PROTECT MEDICAL DEVICES

SUMMARY

Industry

Healthcare

Use Case

Protect medical devices from cyberattacks in healthcare provider environments

Medical Devices

Medical devices are notoriously vulnerable to cyberattacks because security is often an afterthought when the devices are designed and maintained by the manufacturer

Business Benefits

- Decrease risk to patients undergoing treatment via medical devices
- Prevent undesired applications and malicious content in medical device networks
- Improve compliance with HIPAA, GDPR and other applicable data protection regulations

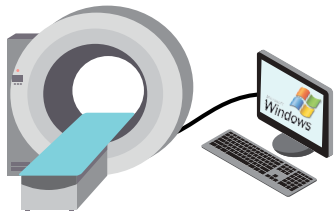
Operational Benefits

- Improve visibility into network traffic traversing medical devices
- More easily maintain medical device network segments through simplified security policies
- Reduce network latency and downtime, particularly for time-sensitive medical applications

Security Benefits

- Reduce risk of successful cyberattacks, including exfiltration of ePHI
- Prevent infected medical devices from mounting attacks against other systems – most commonly ransomware or exfiltration of ePHI off the network

Business Problem



From a cybersecurity perspective, medical devices are the most vulnerable devices on healthcare networks, yet they are often inadequately protected for several reasons:

1. **Lack of Cooperation From Medical Device Manufacturers**

   Healthcare providers are commonly met with resistance when they request help from a medical device manufacturer to secure a device. The manufacturer cites FDA compliance as the reason they can't update it, even though the FDA has repeatedly issued guidance in support of basic security practices, like patching and endpoint protection tools.[1]

2. **Running on End-of-Life Operating Systems**

   Medical devices are often deployed by the manufacturer alongside a Windows-based PC that controls, monitors and collects data from the devices. End-of-life operating systems, such as Windows® XP and even Windows 95, sometimes remain in use due to the high cost to upgrade. For example, a new MRI machine can cost $3 million.[2]

   All Microsoft® operating systems require monthly patching to resolve vulnerabilities that could expose the system to cyberattacks. Failure to mitigate the risk of unpatched Windows PCs connected to medical devices exposes the organization to a variety of cyberattacks. Those resulting in malware on a medical device could create dangerous conditions for patients connected to the device, or exfiltration of electronic protected health information (ePHI) off the network.

3. **Device Management via Nonstandard Remote Access Methods**

   Hospitals can have thousands of medical devices and hundreds of medical device vendors. When each vendor requests a different method to remotely manage their devices, it can expose the organization to unnecessary risk.

4. **Failure to Evaluate Medical Devices Prior to Deployment**

   Given the inconsistent security of medical devices, the healthcare provider has the ultimate responsibility of evaluating each device prior to connecting the device to the network. Healthcare providers that lack the staff or technology to adequately evaluate devices prior to purchase expose the organization to risk that could be avoided.

   The remainder of this paper will focus on solving these four common challenges with medical devices in healthcare provider environments, and suggest solutions for each.

1. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
2. http://www.time.com/money/2995166/why-does-mri-cost-so-much/

Business Drivers

There is growing public awareness of the threat unpatched and unprotected medical devices pose to healthcare organizations as the number of vulnerability disclosures and corresponding media coverage increase.

- 2013 – Dick Cheney, former U.S. vice president, ordered changes to his pacemaker to prevent attackers from compromising it.[3]
- 2015 – FDA confirmed that it is possible to access the Symbiq Infusion System remotely through a hospital's network.[4]
- 2015 – FDA and Hospira® issued a safety communication outlining vulnerabilities in certain Hospira LifeCare Infusion Pump Systems.[5]
- 2016 – Johnson & Johnson® alerted customers that one of its insulin pumps was vulnerable to cyberattacks.[6]
- 2016 – MedSec™ Holdings and hedge fund Muddy Waters announced several critical vulnerabilities in St. Jude Medical® devices in a controversial disclosure after taking a short position on St. Jude stock.[7]
- 2017 – FDA and a third-party security research firm validated the vulnerability with a patch and a security advisory.[8]

It is likely that other vulnerabilities that potentially impact the safety and effectiveness of medical devices are yet to be discovered, given manufacturers' long history of issuing devices that have little to no security built in to the design of the product.

