The Right Approach to Zero Trust for Medical IoT Devices
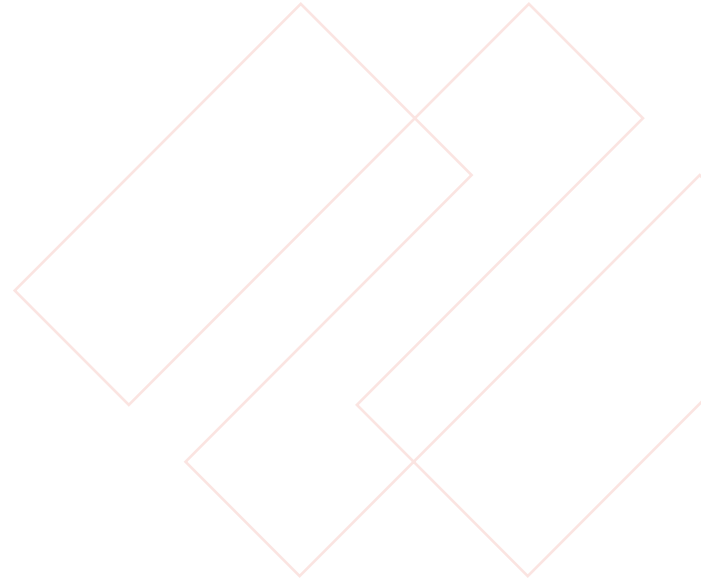
Table of Contents

Introduction

Medical IoT devices are revolutionizing healthcare. The demand for connected medical devices that support functional areas such as remote patient monitoring and contact tracing has escalated since the pandemic. But even before its onslaught, IoT adoption in healthcare was on the rise. As the industry rapidly adopts new and innovative clinical IoT devices (e.g., sensors, monitoring devices), exposure to cyberthreats grows. The healthcare industry continues to be a top target for threat actors.

And the growth is forecasted to continue with an expected 1.3B medical IoT devices by 2030, representing a 244% increase in 10 years according to the Gartner Machina IoT Forecast database.

46%
Infusion
Pumps

19%
Medical Imaging
Systems
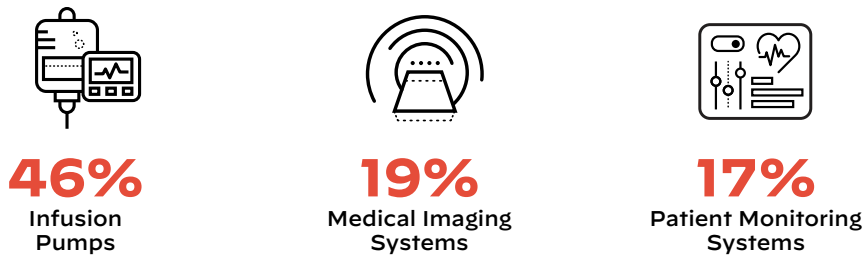
17%
Patient Monitoring
Systems

Figure 1: Most deployed medical IoT devices

Across the healthcare industry, the security risk exposure of these connected medical devices is high. Palo Alto Networks Unit 42 IoT Threat Report found that:

- 83% of medical imaging systems run on unsupported operating systems.
- 75% of infusion pumps have unpatched vulnerabilities.
- 72% of healthcare providers have a mix of IT and medical IoT devices in the same VLANs.
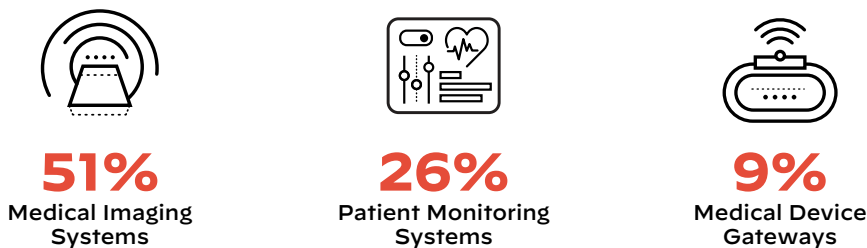
51%
Medical Imaging
Systems

26%
Patient Monitoring
Systems

9%
Medical Device
Gateways

Figure 2: Medical IoT devices with the most security issues

Security approaches historically employed by networking and security teams cannot effectively protect connected medical devices. These systems relied on protections at the network perimeter to secure organizations across the healthcare industry. The internal network was deemed trusted and secure, and application traffic could flow unrestricted. With the rise of connected medical devices and other changes, such as cloud migration and hybrid work, the traditional network perimeter is no longer a circle of trust.

