IoT Security

The 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 30% of the devices on enterprise networks.[1] Organizations require these devices to enable their business, yet they cannot trust them. IoT devices pose immense cybersecurity risks as they are largely unregulated. In fact, 57% of these devices, which often ship with their own vulnerabilities, are susceptible to medium- or high-severity attacks[2]—especially concerning when they are network-connected with unfettered access. Security teams, rarely involved in purchasing, find it extremely challenging to secure these devices due to their incredibly diverse builds, long lifecycles, and lack of coverage from traditional security controls.

1. "2020 Unit 42 IoT Threat Report," Palo Alto Networks, March 10, 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020.
2. Ibid.

Most IoT security solutions limit their visibility to manually updated databases of known devices, require single-purpose sensors, lack consistent prevention, don't help with policy creation, and can only provide enforcement through integrations. 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 industry's most comprehensive IoT security solution, allowing you to stop threats and control the risk of IoT, IoMT, and OT devices on your network. Leveraging a machine learning-based approach, our cloud-delivered IoT Security service quickly and accurately discovers and identifies all unmanaged IoT, IoMT, and OT devices in real time, including those never seen before. IoT Security 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 prevent threats, block vulnerabilities, and automatically enforce policies either directly or through integrations, reducing the strain on your operations team and keeping devices safe. IoT Security deploys effortlessly from the cloud and requires no additional infrastructure.

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 for accuracy with a patented three-tier machine learning (ML) model for speed in device profiling. These profiles classify any IoT, IoMT, OT, 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. For healthcare customers, IoT Security provides additional operational insights into medical device allocation, usage, and utilization, along with healthcare device-specific risk assessment.

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.
- **Enjoy complete IoT security.** Gain ML-powered visibility, prevention, and enforcement for every device in your network from a single platform.
- **Reduce the strain downstream with prevention.** Built-in prevention stops threats as they arrive, eliminating the deluge of alerts on your security team.
- **Leverage your existing talent.** Empower your existing security and operations teams to secure IoT without changing their practices, policies, or procedures.
- **Improve operational efficiency with integrations.** Optimize cross-product operations and new security use cases across ITAM, SIEM, NAC, and more.
- **Use predictable and simplified licensing.** Avoid exhausting device true-up models and get simple licensing based on network coverage.
- **Deploy easily and maximize ROI.** If you already have our ML-Powered NGFWs, they'll become IoT-aware with no more 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, you can prevent threats, segment, and enforce policy as well.
- **Get security built for enterprise use cases.** Secure IoT, whatever your industry: Healthcare, Finance, Retail, Government, Education, Manufacturing, Smart City, Utilities, and more.

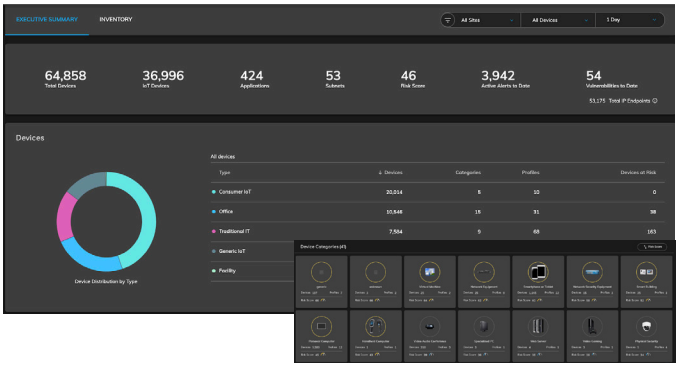

Figure 1: Device inventory at a glance

Prevent Known and Unknown Threats

Stop all threats headed for your IoT devices with the industry's leading IPS, malware analysis, web, and DNS prevention technology. IoT devices are most susceptible to threats and cyberattacks. Our Unit 42 IoT Threat Report found 98% of all IoT device traffic is unencrypted, exposing personal and confidential data on the network. Together with 57% of IoT devices also being vulnerable to medium- or high-severity attacks, this makes IoT low-hanging fruit for attackers. Because of the generally low patch level of IoT assets, the most frequent attacks are exploits via long-known vulnerabilities and password attacks using default device passwords. With roughly one-third of network connected devices being IoT, alert-only solutions potentially add thousands of actionable security events per week, creating extra work for already inundated security teams to investigate and respond.

Seamlessly integrated with IoT Security, our cloud-delivered security services coordinate intelligence to prevent all IoT, IoMT, OT, and IT threats without increasing the workload for your security personnel. To decrease response times, IoT devices with validated threats can be dynamically isolated upon detection of threats by our ML-Powered NGFWs, giving your security team time to form remediation plans without risk of further infection from those devices.

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, enable compliance consistently throughout the entire enterprise and in the cloud, and prevent unsafe data transfers against corporate policies.

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—and then compared over time and against similar crowdsourced devices. These profiles are enhanced with device vendor patching information, Unit 42 threat intelligence, and Common Vulnerabilities and Exposures (CVE®) data to continuously evaluate and score 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.