Risks	Threat	Vulnerabilities
• Patient safety • Patient data • Operational downtime and revenue loss • Patient trust • Public reputation	• Malware • Unauthorized therapy manipulation • Lateral attack • Hacktivism • Cyberwarfare	• Long useful life • Lack of security in design • Lack of endpoint malware protection • Poorly patched • Highly regulated turnkey systems

Figure 1: Overview of medical device risks, threats and common vulnerabilities

In the United States, the Food and Drug Administration is responsible for managing rules and regulations of the medical device industry. In 2014, the FDA issued guidance that recommends that medical device manufacturers and healthcare facilities take steps to ensure appropriate safeguards are in place to reduce the risk of device failure due to cyberattack.[9] The guidance, however, did not specify a framework or specifics around how to reduce those risks. Hence, it has been up to healthcare organizations to determine how to adequately protect their devices.

Traditional Approaches

Considering the lack of guidance around medical device security, healthcare providers have done what they could to secure the systems. Typical approaches usually involve legacy security technologies that neither adequately protect the devices nor scale in a way that can be managed by the network and security teams (typical in many healthcare IT teams).

Traditional Approach #1: Flat Network

Some healthcare organizations – especially smaller clinics – may have neither the capital nor human resources to manage the added complexity of a segmented network. In such environments, medical devices are connected to the same network as all other devices. Flat network architectures fail in two major ways: 1) Medical devices aren't protected from the rest of the network, and 2) the rest of the network isn't protected from medical devices. As mentioned previously, it is common for medical devices to be connected to Windows-based PCs, which do not consistently allow endpoint protection to be installed. Without protection at the network or endpoint level, this approach offers the highest risk for a healthcare organization.

No Segmentation:
- Medical devices and end-user PCs on same network

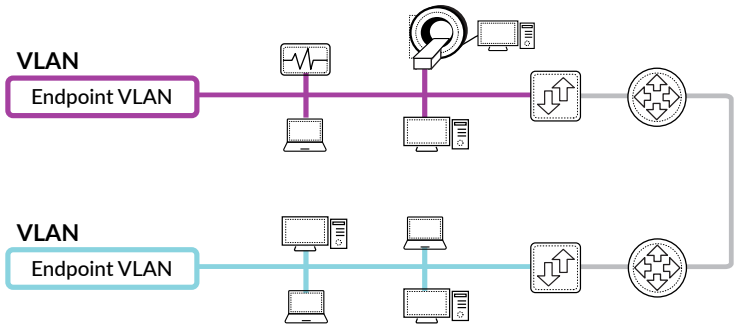
Advantages:
- Easy maintenance

Weaknesses:
- No network security capabilities
- High risk of cross-device malware infection

3. https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/
4. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm
5. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm
6. http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L
7. https://threatpost.com/st-jude-patches-additional-cardiac-device/123596/
8. https://ics-cert.us-cert.gov/advisories/ICSMA-17-009-01A
9. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

Traditional Approach #2: Segmented Network Based Purely on Switch-Based VLANs and ACLs (No Firewall)

A common approach to protecting medical devices in healthcare environments is to define a VLAN for medical devices and Layer 3 access control lists (ACLs) to limit the traffic between the endpoint VLAN. This option lacks internal legacy firewalls and fails to adequately protect medical devices due to an inability to prevent threats targeting medical devices over the network, and it won't scale with the organization.



