The Healthcare
CISO's Guide to IoT Security

Protect Every Device with a 6-Step Approach to Clinical and Device Workflow Management

Table of Contents

IoT Adoption in Healthcare is Surging

IoT is becoming the pulse of healthcare. The pandemic has only served to fuel this adoption.

IoT is changing healthcare. The demand for IoT 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.

Transformation in healthcare delivery by way of IoT has gained traction over the course of the past decade. During this time, IoT use cases supporting patient tracking and management, remote diagnostics, hygiene care, remote monitoring, predictive maintenance of medical devices and others made their way into the healthcare line of business.

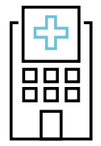
In fact, a Gartner survey analysis published in January 2020 found that 86% of responding healthcare delivery organizations (HDOs) reported an IoT solution in place for most lines of business[1]. Fast forward to now, Omdia estimates more than 250 million medical devices were introduced in the global market in 2020—with an additional 500 million expected to enter the market by 2025[2].

48%

HDOs using IoT in full scale deployments (multiple use cases and projects)[3]

31%

HDOs using IoT in single use case deployments (single use case and projects)[4]

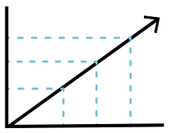


21B

IoT spend by healthcare providers in 2019[5]

54B

IoT spend by healthcare providers in 2029[6]



10%

CAGR[7]

The healthcare industry is embracing IoT with no signs of slowing down. But how well is it prepared to cope with the grave security challenges arising out this adoption trend?

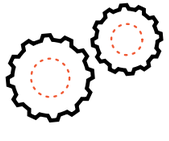
Sources:

1, 3-4 Gartner Survey Analysis: Healthcare Provider IoT Adoption Is Becoming Mainstream, 2020
2 Omdia IoT Devices Intelligence, 2020
5-7 Gartner Forecast Analysis, Healthcare Providers IoT Endpoint Electronics and Communications Revenue, Worldwide, 2020

But Security is the Weakest Link

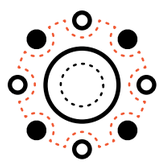
IoMT devices offer a remarkably low barrier to entry for cyber attackers, requiring a new security paradigm.

While the Internet of Things is revolutionizing healthcare, unfortunately there are challenges that need to be addressed. Security is one such challenge and remains to be the greatest barrier to adoption. Healthcare has become a target of strategic interest among cybercriminals for its valuable data, making millions of connected medical devices (IoMT) that collect and store this data vulnerable to attack. Being notoriously difficult to secure, these devices cause significant security risks, much like IoT devices.



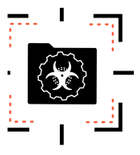
LEGACY OPERATING SYSTEMS

IoMT devices tend to run on outdated operating systems and many were never intended for connectivity so they have no built-in prevention or enforcement.



UNSEGMENTED NETWORKS

Hospital networks are often not segmented, allowing attackers to laterally contaminate an IT device and move laterally to cross-contaminate IoT devices and vice versa.



PRE-EXISTING VULNERABILITIES

Medical devices are often shipped with pre-existing vulnerabilities that are difficult to patch. With long service lives, many are neither recalled or replaced often enough.

In 2020, healthcare institutions reported 616 data breaches of 500 or more records, compromising 28,756,445 healthcare records.[8]

Did you know?

