Palo Alto Networks Medical IoT Security

A comprehensive Zero Trust security solution for connected medical devices (IoMT) providing ML-powered visibility, risk assessment, and automated enforcement.

https://www.paloaltonetworks.com/network-security/medical-iot-security

Overview

Palo Alto Networks Medical IoT Security is a comprehensive, cloud-delivered, Zero Trust security platform purpose-built for the Internet of Medical Things (IoMT) and other connected devices in healthcare environments. The solution addresses the critical challenge of securing medical devices, many of which run on unsupported operating systems and have known security gaps, by eliminating implicit trust and continuously verifying every device.

It operates agentlessly, providing continuous, aggregated visibility into every connected medical, IoT, OT, and IT device on the network using a patented three-tier machine learning (ML) model, App-ID technology, and crowdsourced telemetry. This allows for accurate device discovery and classification, even for never-before-seen devices.

Key capabilities include automated risk assessment and prioritization, which factors in device type, criticality to patient care, and exposure. It can ingest Manufacturer Disclosure Statement for Medical Device Security (MDS2) and Software Bill of Materials (SBOM) information for deeper vulnerability analysis and risk posture insights (e.g., end-of-life status, recall notifications).

The platform enables proactive risk mitigation through identity-aware policies, guided virtual patching for legacy/unpatchable systems, and one-click enforcement of Zero Trust policies. It simplifies operations by providing two distinct dashboards for IT and biomedical engineering teams (Biomed and Utilization Dashboards) and integrates natively with existing security and IT solutions like ServiceNow, Splunk, and Cortex XSOAR for playbook-driven incident response and automated security responses (e.g., quarantining a device that exhibits anomalous behavior). The solution is designed to help organizations improve compliance with regulations like HIPAA and GDPR.

Key Features

- ML-Powered Device Discovery and Classification (IoMT, IoT, OT, IT)
- Continuous Visibility and Inventory
- Automated Risk Assessment and Prioritization
- Zero Trust Policy Recommendations and One-Click Enforcement
- Contextual Segmentation and Virtual Patching
- Built-in Threat Prevention (via Cloud-Delivered Security Services)
- Automated Security Responses and Incident Response Playbooks
- Operational Insights (Utilization Dashboard)

Pricing

Model: enterprise

Subscription-based, requires a custom quote. Pricing is generally considered expensive and licensing can be complex, as noted by users.

Target Company Size: medium, enterprise

Integrations

ServiceNow, Splunk, Cisco ISE, Prisma Access, Cortex XSOAR

Compliance & Certifications

HIPAA, GDPR

This document was generated by IntuitionLabs.ai with the assistance of AI. While we strive for accuracy, please verify critical information independently.