# IoT Security

## IoT Devices Scale Beyond Security Control

Unmanaged internet-of-things (IoT) 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, often ship with vulnerabilities, and are network-connected with unfettered access. Security teams—which are 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.

## Business Benefits

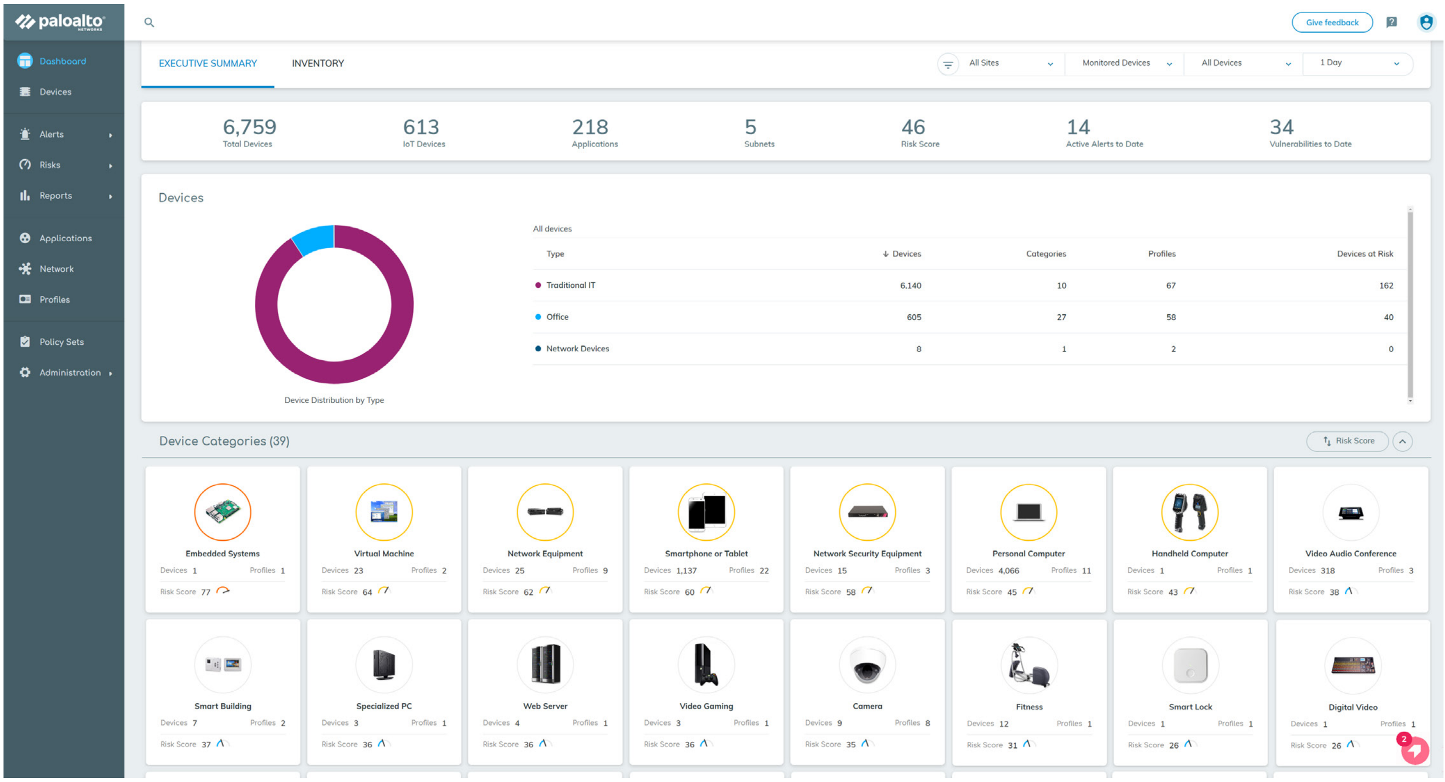
- **Turn unmanaged into managed devices.** Identify all unknown IoT devices and remove up to 30% risk.
- **Reduce the strain on downstream operations.** Built-in prevention stops threats as they arrive, freeing security teams from detection only alerts.
- **Leverage your existing talent**. Empower your network, security, and operations teams to secure IoT without changing practice, policy, or procedure.
- **Predictable and simplified licensing.** Don't suffer through device true-up; IoT Security licensing is simply based on network coverage.
- **Deploy easily and maximize ROI**. Make existing Palo Alto Networks ML-Powered NGFWs IoT-aware, no additional infrastructure required.
- **No more single-purpose sensors.** All solutions require visibility sensors; our IoT Security customers gain prevention, segmentation, and enforcement.
- **Get security built for enterprise use cases.** Finance, Retail, Transport, SLED, Edu., Insurance, Mfg., Healthcare, Smart City, Utilities, Mining, and more.