41% of attacks exploit vulnerabilities in IoT devices

57% of medium to high severity attacks occur on IoMT devices

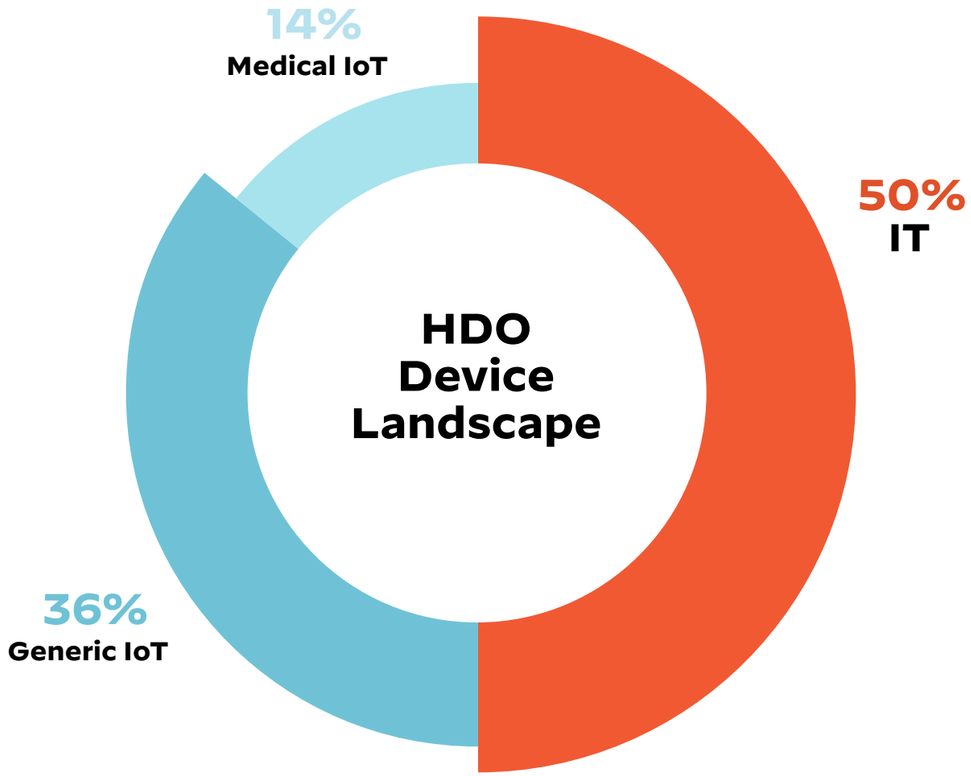
72% of healthcare VLANs mix IT and IoT/IoMT devices

83% of imaging devices have old unsupported OS, a 56% jump from 2018

Source:
2020 Unit 42 IoT Threat Report
8 HIPPA Journal 2021

The Healthcare Delivery Organization Device Landscape

IoMT devices offer a remarkably low barrier to entry for cyber attackers, requiring a new security paradigm.



50% of all devices in Healthcare Delivery Organizations (HDO) are unmanaged

Source:
Zingbox 2019 Medical Threat Report
2020 Unit 42 IoT Threat Report

Most Deployed Medical IoT Devices

46% Infusion Pumps

19% Medical Imaging Systems

17% Patient Monitoring Systems

Medical IoT Devices with the Most Security Issues

51% Medical Imaging Systems

26% Patient Monitoring Systems

9% Medical Device Gateways

Generic IoT Devices with the Most Security Issues Found in All Organizations Including HDOs

33% Security Cameras

24% Printers

10% Video Gaming Devices

Current Solutions Fail to Protect IoT in Healthcare

Outdated security mechanisms simply don't measure up when it comes to truly securing all devices—increasing workloads for the security, infrastructure and clinical teams.

Any exploited vulnerability in IoMT enables cybercriminals to take a number of malicious actions that include seizing control of the medical device, stealing sensitive patient health, personal, and insurance data, stealing proprietary clinical records, obfuscating network traffic, disrupting healthcare delivery processes, and ransoming the device to turn a profit. While the market is slowly yet surely being inundated with many IoT Security offerings, none of the solutions offered today unearth a comprehensive end-to-end security strategy that covers all the bases required to protect every medical device in your network.

These Reasons are Why Current Solutions Fail to Protect IoMT and IoT

SIGNATURE-BASED SOLUTIONS

to identifying devices lack accuracy and simply cannot scale to the numbers required to keep up with the massive proliferation of new devices or variants of devices being launched every day.

