paloalto NETWORKS

The Healthcare CISO's Guide to Medical IoT Security

A Six-Step Approach to Medical Device Security & Workflow Management

Table of Contents

Adoption of Medical IoT in Healthcare Organizations Continues to Surge

Gaining momentum during the pandemic, the expanded use of connected medical devices has become a fundamental part of the healthcare system.

Medical IoT's irrevocable transformation of the healthcare industry was evident after the pandemic. With steady growth over the past decade, connected medical device use has exploded. Medical IoT devices are now routinely used across the continuum of care. However, security for these connected devices has lagged.

Across the healthcare industry, the security risk exposure of IoT devices is high.

- **41%** of attacks exploit vulnerabilities in IoT devices
- **57%** of medium to high severity attacks occur on medical IoT devices
- **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 clinical IoT devices in the same VLANs

"The number of healthcare records exposed in data breaches increased in 1H, 2022 to 279, up 217.33% from 2H, 2021, and 422.53% from 1H, 2021."

Source:
2022 Healthcare Data Breach Report, HIPAA Journal
Unit 42 IoT Threat Report

Most Deployed Medical IoT Devices

46%
Infusion Pumps

19%
Medical Imaging Systems

17%
Patient Imaging Systems

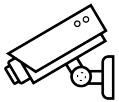
Medical IoT Devices with the Most Security Issues

51%
Medical Imaging Systems

26%
Patient Imaging Systems

9%
Medical Device Gateways

Generic IoT Devices with the Most Security Issues found in Healthcare Organizations



33%
Security Cameras

24%
Printers

Trust-Based Security Is the Weakest Link

Medical IoT devices provide a tremendously expanded attack surface with a remarkably low barrier to entry for cyber attackers. Healthcare providers must adopt a new security paradigm to combat these threats.

Several of the many factors that put medical IoT devices at elevated risk are:

- Legacy operating systems
- Unsegmented networks
- Pre-existing vulnerabilities
- Elusive device discovery and identification
- Authentication challenges

"53% of connected medical devices and other healthcare IoT devices have at least one unaddressed critical vulnerability that could potentially be exploited to gain access to networks and sensitive data or affect the availability of the devices.

Source: HIPAA Journal, January 2022

"Despite the explosion of medical IoT devices, security remains a challenge. According to Gartner, "Today, most solutions in the space take a reactive approach to medical device security."

Source: Market Guide for Medical Device Security Solutions, March 2022

Most existing security systems depend on trusting the connected users, applications, and devices. Because of this, application traffic can flow unrestricted—including that generated from connected medical devices. With the rise of clinical IoT devices and other changes, such as cloud migration and hybrid work, the traditional network perimeter is no longer a circle of trust.

With healthcare now a top target for cybercriminals, the millions of clinical IoT devices that collect and store sensitive data are vulnerable to attack. According to the American Hospital Association, "stolen health records may sell up to 10 times or more than stolen credit card numbers on the dark web."

SOURCE: Unit 42 IoT Threat Report

Implicit Trust Must Be Eliminated

Traditional security models target the protection of the entire attack surface, which is difficult to identify and constantly evolving—especially when it includes medical IoT devices. In addition, this requires opening broad access and creates vulnerabilities.

To effectively defend against persistent threats, healthcare providers need to eliminate implicit trust in all systems and people granted network access. Limiting access to resources and continually evaluating anyone or anything with authorization can protect the vast attack surfaces in healthcare organizations.

Health and Human Services Reports Healthcare Threat Is Increasing

June 2022 saw 70 healthcare data breaches of 500 or more records reported to the Department of Health and Human Services' Office for Civil Rights (OCR) – two fewer than May and one fewer than June 2021. Over the past 12 months, from July 2021 to June 2022, 692 large healthcare data breaches have been reported, and the records of 42,431,699 individuals have been exposed or impermissibly disclosed. The past two months have seen data breaches reported at well over the 12-month average of 57.67 breaches a month.

