The Ultimate IoT Security RFI Checklist for CISOs

Security and risk management leaders have two main challenges that they are grappling with:

1. An accurate inventory of all IoT assets
2. Potential security issues caused by these unmanaged assets

Despite many solutions in the market, many organizations report that selecting the right IoT Security solution for specific organizational needs is challenging.

In other words, as a business decision-maker, you are in the process of determining whether the many types of IoT security solutions available in the market today offer key capabilities that best meet the needs of your organization.

This RFI checklist documents must-have features and capabilities business decision-makers across all enterprises and industries should look for before deciding on a perfect solution to protect all IoT, IoMT, OT, and IT devices in their corporate network.

How to Use

The fillable worksheet is meant to be used as a tool by business decision-makers (BDMs) to obtain clarity on IoT Security product requirements so they appropriately match their needs with providers' capabilities.

The worksheet lists key product capabilities that Palo Alto Networks deems as absolute musts in an IoT Security solution and allows you to match them with the ability of other vendors to meet them.

The RFI checklist in this document is organized into 7 categories listed below. An addendum specific to medical device security is available in addition to the primary checklist.

- Architecture / Topology
- Device Discovery for Complete Visibility
- Proactive Monitoring for Continuous Risk Assessment
- Automated Risk-Based Policy Recommendations for Native Enforcement
- Protection from Known Threats
- Fast Detection of Unknown Threats
- Workflow Orchestration

Select the requirements that your organization is planning to implement from Column A. Then compare and contrast if other vendors you are considering satisfy each requirement in Columns B and C.

Architecture/Topology

	Palo Alto Networks	Vendor 1	Vendor 2
Is the solution cloud-delivered for better scalability.	✓		
Scales to cover devices in remote locations.	✓		
Natively integrated with a firewall for device visibility in a single pass network architecture.	✓		
Central management across locations and branches.	✓		
Easy deployment without friction to current network architecture.	✓		

Device Discovery

	Palo Alto Networks	Vendor 1	Vendor 2
Offers passive profiling of all IoT devices.	✓		
Delivers essential and extensive IoT device attributes such as device make, model, operating system, firmware, ports, applications, VLAN, subnet, presence, and status of anti-virus software, etc.	✓		
Detects new, never-seen-before devices without reliance on human support or constant update of signatures.	✓		
Leverages signature-less AI-based device identification and classification.	✓		
Performs detection of newly plugged-in devices within minutes.	✓		
Identifies at least 90% of devices in visible segments within 48 hours.	✓		
Differentiates unmanaged IoT devices from managed IT assets.	✓		
Logs a tally of IT devices allowing desktop security teams to also identify unmanaged IoT or OT devices.	✓		
Keeps device historical data with searchable history for 365 days.	✓		

Proactive Monitoring and Risk Assessment

	Palo Alto Networks	Vendor 1	Vendor 2
Integrates with multiple threat feeds (industry research, CVE) to accurately map vulnerabilities with the IoT inventory.	✓		
Follows regulatory standards and prescriptions (FDA, ECRI, ISO, NIST, ICS-CERT).	✓		
Creates behavioral baseline for anomaly detection.	✓		
Detects and reports anomalies in IoT device behavioral changes that may lead to risk changes.	✓		
Tracks changes to IoT device risk and keeps complete device risk history for compliance.	✓		
Calculates risk scores on IoT devices and device categories to report.	✓		
Compares device behavior with other crowd-sourced devices.	✓		
Integrates with vulnerability management systems for centralized IoT risk management.	✓		
Ingests device information from the IoT device vendors to deliver actionable insights to security teams.	✓		
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.	✓		
Detects compromised or weak credentials.	✓		
Detects end-of-life devices, operating systems, and applications.	✓		
Shows device connections to cloud and within network.	✓		
Shows internal and external connections by devices.	✓		
Alerts when a device connects to a malicious domain.	✓		
Shows VLAN composition.	✓		
Alerts when a personal device connects to a large number of devices.	✓		

Proactive Monitoring and Risk Assessment (cont.)

