IoT Security for Healthcare

The Healthcare Industry's Most Comprehensive IoT Security Solution

Unmanaged Internet of Things (IoT), Internet of Medical Things (IoMT), and operational technology (OT) devices make up more than 50% of the devices on hospital networks.[1] With Omdia estimating there were more than 250 million medical devices introduced to the market globally in 2020, an expected additional 500 million in 2025,[2] and the US Food and Drug Administration (FDA) approving 153 new healthcare device types between 2018 and 2020,[3] we are at the tip of the iceberg when it comes to device utilization in the healthcare market.

1. "*2020 Unit 42 IoT Threat Report*," Palo Alto Networks, March 10, 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020.
2. According to the Omdia IoT Devices & Components Intelligence Service.
3. "2020 Device Approvals," US Food and Drug Administration, August 16, 2021, https://www.fda.gov/medical-devices/recently-approved-devices/2020-device-approvals.

Health Delivery Organizations (HDOs) depend on these devices to enable their business, yet they cannot trust them. IoMT devices pose a huge risk to organizations and their patients as they often ship with vulnerabilities, run unsupported operating systems, are difficult to patch, and lack encryption in communication. Unit 42 found that more than half of these devices are vulnerable to medium- or high-severity attacks,[4] and almost all imaging systems are powered by end-of-life operating systems—concerning figures when these devices are network-connected with unfettered access. Adding to the issue, Unit 42 also reported that 72% of healthcare organizations have a mix of IT and IoMT devices in the same VLANs, enabling potential lateral movement of threats, expanding the attack surface of both device types.[5] Unfortunately, legacy security solutions employ an alert-only approach, have dated signature-based discovery methods, don't help with policy creation or Zero Trust, and only use single-purpose sensors. All this leaves security teams with the heavy lifting, blind to unknown devices and unable to scale their operations, prioritize efforts, or minimize risk.

Protect Every Device on Your Network

Palo Alto Networks offers the healthcare industry's most comprehensive IoT security solution. Trusted by 20% of the hospitals in the US, our cloud-delivered IoT Security service allows you to prevent threats and control the risk of IoMT, IoT, and IT devices on your network across all sites. Leveraging an approach based on machine learning (ML), it quickly and accurately discovers and identifies all IoMT and other unmanaged devices, including those never seen before. It uses crowdsourced data to identify anomalous activity, continually assess risk, and offer trust-based policy recommendations to improve your security posture.

Combined with our industry-leading ML-Powered Next-Generation Firewall (NGFW) platform, IoT Security can decrease the cost of patient care with operational insights for clinical teams, prevent threats, block vulnerabilities, and automatically enforce 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.

Business Benefits

- **Turn unmanaged devices into managed devices.** Gain visibility into all IT, IoT, IoMT, and OT devices, and control the largest contributor to risk: unknown devices.
- **Enforce prevention and Zero Trust.** Gain visibility, prevention, trust-based policy recommendations, and enforcement for every IoMT, IoT, and IT device through a single integrated product.
- **Reduce the strain downstream with prevention.** Medical devices have many known vulnerabilities. Built-in prevention stops threats as they arrive so your security team doesn't have to deal with another deluge of alerts.
- **Plan your risk management strategy.** Get full details on all devices, including risk, manufacturer information, and FDA recalls, all in one place.
- **Leverage your existing talent.** Empower your existing security and operations teams to secure IoT without changing their practices, policies, or procedures.
- **Reduce the cost of patient care with operational insights.** Improve your bottom line by optimizing resource allocation, patient care, and capital planning on expensive medical equipment.
- **Improve operational efficiencies with integrations.** Unlock the potential of your ITAM, SIEM, NAC, and other solutions by facilitating IoMT information sharing, applying Zero Trust, and enabling new security use cases.
- **Deploy easily and maximize ROI.** If you already have Palo Alto Networks NGFWs, they'll become IoMT-aware with no additional infrastructure required.
- **Don't get caught with single-purpose sensors.** For new customers, every IoT solution requires its own visibility sensor. Only with Palo Alto Networks can you prevent threats, segment, and enforce policy as well.
- **Use predictable and simplified licensing.** Avoid exhausting device true-up models and get simple licensing based on network coverage.

