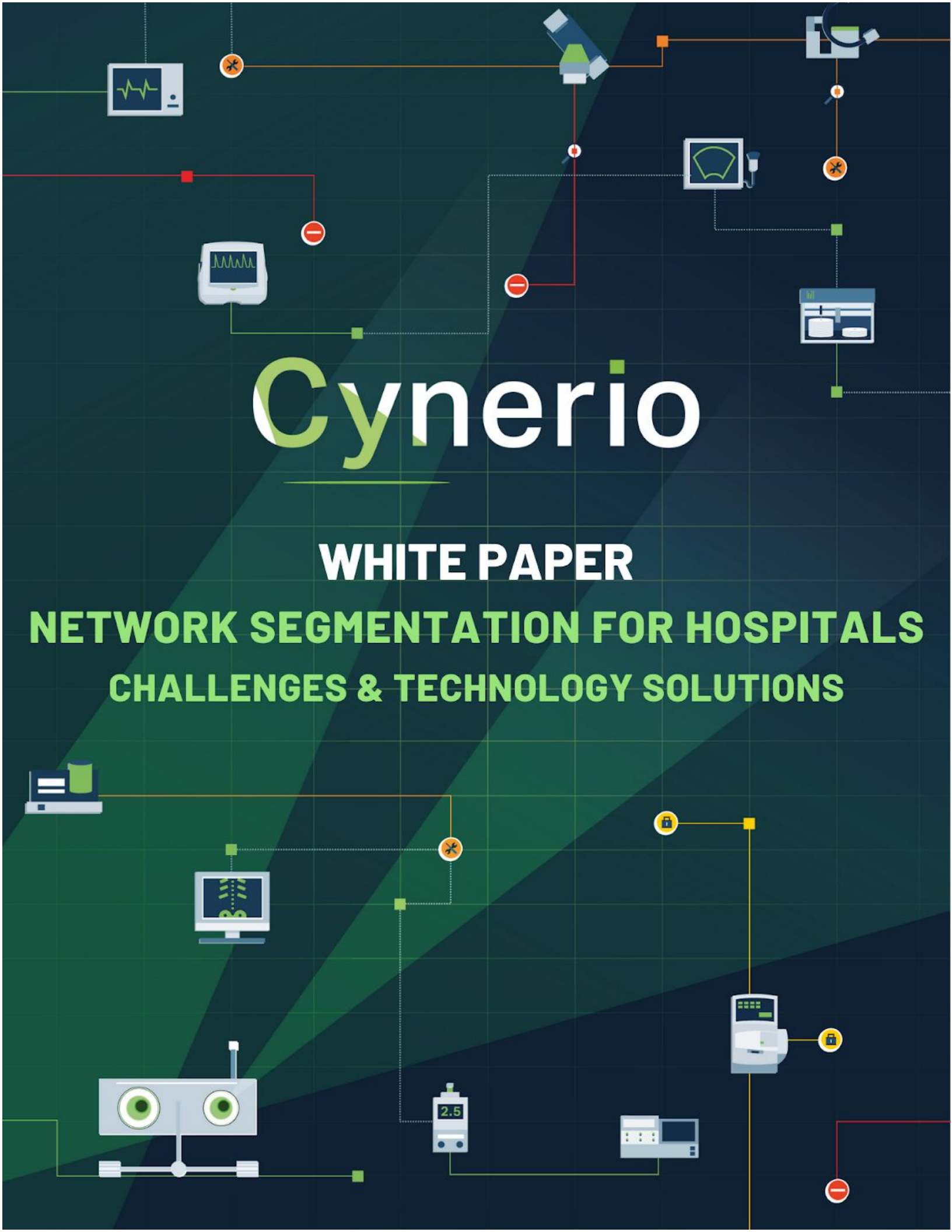
Cynerio

WHITE PAPER

NETWORK SEGMENTATION FOR HOSPITALS

CHALLENGES & TECHNOLOGY SOLUTIONS



Cynerio

Network Segmentation for Hospitals: Challenges and Technology Solutions

Hospitals and other organizations in the healthcare industry are under severe threat of cyber attack. A major problem is the proliferation of connected medical devices, many of which are not secure by design and are difficult to lock down with traditional security approaches. 81% of healthcare organizations reported they were compromised by a cyber attack in the past two years, and 32% of healthcare organizations say connected medical devices are their top security concern.

