Enterprise IoT Security

The Most Comprehensive Zero Trust Security for Smart Devices

There are three times the number of connected IoT devices than users in today's enterprise.[1] Organizations require these devices to enable their business, yet they cannot trust them. Connected devices pose immense cybersecurity risks as they are vulnerable, unseen, and unmanged. In fact, 57% of these devices, which often ship with their own vulnerabilities, are susceptible to medium- or high-severity attacks.[2] It is 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 types, long lifecycles, and lack of coverage from traditional security controls.

[1] *Number of IoT Devices Expected to Reach 24.1 Bn in 2030: Report*, CISO Mag, May 29, 2020, https://cisomag.com/number-of-iot-devices-expected-to-reach-24-1-bn-in-2030-report/.

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

Most security solutions for network-connected devices 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 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 Zero Trust security for smart devices, allowing you to stop threats and control the risk of connected devices on your network. Leveraging a machine learning-based (ML) approach, our cloud-delivered Enterprise IoT Security quickly and accurately discovers and identifies all connected devices in real time, including those never seen before. Enterprise 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, Enterprise 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. Enterprise IoT Security deploys effortlessly from the cloud and requires no additional infrastructure.

Key Capabilities

Complete Device Visibility with ML-Based Discovery

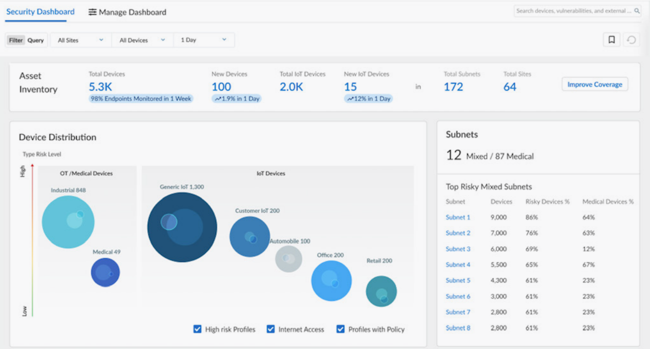
Accurately identify and classify all connected devices in your network, including those never seen before. Enterprise IoT Security combines Palo Alto Networks App-ID technology for accuracy with a patented three-tier machine learning (ML) model and crowdsourced telemetry for speed in device profiling. These profiles classify any network-connected 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. Surpassing the limitations of signature-based solutions in new device discovery, Enterprise IoT Security uses cloud scale to eliminate soak time, validate profiles, and fine-tune models so no device will ever go unmanaged again.

Prevent Known and Unknown Threats

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

Business Benefits

- **Turn unmanaged devices into managed devices.** Gain visibility into all IT and connected network devices, and control the largest contributor to risk—unknown devices.
- **Get best-in-class security for connected devices.** With the industry’s first ML-powered IoT visibility engine, you gain enhanced ML-powered visibility, threat prevention, trust-based policy recommendations, 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 network-connected devices 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 Palo Alto Networks ML-Powered NGFWs, they will become aware of network-connected devices with no additional infrastructure required, reducing TCO by 70X.
- **Don’t get caught with single-purpose sensors.** For new customers, every connected device security solution requires its own visibility sensor. Only with Palo Alto Networks can you prevent threats, segment, and enforce policy with these sensors as well.
- **Get security built for enterprise use cases.** Secure connected devices in any industry: healthcare, finance, retail, government, education, manufacturing, and more.