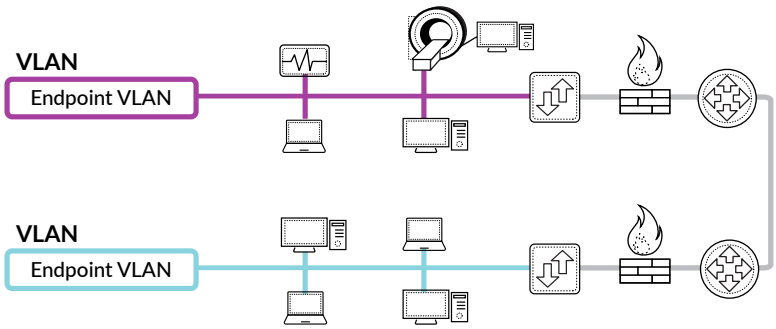
Switch-Based ACLs:
- VLANs used to isolate medical devices
- IP and port-based ACLs on switches control traffic flows

Advantages:
- Basic isolation of medical devices

Weaknesses:
- IP and port-based ACLs
- Difficult to manage at scale
- No protection against active threats like malware

Traditional Approach #3: Segmented Network Based Purely on VLANs and ACLs in Switch and Legacy Firewalls

This approach is similar to Approach #2, except it also uses legacy firewalls to enforce traffic limitations between the VLANs at Layer 3. This is a better approach than the previous one, but it still relies on the same port- and IP-based rules of the previous approach, which results in the same weaknesses.



Switch-Based ACLs With Legacy Firewalls:
- VLANs used to isolate medical devices
- IP and port-based ACLs on switches and firewall control traffic flows

Advantages:
- Better isolation of medical devices

Weaknesses:
- Same IP and port-based ACLs as with previous approach
- Difficult to manage at scale
- No protection against active threats like malware

Because many medical devices are considered "untouchable," since either the vendor restricts endpoint protection or the device physically can't support it, network-based control is the only option healthcare organizations have to secure them. The common thread behind the traditional approaches to network-based controls is that they do not meet four core requirements of medical device protection:

1. Advanced network-based threat prevention
2. Easy to manage
3. Able to scale upward as the organization acquires more medical devices
4. Consistent approach for vendor remote access

Palo Alto Networks Approach

Palo Alto Networks® Next-Generation Security Platform provides medical-grade security for protecting medical devices in a healthcare environment. Through advanced network-based threat prevention and zone-based segmentation, the platform prevents threats from ever reaching medical devices from other areas of the network (and vice versa) in an architecture that facilitates easy management and upward scaling to support any number of medical devices.

- **Control of all traffic at the application level** (Layer 7 of the OSI Model). At the heart of our platform, innovative App-ID™ technology accurately identifies and classifies all traffic by its corresponding application, regardless of ports and protocols, evasive tactics such as port hopping, or encryption. In highly sensitive or specialized zones of the network, like the CDE, this provides the best possible control by allowing security administrators to deny all traffic except the few applications that are explicitly legitimate.

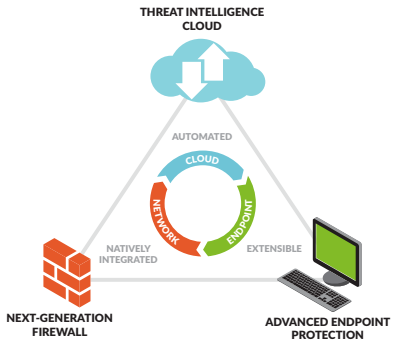


Figure 2: Palo Alto Networks Next-Generation Security Platform

- **Least-privileged access control** across the network. Along with App-ID, our User-ID™ and Content-ID™ technologies enable organizations to tightly control access to the CDE based on a range of business-relevant attributes, including the specific application and individual functions being used, the actual identity of individual users and groups, and the specific elements of data being accessed (e.g., credit card or Social Security numbers). The result is a definitive implementation of least-privileged access control where administrators can create straightforward security rules to allow only the absolute minimum, legitimate traffic in the zone while automatically denying everything else.
- **Advanced threat protection.** A combination of antivirus/anti-malware, intrusion prevention and advanced threat prevention technologies (Content-ID and WildFire™ threat analysis service) filter all allowed traffic for both known and unknown threats.
- **Flexible data filtering.** Administrators can allow necessary applications yet still block unwanted file transfer functionality, block unwanted file types, and control the transfer of sensitive data, such as credit card numbers or custom data patterns in application content or attachments.