To provide adequate security, the healthcare industry must account for all types of devices accessing the network, from conventional IT devices to connected medical devices and other IoT devices. The way to do this is by adopting a Zero Trust approach to security and applying it to all connected devices and systems.

What Is Zero Trust Security

Zero Trust is a cybersecurity strategy that protects an organization by eliminating implicit trust and continuously validating every stage of digital interaction. The Zero Trust security approach is based on the principle that no user, device, or transaction from inside or outside the network can be assumed to be authorized. Eliminating implicit trust through a Zero Trust approach promotes a consistent security policy regardless of the situation. The Zero Trust framework focuses on resource protection and the premise that trust is never granted implicitly. Rather, it must be continually evaluated.

Traditional security models target the protection of the entire attack surface, which is difficult to identify and constantly evolving—especially when it includes connected medical devices. In a Zero Trust framework, a "protect surface" is defined. It comprises the most critical and valuable data, assets, applications, and services. Because it contains what is most critical to an organization's operations, the "protect surface" is orders of magnitude smaller than the attack surface and is always knowable.

Identify assets, critical data, and transaction flows

Adopt a Zero Trust architecture and "least access" controls

Continuously monitor and audit

Figure 3: Overall Zero Trust strategic objectives

Following a Zero Trust approach, only known, allowed traffic can access the "protect surface." In the case of healthcare organizations, connected medical devices should only have access to the data and applications they need to perform their tasks but nothing more. This is known as least-privileged access.

Zero Trust provides a security framework for connected medical devices that continuously validates their integrity. Zero Trust also enforces least-privileged access for connected medical devices, limiting exposure of data and applications. With Zero Trust, connected clinical devices' transactions are secure and validated to thwart cyberthreats and protect data.

Palo Alto Networks has outlined the Zero Trust framework with the following guiding principles that encompass security for all users, applications, and infrastructure within a healthcare organization across the four pillars of Identity, Device/Workload, Access, and Transaction, as represented in table 1. These are also applicable to connected medical devices.

Table 1: Key Zero Trust Capabilities and Continuous Validation				
	Identity	**Device/Workload**	**Access**	**Transaction**
Zero Trust for Users	Validate users with strong authentication	Verify user device integrity	Enforce least-privileged user access to data and applications	Scan all content for malicious activity and data theft
Zero Trust for Applications	Validate developers, DevOps, and admins with strong authentication	Verify workload integrity	Enforce least-privileged access for workloads accessing other workloads	Scan all content for malicious activity and data theft
Zero Trust for Infrastructure	Validate all users with access to the infrastructure	Identify all devices including IoT	Least-privileged access segmentation for native and third-party infrastructure	Scan all content within the infrastructure for malicious activity and data theft

Securing unmanaged IoT devices is essential to achieving Zero Trust for infrastructure. These guiding principles help define actionable Zero Trust security for connected clinical devices within a healthcare organization's infrastructure.

The Right Approach to Zero Trust for Connected Medical Devices

The Zero Trust guiding principles outlined in the previous section translate into further granular guiding principles specific to achieving Zero Trust for connected medical devices. Table two presents a Zero Trust framework organizations should consider for securing connected clinical devices.

Table 2: Zero Trust for Infrastructure Extended to Medical IoT Devices		
Device/Workload	**Access**	**Transaction**
Discover all medical IoT devices	Recommend Zero Trust policies	Continuously monitor medical IoT and other IoT devices
Assess medical and IoT security risk	Enforce Zero Trust policies	Prevent known and unknown threats

Challenges in Implementing Zero Trust Security for Connected Medical Devices

While connected clinical devices revolutionize healthcare, they also bring problems that put patients and organizations at risk. The following are several of the many challenges that plague managing the security of connected medical devices:

- **You can't secure what you can't see**. Lack of clear visibility into medical and other unmanaged IoT devices and no clear understanding of their risk exposure.
- **Unseen vulnerabilities create exponential risk**. Manual, error-prone methods to applying security policies to IoMT devices.
- **Threats are outpacing your ability to stop them**. The fact that 82% of IoMT devices experienced an attack in 2021 illustrates that current security mechanisms are unable to defend against threats to the medical device infrastructure.
- **Legacy security architectures hinder compliance with regulatory compliance**. Managing multiple point security products and cross-product workflows is time-consuming and complex, delaying security compliance.