ALERT-ONLY BASED APPROACHES

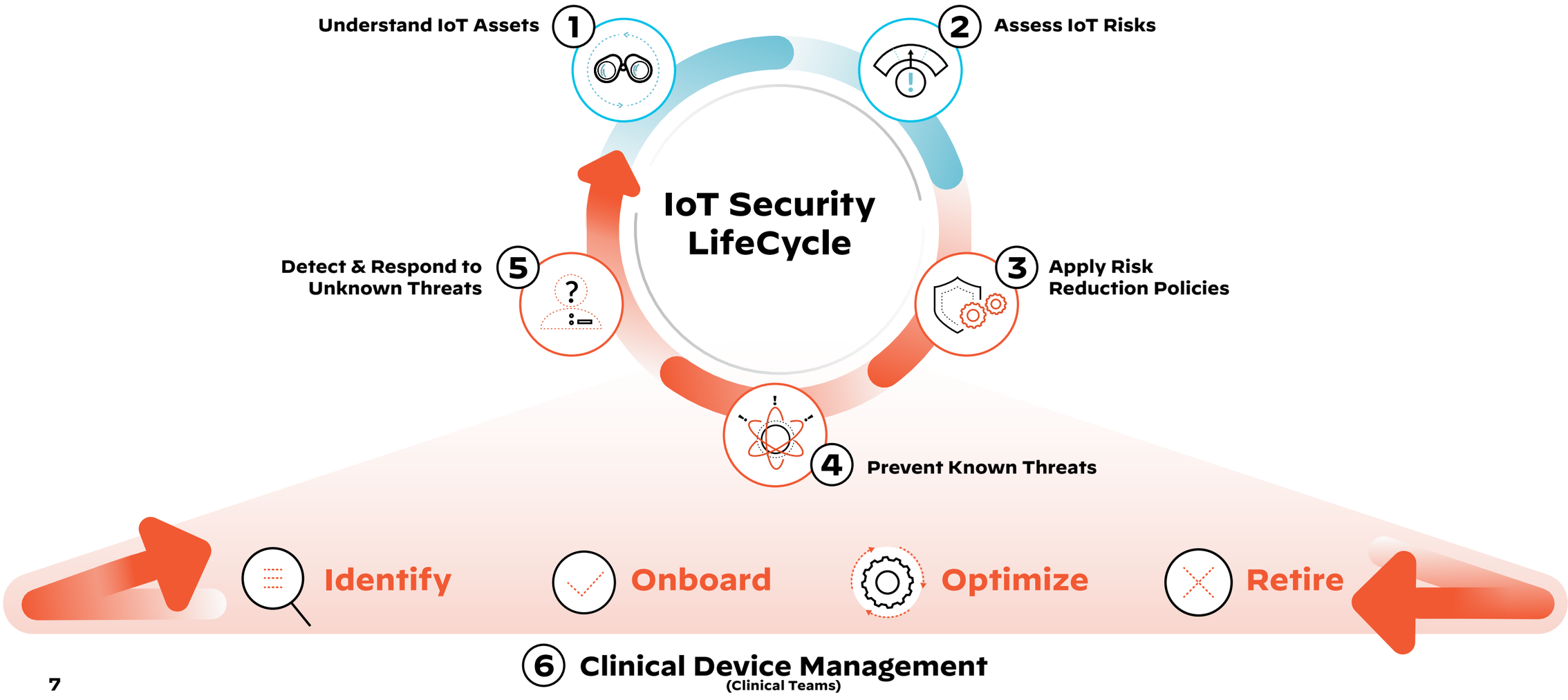
lack the capacity to recommend policies or enforce them and neither do they prevent IoMT and IoT devices from known and unknown threats.

POINT SOLUTIONS

introduce significant deployment challenges and friction by requiring you to change your network infrastructure or deploy new network sensors to process traffic and identify devices.

Take the A-Z Approach to Securing and Managing Clinical Devices

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.



Attack surfaces are widening and attack vectors are becoming more sophisticated than before. Now's the time to step up your IoMT security with a new level of sophistication.