Security Function	Product
• Layer 7 firewall (physical and virtual) • Application whitelisting • URL filtering • Intrusion Protection System, including anti-exploit • Intrusion Detection System • Network-based polymorphic anti-malware • Polymorphic command and control prevention • Credential theft prevention	• Next-Generation Firewall • URL Filtering subscription • Threat Prevention subscription
• Malware analysis environment (sandboxing) with automatic signature creation for closed-loop protection from new threats at security enforcement points	• WildFire subscription or appliance
• Device and policy management and threat visibility	• Panorama™ network security management
• Endpoint-based anti-exploit (signature-less) • Endpoint-based anti-malware (signature-less)	• Traps™ advanced endpoint protection
• Threat intelligence analysis, hunting and response • Closed-loop preventive automation of threat intelligence feeds	• AutoFocus™ contextual threat intelligence • MineMeld™ threat intelligence syndication engine, stand-alone or as part of AutoFocus
• SaaS application visibility, intellectual property protection and threat prevention	• Aperture™ SaaS security service
• Always-on client VPN for endpoints. Ensures that all traffic from endpoint passes through a next-generation firewall.	• GlobalProtect™ network security for endpoints

Figure 3: Core security functions provided by the Next-Generation Security Platform

Palo Alto Networks approach to securing medical devices primarily involves Palo Alto Networks Next-Generation Firewall, which relies on other products described above for enhanced security features. The next-generation firewall is used to define zones for segmentation within the healthcare environment. Refer to Figure 4 for examples of zones in a hospital.

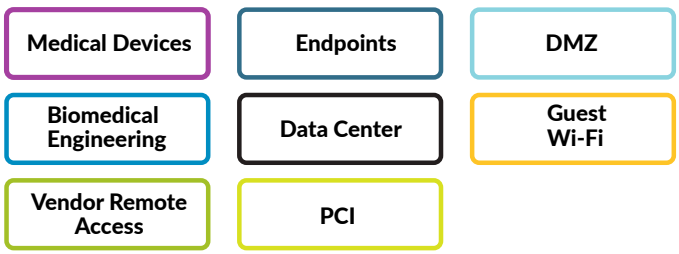


Figure 4: Example security zones for segmentation in hospitals

Additional security zones are often defined in hospital environments for further isolation to improve the security infrastructure.

1. Additional zones in the medical device segment further restrict vendor access and highly critical functions like patient monitoring
2. Additional zones in the PCI segment delineate endpoint-based versus data center-based PCI devices
3. Additional zones in the endpoints segment isolate departments from others (e.g., finance from nursing)
4. Dedicated zones for IP phones and/or badging systems

The following diagram outlines an example high-level logical architecture that shows how the next-generation firewall enforces zones of isolation between devices attached to a hospital network. Any zone-to-zone traffic must pass through a next-generation firewall to be evaluated for threats and only passes if explicitly allowed by the security policy. A zone is a grouping of interfaces (physical or virtual) that represents a segment of your network that is connected to, and controlled by, the firewall. Zones can be defined based on many factors, but VLANs are most commonly used as the basis for separation. For example, as in Figure 5, there is usually a corresponding VLAN for each of the zones.