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

Existing IoT security solutions limit their visibility to known devices, require single-purpose sensors, lack consistent prevention, and can only provide enforcement through integrations. All this leaves security teams with the heavy lifting, unable to scale their operations, prioritize efforts, or minimize risk.

## Trust Every Device on Your Network

Palo Alto Networks offers the industry's first turnkey IoT security solution that allows you to manage and control the risk of IoT and OT devices on your network. Leveraging a machine learning-based approach to accurately identify and classify all unmanaged IoT devices, including those never seen before, our cloud-delivered IoT Security subscription uses crowdsourced data to identify anomalous activity, continually assess risk, and offer policy recommendations to improve security posture. Combined with our industry-leading ML-Powered Next-Generation Firewall (NGFW) platform, IoT Security can automatically enforce policies to reduce strain on your operations team and prevent all threats to keep devices safe, and it requires no additional infrastructure for an effortless deployment.



6,759 Total Devices
613 IoT Devices
218 Applications
5 Subnets
46 Risk Score
14 Active Alerts to Date
34 Vulnerabilities to Date

All devices

| Type | ↓ Devices | Categories | Profiles | Devices at Risk |
|---|---|---|---|---|
| ● Traditional IT | 6,140 | 10 | 67 | 162 |
| ● Office | 605 | 27 | 58 | 40 |
| ● Network Devices | 8 | 1 | 2 | 0 |

Device Categories (39)

| | Devices | Profiles | Risk Score |
|---|---|---|---|
| Embedded Systems | 1 | 1 | 77 |
| Virtual Machine | 23 | 2 | 64 |
| Network Equipment | 25 | 9 | 62 |
| Smartphone or Tablet | 1,137 | 22 | 60 |
| Network Security Equipment | 15 | 3 | 58 |
| Personal Computer | 4,066 | 11 | 45 |
| Handheld Computer | 1 | 1 | 43 |
| Video Audio Conference | 318 | 3 | 38 |
| Smart Building | 7 | 2 | 37 |
| Specialized PC | 3 | 1 | 36 |
| Web Server | 4 | 1 | 36 |
| Video Gaming | 3 | 1 | 36 |
| Camera | 9 | 8 | 35 |
| Fitness | 12 | 1 | 31 |
| Smart Lock | 1 | 1 | 26 |
| Digital Video | 1 | 1 | 26 |

**Figure 1:** IoT Security device inventory

# 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, OT, or IT device to reveal its type, vendor, model, and an industry-leading 50+ unique attributes, including firmware, OS, serial, 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.

## 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 against themselves over time, as well as against similar crowdsourced devices, device vendor patching information, Unit 42 threat intelligence, and common vulnerabilities and exposures (CVEs), to continuously evaluate 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 Policy 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. 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 new 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 into different VLANs and applying the Zero Trust methodology.

