# How Palo Alto Networks IoT Security Achieves 70x Time Savings Protecting IoT Devices in the Enterprise

The mission of Palo Alto Networks is to ensure that each day is more secure than the last. As part of that mission, Palo Alto Networks has delivered a steady stream of innovations to help organizations secure their digital transformation technologies.

One prime example of digital transformation is the rise of the Internet of Things (IoT), Internet of Medical Things (IoMT), and Operational Technology (OT) devices, including surveillance cameras, temperature monitoring sensors, public retail kiosks, and healthcare as well as manufacturing equipment that streamline business processes and transmit data to applications for monitoring business functions. IoT devices have seen exponential growth in the enterprise in the past five years. According to a 2020 Gartner study, more than 80% of organizations currently use IoT technology to solve their business challenges. Palo Alto Networks Unit 42 IoT Threat Report found that, on average, 30% of the devices found on a typical enterprise network can be defined as IoT devices.

Unfortunately, securing all these devices, with their different embedded systems, diverse features, and mostly unencrypted traffic is often an afterthought, which is probably why almost 20% of organizations have reported IoT-based attacks in the past three years, according to Gartner.

IoT devices represent a serious enterprise security challenge because they are based on no-longer-supported operating systems and lack built-in security controls. This increases the attack surface and exposes you to a huge number of potential vulnerabilities and attack targets—an urgent issue that needs a viable resolution. 57% of these devices are susceptible to medium- or high-severity attacks, according to Palo Alto Networks Unit 42 IoT Threat Report, and 98% of IoT traffic is unencrypted. Traditional security tools such as Network Access Control (NAC) and endpoint protection solutions struggle to accurately discover, classify, group, and understand IoT devices.

There are solutions available for securing IoT devices, but most require a lot of IT time and resources to install, configure, and maintain. IT has to provision servers, install software and IoT sensors for hundreds of IoT devices, as well as create policies—including access control lists (ACLs)—for each. All of this can take days or weeks, after which there are continual security updates and changes to keep up with as new devices or new types of attacks arrive.

Many of these solutions can only discover and manage a fraction of the total number of IoT devices on an enterprise network, as they use a static, signature-based approach to identification that struggles to keep up with the constant onslaught of new devices and device variants.

## The Palo Alto Networks Solution

There is an alternative, however. Palo Alto Networks IoT Security is the industry's most advanced, comprehensive IoT security solution, harnessing a patented and behavior-based three-tier machine-learning model, crowdsourced IoT data, patented App-ID™ technology, and a cloud SaaS architecture to:

- Discover and identify *all* unmanaged devices, including type, vendor, model, OS, and rich device context encompassing 50+ attributes for each.
- Provide deep insights into device security posture, user and network information.
- Assess risk and an associated risk score for every IoT device, taking into account device compliance, vulnerabilities, threats, anomalies, and exploits.
- Establish normal device baseline behaviors in comparison to crowdsourced behavioral data for similar devices.
- Detect any behavioral anomalies that might indicate an attack.
- Provide actionable policy recommendations for native enforcement.

This is all without the need for current Palo Alto Networks NGFW customers to install any agents, additional sensors, or forklift upgrades.

### Key Capabilities

#### Quick & Accurate Discovery

- Discover more than 90% of all IoT, OT, or IT devices within 48 hours, and increasing thereafter
- Gain deep insights from 50+ device attributes

#### In-Depth IoT Risk Assessment

- Unit 42 threat intelligence, CVEs, and third-party vulnerability assessment solutions
- Additional assessment for healthcare with FDA recalls, MDS2, and PHI information

#### Risk Reduction Policy Recommendations

- Eliminate painstaking policy creation for Zero Trust with recommended policies
- Enforce policies natively or via NAC integration in just a few clicks

#### Prevention of Known and Unknown Threats

- Block known IoT malware, spyware, and exploits; stop access to malicious websites and prevent the use of DNS for C2
- Block unknown file- and web-based threats

Unlike other IoT security solutions, which often only *alert* you to security issues and then leave it to you to address them, Palo Alto Networks IoT Security applies its own best-in-class prevention capabilities to secure IoT devices, integrating natively with the Palo Alto Networks NGFW and ITAM/ITSM, NAC, SIEM and CMMS workflows.