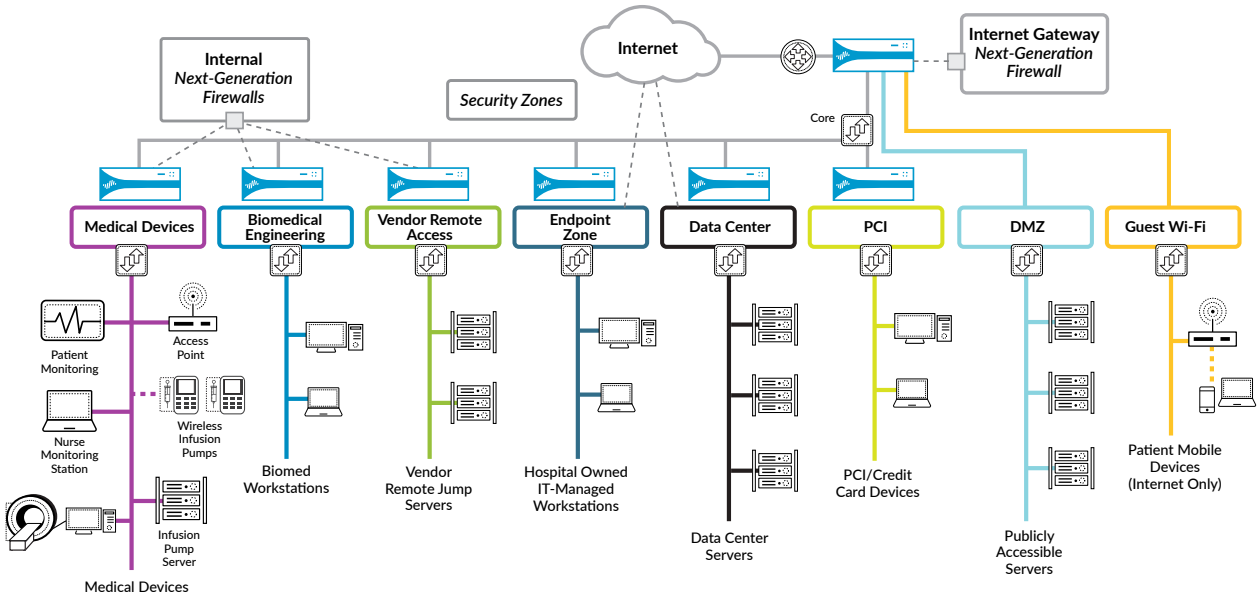


Figure 5: High-level medical device security zone architecture diagram

The three zones related to medical devices include those labeled 1) Medical Devices, 2) Biomedical Engineering and 3) Vendor Remote Access.

- The Medical Devices zone includes all medical devices, both wired and wireless.
- The Biomedical Engineering zone includes all workstations used by the staff dedicated to supporting medical devices, typically referred to as the Biomed Engineering team. This zone can also include PCs used by hospital staff to analyze data generated by medical devices.
- The Vendor Remote Access zone is intended to contain the jump servers that vendors, like medical device manufacturers, access as intermediary servers from which they can remotely access and manage individual medical devices.

The security policies that define data flows allowed through each of these zones follow a Zero Trust model. All network traffic between the zones is blocked by default. Only application traffic (with App-ID) and users (with User-ID) that are explicitly allowed are permitted.

Common Inter-Zone Data Flows to Consider

Below are some data flows that should be considered as the zones and associated security policies are defined in the next-generation firewall. Note that Dynamic Address Groups in PAN-OS® make it easy to group devices in PAN-OS and automatically adapt to changes – adds, moves or deletions of devices based on some defined criteria (like a range of IP addresses).