HIPAA Journal on Jul 20, 2022

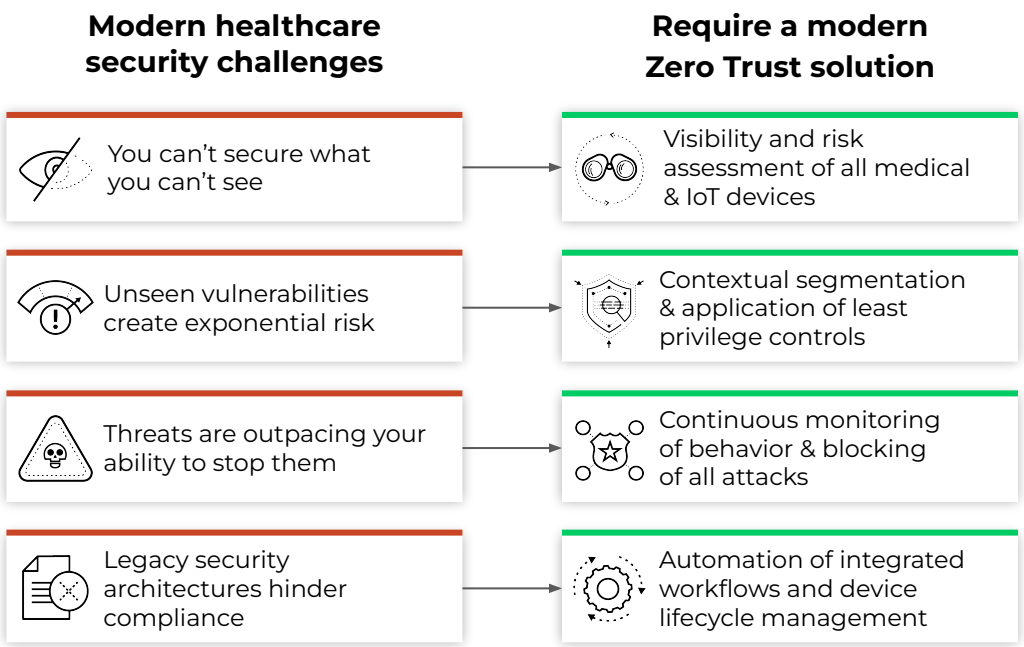
Use Zero Trust as a Foundation for Security

Zero Trust enforces least-privileged access for connected medical devices, limiting exposure of data and applications.

Zero Trust provides a security framework for connected medical devices that continuously validates their integrity. With Zero Trust, clinical IoT devices' transactions are secure and validated to thwart cyberthreats and protect data.

Areas of focus when applying a Zero Trust strategy to protect medical IoT devices are:

- Identify all medical IoT devices and workloads and assess risk.
- Limit access by applying least access and network segmentation policies.
- Continuously monitor all connected medical devices and block any that show signs of unusual behavior.