	Palo Alto Networks	Vendor 1	Vendor 2
Alerts in case of a policy violation both at the device level and at the network level.	✓		
Assesses device misconfigurations.	✓		
Alerts when a device tries to make multiple attempts to connect to a network.	✓		
Delivers customizable risk levels to balance scores with the existing customer risk framework.	✓		

Automated Risk-Based Policy Recommendations

	Palo Alto Networks	Vendor 1	Vendor 2
Automatically converts IoT device behaviors into policies to only allow trusted behaviors.	✓		
Allows administrators to apply consistent policy control and threat prevention to a device no matter where it moves within the network or what its IP address is at any given time.	✓		
Allows multi-tier policy enforcement for a group of devices.	✓		
Supports both allow lists and block lists.	✓		
Tracks devices and applications to enforce policies regardless of where they reside within the network.	✓		
Offers real-time anomaly detection based on abnormal traffic between devices.	✓		
Updates policies automatically once set limiting manual updates every time a change occurs.	✓		

Protection from Known Threats

	Palo Alto Networks	Vendor 1	Vendor 2
Selectively enables security threat protections based on the IoT device group's risk posture.	✓		
Detects and prevents known threats from IoT malware, spyware, exploits.	✓		
Blocks IoT attacks stemming from bad URLs and malicious websites.	✓		
Prevents IoT attacks that use DNS for command and control and data theft.	✓		

Fast Detection of Unknown Threats

	Palo Alto Networks	Vendor 1	Vendor 2
Prohibits unknown IoT threats delivered via payloads.	✓		
Applies a smarter way to detect unknown threats by leveraging crowdsourcing intelligence using machine learning enhanced with threat modeling.	✓		
Provides proactive notifications or actions.	✓		

Workflow Orchestration

	Palo Alto Networks	Vendor 1	Vendor 2
Integrates into existing technologies and workflows using a playbook-based approach to orchestrate actions.	✓		
Utilizes multipurpose sensors that provide visibility, security, and native integrations with existing workflows.	✓		
Provides built-in policy enforcement capabilities using NGFW.	✓		
Provides policy enforcement by integrating with NAC.	✓		
Automatically updates asset management solutions such as ITSM to update their asset inventory with IoT data.	✓		
Creates service tickets automatically within ITSM solutions.	✓		
Automatically provides IoT device data to SIEM solutions for enhanced investigation and analysis.	✓		
Natively quarantines a risky or compromised device.	✓		
Integrates with any 3rd party tool with an open API.	✓		

Curious About Palo Alto Networks IoT Security?

Connect with us to learn more about how our industry-first IoT Security protects every single device in your network while making single-purpose sensors a thing of the past. Register to view a product demo and request a free trial.

View a Product Demo

Request a Free Trial

Additional Checklist for Medical Devices in Healthcare

Medical Device Security Risk Assessment

	Palo Alto Networks	Vendor 1	Vendor 2
Includes Manufacturer Disclosure Statement for Medical Device Security (MDS2) information like antivirus capabilities, ePHI, FDA recalls, and vendor patching information for healthcare delivery organizations.	✓		
Monitors and reports on PHI compliance.	✓		
Swiftly manages manufacturer notices, FDA recalls and issues in one place without the need for manual investigation.	✓		
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.	✓		
Monitors key medical protocols (DICOM, HL7, IHE, and more).	✓		

Medical Device Utilization Insights

	Palo Alto Networks	Vendor 1	Vendor 2
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.	✓		
Provides utilization insights on CT scanner, Infusion System, MRI Machine, Nuclear-Medicine Imager, PET Scanner, UltraSound Machine, X-Ray Machine).	✓		
Assists in the management of Medical Device Contracts.	✓		
Updates inventory systems to keep a continuous log of devices ensuring all other departments are aware of new and decommissioned devices.	✓		
Provides out of the box reports for customized visualization.	✓		

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