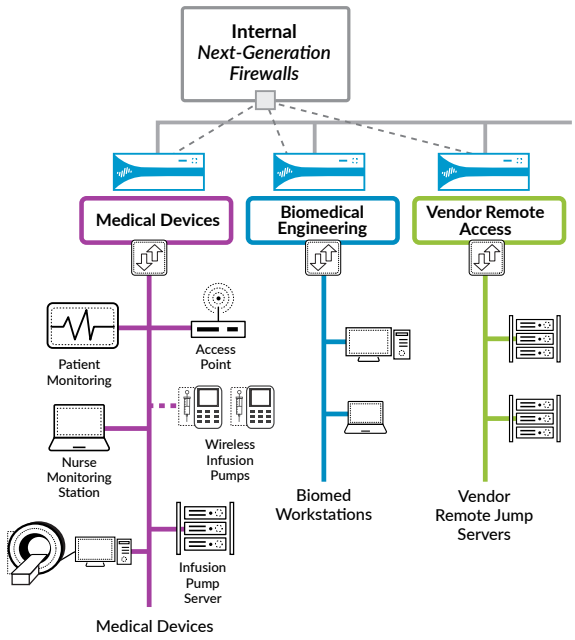


Figure 6: Close-up on medical device-related security zones

Example Data Flow Requirement	Zone-to-Zone Security Policy in Security Platform

Medical devices transmit data to EHR application to be linked with user's medical record	• Configure two Dynamic Address Groups:
	  · One contains a group of approved medical devices
	  · One contains EHR servers in the data center zone
	• Create a security policy to allow specific App-IDs between both Dynamic Address Groups

Medical devices transmit data to PCs in Biomed Engineering zone for analysis by techs and doctors	• Configure two Dynamic Address Groups:
	  · One contains a group of approved medical devices
	  · One contains Biomed Eng. PCs in the Biomedical Engineering zone
	• Create a security policy to allow specific App-IDs between both Dynamic Address Groups

Medical device manufacturers remotely manage a group of medical devices	Require the vendor to use GlobalProtect client • Configure a security policy to assign vendors access to an individual jump server in the Vendor Remote Access zone (based on security group in enterprise directory) • Configure a Dynamic Address Group for a group of medical devices • Configure a policy to allow certain App-IDs (e.g., RDP) from the jump server the jump Vendor Remote Access zone to the Dynamic Address Group of devices
Wireless devices connect to a server (e.g., wireless infusion pumps connect to an infusion pump server) to access drug libraries and to report diagnostics and therapy statistics	• No security policy required as this traffic is internal zone traffic and hence does not pass through the next-generation firewall

Figure 6: Example data flow requirements mapped to possible security policies in the security platform

As the previous sections have pointed out, the next-generation firewall enforces traffic flows between zones using a combination of App-ID, User-ID and Dynamic Address Groups to create security policies that are easy to understand and maintain. However, customers often inquire how traffic within a zone can be restricted at the access switch level (Layer 2) – closer to the device than the firewall level. Such Layer 2 controls are required to meet more restrictive policies, such as limiting the ability for medical devices on the same switch and VLAN to communicate. The next section outlines different options available to hospitals to achieve these requirements.

Options for Controlling Layer 2 Data Flows

Refer to the following table for options to achieve further control of data flows at the access switch level (Layer 2), typically downstream from the next-generation firewall.

Option 1 – Create a VLAN for each medical device type The most common approach followed by hospitals to segment within their medical device zone is to create additional VLANs (and zones) – with a dedicated VLAN for each medical device type (e.g., infusion pumps and MRI machines each have a dedicated VLAN and zone). Any VLAN-to-VLAN traffic is trunked upstream to the next-generation firewall for Layer 3 inspection. Mid-sized hospitals could expect to have 20 to 30 VLANs and zones dedicated to medical devices. **Most Common Approach**	**Advantages:** • Most straightforward option to provide adequate segmentation with the least management overhead. **Disadvantages:** • Intra-VLAN traffic (i.e., data between medical devices of the same type) is not controlled because it does not pass through the next-generation firewall. • VLAN assignments do not follow the device on a wired network. If a device is moved, the port VLAN assignment on the switch must be updated.
Option 2 – ACLs on the Access Switch Use ACLs on the access switch to control traffic, rather than VLANs.	**Advantages:** • Capable of providing fine-grained restrictions on a per-device basis. **Disadvantages:** • Difficult to maintain; often results in a significant volume of ACLs that quickly becomes too unwieldy to manage. Large hospital networks struggle to manage the "ACL explosion" effect of this option. • No intra-VLAN threat prevention capability to prevent malware from spreading directly to other medical devices.
Option 3 – Deploy small form factor next-generation firewalls at each access switch Achieve switch-level enforcement by attaching an appropriately sized next-generation firewall to each access switch.	**Advantages:** • Next-generation security features prevent threats like malware from spreading between medical devices. **Disadvantages:** • May be cost-prohibitive depending on the number of access switches to which medical devices connect.