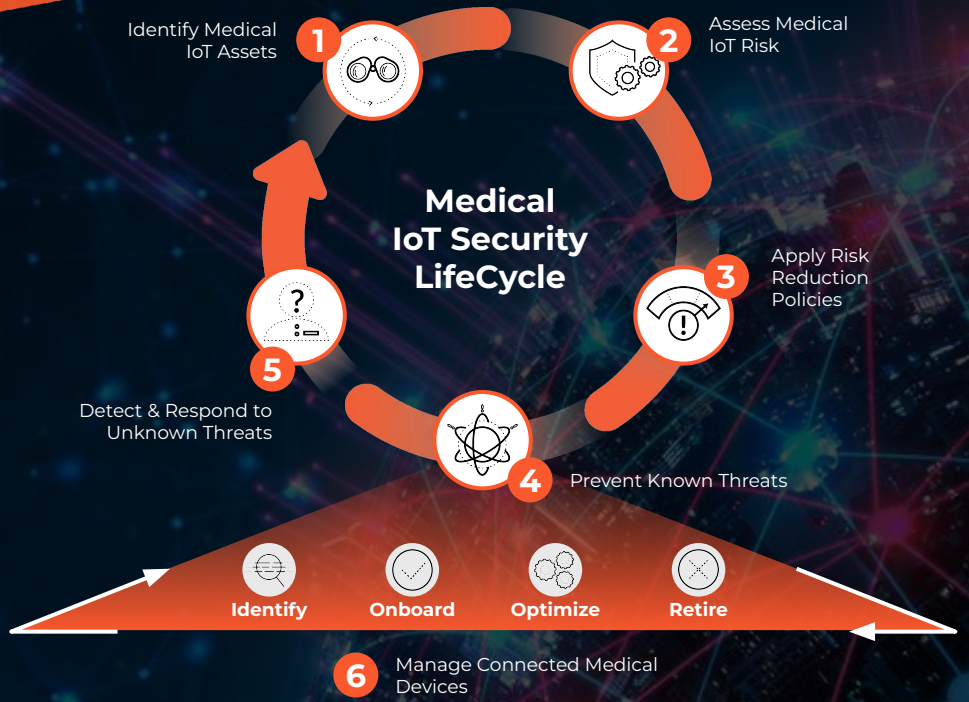


Implement a Proven Process to Secure and Manage Medical IoT Devices

Secure network-connected device workflows in six steps that cover the entire device lifecycle and support a zero-trust security framework.

Connected medical devices need to be understood in the context of a complete clinical device management methodology to minimize risk to patients and the network. The ideal methodology relieves both network security and clinical teams from the day-to-day operational burdens of securing and managing these devices.

1. Identify medical IoT assets
2. Assess medical IoT risks
3. Apply risk reduction policies
4. Prevent known threats
5. Detect and respond to unknown threats
6. Manage connected medical devices



To implement the IoT Security lifecycle, look for **6 must-haves** in your medical IoT security solution.

1. Identify Medical IoT Assets

Get complete visibility into all connected medical devices in the healthcare organization.

The medical IoT lifecycle begins with determining the state of your security posture by gaining complete visibility into the attack surface. Collect an up-to-date inventory of all connected medical devices. This includes the ones you are aware and not aware of—and even those forgotten. During this device discovery process, the Medical IoT Security solution will capture essential device attributes to provide full context on each medical device.

Employing medical IoT device discovery allows all IT and business stakeholders to get a full picture of what the connected medical device asset landscape looks like in your healthcare organization.

An ideal connected medical device security solution should do the following:

- Identify at least 90%+ of devices in visible segments within 48 hours.
- Detect new, never-seen-before devices with ML-based device classification to categorize devices by a variety of classifications, including vendor, make, model, type, operating system, firmware, location, subnet, risk score, PHI type, and MDS2.
- Perform detection of newly plugged-in devices within minutes–not hours or weeks.
- Differentiate unmanaged medical IoT and other IoT devices from managed IT assets.
- Log all medical IoT and other IoT devices to help IT and security teams identify unmanaged devices.
- Be able to automatically update your asset management solutions, such as CMMS, ITSM, and CMDB, with rich medical IoT device information.
- Leverage multipurpose sensors that integrate into existing infrastructure.

2. Assess Medical IoT Risks

Proactively reduce risk with continual risk monitoring and assessment of connected medical devices.

In the risk assessment stage of the medical IoT security lifecycle, you must monitor connected medical devices at all times. Real-time risk monitoring, reporting, and alerting are crucial for organizations to reduce medical IoT risks proactively. Signature-based solutions lack accuracy and speed, which limits your ability to protect these assets.

Accurate risk assessment in your Medical IoT Security lifecycle lets you take a better approach. It allows your IT security teams to continuously scrutinize devices and monitor their traffic patterns to drive proactive NAC segmentation and reduce the threat surface. Risk assessment also prompts IT teams to proactively consider micro-segmenting the network by different device types and classes, such as clinical IoT or general IT, to forestall the possibility of lateral movement of threats.

An ideal connected medical device security solution should do the following:

- Leverage multiple threat feeds, such as CVE, MDS2, and RSSI, to accurately map vulnerabilities with the medical IoT inventory.
- Include Manufacturer Disclosure Statement for Medical Device Security (MDS2) specifications, such as antivirus capabilities, ePHI, FDA recalls, and vendor advisories for patching.
- Detect and report anomalies in connected medical devices that may affect risk scores—in real-time.
- Calculate risk scores on medical IoT devices and device categories.
- Track changes to risk scores and store complete device risk history for compliance purposes.
- Integrate with vulnerability management systems and device vendors for centralized medical risk management and to deliver information to security teams.

3. Apply Risk Reduction Policies

Leverage automated risk-based security policy recommendations and enforcement.

An uncomplicated connected medical device security solution will not burden you with additional infrastructure or investment. It will allow your IT security teams to simply leverage your existing next-generation firewall investment for comprehensive and integrated security posturing. With this, security policies can be automatically recommended and natively enforced based on the level of risk and, the extent of untrusted behavior detected in your clinical IoT devices.