Addressing Challenges with Zero Trust for Connected Medical Devices

Palo Alto Networks Medical IoT Security brings clinical and operational devices into the Zero Trust Model fold and addresses these challenges following principles based on three core areas:

1. Complete and accurate device discovery and risk assessment
2. Recommendation and enforcement of least access policy
3. Continuous monitoring and threat prevention

With alignment under the Zero Trust framework, these principles minimize connected clinical device security risks to keep your healthcare organization safe from cyberattacks and protect patients' health and privacy. Palo Alto Networks has made it exceedingly easy to achieve Zero Trust for clinical IoT devices, thus elevating organizations' overall security posture. The following is the Palo Alto Networks practical approach to how organizations can achieve Zero Trust for connected medical devices.

Zero Trust Principle One: Identify Devices and Assess Risk

Device Discovery

You can't secure what you can't see. To extend the principles of Zero Trust to connected medical devices, it is essential to go beyond standard IT devices to include all unmanaged IoT and connected medical devices in the network. Medical IoT Security from Palo Alto Networks is the only agentless connected

medical device security solution that uses machine learning (ML) and deep packet inspection with crowdsourced telemetry to discover and classify every connected device in the network, including the never-seen-before ones.

ML is not only a superior approach as compared to the reactive, traditional, signature-based methods of device discovery; it is critical to achieving Zero Trust security. The volume of clinical devices unknown to IT is staggering, and the growth continues. In just the last five years, the U.S. Food and Drug Administration (FDA) approved 220 new healthcare device types. Using an ML-powered device discovery approach ensures that the new devices are quickly and accurately discovered and classified in real time. It provides an approach that addresses the challenges associated with new connected medical devices being added to the network.

Our Medical IoT Security analyzes 200 parameters to accurately match each connected medical device's IP address with its type, vendor, and model to surface 50+ essential device attributes that completely profile the device. Accurate and granular device classification is necessary to differentiate unmanaged connected medical devices from managed IT assets. Doing that enables enforcement of Zero Trust-driven security policies that only allow approved traffic across your network.

The following are the top categories of contextual information that Medical IoT Security provides.

? **What is the device**	? **What is running on the device**	? **Who owns this device**	? **Where are you connecting the device**	? **How is this device behaving**
• Ultrasound machine • CT scanner • Infusion pump • MRI machine	• Application name/version • OS name/version • Endpoint security software	• IT • BioMed • Shadow • Custom tag	• VLAN • Subnet • Wireless/Controller • Switch/Port	• Establish a baseline • Compare a device behavior with other crowdsourced devices • Communication patterns • Cloud/Network communications

Figure 4: Medical IoT Security can discover 90% of the devices within 48 hours—and more after that

Risk Assessment

The next step in applying the Zero Trust framework is to assess the risk with high confidence and determine the level of risk for connected medical devices. However, to assess risk effectively, one needs to know what it means, then classify it relative to threats and vulnerabilities.

Risk is a function of threats exploiting vulnerabilities to compromise or damage network assets. Connected medical device risk is measured using three vectors:

1. Threats
2. Vulnerabilities
3. Asset context

Medical IoT Security from Palo Alto Networks detects and assesses risk across all three vectors. This is done by leveraging crowdsourced device data, machine learning-powered device behavior anomaly assessment, proprietary Unit 42 threat research, CVEs, third-party vulnerability management information, and more.
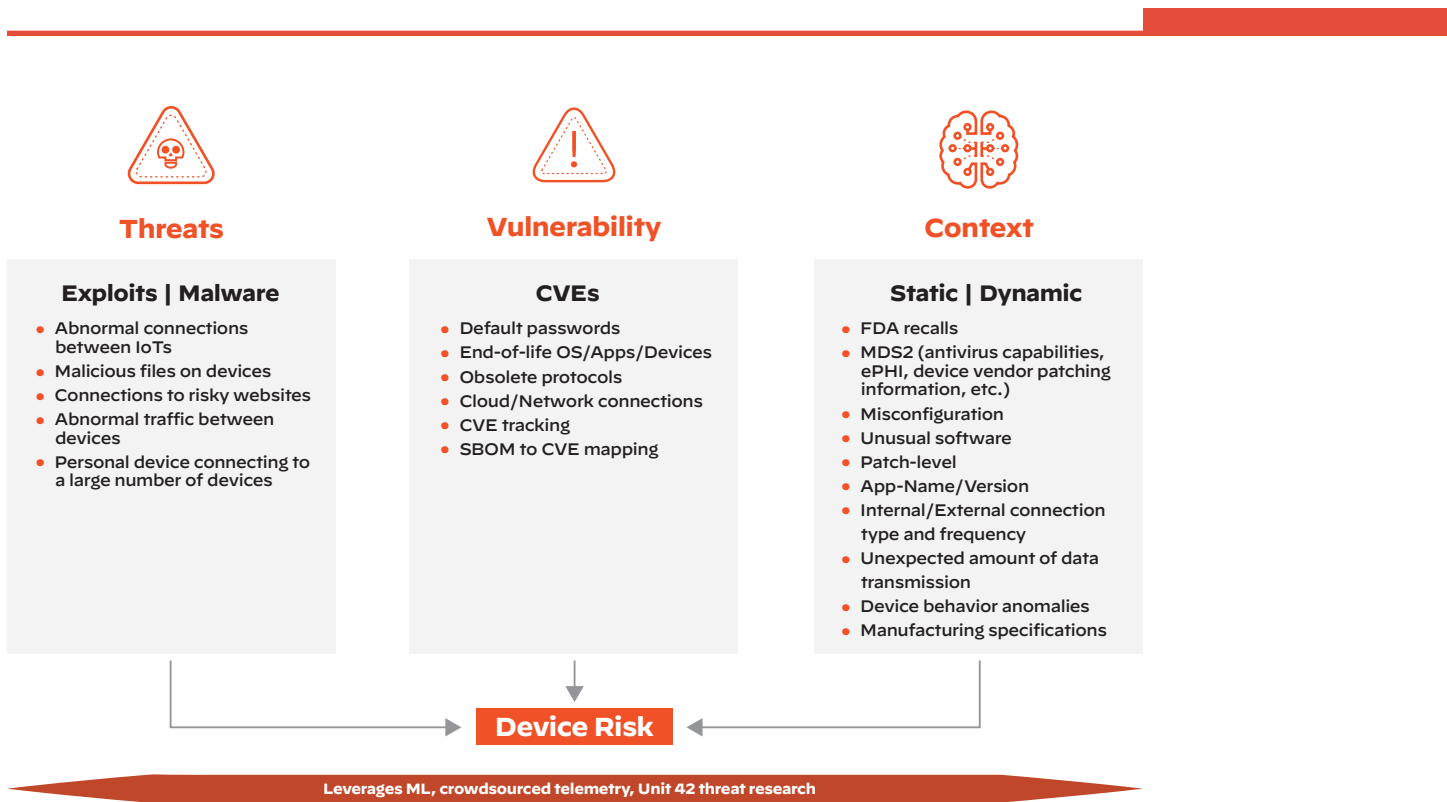
Threats

Exploits | Malware
- Abnormal connections between IoTs
- Malicious files on devices
- Connections to risky websites
- Abnormal traffic between devices
- Personal device connecting to a large number of devices

Vulnerability

CVEs
- Default passwords
- End-of-life OS/Apps/Devices
- Obsolete protocols
- Cloud/Network connections
- CVE tracking
- SBOM to CVE mapping

Context

Static | Dynamic
- FDA recalls
- MDS2 (antivirus capabilities, ePHI, device vendor patching information, etc.)
- Misconfiguration
- Unusual software
- Patch-level
- App-Name/Version
- Internal/External connection type and frequency
- Unexpected amount of data transmission
- Device behavior anomalies
- Manufacturing specifications

Device Risk

Leverages ML, crowdsourced telemetry, Unit 42 threat research

Figure 5: Medical IoT Security detects and assesses risk across these three vectors

Medical IoT Security measures risk and assigns a score for the amount of risk it observes at four levels:
1. Individual clinical IoT devices
2. Device profile
3. Site
4. Organization

When calculating the risk scores of clinical IoT device profiles, sites, and organizations, Medical IoT Security considers the scores of individual devices within a particular group and the percentage of risky devices in the group. The different scores provide a simple means to check the risk posed at various points and areas of your network.