Implement Secure Clinical and Device Workflow Management in 6 Steps

1

Get complete visibility into all IoMT Devices in your healthcare delivery organization

Complete visibility into your IoMT attack surface helps determine the state of your security posture. Your IoMT security lifecycle begins here. Employing device discovery will allow all stakeholders, IT, security and biomedical teams to get a full picture of what the IoMT asset landscape looks like in your healthcare delivery organization. Collect an up-to-date inventory of all IoMT assets, the ones you are aware and not aware of—and even those forgotten. During this device discovery process, the IoMT security solution should essential device attributes to provide full context on each medical device.

An ideal IoMT 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 vendor, make, model, type, operating system, firmware,, location, subnet, risk score, PHI type, MDS2 and more.
- ✓ Perform detection of newly plugged-in devices within minutes, not hours or weeks.
- ✓ Differentiate unmanaged IoMT and IoT devices from managed IT assets.
- ✓ Log a total of IT devices allowing IT and security teams to also identify unmanaged IT devices.
- ✓ Be able to automatically update your asset management solutions such as CMMS, ITSM and CMDB with rich IoMT device information.
- ✓ Leverage multipurpose sensors that integrate into existing infrastructure.

2

Proactively reduce risk with continual risk monitoring and assessment of IoMT devices

In the **risk assessment** stage in the IoT security lifecycle, you must actively monitor IoMT devices at all times. Real-time risk monitoring, reporting, and alerting are crucial for organizations to proactively reduce IoMT risks and threat surface. Signature-based solutions lack accuracy and speed limiting your ability to protect these assets. Accurate risk assessment in your IoT security lifecycle lets you take a better approach because 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 - IoMT, IoT or IT to forestall the possibility of lateral movement of threats.

An ideal IoMT security solution should do the following:

- Integrate with multiple threat feeds such as CVE, MDS2, RSSI, etc to accurately map vulnerabilities with the IoMT inventory.
- Include Manufacturer Disclosure Statement for Medical Device Security (MDS2) specifications like antivirus capabilities, ePHI, FDA recalls, and vendor advisories for patching.
- Detect and report anomalies in real time in IoMT devices that may affect risk scores.
- Calculate risk scores on 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 with device vendors for centralized IoMT risk management and to deliver information to security teams.

3

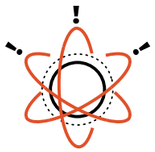
Leverage automated risk-based security policy recommendations and enforcement

An uncomplicated IoMT security solution will not burden you with additional infrastructure or investment. It would allow your IT security teams to simply leverage your existing Next-Generation Firewall investment for comprehensive and integrated security posturing. Leverage a solution that runs in conjunction with the capabilities of your firewall to **automatically recommend and natively enforce security policies** based on the level of risk and the extent of untrusted behavior detected in your IoT devices. Taking into account that trust is nothing but a vulnerability, your IoMT 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 IoT assets.

An ideal IoMT security solution should do the following:

- ✓ Provide mechanisms to convert IoMT device behavior baseline into policies that only allow trusted behaviors.
- ✓ Automate enforcement with device and application identification.
- ✓ Support both allow lists and block lists.
- ✓ Track device and application to enforce policies regardless of where they reside within the network.
- ✓ Update policies automatically once set to limit manual updates every time a change occurs.
- ✓ Integrates into NAC and automatically shares IoT device information to enforce device controls and context aware segmentation.

4



Take swift action on preventing known threats

The diverse nature of IoMT 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 IoT security lifecycle will require actionable insights into **detection and prevention of known threats** of your IoMT devices for a swift response to 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 defense known threats for rapid, real-time responsiveness to anomalous IoMT device vulnerabilities and weaknesses across your network—and importantly—won't overburden security teams with detection alerts that could be stopped—saving time and heartache.