Option 4 – Deploy ForeScout to automate VLAN assignment at access switch-level and integrate with NGFW

ForeScout® integrates with upstream next-generation firewalls for automatic segmentation and quarantining of infected devices.

ForeScout CounterACT® integrates directly with access switches to perform NAC-like activities. CounterACT can see, control and orchestrate responses when medical devices are connected to the network.

Dynamically Apply Network Segmentation
ForeScout and Palo Alto Networks integration enables hospitals to dynamically segment the network and automate policy actions between the products.

When a medical device is plugged into the network, CounterACT recognizes the device's type and communicates with the next-generation firewall to automatically populate Dynamic Address Groups with tags for network segmentation.

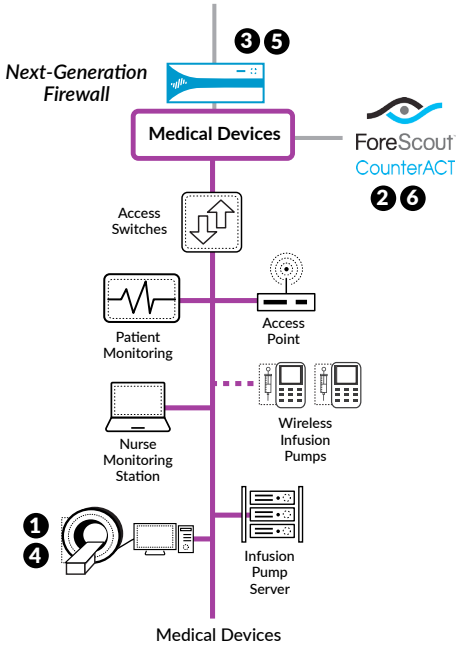
Automatically Quarantine Infected Devices
If the next-generation firewall or WildFire detects a medical device is infected, CounterACT is notified, and can be configured to quarantine the device on the network, preventing malware from spreading.

Advantages:

- Highest degree of automation and threat prevention.
- VLAN assignments "follow" devices as they are plugged into different network ports on the network.
- Excellent threat prevention – next-generation security features prevent threats like malware from spreading between medical devices.
- Significant reduction in maintenance – solves the "ACL explosion" issue of previous options by automatically classifying medical devices (via CounterACT) and placing them into an appropriate VLAN and next-generation firewall zone.

Disadvantages:

- May be cost-prohibitive depending on the number of access switches to which medical devices connect.



Scenario 1: Automatic Network Segmentation for Different Types of Medical Devices

1. Different types of medical devices connect to the network.
2. ForeScout CounterACT automatically detects, classifies and categorizes medical devices based on their identity, function, etc.
3. ForeScout Extended Module then registers the medical device in a Dynamic Address Group with tags, along with information like function, compliance, etc. with Palo Alto Networks Next-Generation Firewall.
4. NGFW leverages this information from ForeScout to provide access based on predefined policies. Untrusted devices are blocked, and medical devices are limited only to their functional needs.

Scenario 2: Automatic Network Quarantine for Medical Devices

5. Next-generation firewall determines a medical device is infected with malware and notifies CounterACT.
6. ForeScout CounterACT quarantines the medical device on the network, preventing further spread to other devices.

Figure 7: Palo Alto Networks Next-Generation Firewall integration with ForeScout CounterACT

Real-World Hospital Customer Deployment

Fisher-Titus Medical Center provides comprehensive, state-of-the-art healthcare services for more than 70,000 residents throughout North Central Ohio. Its full continuum of care includes a 99-bed acute care hospital, a 69-bed skilled nursing facility, a 48-unit assisted living facility, a Home Health Center and outpatient services. Fisher-Titus Medical Center is a nonprofit community hospital that leverages technology extensively to enhance patient care and drive administrative efficiency. Potential vulnerabilities in its medical devices, increased cyberthreats and an expanding facility prompted the medical center to replace its end-of-life Juniper Networks® firewalls and scale out with Palo Alto Networks Next-Generation Security Platform.