Zero Trust Principle Two: Policy Recommendation and Enforcement

The Least Access Policy

Least-privileged access is a key tenet of Zero Trust. Least access as a Medical IoT Security policy is intended to offer a minimum level of network access to a connected medical device. Since most connected medical devices are "purpose-built" and have predictive behavior, the least access policy can be used in the following scenarios:

- **Virtual patching to keep connected medical devices operational**: The least access policy can allow even vulnerable connected clinical devices to operate by blocking or restricting their access to specific resources. This is a temporary strategy to limit the exploitation of a vulnerability while it is remediated.

- **Network access control policy**: The least access policy is also used to limit or restrict the access of connected medical devices to specific resources to carry out their required task.

Today, one has to go through multiple labor-intensive steps to define and develop risk reduction policies per device profile. The manual steps include inventorying connected medical devices, defining device profiles by device type or function, establishing behavioral baselines, defining policies that do not disrupt patient care or operations, and integrating with other technologies to enforce those policies. It also includes gathering the application usage, connection, and port/protocol data needed to create policies for each device.

Medical IoT Security from Palo Alto Networks is the only solution on the market today that goes beyond risk assessment to automatically provide least access policy recommendations. By comparing metadata across millions of connected medical devices with those found in your network, Medical IoT Security can use its device profiles to determine normal behavior patterns. Then, for each IoT device and category of devices, it provides a recommended policy to restrict or allow trusted behaviors and help implement Zero Trust strategies automatically. Once reviewed, a policy can be quickly imported by your ML-Powered NGFW, and any changes will be updated automatically, keeping your administration overhead to a minimum.

Read how you can achieve 20X time savings with automated policy creation and enforcement.

Network Segmentation Policy

Segmenting connected clinical devices can be viewed as a step toward the Zero Trust guiding principle of "never trust, always verify." For instance, housing mission-critical heart rate monitors in the same network as imaging systems would not be sound practice for healthcare organizations. A profile-based device segmentation approach that considers many factors, including device type, function, mission criticality, and threat level, provides an isolation approach that significantly reduces the potential impact of cross-infection by cyberthreats.
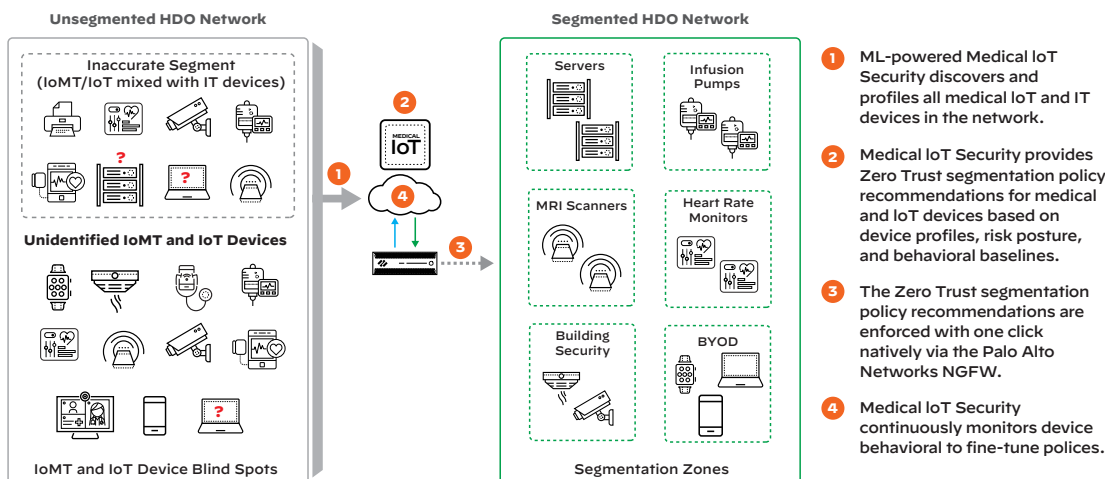

Figure 6: Segmentation workflow through Palo Alto Networks Medical IoT Security

Medical IoT Security enabled on the Palo Alto Networks Next-Generation Firewall (NGFW) takes a device profile-based fine-grained segmentation approach that considers those factors to enable sequestration. This significantly reduces the potential impact of cross-infection between IT and IoT devices. In addition, using a Palo Alto Networks NGFW as a segmentation gateway leverages its inherent networking capabilities for seamless deployment into an existing environment and allows for the controlled introduction of security controls over connected medical devices within a network.