4. *2020 Unit 42 IoT Threat Report*, https://unit42.paloaltonetworks.com/iot-threat-report-2020.
5. Ibid.

Key Capabilities

Complete Device Visibility with ML-Based Discovery

Accurately identify and classify all IoT and OT devices in your network, including those never seen before. IoT Security combines Palo Alto Networks App-ID™ technology and deep packet inspection (DPI) for accuracy with a patented three-tiered machine-learning (ML) model for speed in device profiling. These profiles classify any IoMT, IoT, or IT device to reveal its type, vendor, model, and more than 50 unique attributes, including firmware, OS, serial number, MAC address, physical location, subnet, access point, port usage, applications, and more. Bypassing the limitations of signature-based solutions in new device discovery, IoT Security uses cloud scale to compare device usage and eliminate soak time, validate profiles, and fine-tune models so no device will ever go unmanaged again.

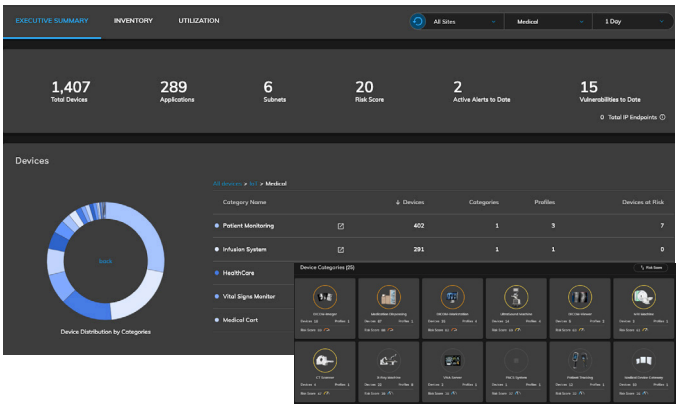

Figure 1: Device inventory at a glance

Prioritize Risk with Continuous Vulnerability Assessments

Find all the information you need to quickly evaluate vulnerable devices and initiate next steps. IoT Security unites disparate solutions from traditional IT security technology into one, simplifying analysis and assessment for security teams. Powered by ML, device profiles are generated from five key behaviors—internal connections, internet connections, protocols, applications, and payloads—then compared over time and against similar crowdsourced devices. The risk assessment also includes Manufacturer Disclosure Statement for Medical Device Safety (MDS2) security information, such as antivirus capabilities, ePHI, device vendor patching information, Unit 42 threat intelligence, and Common Vulnerabilities and Exposures (CVEs) data, to continuously evaluate and adjust risk. Generated risk scores, based on the Common Vulnerability Scoring System (CVSS), provide an effective way to prioritize results, quickly exposing any behavioral anomalies and threat details for security teams to initiate a response—and consistently reducing the attack surface area.

Quickly Implement Trust Policies with Automated Risk-Based Recommendations

Confidently apply policy changes to reduce risk from IoMT, IoT, and IT devices. By comparing metadata across millions of devices with those found in your network, IoT Security can use its device profiles to determine normal behavior patterns. For each IoT device and category of devices, it provides a recommended policy to restrict or allow trusted behaviors. Recommended policies save countless hours per device in gathering the application usage, connection, and port/protocol data otherwise needed to create policies manually. Once reviewed, a policy can be quickly imported by your ML-Powered NGFW, and any changes will be automatically updated, keeping your administration overhead to a bare minimum.

Segment Devices and Reduce Risk with Built-In Enforcement

Implement security best practices with context-aware segmentation to restrict lateral movement between IoMT, IoT, and IT devices. Risk-based policy recommendations from IoT Security allow control of IoMT and IoT device communication. The unique pairing with the ML-Powered NGFW for enforcement uses our patented Device-ID™ policy construct to share device profile information and ensures that control placed on an individual device is consistent regardless of network location. IoT Security can further reduce your attack surface by providing context to segment IoMT and IT devices into different VLANs and applying the Zero Trust methodology. Alternatively, if integrations are your preferred method of enforcement, our native integrations with network access control (NAC) and other solutions fit seamlessly into existing workflows with pre-built playbooks ready for use.