### Zero Trust Architecture

The Palo Alto Networks solution is architected using a Zero Trust methodology that makes no assumptions about the credibility of users, IoT devices, applications, or data accessing or being accessed on an organization's network. Everything is verified every time all the time using a variety of powerful technologies and implementation strategies such as microsegmentation and least-privileged access. The Zero Trust Model doesn't stop at the point of policy creation but continues monitoring IoT devices and adjusts its actions based on new threat information, new policies, and continual analysis of user and device behavior.

## Return on Investment

In its January 2021 report, The Total Economic Impact of Palo Alto Networks for Network Security and SD-WAN, Forrester demonstrated that Palo Alto Networks IoT Security could reduce IoT device management hours by 20% and slash the number of new IoT devices purchased by 10%. In all, its ROI model calculated an enterprise could save US$1,702,020 over three years using IoT Security, compared to having no centralized IoT management platform.

Palo Alto Networks has gathered information through engagement with more than 100 current NGFW customers that shows:

- 15x to 20x deployment time savings using IoT Security that would otherwise be spent setting up new infrastructure for securing IoT devices
- 20x time savings from IoT Security's automated policy creation
- Reduce time to discover vulnerabilities from 3+ weeks to a few hours.
- Up to 70x savings total (12.45 hours total for IoT Security vs. up to 863.4 hours total for other solutions)


**Figure 1:** Increase ROI with IoT Security

## Fast and Easy Implementation

Deploying an IoT security solution on-premises in a production environment can take weeks or months of planning, preparation, and installation. Doing so requires installing IoT sensors on network segments that collect IoT device metadata and sending it to the IoT Security server or the cloud. Our research shows that organizations install an average of five sensors per IoT security solution deployment. Then IT has to install and configure security software and devise and deploy policies to all the devices.

With Palo Alto Networks IoT Security, there is no need to install any sensors at all. As the Palo Alto Networks NGFWs are already installed on your network, they fulfill all the functions of IoT sensors. There is also no need to provision servers or install or even update software, as Palo Alto Networks IoT Security is delivered via a SaaS architecture in which all software runs and is maintained in the cloud. Palo Alto Networks own suggested policies can save hours or days spent devising and deploying your own.

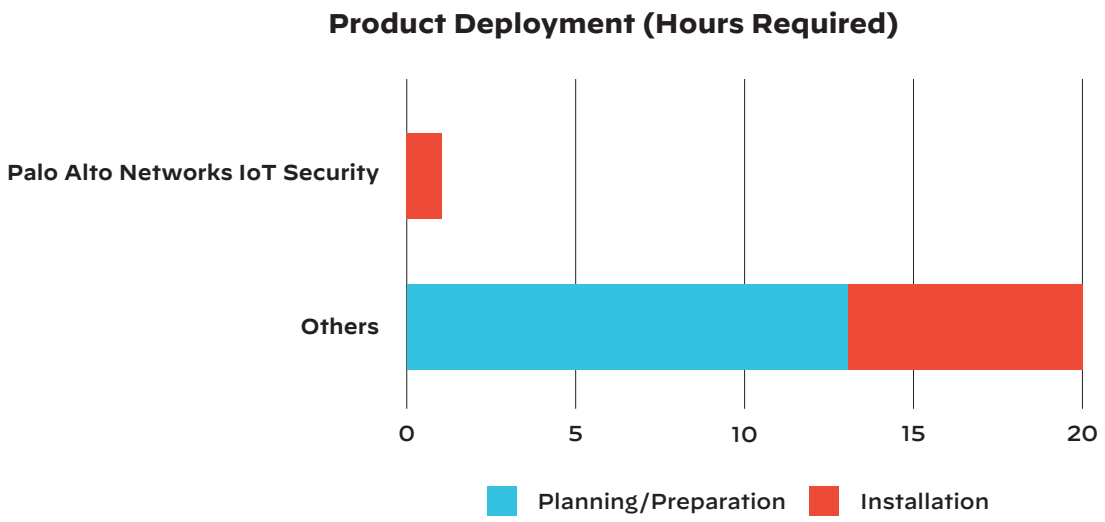


**Figure 2:** IoT Security requires up to 20X less time for product deployment

Rather than installing and configuring new software, any current Palo Alto Networks customer can activate IoT Security from their Palo Alto Networks NGFW (PA-Series, VM-Series, or Prisma® Access) in minutes, simply by flipping a switch. In doing so, Palo Alto Networks customers can implement complete IoT security without any delay.

Here's a comparison of the steps involved in deploying traditional on-premises IoT security solutions vs. Palo Alto Networks IoT Security for a typical five-sensor deployment and the time savings IoT Security allows.