An ideal IoMT security solution should do the following:

- ✓ Selectively enables security threat protections based on the IoMT device group's risk posture.
- ✓ Detects and prevents known threats from IoMT malware, spyware, exploits.
- ✓ Blocks IoMT attacks stemming from bad URLs and malicious websites.
- ✓ Prevents IoMT attacks that use DNS for command and control and data theft.
- ✓ Prohibits unknown IoMT threats delivered via payloads.

Quickly detect and respond to unknown threats

When it comes to **detecting and preventing truly unknown threats,** legacy approaches isolate threat data each organization receives and generates, creating silos and reducing the possibility of prevention. To meet the requirements of the last step in the IoT security lifecycle, your IoMT security solution should be capable of leveraging a new approach, drawing from a collective threat intelligence engine that delivers real-time malware analysis and protections from zero-day attacks to your IoMT devices. Tapping into crowdsourced data from a global community of subscribers not only provides collective immunity but also saves your IT security team valuable time by leveraging IoMT identity information, risk scores, vulnerability data, and behavioral analytics investigate never-heard-before threats unique to your IoMT 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 IoMT security solution should do the following:

- Detects 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.
- Leverages crowdsourcing intelligence using machine learning enhanced with threat modeling to detect unknown threats or attacks and provide proactive notifications or actions.
- Integrates into SIEM, and SOAR using a simplified playbook-based approach to orchestrate actions for incident response and threat prevention.
- Streamlines with active IoT security researchers to discover any new IoT threats.

6

Gain Operational Intelligence for Clinical and Biomedical 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. Apart from that, because medical devices are regulated by the FDA, 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 medical devices need actionable business and operational insights that alleviate the pain of capital planning and preventive maintenance while staying informed on when a device may be ready for patching and software upgrades. This is where an IoT security solution steps in to help make important decisions. Operational insights derived from the solution 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 IoMT security solution should do the following:

- Tracks and reports device usage stats for individual medical devices to help decide when to purchase a new device or replace an old one.
- Provides peak usage times to plan for preventive maintenance and software updates ensuring critical medical scheduling or patient experience is not affected.
- Provides analytical data on imaging device usage including which staff members are using the devices and how they are being used to ensure personnel resources are located close to the devices they use.
- Swiftly manages manufacturer notices, FDA recalls and issues in one place without the need for manual investigation.
- Updates inventory systems to keep a continuous log of devices ensuring all other departments are aware of new and decommissioned devices.
- Protects patient records by unearthing how each device uses and stores data to allow easy onboarding and decommissioning of devices in compliance with HIPAA regulations.

IoT Security for Healthcare by Palo Alto Networks

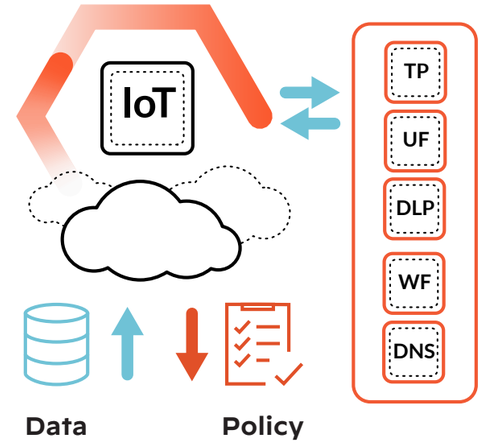
The Healthcare Industry's Most Comprehensive IoT Security Solution

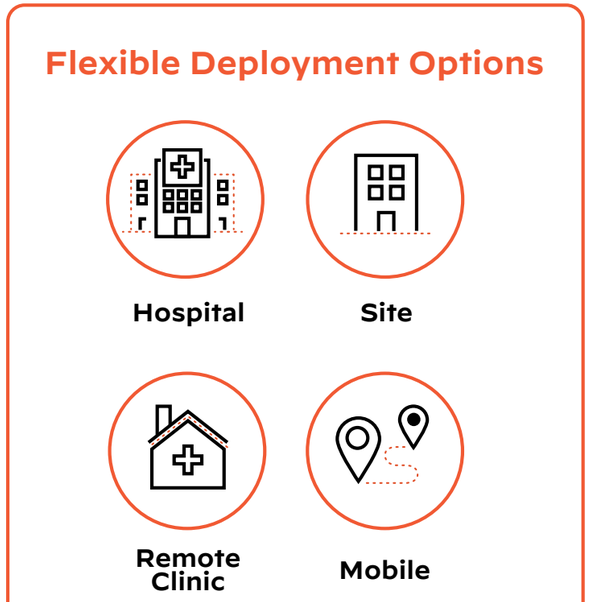
Palo Alto Networks IoT Security is the healthcare industry's most comprehensive IoT Security solution delivering ML-powered visibility, prevention, enforcement, and operational insights in a single platform.