Network segmentation is a proven strategy to improve security and control over large-scale network environments. It is very applicable to the problem of cybersecurity in hospitals, and is especially useful for securing connected medical devices. However, segmenting a hospital network raises major challenges for organizations, and can turn into a huge, costly project that can place organizational goals and even patient well-being at risk.

In this white paper we explore basic concepts of segmentation, explain why it is difficult for hospitals to achieve, and present an innovative technical solution that can make segmentation achievable and practical for any hospital network.

Cynerio

Table of Contents

Chapter 1: Introduction to Network Segmentation

What Is Network Segmentation?

Network segmentation divides a network into multiple parts, known as segments. Each segment acts as an isolated fragment of the network. Network administrators can assign different monitoring policies to different segments and put access controls on the traffic between segments. If a corporate network is segmented wisely, most traffic stays between devices and applications within each segment, with much less traffic crossing segment boundaries. Hence, segmentation improves network monitoring, performance, and security.

Network segmentation prevents unauthorized user access and malicious attacks on medical devices by containing attacker activity to disparate parts of the network. Generally speaking, more network segments lead to a more secure network. The challenge is to avoid over-segmentation which can hurt connectivity, or under-segmentation which can create security and operational risks, while maintaining segmentation integrity over time.

One of the most common ways to segment your network is using Virtual Local Area Networks (VLANs). VLANs operate at level 2 (the data link layer) and break down the physical network down into logical networks. VLANs can also be used to achieve segmentation for security purposes by applying ACL rules.

Why Is Network Segmentation Important?

A large unsegmented network presents a large attack surface that can be difficult to manage and protect. Applications and hosts in an unsegmented network have access to the entire network. As a result, attackers who gain access to a network can move laterally to access critical data and resources beyond their original entry point. In addition, large networks are difficult to monitor and control because they generate a huge quantity of logged events.

Network segmentation creates internal barriers, making it more difficult for attackers to penetrate the network and cause damage. Moreover, segmentation isolates sensitive data from malicious insiders to ensure that critical information does not fall into the wrong hands.

The Benefits of Network Segmentation

Most cybersecurity professionals claim that organizations should isolate different parts of a network for better security. However, only a small portion of organizations have actually implemented this strategy. According to the Fortinet Global Enterprise Security Survey, only 29% of businesses have successfully implemented segmentation.

The main reason for failing to apply segmentation is the amount of time and effort required to correctly split a network into segments. However, after overcoming the setup challenges, organizations can gain many benefits like:

- **Monitoring**—network segmentation enables you to monitor internal communication, to log events, and detect suspicious behavior. In particular, segmentation makes it easy to distinguish internal communication from inter-segment communication—which may represent lateral movement. Event logging and monitoring prevents breaches by identifying irregular user behavior that can indicate a potential attack.
- **Isolation of cyberattack damage**—network segmentation isolates network traffic to limit and prevent access between segments. As a result, a data breach can be contained to a single segment without affecting other segments.
- **Access control**—you can limit access to sensitive information in a particular segment. Only certain users will be allowed to access the information. In the event that attackers compromise accounts in a specific network segment, their ability to escalate privileges or perform lateral movement across the network will be contained to that segment.
- **Compliance**—segmentation reduces regulatory compliance costs by limiting the number of systems subject to regulation. For instance, segmentation separates between payment systems and other network components. In this way, expensive compliance requirements apply only to payment systems, not the entire network.
- **Operational performance**—segmentation reduces network congestion. It reduces the amount of traffic between hosts across the enterprise network and focuses most network communication on a smaller number of hosts within a segment.

Chapter 2: Why Is Segmentation Difficult for Hospitals to Achieve?

The healthcare industry is among the most targeted by cybercriminals. Over 90% of all healthcare organizations have experienced a breach and 57% have experienced more than five data breaches. Moreover, about 300 million healthcare records have been stolen in the past five years.

Despite the statistics above, most hospitals are still using rudimentary security practices to protect their clinical networks. A typical hospital has many Internet of Things (IoT) and smart medical devices that are organized into segments across buildings and floors, typically defined using Virtual Local Access Networks (VLAN).