Asset Inventory

Total Devices 5.3K — 98% Endpoints Monitored in 1 Week
New Devices 100 — 1.9% in 1 Day
Total IoT Devices 2.0K
New IoT Devices 15 — 12% in 1 Day
in
Total Subnets 172
Total Sites 64

☑ High risk Profiles ☑ Internet Access ☑ Profiles with Policy

Subnets

12 Mixed / 87 Medical

Top Risky Mixed Subnets

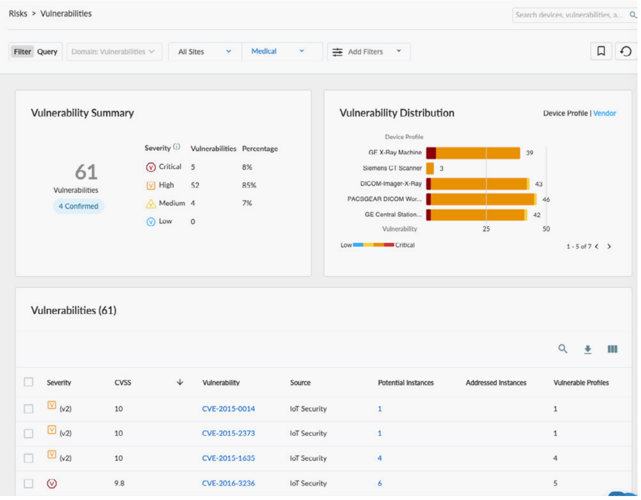
Subnet	Devices	Risky Devices %	Medical Devices %
Subnet 1	9,000	86%	64%
Subnet 2	7,000	76%	63%
Subnet 3	6,000	69%	12%
Subnet 4	5,500	65%	67%
Subnet 5	4,300	61%	23%
Subnet 6	3,000	61%	23%
Subnet 7	2,800	61%	23%
Subnet 8	2,800	61%	23%

Figure 1: IoT device distribution at a glance

Seamlessly integrated with Enterprise IoT Security, our Cloud-Delivered Security Services coordinate intelligence to prevent all network-connected device and IT threats without increasing the workload for your security personnel. To decrease response times, connected 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 Enterprise IoT Security without additional security subscriptions:

- **Advanced Threat Prevention**: Stop known exploits, malware, spyware, and command and control (C2) threats, while utilizing industry-first prevention of zero-day attacks – prevent 60% more unknown injection attacks and 48% more highly evasive command and control traffic than traditional IPS solutions.
- **Advanced WildFire**: Ensure files are safe by automatically preventing known, unknown and highly evasive malware 60x faster with the industry-largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering**: Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security**: Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command-and-control and data theft, without requiring changes to your infrastructure.
- **Enterprise DLP**: Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2x greater coverage of any cloud-delivered enterprise DLP.
- **SaaS Security**: The industry's only Next-generation CASB natively integrated into Palo Alto's SASE offers proactive SaaS visibility, comprehensive protection against misconfigurations, real-time data protection, and best-in-class security.
- **AIOps**: AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions.



Severity	Vulnerabilities	Percentage
Critical	5	8%
High	52	85%
Medium	4	7%
Low	0	

Severity	CVSS	Vulnerability	Source	Potential Instances	Addressed Instances	Vulnerable Profiles
(v2)	10	CVE-2015-0014	IoT Security	1		1
(v2)	10	CVE-2015-2373	IoT Security	1		1
(v2)	10	CVE-2015-1635	IoT Security	4		4
	9.8	CVE-2016-3236	IoT Security	6		5