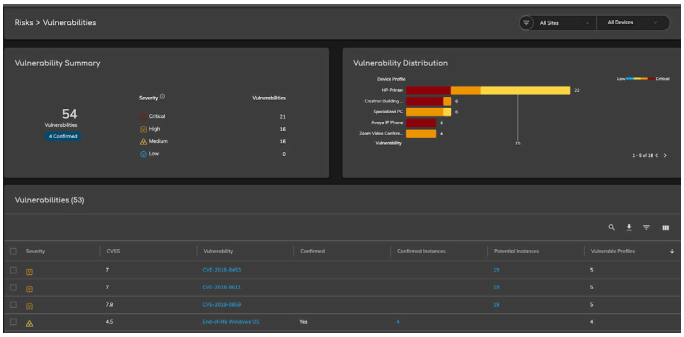

Figure 2: Vulnerability summary and distribution view

Quickly Implement Trust Policies with Automated Risk-Based Recommendations

Confidently apply policy changes to reduce risk from IoT devices. By comparing metadata across millions of IoT 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 and help implement Zero Trust strategies without painstaking manual processes. Recommended policies save countless hours per device in gathering the application usage, connection, and port/protocol data 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 IoT and IT devices. Risk-based policy recommendations from IoT Security allow control of IoT device communication. The unique pairing with the ML-Powered NGFW for enforcement uses a Device-ID™ policy construct to share device profile information and ensure the control placed on an individual device is maintained regardless of network location. IoT Security can further reduce your attack surface by providing context to segment IoT and IT devices, visualizing device placement in the network before implementing VLANs, and applying the Zero Trust methodology. Alternatively, if integrations are your preferred method of enforcement, our native integrations with NAC and other solutions fit seamlessly into existing workflows with prebuilt playbooks ready for use.

Improve Operational Efficiency with Native Integrations

Share IoMT and IT device visibility, and automate cross-product workflows. Despite having multiple IT and security tools, teams are unable to assess the true asset inventory and risk exposure for unmanaged IIoT, IoMT, OT, or IT devices. This is because most solutions work on partial device insight, resulting in low-fidelity device visibility that correlates to poor asset management, limited details for security event investigation and threat response, and lack of access to appropriate resources.

Unlike other solutions in the market, Palo Alto Networks IoT Security eases the pain of API-led integrations and offers prebuilt, customizable playbooks with native interoperability for market-leading IT and security solutions such as ServiceNow®, Cisco ISE, and Splunk®. For example, with IoT Security, you can turn the static inventory of IT asset management and IT service management (ITAM/ITSM) into a dynamic one by directly forwarding inventory of all connected devices as well as raising device vulnerabilities as actionable work orders with remediation recommendations. Security teams can map device classification and behavioral information to alerts, providing context and visibility to each investigation while saving time spent trying to track, interpret, and understand devices behind IP addresses. Network teams can also leverage the IoT/OT data in network access control policies to segment the network and apply Zero Trust policies for reduced risk exposure.

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 solution offering visibility, prevention, risk assessment, and enforcement for IoT. This combination empowers security teams to seamlessly enhance existing network and security operational processes to secure IoT—no more relying on time-intensive integrations with third-party tools just to gain enforcement.

Existing Palo Alto Networks Customers

IoT Security is delivered as a cloud-delivered security subscription that empowers your security teams to start reclaiming unmanaged IoT 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 IT and IoT devices.

Potential Palo Alto Networks Customers

We package our industry-leading ML-Powered NGFW as a sensor and enforcement point for our IoT Security service. This powerful combination is unmatched in value, offering unmanaged device discovery, risk assessment, workflow integration, prevention, 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 IoT security.

Every IoT security solution requires a sensor. Only Palo Alto Networks IoT Security can offer physical, software, and cloud-delivered form factors as well as prevent threats and enforce policy to increase your return on investment and reduce your 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 IoT device, including unknown devices, within 48 hours.
- **Quickly discover all devices with machine learning.** Take advantage of a signatureless approach to identify and understand rapidly changing IoT devices.
- **Understand full device context.** Utilize IoT device information across your security operations for context-aware segmentation, policies, and incident response.
- **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.
- **Fortify current workflows with additional IoT insights.** Strengthen your current ITAM/ITSM, NAC, SIEM, and other use cases with native integrations.
- **Deploy and maintain with ease.** Enable cloud-delivered subscriptions and manage your security centrally with Panorama™ network security management.
- **Leverage a single offering for comprehensive industry-specific intelligence.** Secure across Healthcare, Enterprise IT, Oil and Gas, Smart City, and ICS/SCADA environments, with support for ICS/SCADA protocols and transactions.

Table 1: Palo Alto Networks IoT Security Features and Capabilities	
IoT, IoMT, and OT device discovery and classification (type, vendor, model, 50+ unique attributes)	Vulnerability assessment with CVE integration
IoT and OT device profiling with patented three-tiered ML	Risk scoring based on the CVSS
Behavioral anomaly detection	IoT device visualization 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 and unknown 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 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