Taking into account that trust is nothing but a vulnerability, your connected medical device security solution must directly align with the principle of zero-trust to enforce policies for least-privileged access control. This significantly reduces the pathways for adversaries, whether they are inside or outside your organization, to access your critical clinical IoT assets.

An ideal connected medical device security solution should do the following:

- Leverage multiple threat feeds, such as CVE, MDS2, and RSSI, to accurately map vulnerabilities with the medical IoT inventory.
- Include Manufacturer Disclosure Statement for Medical Device Security (MDS2) specifications, such as antivirus capabilities, ePHI, FDA recalls, and vendor advisories for patching.
- Detect and report anomalies in connected medical devices that may affect risk scores—in real-time.
- Calculate risk scores on medical IoT devices and device categories.
- Track changes to risk scores and store complete device risk history for compliance purposes.
- Integrate with vulnerability management systems and device vendors for centralized medical risk management and to deliver information to security teams.

4. Prevent Known Threats

Take swift action to mitigate risks as soon as the threat is made known.

The diverse nature of clinical IoT devices creates a highly-distributed environment in your network with numerous points of compromise. Successful outcomes of your security posturing in stage four of the Medical IoT security lifecycle will require actionable insights. It is important to have information related to the detection and prevention of known threats that impact your medical IoT devices to enable a swift response for threat mitigation.

Look for a threat prevention mechanism that uses payload-based signatures to block advanced threats. This will ensure the most up-to-date security posture and enable defense against known threats for rapid responses to anomalous medical IoT device vulnerabilities and weaknesses across your network. In addition, this type of solution will not overburden security teams with detection alerts that could be stopped.

An ideal connected medical device security solution should do the following:

- Selectively enable security threat protections based on the medical device group's risk posture.
- Detect and prevent known threats from clinical IoT malware exploits.
- Block clinical IoT malware attacks that stem from malicious websites.
- Prevent clinical IoT attacks that use DNS for command and control to steal data.
- Prohibit unknown threats to connected medical devices that are delivered via payloads.

5. Detect and Respond to Unknown Threats

Quickly detect and respond to zero-day vulnerabilities.

When it comes to detecting and preventing truly unknown threats, legacy approaches isolate the threat data that each organization receives and generates. The result of these legacy approaches is silos, which reduce the possibility of prevention. To meet the requirements of the last step in the Medical IoT Security lifecycle, your security solution should be capable of leveraging a new approach.

It needs to draw from a collective threat intelligence engine that delivers real-time malware analysis and protections from zero-day attacks. Tapping into crowdsourced data from a global community of subscribers provides collective immunity and saves your IT security team valuable time. It achieves this by leveraging information from connected medical devices, risk scores, vulnerability data, and behavioral analytics to investigate never-heard-before threats unique to your clinical IoT environment—right from the outset. This last step will also uncover potential threats missed in earlier stages and leads you into a cyclical process for continual improvement.

An ideal connected medical device security solution should do the following:

- Detect abnormal behaviors at different tiers—first at the device category level, then at the device vendor/model level, and last at the device instance level.
- Leverage crowdsourcing intelligence using machine learning enhanced with threat modeling to detect unknown threats or attacks and provide proactive notifications or actions.
- Integrate into SIEM and SOAR using a simplified playbook-based approach to orchestrate incident response and threat prevention actions.
- Connect with active medical IoT security researchers to discover any new threats as soon as information is available.

6. Manage Connected Medical Devices

Gain operational intelligence for clinical and biomedical engineering teams.

Although most medical devices never reach full utilization despite a surplus in inventory, they often require capital and operating expenditures that fuel unnecessary spending. In addition, because the FDA regulates medical devices, all software updates on them require a review by the Original Equipment Manufacturer (OEM) to validate that the software changes continue to ensure the device is safe for patient use.

Biomedical clinical teams that deal with these aspects of using or managing connected medical devices need actionable business and operational insights. This will alleviate the pain of capital planning and preventive maintenance while staying informed on when a device may be ready for patching and software upgrades. A security solution for connected medical devices can facilitate and streamline these important decisions. Operational insights derived from the connected medical device solution should also help teams identify devices, onboard them for use as required, optimize their performance based on usage data, and safely retire them in compliance with industry regulations.