While hospitals do perform segmentation, in many organizations it is very limited. According to Forescout, 49% of healthcare organizations have deployed medical devices in 10 VLANs or less—a very small number considering that organizations can have tens or hundreds of thousands of connected devices.

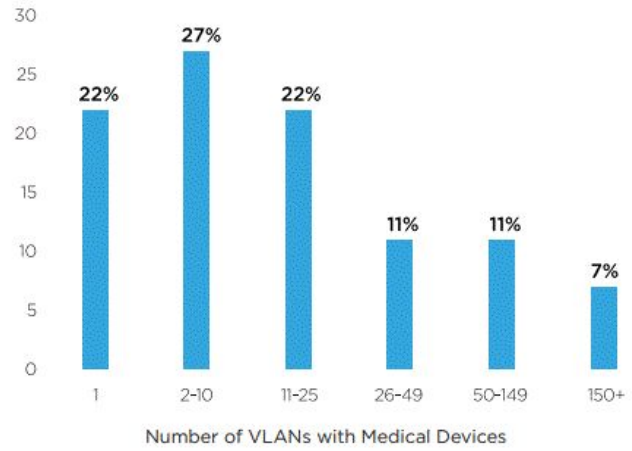


Image Source

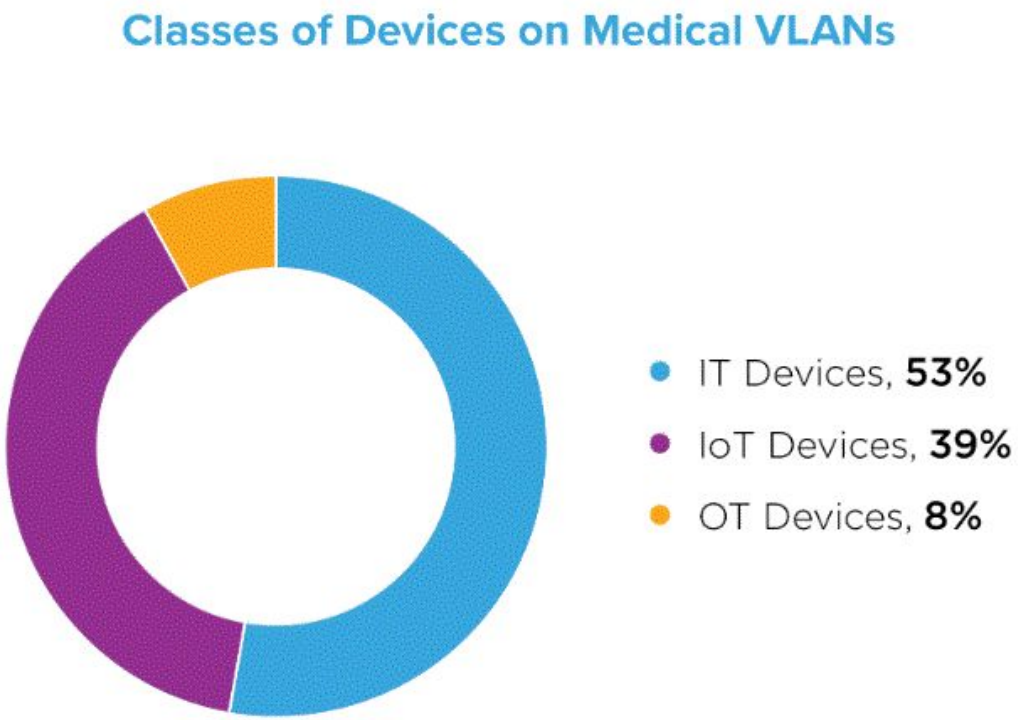
Below we review the main reasons most hospitals haven't implemented segmentation yet.

Multiple Classes of Devices

Many healthcare networks still operate in organizational silos. Clinical engineers focus on medical device security, while operations teams focus on the security of IT systems. No one takes responsibility for security in a holistic manner. Healthcare organizations need to be aware of all connected devices in their networks to plan holistic security strategies.

Classes of devices include:

- **Operational Technology (OT) devices**—critical care systems including connected medical devices, power generators, building automation systems, badging, security cameras, physical security systems, and other facilities-related devices.
- **Internet of Things (IoT) devices**—network printers, VoIP phones, mobile devices, tablets, video conferencing devices, presentation systems, entertainment consoles, and more.
- **Information Technology (IT) devices**—personal computers, laptops, servers, workstations, virtualization hypervisors, and enterprise networking equipment.