**Table 1: Palo Alto Networks IoT Security Deployment vs. Other IoT Security Solutions**

| Palo Alto Networks IoT Security (5 sensors) | Other IoT Security Solutions (5 sensors) |
|---|---|
| **Total deployment time: 1- 4 Hours** | **Total deployment time: 15 - 20 hours** |
| **Planning and Preparation: 0 Hours**<br><br>**Planning:** Little or no planning time is required to deploy Palo Alto Networks IoT Security.<br><br>**Preparation:** There is usually no need to preconfigure or install sensors, as NGFWs already installed on the network act as IoT sensors. | **Planning and Preparation: 10 - 13.34 hours**<br><br>**Planning:** A sensor deployment typically involves analyzing customer sites, customer server infrastructure, network topology, and subnets to determine the number, locations, capacity, and configuration requirements of sensors.<br><br>**Preparation:** Includes preconfiguring sensors with IP addresses, hostnames, and other information and preparing the network and server systems for deployment.<br><br>The time required for planning and preparation averages 2 hours to 2 hours and 40 minutes per sensor, depending on the complexity of the customer environment.<br><br>For 5 sensors, this amounts to 10 - 13.34 hours of preparation time.<br><br>[2 hours x 5 sensors = 10 hours total]<br>[2.67 hours x 5 sensors = 13.34 hours total] |
| **Installation: 1 to 4 hours**<br><br>A customer can activate IoT Security networkwide in **1 hour** simply by flipping a switch on the Palo Alto Networks Panorama central management console.<br><br>Alternatively, the customer can activate an IoT Security subscription manually on each individual NGFW, which would take closer to **4 hours** for 5 NGFWs. | **Installation: 5 to 6.67 hours**<br><br>Installation of a sensor typically takes 1 hour to 1 hour and 20 minutes. For a 5-sensor deployment, this amounts to 5 - 6.67 hours of installation time.<br><br>[5 sensors x 1 hour installation time per sensor = 5 hours total]<br>[5 sensors x 1.34 hours installation time per sensor = 6.67 hours total] |

## Creating and Deploying Policies

Other IoT solutions are limited to IoT device discovery and security alerts. The responsibility for actually creating and deploying security policies typically falls on the network administrator or security operator, who must define ACLs and policies for IoT device application access based on research, device manufacturer documentation, and perceived risk assessment. Then they must assign policies either to individual devices or, more commonly, to device profiles[1] (which typically include about 10 devices per profile) manually in a long, often error-prone process. Each device profile consists of devices with similar characteristics and expected behaviors.

Our client research has found that, on average, a mid-sized enterprise creates 65 device profiles. The first round of policy creation typically focuses on mission-critical devices, which, from our client research, represent roughly 60% of the total number of IoT device profiles. Once those policies are applied, they often remain for the life of the device.

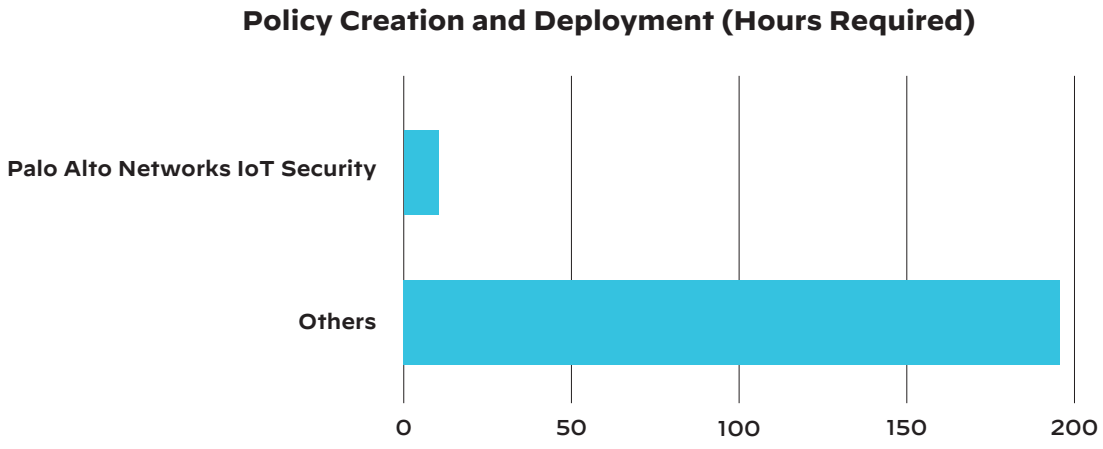


**Figure 3:** IoT Security takes 20X less time for policy creation

Palo Alto Networks IoT Security automatically generates policies for all your IoT devices, using extensive, continually updated and crowdsourced data for thousands of IoT devices together with an analysis of your own network and devices. In keeping with Palo Alto Networks Zero Trust framework, it doesn't stop with initial policy deployment but continually reassesses risk and device behavior and offers trust-based policy recommendations to improve your IoT security posture when necessary.