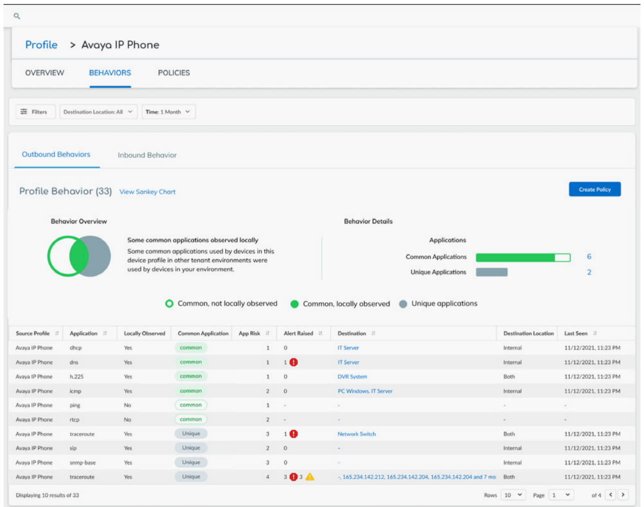
Figure 2: Vulnerability summary view

Prioritize Risk with Continuous Vulnerability Assessments

Find all the information you need to quickly evaluate vulnerable devices, assess security compliance, and initiate the next steps. Enterprise IoT Security unites disparate solutions from traditional IT security technology into one by simplifying and automating 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, third-party vulnerability management systems, and Common Vulnerabilities and Exposures (CVEs) data to continuously evaluate and score risk. In addition, Enterprise IoT Security offers visibility into IoT devices' Software Bill of Materials (SBOM) and maps them to the CVE. This mapping helps to accurately identify the software libraries used on these unmanaged devices and any associated vulnerabilities. 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 Zero Trust Policies with Automated Risk-Based Recommendations

Confidently apply policies to reduce risk from connected devices. By comparing metadata across millions of connected devices with those found in your network, Enterprise IoT Security can use its device



Some common applications observed locally

Some common applications used by devices in this device profile in other tenant environments were used by devices in your environment.

Source Profile	Application	Locally Observed	Common Application	App Risk	Alert Raised	Destination	Destination Location	Last Seen
Avaya IP Phone	dhcp	Yes	common	1	0	IT Server	Internal	11/12/2021, 11:23 PM
Avaya IP Phone	dns	Yes	common	1	1	IT Server	Internal	11/12/2021, 11:23 PM
Avaya IP Phone	h.225	Yes	common	1	0	DVR System	Both	11/12/2021, 11:23 PM
Avaya IP Phone	icmp	Yes	common	2	0	PC Windows, IT Server	Internal	11/12/2021, 11:23 PM
Avaya IP Phone	ping	No	common	1	-	-	-	-
Avaya IP Phone	rtcp	No	common	2	-	-	-	-
Avaya IP Phone	traceroute	Yes	Unique	3	1	Network Switch	Both	11/12/2021, 11:23 PM
Avaya IP Phone	sip	Yes	Unique	2	0	-	Internal	11/12/2021, 11:23 PM
Avaya IP Phone	snmp-base	Yes	Unique	3	0	-	Internal	11/12/2021, 11:23 PM
Avaya IP Phone	traceroute	Yes	Unique	4	3 3	-, 165.234.142.212, 165.234.142.204, 165.234.142.204 and 7 mo	Both	11/12/2021, 11:23 PM

Displaying 10 results of 33 Rows 10 Page 1 of 4

Figure 3: Automated policy recommendation

profiles to determine normal behavior patterns. By studying the behavior of each network-connected device as well as those with the same identity across crowdsourced data, Enterprise IoT Security 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. Paired with the Device-ID feature of the NGFW, the recommended policies are created for ease of understanding and low maintenance. Once reviewed, a policy can be imported automatically by your ML-Powered NGFW, and any changes will be updated automatically, keeping your administration overhead to a bare minimum. Read how you can enjoy 20X time savings with Enterprise IoT Security's automated policy creation.

Segment Devices and Reduce Risk with Built-in Enforcement

Implement security best practices with context-aware segmentation to restrict lateral movement of threats between connected and IT devices. Risk-based policy recommendations from Enterprise IoT Security allow control of network-connected 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. Enterprise IoT Security can further reduce your attack surface by providing context to segment connected 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.