Source: Forescout

Traditional IT Tools Fall Short

Traditional IT security tools are excellent for firewalling and segmenting standard devices, including security cameras, tablets, enterprise networking equipment, and personal computers. However, firewalls and NACs do not have the ability to differentiate connected medical devices from standard connected devices. This deficiency poses a number of critical issues when preparing to segment devices in clinical environments:

- **Lack of medical device inventory**—standard IT tools cannot differentiate medical devices from standard devices connected to the network, resulting in a lack of visibility.

- **No understanding of device utilization and criticality**—medical devices are not all equal. Some connected medical devices have a greater impact on clinical operations and patient care than others. Reconfiguring medical device communications or disconnecting them

  from the clinical network without considering their clinical impact could negatively affect patient care and damage hospital workflows.
- **No documentation of device connections and disconnections**—without a record of what medical devices are being connected and disconnected, devices can get lost in the system and miss crucial security patches and OS updates, making them vulnerable to cyber threats. Disconnecting life-sustaining devices can damage patient welfare and disrupt clinical workflow.
- **Lack of organizational oversight**—because standard IT tools cannot differentiate between standard connected devices and medical devices, hospitals cannot rely on them to help with organizational oversight. Oversight of thousands of medical devices on a clinical network needs to be done manually without a medical-first IT tool designed to identify medical devices and understand their unique clinical impact and connections.

The Unique Challenges of Connected Medical Devices

The number of devices that are directly used in patient care is growing every day. Per-patient equipment like tracking systems, patient identification, infusion pumps, and patient monitors represent the majority of connected devices on clinical networks. These devices become long-lived legacy systems that commonly outlive their operating systems. Devices running on operating systems that are no longer supported are challenging to patch and update.

In addition, VLANs set up for connected medical devices often contain devices from multiple vendors. Different devices may have different communication requirements and maintenance lifecycles. VLAN configuration is often set to the lowest common denominator, to allow all devices in the segment to communicate and perform remote maintenance. It would be much more effective to limit each group of devices to the specific network communications they actually need.

Moreover, many medical devices connect to a vendor's external server as part of normal clinical operations, or for maintenance and updates. This increases the attack surface of the device and places the entire network segment at risk. If the vendor is attacked, attackers could use the open communication channel to attack the hospital network.

The Inherent Vulnerabilities of Medical Devices

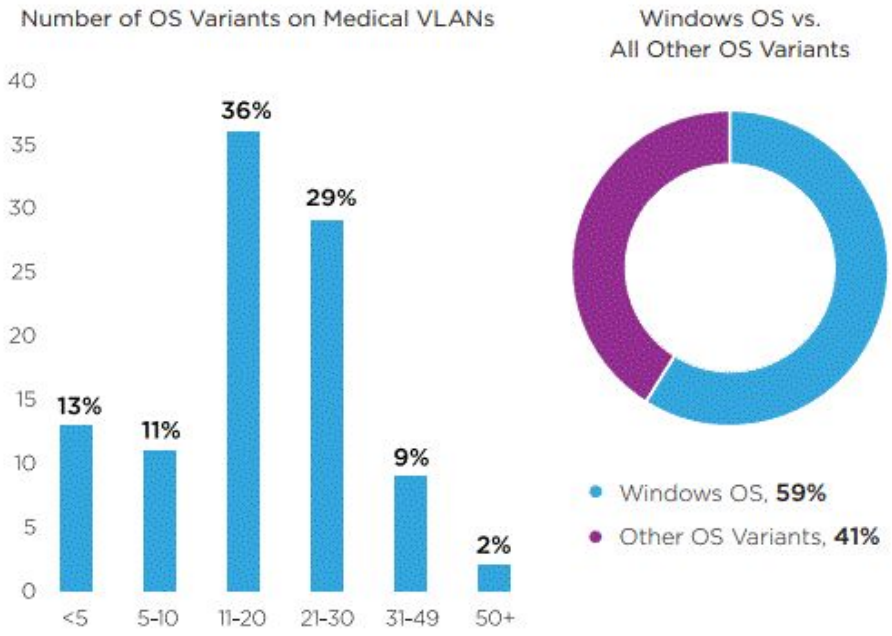
Medical devices are vulnerable by nature to cyber threats and traditional cybersecurity measures cannot protect them. Successful cyber attacks against connected medical devices can cause significant damage to business-critical operations, especially if the attack is targeted at patient-critical devices like Magnetic Resonance Imaging (MRI) machines.