For customers who prefer to choose a network access control (NAC) solution to segment their network, Medical IoT Security provides built-in integration with Cisco ISE, Forescout, and Aruba ClearPass to implement segmentation. Medical IoT Security provides discovered unmanaged device information to the NAC solution and provides additional device context to segment them intelligently. This addresses the limitation of NAC only having visibility in devices that can be authenticated by eliminating blind spots for connected medical devices that cannot be authenticated as they do not have users associated with them.

Table 3 shows a sample of one of our live customers showcasing how Medical IoT Security plugs in the NAC solution's visibility and context blind spots.

Table 3: How Medical IoT Security Plugs in NAC Blind Spots		
MAC	**NAC Identity**	**Medical IoT Security Identity**
00:*0:7*:73:37:5*	AmbiCom-Device	Carefusion Infusion Pump Base Station
c8:2*: *4:56:27:06	Apple-Device	Medical Workstation
08:60:6*:*8:06:83	Asus-Device	Medical Workstation
00:08:74:*2:50:*5	Dell-Device	DICOM-Viewer
00:2*:5*: 6*:06:72	HP-Device	DICOM-Imager
00:09:6*:*6:60:7*	IBM-Device	Medical Workstation
00:*0:*4:2*·*0:94	INSIDE-Technology-Device	Medical Workstation
Total Devices	**5,958**	**12,012**

Table 4: Discovered NAC and Medical IoT Security Devices	
NAC	**Medical IoT Security Identity**
Discovered devices= 5,698	Discovered devices=12,012
NAC Context= AmbiCom-Device	Medical IoT Security Context= AmbiCom Carefusion Infusion, base station

In addition, context-aware partitioning of connected medical devices ensures they have least-privileged access and connect only to required applications. It keeps them quarantined from guest and business networks and minimizes operational downtime for critical connected clinical devices by mitigating incompatibility issues that crop up between systems.

Policy Implementation

Medical IoT Security can implement the recommended Zero Trust security policies natively with its NGFW or via third-party enforcement points in two primary ways:

1. Enforce recommendations with one click via Palo Alto Networks NGFW. Our patented Device-ID policy construct tracks an individual device across the network, providing detailed information as a context within the ML-Powered NGFW for any alert or incident that may occur—regardless of changes to the device's IP address or location. In addition, policy rules and Layer 7 controls are automatically updated as the location and identified risks change. Table 5 shows how Device-ID is more scalable and provides faster remediation and response to threats.

2. Enforce the recommended policies using our NAC integrations with Cisco ISE, Forescout, or Aruba ClearPass.

Table 5: How Device-ID Helps Administrators Get Fast and Accurate Policy Implementation	
Without Device-ID	**With Device-ID**
Reliance on IP address as a proxy for device identity does not provide accurate device identity	Device identity is available within policy
Reliance on users, network, or device admins to properly address device issues is error-prone and creates an opportunity for exploitation	Consistent policy enforcement regardless of where the device is connected or how it is configured
Reliance on external systems such as NAC or asset management requires integrations to be built and maintained	Directly feed Device-ID using IoT Security, eliminating the need for complex integrations
Threat or incident investigation needs SOC to touch multiple systems to track down which specific device generated the alert	Threats alert with device info received by SIEM

Zero Trust Principle Three: Continuous Monitoring and Threat Prevention

Continuous Monitoring

Continuous monitoring is the final and crucial step in closing the Zero Trust security loop for connected medical devices. Even if a device has been profiled and placed in the correct segment, it could still be compromised during its connection to the network. If a connected medical device is compromised, its access to the resources and the network is immediately blocked.

Our ML-based Medical IoT Security automatically ascertains a connected medical device's identity and verifies normal behaviors. Once normal behaviors are established, the solution kicks in anomaly detection to uncover and prioritize any potential deviation from the baseline. Our machine learning establishes a baseline of Layer 7 connected medical device behaviors and provides two types of insights:

1. Medical IoT Security uses ML to compare the behaviors with similar crowdsourced devices to establish a behavior baseline and monitor deviation continually. This information helps automate Zero Trust policy creation.