Eliminate Connected Device Blind Spots

Share connected and IT device visibility, and automate cross-product workflows. Despite having multiple IT and security tools, teams are unable to assess the true risk exposure for network-connected devices. This is because most solutions work on partial device insight, resulting in low-fidelity device visibility that correlates to poor asset management, compliance gaps due to vulnerable connected devices, 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 Enterprise IoT Security eases the pain of API-led integrations and offers playbook-driven built-in integrations to increase ROI on existing solutions. Enterprise IoT Security helps customers:

- Confidently segment IoT devices and apply Zero Trust policies through NGFW or NAC.
- Narrow compliance gaps by bringing network-connected visibility and vulnerabilities into vulnerability management systems.
- Understand all assets at all times by turning static IT Service Management (ITSM) or computerized maintenance management system (CMMS) inventory into a dynamic one.
- Enhance SOC and SIEM context for alert triage, investigation, and threat response with complete visibility, context, and actionable insights.
- Decrease mean time to response (MTTR) by quickly pinpointing the device's physical and network location for remediation through network management.

Learn more about playbook-driven integrations for Enterprise IoT Security.

Ease Deployment and Operationalization with Cloud Delivery

Palo Alto Networks Enterprise 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 connected devices. This combination empowers security teams to seamlessly enhance existing network and security operational processes to secure network-connected devices—no more relying on time-intensive integrations with third-party tools just to gain enforcement.

Existing Palo Alto Networks Customers

Enterprise IoT Security is a cloud-delivered security subscription that empowers your security teams to start reclaiming unmanaged connected devices within minutes of its activation. Simply activate Enterprise IoT Security for any form factor of your existing ML-Powered NGFW (PA-Series, VM-Series, or Prisma Access). Read how you can achieve 70X time savings protecting network-connected devices in your enterprise.

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

New Palo Alto Networks Customers

We package our industry-leading ML-Powered NGFW as a sensor and enforcement point for our Enterprise 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 connected device security.

Every security solution for network-connected devices requires a sensor. Only Palo Alto Networks Enterprise 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 Enterprise IoT Security subscription enables you to:

- **Limit operational and infrastructure overhead.** There is no need to deploy and maintain siloed sensors or change network topology—use your current NGFW to inspect traffic from deep network segments using ERSPAN and other techniques.
- **Cut the time to deploy connected device security by 90%.** Don't wait several months. Deploy Enterprise IoT Security in minutes to identify and classify every network-connected device, including never-before-seen devices, within 48 hours.
- **Quickly discover all devices with machine learning.** Take advantage of a signatureless approach to identify and understand rapidly changing network-connected devices.
- **Understand full device context.** Utilize connected 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 connected device behaviors with App-ID, User-ID, and Device-ID technology on your ML-Powered NGFWs.
- **Fortify current workflows with additional network-connected device 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, finance, retail, government, education, manufacturing, and more industries.

Table 1: Palo Alto Networks Enterprise IoT Security Features and Capabilities	
Network-connected device discovery and classification (type, vendor, model, 50+ unique attributes)	Vulnerability assessment with CVE integration
Connected device profiling with patented three-tiered ML	Risk scoring based on the CVSS
Behavioral anomaly detection	Connected device inventory, vulnerabilities, and overall risk visualization and reports
Risk-based policy recommendations	Native playbook-driven integrations with third-party systems, such as ITAM/ITSM/CMMS, NAC, SIEM, and network management infrastructure
Prevention of all known and unknown threats	Automated enforcement
SOC 2 Type II certification	FedRAMP Authorized (Moderate)

Table 2: Privacy and Licensing Summary	
Privacy	
Regional Cloud Locations	Palo Alto Networks deploys local cloud infrastructure all around the world so our diverse customer base can utilize our cloud-delivered services to secure their organization while meeting data location preferences.
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 Enterprise IoT Security subscription, you will need: • Palo Alto Networks ML-Powered NGFWs running PAN-OS 8.1 or later
Recommended Environment	Palo Alto Networks ML-Powered NGFWs deployed in network segments and egress points where network-connected devices exist.
Enterprise IoT Security License	Enterprise IoT Security requires a standalone license, delivered as an integrated, cloud-based subscription for Palo Alto Networks ML-Powered NGFWs. Enterprise IoT Security Plus covers all the features listed above. Customers who only need IoT device discovery to make their firewall policy and segmentation more effective can choose to buy the Enterprise IoT Security base license
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