Common medical device threat vectors include:

- **Malware**—medical devices usually have no endpoint protection and are especially vulnerable to malware.
- **Web application attacks**—some medical devices are managed through web interfaces. External web interfaces create a wide range of security risks like code injection and path traversal.
- **Insider threats**—malicious insiders can easily gain unauthorized access and tamper with devices due to weak authentication.
- **Device misuse**—Connected medical devices often run Windows operating systems. Hospital staff can use the machines to browse the Internet or install software, creating additional risk.

Multiple Operating Systems

The diversity of operating systems in medical devices makes security management challenging. A report by Forescout surveying 1,500 medical VLANs and 430,000 devices showed that there were more than 20 different versions of operating systems on 76% of an organization's medical devices.



Source: Forescout

In healthcare environments, many medical devices must remain online and available at all times. Taking a device offline to update or patch it may not be an option, because it may disrupt critical services or even affect patient well-being, in a critical-care setting. As a result, some medical devices cannot be patched or may require vendor approval or manual patching. Unpatched and outdated systems are vulnerable to cyber threats and negatively impact compliance.

The Legacy Windows Problem

Most healthcare organizations are still using devices running legacy operating systems because many devices cannot be updated, and purchasing a new device or series of devices may be prohibitively expensive. More than 70% of healthcare devices run on unsupported Windows operating systems, such as Windows 7. Microsoft stopped support and security updates for Windows 7, Windows Server 2008, and Windows Mobile since January 14, 2020.

Hospitals prefer to keep legacy operating systems because many applications and devices rely on them for normal operations. The need to run legacy operating systems on medical devices will not go away. Since legacy devices do not get security updates and most likely already have known vulnerabilities, the only way to reduce the attack surface is by applying a network segmentation policy.

Chapter 3: Healthcare Network Segmentation: Can You Do It Yourself?

This chapter presents a practical example of network segmentation using a common, patient-critical connected medical device—an infusion pump (IV pump). We'll use this example to illustrate the challenges of segmenting critical medical devices, and begin to explore a solution.

A Practical Example: Network Segmentation for Infusion Pumps

An infusion pump (AKA IV pump) is a medical device that delivers fluids and medications in controlled amounts to a patient. Infusion pumps are widely used in clinical settings such as hospitals and nursing homes. They are usually connected to a central monitoring station so medical staff can check on multiple patients at the same time.

Modern infusion pumps are connected to a wide range of healthcare systems, networks, and other tools to enable central control, policy management, and gathering of analytics. Connecting devices to point-of-care medication systems and electronic health records can increase cybersecurity risks. Potential threats include changes to prescribed drug doses, unauthorized access to protected health information (PHI), and interference with a pump's operation.

Using Network Access Control (NAC) to Build VLANs and Set Access Control Lists (ACLs)

Network Access Control (NAC) solutions provide access management and network visibility through policy enforcement on network devices and users. Once medical devices have been identified and profiled, you can use the NAC to assign different switch ports to VLANs. After your VLANs are defined, you can define ACLs to restrict specific communications to and from the VLAN and all devices within it.

A NAC can reduce the security risks inherent in legacy infusion pumps by segmenting the network and applying defined access policies for the pumps. The process is as follows:

1. **Identify and profile pumps**—find IV pumps and assign risk impact scores based on usage and criticality.
2. **Pinpoint vulnerabilities**—identify device-specific vulnerabilities and tag device IP addresses.
3. **Configure access control rules in the NAC**—segment the devices on a seperate VLAN to isolate vulnerable IV pumps from the rest of the network and allow only necessary communications.
4. **Monitor communications**—all communications should be monitored to guarantee continuous service and ensure devices adhere to policy before pushing configuration to the NAC.