2. Medical IoT Security also monitors device traffic and communication patterns and continually contrasts them against existing VLAN designs to simulate the right microsegmentation design and, after that, enforcement.

Connected medical devices generate unique, identifiable patterns of network behavior. Using machine learning and AI, Medical IoT Security recognizes these behaviors and identifies every device on the network. It then creates a rich context-aware inventory that is dynamically maintained and always up to date.

After identifying a device and establishing a baseline of its normal network activities, Medical IoT Security monitors network activity to detect any unusual behavior indicative of an attack or breach. If suspicious activity is detected, Medical IoT Security notifies administrators through security alerts in the portal. Medical IoT Security also blocks devices that are not compliant with the established security and compliance policy from accessing the network.

Built-in Prevention

Medical IoT Security monitors all connected clinical devices and stops all threats with the industry's leading IPS, malware analysis, web, and DNS prevention technology. Seamlessly integrated with Medical IoT Security, our Cloud-Delivered Security Services coordinate intelligence to prevent all threats from connected medical devices without increasing the workload for your security personnel. To decrease response times, connected clinical devices with validated threats can be dynamically isolated upon detection of threats by our ML-Powered NGFWs. This gives your security team time to form remediation plans without the risk of further infection from those devices.
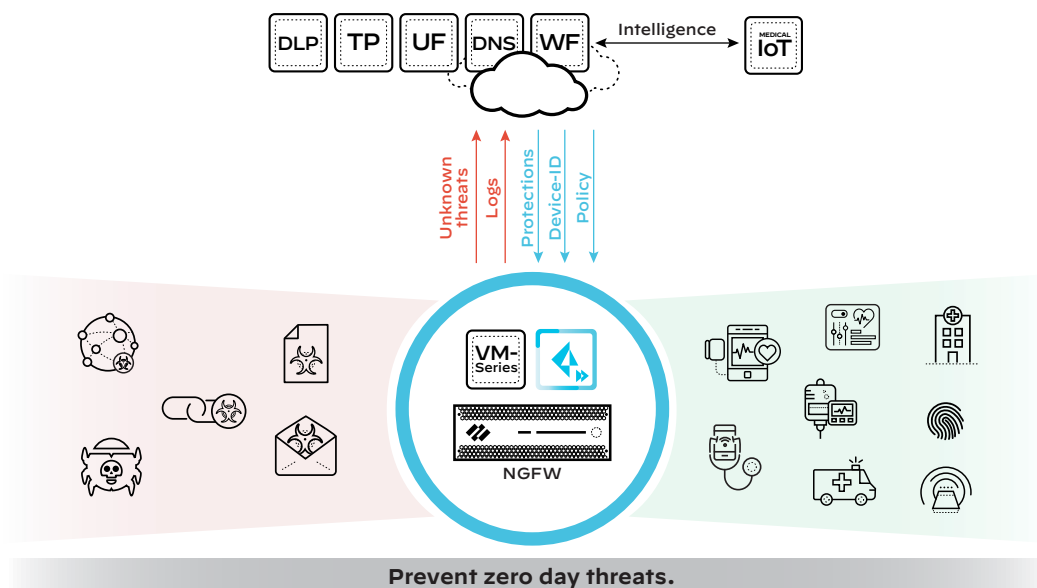

Figure 7: Medical IoT Security built-in threat prevention

Zero Trust for All Connected Devices in Healthcare Organizations' Ecosystems

Breaches and operational stoppage can have serious consequences for healthcare organizations and their patients. Zero Trust provides the framework needed to protect healthcare organizations from cyberthreats by limiting the network access capabilities of connected medical devices.

The Palo Alto Networks Zero Trust approach is the most comprehensive security for connected medical devices. By applying the principle of least-privileged access to connected clinical devices, the Palo Alto Networks Zero Trust approach allows healthcare organizations to extract the maximum benefit from all clinical and operational devices with the least risk of exposure to cyberthreats. Request a demo and see for yourself how Palo Alto Networks Medical IoT Security significantly simplifies the adoption of the Zero Trust framework for unmanaged medical IoT devices.