The Right Approach to Zero Trust for IoT Devices

Table of Contents

Introduction

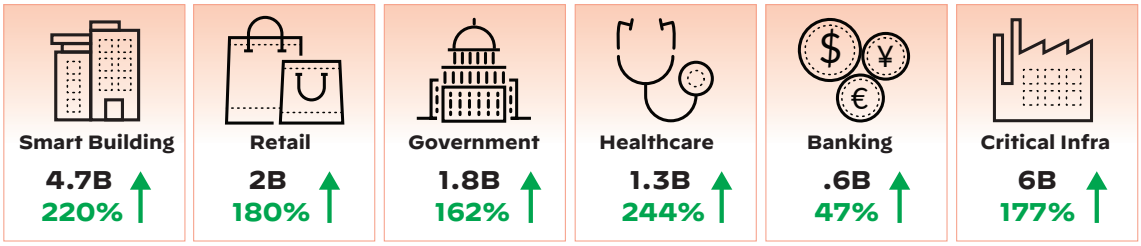
Networking and security teams have historically relied on protections at the network perimeter to secure the entire enterprise. The internal network was deemed trusted and secure. While everything outside was considered "dirty," everything on the internal network was considered "clean," and application traffic would flow unrestricted. However, recent and developing shifts in enterprise working models are having a far-reaching effect on the traditionally managed network perimeter for security.

The following trends are making organizations reassess their approach to security:

- **Digital transformation:** Increased IoT device adoption is helping organizations increase value, productivity, and reduce costs.
- **Cloud migration:** More and more devices, managed and unmanaged, are increasingly sending data to the cloud or multicloud.
- **Hybrid work:** Employees moving freely on and off the campus network are exposing the corporate network to outside threats.

The traditional network perimeter is no longer a circle of trust, which is proven by an increase in the cyberthreats and cyberattacks on an organization. The modern enterprise network now has to take into account all types of devices accessing the network, from conventional IT devices to non-conventional IT devices that are now internet-enabled and connected to the network, including security cameras, HVAC, smart lighting, smart blinds, infusion pumps, printers, smart coffee machines, smart TVs, virtual assistants, ATMs, and point-of-sale terminals, to name a few, comprising what is popularly called the Internet of Things (IoT). These devices reduce risk levels to the lowest common denominator and significantly widen the threat surface, making the network gravely susceptible to lateral exploits.

Palo Alto Networks Unit 42 2020 IoT Threat Report, based on 1.2 million endpoints, found that IoT devices comprised 30% of all enterprise devices in 2020. On top of that, Gartner's Machina IoT database predicts approximately 13% CAGR growth of IoT devices from 2020 to 2030.



10M new IoT devices onto the network every day*

30+% of your enterprise devices are IoT*

* Expected number of devices in 2030, and percent increase from 2020 to 2030.

Figure 1: Projected IoT growth by industry, according to Gartner's Machina database

The IoT explosion creates serious security concerns for enterprises as the IoT devices are shipped with vulnerabilities, are difficult to patch, lack security controls, and yet have unfettered access to the network. Here is a glimpse of some recent IoT attacks on enterprises.

Palo Alto Networks Unit 42's IoT Threat Report found that:

- Top threats for IoT devices are:
  - Network Scan Exploits (14%)
  - Password User Practices (13%)
  - Worms (12%)
  - Ransomware (8%)
- 57% of IoT devices are vulnerable to medium- or high-severity attacks
- 83% of medical imaging devices run on unsupported operating systems

An increase in the number of IoT devices and attacks thereon have necessitated that organizations reassess their risk management strategy and move toward adopting a Zero Trust approach to securing IoT devices.

Figure 2: IoT attacks across industries

What Is Zero Trust Security

With traditional network perimeter dissipating with work from home, BYOD, corporate resources shifting to the cloud, and IoT trends, along with the increase in cyberthreats, the need to adopt a Zero Trust approach as a core strategy to enterprise security is becoming undeniable. Palo Alto Networks defines Zero Trust as a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction. In addition, the robust framework as a security backbone provides an opportunity for enterprises to modernize and rebuild networks, pursue cloud adoption, and strengthen security operations.