Prevent Known and Unknown Threats

Stop all threats headed for your IoMT, IoT, and IT devices with the industry's leading IPS, malware analysis, web, and DNS prevention technology. IoMT and IoT devices are most susceptible to cyberthreats and targeted attacks. Our 2020 Unit 42 IoT Threat Report found that 41% of attacks exploit vulnerabilities such as weak passwords, remote code execution, and network scans, allowing IT-borne attacks to spread systemically and reach medical devices with ePHI information.[6]

Alert-only solutions are not enough, as every alert generated by a security product creates extra investigation and response work for already inundated security teams. With IoMT accounting for 50% of all devices in an HDO,[7] alert-only solutions can add thousands of actionable events on a weekly basis. Seamlessly integrated with IoT Security, our cloud-delivered security services coordinate intelligence to prevent all IoMT and IT threats without increasing workloads for your security personnel. To decrease response times, our ML-Powered NGFWs can dynamically isolate IoMT devices with validated threats upon detection, giving your security team time to form remediation plans without risk of further infection from that device.

Enhance IoT Security further with any of our additional security subscriptions:

- **Threat Prevention**: Go beyond traditional intrusion prevention system (IPS) solutions to automatically prevent all known threats across all traffic in a single pass.
- **WildFire® malware prevention service**: Ensure files are safe by automatically detecting and preventing unknown malware with industry-leading cloud-based analysis.
- **URL Filtering**: Enable the safe use of the internet by preventing access to known and new malicious websites before your users can visit them.
- **DNS Security**: Disrupt attacks that use DNS for command and control and data theft without requiring any changes to your infrastructure.
- **Enterprise DLP**: Minimize data breach risks by identifying sensitive data consistently throughout the entire HDO and prevent unsafe transfers and corporate policy violations.

Get Unprecedented Business and Operational Insights

Improve patient experience and operations with vendor-agnostic business intelligence, helping you organize and optimize expensive resources. Biomedical and clinical teams often find themselves over budget while medical devices remain underutilized and maintenance costs soar. IoT Security alleviates the pain of capital planning and preventive maintenance while saving costs on patient care by automatically tracking and reporting on IoMT device usage and resource allocation. Some of the operational insights include IoMT device operating hours, scan insights, patient experience, average use, vendor remote maintenance activity, side-by-side comparisons of IoMT devices, and many more. Furthermore, you can generate reports to plan and implement efficient capital planning and business operations optimization.

Leverage Native Integration with Your Existing IT and Security Workflows

Share IoMT, IoT, and IT device visibility, and strengthen your current ITSM, NAC, SIEM, and other use cases. The IoT Security integrations module is powered by Cortex® XSOAR, the industry's leading security orchestration, automation, and response (SOAR) platform, with more than 500 third-party integrations. Some of the common integrations are with market-leading IT asset management and IT service management (ITAM/ITSM) such as ServiceNow®, security information and event management (SIEM) such as Splunk®, and NAC such as Cisco ISE. Operational efficiencies are realized with playbook-driven orchestration across products to enrich asset inventories, accurately onboard IoMT devices and enforce device controls with NAC, and manage day-to-day operations in SIEM and ticketing systems. Learn more about playbook-driven integrations for IoT Security.

6. Ibid.
7. Ibid.

Ease Deployment and Operationalization with Cloud Delivery

Palo Alto Networks IoT Security uniquely pairs with our ML-Powered NGFWs to provide the industry's first complete security solution offering visibility, prevention, risk assessment, and enforcement for IoT and IoMT. This combination empowers security teams to seamlessly enhance existing network and security operational processes to secure IoMT—no more relying on time-intensive integrations with third-party tools just to gain enforcement.

Existing Palo Alto Networks Customers

IoT Security is a cloud-delivered security subscription that empowers your security teams to start reclaiming unmanaged IoMT devices within minutes of its activation. Simply activate IoT Security for any form factor of your existing ML-Powered NGFW (PA-Series, VM-Series, or Prisma® Access).