## Prevent Known and Unknown Threats with Security Subscriptions

**Stop all threats headed for your IoT devices with the industry's leading IPS, malware analysis, web, and DNS prevention technology**. Every alert generated by a security product creates extra work for already inundated security teams to investigate and respond. IoT devices are susceptible to targeted attacks as well as older, forgotten viruses and worms originally built for IT devices. Seamlessly integrated with IoT Security, our cloud-delivered security subscriptions coordinate intelligence to prevent all IoT and IT threats without increasing workloads 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 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**: Enables the safe use of the internet by preventing access to known and new malicious websites before your users can access them.
- **DNS Security**: Disrupt attacks that use DNS for command and control and data theft without requiring any changes to your infrastructure.
- **GlobalProtect™** network security for endpoints: Extend ML-Powered NGFW capabilities to your remote users to provide consistent security everywhere in your environment.

## Ease Deployment and Operationalization with Cloud Delivery

Palo Alto Networks IoT Security is uniquely paired with our ML-Powered NGFWs to provide the industry's first complete solution offering visibility, prevention, risk assessment, and enforcement for Palo Alto Networks customers. 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 new 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 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 subscription. This powerful combination offers unmanaged device discovery, prevention, risk assessment, and enforcement in network locations where traditional firewalls are rarely deployed. You'll no longer need to purchase, integrate, and maintain multiple point products as well as change your operational processes to get full IoT security.

Every IoT security solution requires a sensor. Only Palo Alto Networks IoT Security provides one that also prevents threats and enforces policy, increasing your return on investment and reducing your operational overhead.

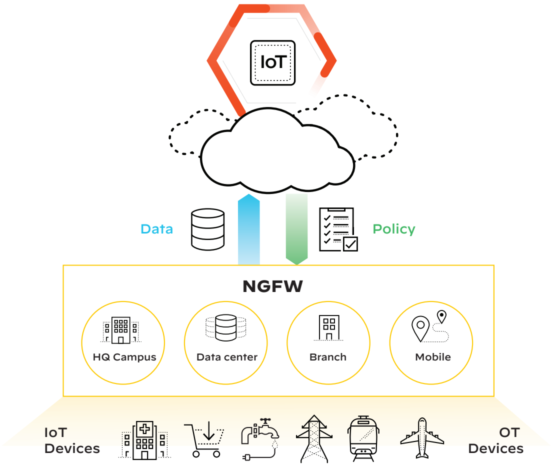


**Figure 2:** IoT Security architecture with NGFW for visibility, prevention, and enforcement

## 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 identity and understand rapidly changing IoT devices.
- **Understand full device context**. Utilize IoT device information across your ML-Powered NGFWs 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
- **Deploy and maintain with ease**. Enable cloud-delivered subscriptions and manage your security centrally with Panorama.
- **Leverage a single offering for comprehensive industry-specific intelligence**. Secure across Healthcare, Enterprise IT, Oil and Gas, Smart Cities, and ICS/SCADA environments, with support for ICS/SCADA protocols and transactions.
- **Enjoy complete IoT security**. Gain visibility, prevention, and enforcement for every IoT and OT device in your network through one product.

**Table 1: Palo Alto Networks IoT Security Features and Capabilities**

| | |
|---|---|
| IoT and OT device discovery and classification (type, vendor, model, 50+ unique attributes) | Prevention of all known threats |
| IoT and OT device profiling with patented three-tier ML | Vulnerability assessment with Common Vulnerabilities and Exposures (CVE) integration |
| Behavioral anomaly detection | Risk scoring based on the Common Vulnerability Scoring System (CVSS) |
| Risk-based policy recommendations | 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 | Palo Alto Networks Next-Generation Firewalls running PAN-OS 8.1 or later (PAN-OS 10.0 includes native and automated enforcement due to new Device-ID policy construct |
| Recommended Environment | Palo Alto Networks Next-Generation Firewalls 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 Next-Generation Firewalls. |
| Supported Next-Generation Firewalls | All models of PA-Series and VM-Series firewalls except VM-50 and VM-200. |

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