An ideal connected medical device security solution should do the following:

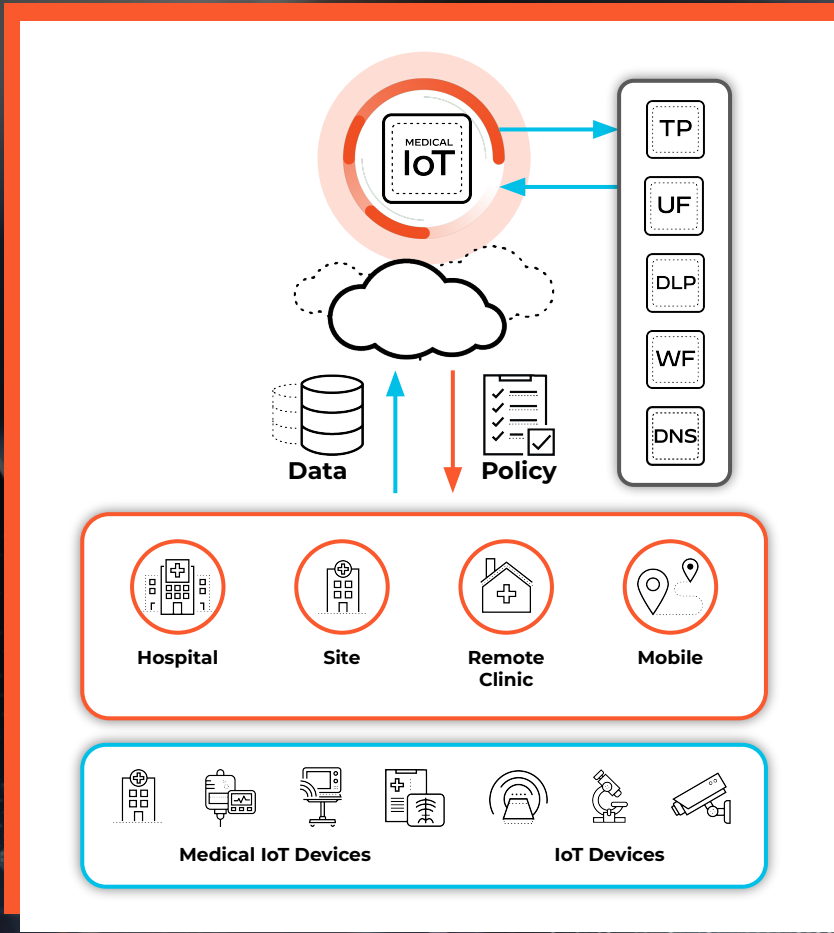
- Track and report device usage stats for individual medical IoT devices to inform decisions to purchase a new device or replace an old one.
- Identify peak usage times to schedule preventive maintenance and software updates at times that do not impact patients or others.
- Provide analytical data on imaging device usage, including which staff members are using them and how they are being used, to ensure that personnel resources are located close to the devices they use.
- Swiftly manage manufacturer notices, FDA recalls, and issues in one place without the need for manual investigation.
- Update inventory systems to keep a continuous log of devices to ensure that all other departments are aware of new and decommissioned devices.
- Protect patient records by unearthing how each device uses and stores data.
- Allow for easy onboarding and decommissioning of devices in compliance with HIPAA regulations.

Medical IoT Security for Healthcare by Palo Alto Networks

The Healthcare Industry's Most Comprehensive Zero Trust Solution for Medical IoT Security

- Provides visibility, prevention, enforcement, and operational insights in a single platform powered by machine learning.
- Uses machine learning with crowdsourcing to quickly and accurately discover all devices, even the unknown ones.
- Offers built-in prevention, instead of an alert-only approach, to keep unmanaged devices safe from all known/unknown threats and vulnerabilities by preventing threats and blocking vulnerabilities from entering your network.
- Decreases the cost of patient care with operational insights for medical teams.
- Automatically enforces policies directly or through integrations to help reduce the strain on your network and security operations teams, keep all devices safe, and increase their uptime and availability.
- Delivers medical IoT security from a single platform that can be deployed effortlessly without requiring additional infrastructure.

Palo Alto Networks Medical IoT Security, complemented with its Zero Trust framework, is the only solution in the market today that enables maximum return on investment (ROI) and patient experience. Its unique solution provides deep visibility, focused operational insights, and enhanced security for connected medical devices all in one platform.