**Table 2: Palo Alto Networks Policy Creation Hours vs. Other Vendors**

| Palo Alto Networks | Other Vendors |
|---|---|
| **Automated policy creation: 9.75 Hours** | **Manual policy creation: 195 Hours** |
| There is no need to define policies for your IoT devices manually. IoT Security defines ACL and security policy risk reduction recommendations automatically for all profiles and devices based on IoT device classification, crowdsourced IoT device data, and device posture, applications, and risk assessments.<br><br>You can enable and enforce IoT Security recommended policies with a single click within our NGFW or orchestrate them via any NAC solution.<br><br>On average, the entire process takes about 15 minutes, or a quarter of an hour, per device profile, irrespective of the number of devices within a device profile.<br><br>[65 device profiles x 0.6 (60% of device profiles) x 0.25 hours per profile = 9.75 hours total] | ACLs and policies typically must be created manually for a group of IoT devices fitting a particular device profile.<br><br>In our experience, the number of devices per device profile ranges from 50 - 500, and an average of 65 device profiles per deployment.<br><br>They typically assign policies to 60% of those profiles in the first round (39 profiles).<br><br>It takes about 5 hours to define policies for a single profile. So for 60% of the 65 device profiles, it takes 195 hours to create security policies.<br><br>[65 device profiles x 0.6 (60% of device profiles) x 5 hours per profile = 195 hours total] |

1. Device profile: Each IoT device exhibits unique characteristics on the network. When an unknown device joins the network, one or more Palo Alto Networks firewalls use its advanced machine-learning algorithms and three-tier profiling system to determine the unique personality of the device and create a profile for it consisting of device type, category, vendor, model, operating system, and other characteristics.

## Continuous Risk Assessment and Threat Mitigation

The risks don't end with deployment and policy creation. The security landscape changes continually as new vulnerabilities and exploits are discovered, and IoT devices can be compromised at any time. Any unusual device behavior could indicate a threat and must be detected and addressed immediately. That's why continuous device monitoring, risk assessments, updates, and a steady schedule of vulnerability scans are necessary to keep the enterprise networks safe. This process is another feature of Palo Alto Networks Zero Trust framework: IoT Security monitors device behavior throughout its life on the network for vulnerabilities and indications of an attack, regardless of policies applied.