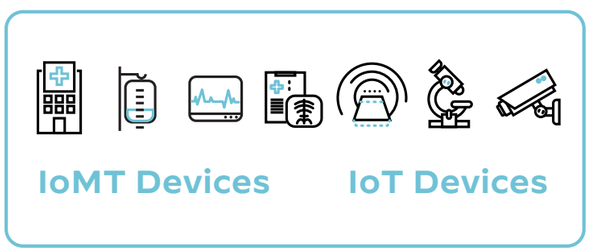
Here's everything IoT Security does for you!

- It is the only solution to use **machine learning with crowdsourcing** to quickly and accurately discover all devices, even the unknown ones.
- It is the only solution with **built-in prevention.** Instead of an alert-only approach, it keeps unmanaged devices safe from all known/unknown threats and vulnerabilities by preventing threats and blocking vulnerabilities from entering your network.
- IoT Security also decreases the cost of patient care with **operational insights** for clinical teams and **automatically enforces policies either directly or through integrations.** This helps reduce the strain on your network and security operations teams, keeps all devices safe, and increases their uptime and availability.
- Delivered as a single platform, IoT Security **deploys effortlessly** without requiring additional infrastructure.

Palo Alto Networks IoT Security is the only solution in the market today that enables maximum return on investment (ROI) and patient experience with deep visibility, focused operational insights, and enhanced security for medical devices all in one platform. **1 in every 5 hospitals in the US is protected by us!**