Three Challenges with the DIY Process

Placing IV pumps into VLANs manually, and filtering traffic through access-control lists, has severe limitations:

1. **The NAC cannot identify an IV pump on its own**—you need to manually configure the NAC when new pumps are added or removed, or when the IP changes. In large organizations there could be hundreds of IV pumps.
2. **The NAC does not provide traffic visibility and monitoring**—you do not have enough information about the traffic between the pump and other devices. As a result, you need to carefully analyze the traffic to determine which communication is critical for clinical purposes, legitimate or not.
3. **High level of confidence is required to make access control changes**—you need a complex project involving many parts of the organization to ensure you are not cutting off devices and disrupting operations or endangering patients.

The Need for a Medical-First Solution for Healthcare Network Segmentation

The main goal of security teams in Healthcare Delivery Organizations (HDO) is to reduce and control the traffic between medical devices and external networks without interrupting service. However, vulnerable devices, poor network security, and lack of awareness about safe cybersecurity practices lead to the following security concerns:

Concern #1	**Misuse** Misuse of a medical IoT device happens when either an application or a person uses the device to connect to unauthorized external networks. • Clinical staff and medical professionals may use medical devices to browse the web, unaware of security risks, or download and install apps that connect to external networks.
Concern #2	**Misconfiguration** Most medical devices connect to external networks for operating systems and software updates. Attackers can hijack the session and reroute the communication to a server that will provide a malicious update, instead of a legitimate one, thus infecting the device.
Concern #3	**Required External Connections** Some medical devices require a continuous external connection for standard operation. Unauthorized users can take advantage of unprotected external connections to penetrate patient-critical devices and exfiltrate data, like PHI.

Concern #4	**Vendor Access** Medical devices often require vendor access for OS updates, to receive support services, and to send logs. Communication with vendors is usually conducted over a VPN. Organizations must control and monitor VPN connections because vendor networks cannot be trusted, and are not under the control of security teams.
Concern #5	**3rd-Party Apps & Libraries** ● Patient-critical devices often include pre-installed software that runs in the background and may connect to external networks. ● Patient-critical devices often include software with a 3rd-party library component (commonly open source). These libraries may contain vulnerabilities or backdoors of which IT is unaware.

Chapter 4: How Cynerio Solves the Challenges of Healthcare Network Segmentation

Cynerio solves healthcare network segmentation challenges in four phases. Each phase provides different techniques for mitigating the security risks of connected medical devices. These four phases work as a cycle that offers continual protection, rather than a one-time fix, and adapts to hospitals' evolving needs.

IT security and clinical engineering teams at healthcare centers should continuously perform these phases—surveying the environment, assessing risks, and addressing security issues they discover on a day-to-day basis.

Cynerio's Three Phases for Mitigating Security Risks

Cynerio solves the segmentation problem in health organizations using the following process:

1. **360° View Beyond Devices**—continuously discover and profile connected medical devices existing on the network and update the inventory on an ongoing basis; map the network topology and contextualize device behavior based on clinical impact and workflow.
2. **Impact-Focused Services**—analyze the risk posed by each device and assign risk impact scores according to its impact on patient safety, privacy, and service continuity; detect anomalies, vulnerabilities, and breaches; track PHI, schedule reports, and issue meaningful alerts.
3. **Actionable Security**—provides robust and enforceable segmentation policies by integrating with and enriching top-tier security tools with a medical-first context.

Phase 1: Gain a 360° View Beyond Connected Medical Devices

Create an Inventory of Connected Medical Devices

Cynerio discovers and classifies all connected medical devices according to type, model, operating system, and the latest versions of security patches. However, you cannot actively scan on medical devices like you would on traditional IoT devices. Active scanning of medical IoT devices may affect their operation and lead to clinical service disruption and patient harm. This poses some unique challenges:

- **A large number of devices**—healthcare networks may contain thousands of different devices of different makes and models, running several different operating systems.
- **Sensitive devices**—the discovery process must be passive because active network scanning can interrupt critical operations of medical devices.
- **Invisible to traditional network discovery tools**—most connected medical devices do not advertise their information on the network. Detecting connected medical devices over the

network requires careful analysis of traffic at the application layer. Traditional tools cannot discover the majority of connected medical devices.
- **Ongoing changes**—discovery has to be ongoing because devices are constantly replaced, added, or removed from the network. Due to the large number of devices, manual discovery is not feasible.