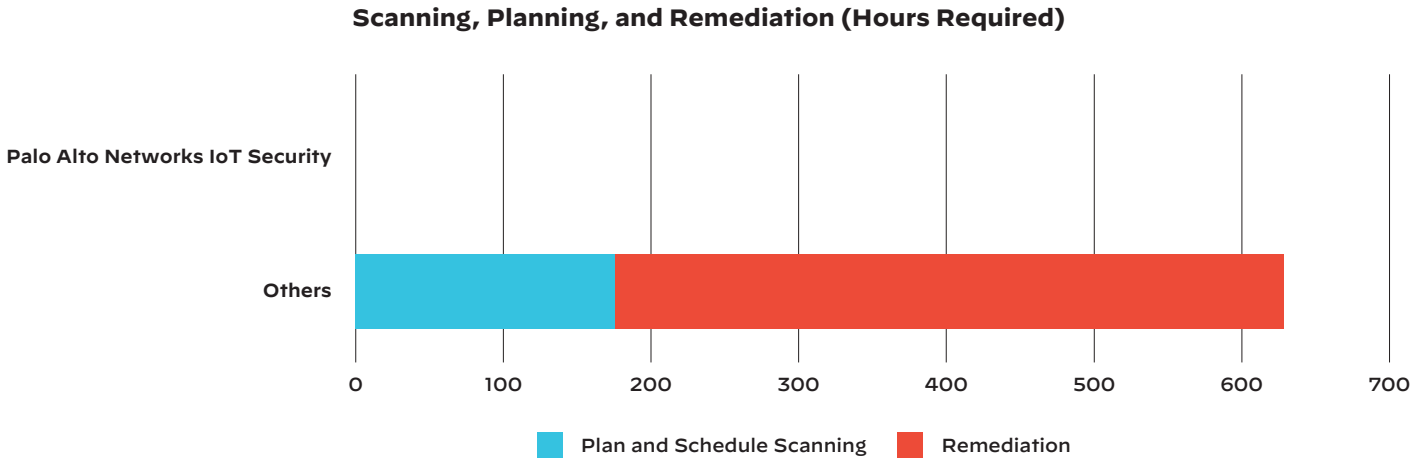


**Figure 4:** Understand and remediate risks and vulnerabilities in 381X less time with IoT Security

If any vulnerabilities or exploits are found, Palo Alto Networks NGFWs' built-in threat prevention can take actions to prevent and eliminate the IoT threat. With Palo Alto Networks Threat Prevention (an add-on service), it is not even necessary in many cases to create a vulnerability alert for each new threat, saving hours of time for Security Operations Center staff that can be spent on other critical security challenges. On average, 85% of new IoT threats are already covered by the NGFW's threat prevention features alone, leaving only 15% of vulnerabilities that need to be remediated manually.

Ideally, all IoT devices should be scanned, but in practice, our research shows that typically, 70% of device profiles and 50% of devices in each profile are scanned.

**Table 3: Understanding and Mitigating Risk**

| Palo Alto Networks IoT Security | Other Vendors |
|---|---|
| **Automated risk assessment: Total time needed to understand and mitigate/remediate risks: 1.7 Hours** | **Manual scanning: Total time needed to scan devices and understand and mitigate/remediate risks: 648.4 Hours** |
| **Step 1: Plan and schedule scans: 0 hours**<br><br>IoT Security continually monitors device behaviors and vulnerabilities. No manual scanning is required. | **Step 1: Plan and schedule scans: 193.4 hours**<br><br>Planning and scheduling vulnerability scans take about 4 hours per device profile.<br><br>It takes about 30 minutes or 0.5 hours to initiate scans manually on each individual device.<br><br>Typically only 70% of profiles are scanned, and it's only necessary to scan half the devices in each profile. In total, it takes 193.4 hours to plan, schedule, and implement IoT device scans<br><br>[65 device profiles x 0.7 (70% of device profiles) x 4 hours per profile = 182 hours total]<br><br>[65 profiles x 0.7 (70% of device profiles) x 0.5 (50% devices scanned per profile) x 0.5 hours per device scan = 11.4 hours]<br><br>**Total 193.4 hours** |

| Table 3: Understanding and Mitigating Risk (continued) | |
|---|---|
| **Palo Alto Networks IoT Security** | **Other Vendors** |
| **Step 2: Understand risks, plan and implement mitigation/ remediation: 1.7 hours**<br><br>With IoT Security, it takes an average of 15 minutes per profile to understand risk, assess, plan, and implement risk mitigation, irrespective of the number of devices in a profile.<br><br>The NGFW's built-in Threat Prevention safely prevents 85% of IoT threats without the need for any customer involvement, leaving only 15% of vulnerabilities or threats that actually have to be remediated by the customer. Only 1.7 hours are required to plan and implement mitigation/remediation for the same number of profiles as other solutions.<br><br>[65 profiles x 0.7 (70% of device profiles) x 0.25 hours per profile x 0.15 (15% of vulnerabilities/threats needing manual remediation) = 1.7 hours] | **Step 2: Understand risks, plan and implement mitigation/ remediation: 455 hours**<br><br>It takes an average of 10 hours to interpret results and plan and implement actions for a single profile. With 65 device profiles in a typical enterprise, it would take 650 hours to plan and implement mitigation actions. More typically, however, actions are taken for 70% of device profiles, or 455 hours total.<br><br>[65 profiles x 0.7 (70% of device profiles) x 10 hours per profile = 455 hours] |

## Summary

IoT devices will continue to grow rapidly in the enterprise, leaving unprotected gaps in the attack surface for organizations that fail to take steps to secure them. Most current IoT security products require many hours of planning, preparation, installation, policy creation, vulnerability scans, and risk remediation. With its SaaS delivery model, comprehensive IoT device discovery, integration with Palo Alto Networks NGFW, and automated policy creation and threat prevention, IoT Security can save you many hours, days, and weeks you would normally spend protecting your organization from the latest IoT device threats.

Click here to get a free 30-day trial of IoT Security, the industry's most comprehensive IoT security solution. You'll enjoy the benefits of our unique ML-powered solution and discover more than 90% of all IoMT, IoT, OT, and IT devices within 48 hours. These deep insights will help you realize a significantly better return on your investments in unmanaged devices.

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