Zero-Trust Framework by Palo Alto Networks

Provides complementary security for all users, applications, and infrastructure within a healthcare organization as well as all medical IoT devices.

	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 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

Palo Alto Networks Medical IoT Security Integrates with Third Parties

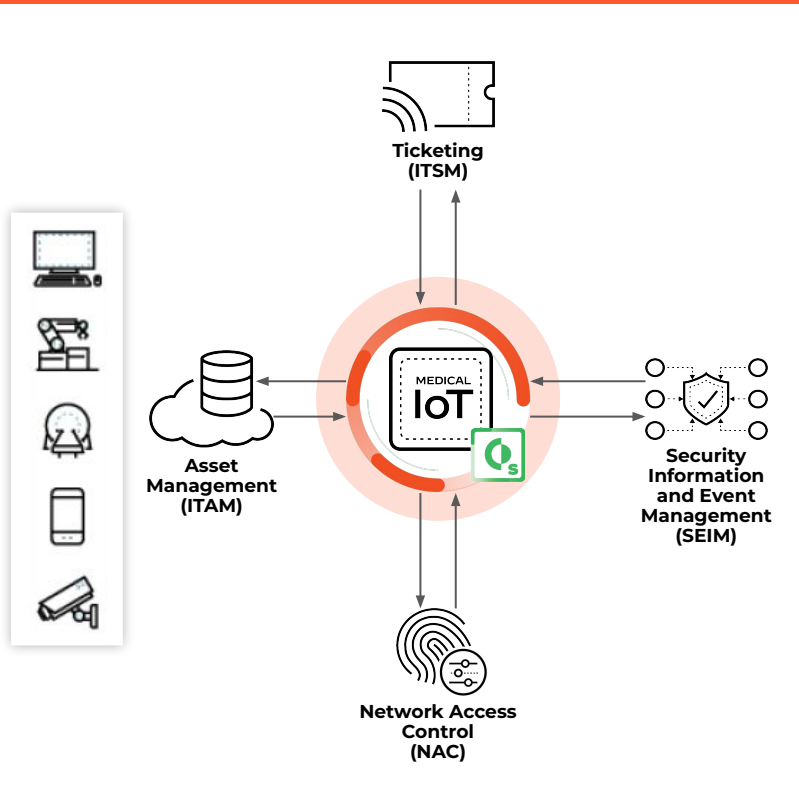
Powered by Built-in XSOAR Technology

Leverage seamless integration into your existing workflows. This eliminates resource-intensive API-led integrations and reduces the burden on infrastructure and security teams.

By leveraging native integrations from Palo Alto Networks into your existing medical IoT, IT, and security workflows, you can strengthen your current IT Service Management (ITSM), Network Access Control (NAC), Security Information and Event Management (SIEM), and other use cases.

Using a modular and customized playbook-driven orchestration, Palo Alto Networks lets your security team:

- Improve operational inefficiencies
- Enrich asset inventories
- Accurately onboard clinical IoT devices
- Enforce device controls
- Automate incident responses without having to build integrations from scratch



Leverage Your Current IT Security Team

Without the need to form a new team, deploy new infrastructure, or change existing operational processes.

Unprecedented Visibility and Protection
- ML-based connected device discovery
- Automated risk assessment
- Native security policy enforcement
- Context-aware network segmentation

Easy deployment with flexible form factor options
- Hardware firewalls
- Software firewalls
- Cloud-delivered firewalls

Full range of medical IoT, IoT, and IT device coverage
- Unmanaged medical IoT devices
- Unmanaged operational IoT devices
- Managed IT devices

Leverage leading prevention from other security services

Scale linearly as your business grows with elastic multi-tenant cloud infrastructure

Automate workflows with playbook-driven integrations

Think Medical IoT Security. Think Palo Alto Networks.

Founded in 2005, Palo Alto Networks is based in Santa Clara, California, and serves customers globally with offices worldwide.

At Palo Alto Networks our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We are at the forefront of protecting tens of thousands of organizations across clouds, networks, and devices and help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

Curious to learn more about Medical IoT Security?
Check out these resources.

"Within hours we identified thousands of devices, allowing us to implement preventive measures on activities not visible before."

Manager, Medical Device Integration & Security, BayCare

BayCare

Read the case study

www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

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