The medical center defined multiple VLANs and zones for different types of medical devices and locations. They now have specific policies in place on the next-generation firewall that define which medical devices can communicate with each other. Using a careful mix of VLANs and zones that worked for them, they have been able to minimize the amount of ACL maintenance, and develop a repeatable process to deploy medical devices safely and securely onto their network.

FISHER | TITUS MEDICAL CENTER
Simply Smarter Care

"Our traditional firewalls blocked traffic just based on services and ports. You couldn't get clear visibility into what applications the medical devices were running, so it was easy for a malicious program to slip through the cracks."

– Dylan Border
Lead Project Engineer

Read the whole customer story here

The security team has a granular view of known good traffic as well as known malicious or suspicious traffic that can be quickly and easily addressed with new policies. Plus, with features like App-ID and User-ID, the team can manage which applications and systems individual users are permitted to access based on their roles.

Implementation Overview

Products:

- Palo Alto Networks Next-Generation Firewall
- Subscriptions: URL Filtering, Threat Prevention, WildFire (optional)

How you will do it:

Phased Deployment Plan: As with any large-scale technology deployment, it is best to introduce the next-generation firewall in phases with increasing coverage and control. Often in healthcare organizations with multiple locations, next-generation firewalls are deployed in phases by location, starting with less critical segments.

Define VLANs, Zones and Scope for Phases: Securing medical devices is typically one of many use cases in scope for a next-generation firewall deployment as they are only one of many types of devices in a hospital network that should be segmented. First, inventory the high-level categories of devices deployed on the network, and identify a zone for each (see Figure 4). Once you know how many zones you want, formally document it for stakeholder approval. You will want approval/agreement on 1) the as-is VLAN/zone architecture, 2) how the architecture changes throughout the phases and 3) the end state.

Spend some time with your network and security architects to carefully weigh the pros and cons of each of the options outlined in the section above, "Options for Controlling Layer 2 Data Flows," if there is a desire to mitigate the risk of intra-VLAN (or medical-device-to-medical-device) traffic.

Migration of a flat legacy hospital environment to a highly segmented one will require careful planning, change management and an adequate amount of time to avoid the bad publicity that could derail the project. It is worth the effort, though – especially once the automation of the platform shows its value.

Benefits of Using Palo Alto Networks to Protect Medical Devices

Business Benefits

- Decrease risk to patients undergoing treatment via medical devices
- Prevent undesired applications and malicious content in medical device network
- Improve compliance with HIPAA, GDPR and other applicable data protection regulations

Operational Benefits

- Improve visibility into network traffic traversing medical devices
- More easily maintain medical device network segments through simplified security policies
- Reduce network latency and downtime, particularly for time-sensitive medical applications

Security Benefits

- Reduce risk of successful cyberattacks, including exfiltration of ePHI
- Prevent infected medical devices from mounting attacks against other systems – most commonly ransomware or exfiltration of ePHI off the network

Conclusion

Hospitals and other healthcare providers will continue to be targeted by cyberattackers looking to either exfiltrate PHI data from the hospital network or launch ransomware attacks. Medical devices are especially at risk for cyberattacks due to many contributing factors. A comprehensive security strategy for healthcare organizations requires special consideration for detecting and preventing attacks on medical devices. Palo Alto Networks Next-Generation Security Platform provides the most effective approach, with integrated core security capabilities and flexible segmentation based on application identification (via App-ID) and user identification (via User-ID). With a comprehensive segmentation approach that supports the ever-expanding types of medical devices and the vast internet of medical things, healthcare organizations can effectively mitigate many of the threats facing their devices while maintaining the high quality of care patients expect.

paloalto NETWORKS®

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com