The prevention capabilities of your cloud-delivered Threat Prevention, WildFire, URL Filtering, and DNS Security subscriptions will automatically expand to share intelligence and stop all known and unknown threats targeting your IoMT, IoT, and IT devices.

Figure 2: Device usage and trends over time

Potential Palo Alto Networks Customers

We package our industry-leading ML-Powered NGFWs as a sensor and enforcement point for our IoT Security service. This powerful combination is unmatched in value, offering comprehensive device discovery, risk assessment, prevention, workflow integration, and enforcement. The sensor is deployed in network locations optimal for device discovery and where traditional firewalls and other controls are rarely deployed. You'll no longer need to purchase, integrate, and maintain multiple point products or change your operational processes to get full IoMT security.

Every IoT security solution requires a sensor. Only Palo Alto Networks IoT Security provides a unified platform across physical, software, and cloud-delivered form factors, prevents threats and enforces policy consistently to increase your return on investment and reduce operational overhead.

Operational Benefits

The IoT Security subscription enables you to:

- **Limit operational and infrastructure overhead.** No need to deploy and maintain siloed sensors, change processes, or create integrations—simply empower your existing security teams to get visibility into your devices.
- **Cut the time to deploy IoT Security by 90%.** Don't wait for several months. Deploy IoT Security in minutes to identify and classify every IoMT, IoT, and IT device, including unknown devices, within 48 hours.
- **Quickly discover all devices with machine learning.** Take advantage of a signatureless approach to identity and understand rapidly changing IoMT and IoT devices.
- **Understand full device context.** Utilize IoMT, IoT, and IT device information across your security operations for context-aware segmentation, policies, and incident response.
- **Visualize operational insights.** Automatically track and visualize IoMT device usage, location, and more across sites, and easily generate reports.
- **Save significant working hours in risk assessment, patching, and policy creation.** Protect devices with automated risk analysis, policy recommendations, and behavioral profiling.
- **Enforce Zero Trust policies effortlessly.** Allow only trusted IoT behaviors with App-ID™, User-ID™, and Device-ID™ technology on your ML-Powered NGFWs.
- **Deploy, maintain, and report with ease.** Enable cloud-delivered subscriptions, get automated best practice and assessment reports, and manage your security centrally with Panorama™ network security management.
- **Fortify current workflows with additional IoMT, IoT, and IT device insights.** Strengthen your current ITAM/ITSM, NAC, SIEM, and other use cases with native integrations and open APIs.
- **Leverage a single offering for comprehensive industry-specific intelligence.** Identify and secure all IoMT, IoT, and IT devices mapped to the HIPAA framework.

Table 1: Palo Alto Networks IoT Security Features and Capabilities	
IoMT and IT device discovery and classification (type, vendor, model, and 50+ unique attributes)	Vulnerability assessment with CVE integration
IoMT, IoT, and IT device profiling with patented three-tiered ML	Risk scoring based on the CVSS and MDS2 information
Behavioral anomaly detection	IoMT device operational insights, utilization, and reports
Risk-based policy recommendations	Native playbook-driven integrations with third-party systems such as ITAM/ITSM, NAC, and SIEM
Prevention of all known threats	Automated enforcement
SOC 2 Type II certification	—

Table 2: Privacy and Licensing Summary	
Privacy	
Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.
Licensing and Requirements	
Requirements	To use the Palo Alto Networks IoT Security subscription, you will need: • Palo Alto Networks ML-Powered NGFWs running PAN-OS® 8.1 or later • Cortex Data Lake for log storage (optional)
Recommended Environment	Palo Alto Networks ML-Powered NGFWs deployed in network segments and egress points where IoMT and IoT devices exist.
IoT Security License	IoT Security requires a standalone license, delivered as an integrated, cloud-based subscription for Palo Alto Networks ML-Powered NGFWs.
Supported NGFWs	All models of PA-Series firewalls, VM-Series firewalls (except VM-50 and VM-200), and Prisma Access.

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