Cynerio overcomes these challenges by automatically discovering medical devices on the network and maintaining a broad inventory of device types.

Network Mapping and Clinical Context

Cynerio not only provides information on device inventory—the what and why of medical devices—but provides the essential medical context hospitals need regarding how and why devices operate and communicate the way they do. Cynerio inspects the network and communication configuration of discovered medical devices and identifies:

- The device's clinical function
- How the device communicates over the network
- Which of those communications are required for the device's critical clinical operations, which are non-critical but acceptable, and which are risky or anomalous

Mapping makes it easy to identify which devices might represent a risk to the organization, and how the network should be segmented to avoid disrupting critical functions.

Phase 2: Impact-Focused Services: Analyzing Risk

Cynerio assesses the risks affecting each device, and how each risk might affect the organization. The impact of an attack on connected devices is not limited to data security and privacy.

Consequences of a successful cyber attack include:

- **Patient safety**—attacks on devices that are life supporting or represent a risk to patient well-being can cause direct physical harm to patients.
- **Privacy**—devices that store large amounts of Protected Health Information (PHI) are more likely to be targeted by cyber criminals.
- **Service disruption**—attacks that cause device failure can disrupt critical medical treatment, such as surgery, respiratory equipment, or the delivery of life-sustaining medication.

Potential risks include:

- **Authentication**—identify if the device has an authentication mechanism. Ensure existing authentication enforces usage of secure passwords.

- **Misconfigurations**—look for general vulnerabilities, such as hard-coded or default passwords, and unpatched operating systems or software.
- **Encryption**—check if the device transmits or receives unencrypted dataflows.
- **Connections to less secure devices**—check if the device can connect to a less-secure device or endpoint, such as a physician's workstation, and whether it exposes management or data services like FTP or SSH.
- **Non-secure protocols**—check if the device uses protocols that offer weak authentication, no authentication, or contain vulnerabilities.

Phase 3: Actionable Security

Phases 1 and 2 form the discovery and risk assessment process, which ranks devices according to the individual risks they represent. Each device is assigned a risk impact score according to its effect on patient safety, privacy, and service disruption.

Organizations can define their acceptable level of risk. Security teams can then prioritize security tasks according to risk scores, ensuring high-level risks are mitigated at all times. For example, all vulnerable IV pumps can be grouped into one risk level, and any new IV pump is automatically added to this group. Cynerio can then help organizations define network segmentation rules to protect devices representing a high risk. Integration with top-tier security tools enables the enforcement of these policies.

How Cynerio Solves Segmentation Challenges in Medical Organizations

The following process provides a solution for each of the unique challenges mentioned in Phase 1, with a description of how Cynerio would perform network segmentation on an IV pump, continuing the example from chapter 3.

1. Cynerio automatically identifies all IV pumps on the network, and then tags them in the NAC as "IV pump."
2. Cynerio uses a database of devices and network patterns to identify the most appropriate VLAN configuration for IV pumps. For example, an Alaris Infusion Pump should only communicate using the Alaris protocol on port 3613.
3. Cynerio's virtual segmentation helps you create segmentation rules. You can create rules that you want to enforce and apply them virtually. Nothing changes in production, but you get an alert when any network communication violates the policy.
4. When you get an alert informing you that the virtual segmentation rules violate the policy, you can decide to:
    - Add the alert to the virtual segmentation rules
    - Investigate the alert as a security incident or misconfiguration
    - Ignore the alert—the event is not malicious, but nevertheless should not be allowed in the production environment

5. Once you are confident that the network rules are working properly, you can push the rules to the NAC and enforce the new segmentation policy in your production environment. Because they were previously tested and exceptions to the rules were noted and incorporated into the rules, you can be confident the segmentation rules will be effective and will not disrupt critical operations..

Conclusion

Healthcare organizations face growing cybersecurity threats, yet critical security measures, such as patching and updating legacy systems, may not be available to them.

Network segmentation is a proven, powerful tool for containing attacks and preventing them from spreading across the entire network. It can be effective even for legacy equipment that is difficult or impossible to patch for vulnerabilities. However, the unique challenges of medical IT environments made it very difficult for hospitals and other healthcare organizations to employ this tool. We have shown that with the right tools in hand, hospitals can achieve effective network segmentation in a safe and efficient way.