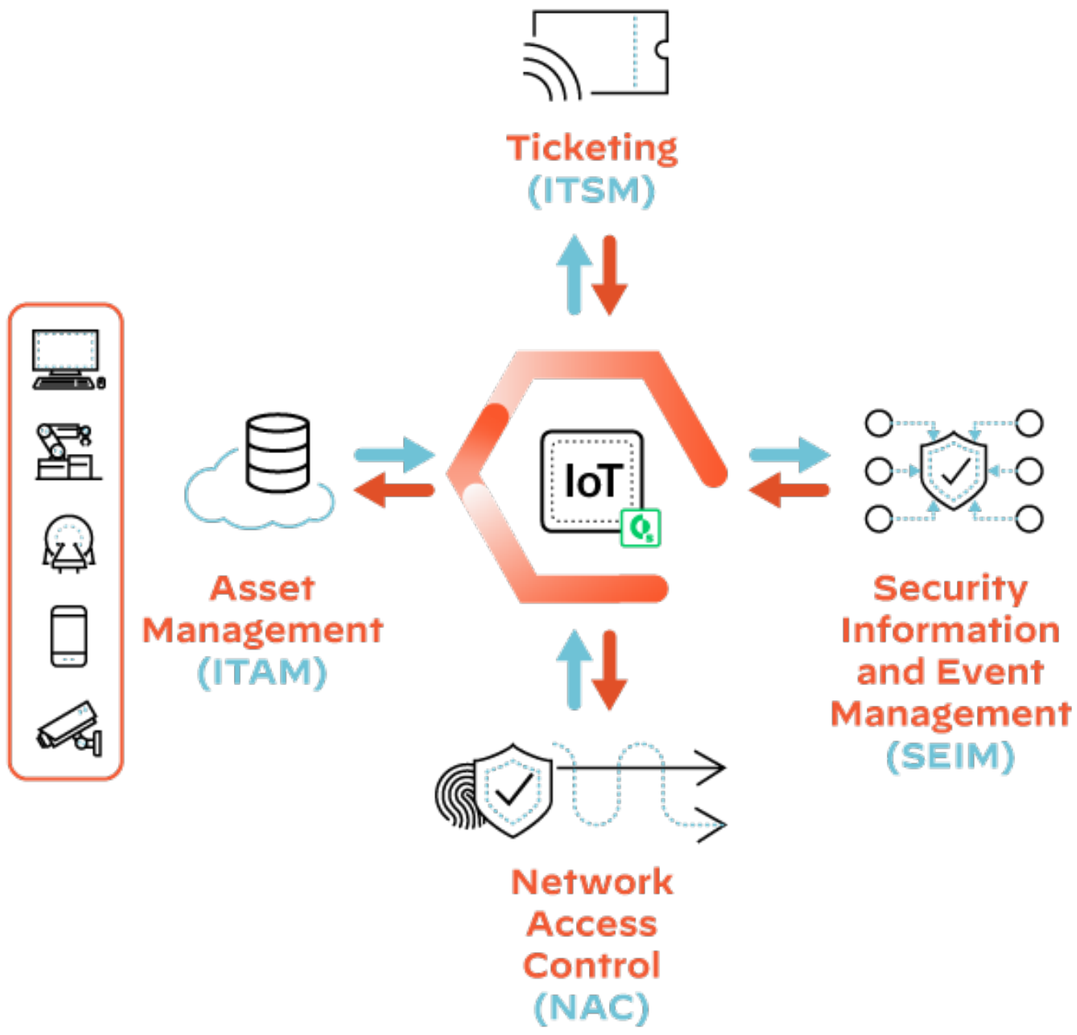
Integrates with Third Parties

Powered by Built-in XSOAR Technology

Our IoT Security seamlessly integrates into your existing workflows and avoid resource intensive API led integrations, reducing the burden on infrastructure and security teams.

Leverage native integrations into your existing IT and security workflows to strengthen your current IT Service Management (ITSM), Network Access Control (NAC), Security Information and Event Management (SIEM) and other use cases.

Our modular and customized playbook-driven orchestration lets your security team improve operational inefficiencies, enrich asset inventories, accurately onboard IoMT devices, enforce device controls and automate incident responses without having to build integrations from scratch.



Leverage Your Current IT Security Team

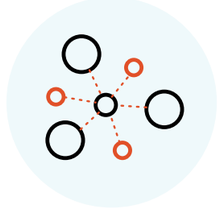
Without the need to form a new team, deploy new infrastructure or change existing operational processes.

Unprecedented Visibility and Protection

- ML-Based IoT Device Discovery
- Automated Risk Assessment
- Native Security Policy Enforcement
- Context-Aware Network Segmentation

Easy Deployment with Flexible Form Factor Options

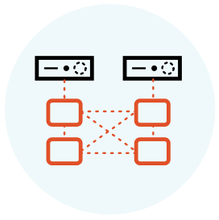
- Hardware Firewalls
- Software Firewalls
- Cloud-delivered Firewalls



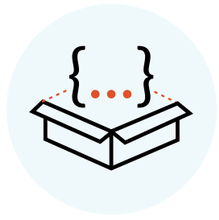
Full Range of IoT, IoMT and IT Device Coverage

- Unmanaged IoMT Devices
- Unmanaged 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 Healthcare IoT Security.
Think Palo Alto Networks.

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.

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

For more information, visit: www.paloaltonetworks.com

Curious to learn more? **Watch the Product Demo**

See what our customer had to say

"Palo Alto Networks IoT Security is simple, cloud-delivered, and can be deployed quickly. With Palo Alto's IoT Security tool, we gained complete visibility to over 4,000 IoT and medical devices, about 30% more devices than what we had prior."

Miroslav Belote
Chief Information Security Officer
Valley Health System

Valley Health System

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