Figure 3: Overall Zero Trust strategic objectives

Palo Alto Networks has outlined the Zero Trust framework with the guiding principles that follow, encompassing security for all users, applications, and infrastructure within an enterprise across the four key pillars of Identity, Device/Workload, Access and Transaction as represented in table 1.

Table 1: Key Zero Trust Capabilities and Continuous Validation

	Identity	Device/Workload	Access	Transaction
Zero Trust for Users	Validate users with strong authentication	Verify user device integrity	Enforce least-privileged user access to data and applications	Scan all content for malicious activity and data theft
Zero Trust for Applications	Validate developers, DevOps, and admins with strong authentication	Verify workload integrity	Enforce least-privileged access for workloads accessing other workloads	Scan all content for malicious activity and data theft
Zero Trust for Infrastructure	Validate all users with access to the infrastructure	Identify all devices including IoT	Least-privileged access segmentation for native and third-party infrastructure	Scan all content within the infrastructure for malicious activity and data theft

Securing unmanaged IoT devices makes for an essential pillar to achieve Zero Trust for infrastructure, and the guiding principles help define actionable Zero Trust security for unmanaged IoT devices.

The Right Approach to Zero Trust for IoT Devices

The Zero Trust framework for infrastructure guiding principles outlined in the previous section translates into further granular guiding principles specific to achieving Zero Trust for IoT devices. What follows is a Zero Trust framework that organizations should consider for securing IoT devices.

Table 2: Zero Trust for Infrastructure Extended to IoT Devices

Device/Workload	Access	Transaction
Discover all IoT devices	Recommend Zero Trust policies	Continously monitor IoT devices
Assess IoT security risk	Enforce Zero Trust policies	Prevent known and unknown threats

While many solutions in the market tout Zero Trust for IoT devices, they fail to truly meet the complex needs of IoT security. Here are some challenges of implementing Zero Trust for IoT devices.

Challenges in Implementing Zero Trust Security for IoT Devices

1. Hard to discover and identify

- Traditional agent-based endpoint security solutions are unable to discover and manage them. Given low processing power and CPU for most IoT devices, they are unable to have an endpoint agent installed on them.
- Most IoT discovery technologies only discover and classify the IoT devices for which they have pre-populated signatures. Unfortunately, approaches based on device fingerprinting or signatures are unable to scale to discover all IoT devices because of the sheer variety in operating protocols, standards, and newer types of devices coming onto the network.
- IoT devices are rarely assigned a unique hardware identifier (unlike IT devices) and are manufactured in batches. Given this, most of these devices remain undiscovered or unidentified and unaccounted for in an IT team's device inventory creating shadow IoTs.

2. Hard to authenticate, define policy, and segment

- Most IoT devices don't support traditional enterprise authentication and authorization processes such as 802.1X or single sign-on. Alternatively, MAC Authentication Repository (MAR) list does not work either due to poor device classification. Since IoT devices are business enablers, network teams must onboard them manually without thoroughly risking their risk posture.
- Segmentation policies and rule creation require hours of manual work. Furthermore, the limited visibility into the unmanaged devices makes it additionally hard to segment them properly as a sound practice of preventing lateral movement of threats.

3. Hard to continually assess

- IoT devices remain out of vulnerability scanner scope due to their lack of visibility into IoT devices.
- A lot of IoT and OT devices are part of the critical infrastructure, and active probing or scanning of these devices for risk and vulnerability assessment could also result in network disruption.

4. IoT security solutions lack security

- Existing IoT security solutions also do not have the intelligence or capability to recommend Zero Trust risk reduction policies. It is up to the security teams to gather device insight and context and come up with Zero Trust policies manually. That can be a long and error-prone process.
- Existing IoT security solutions are alert-only and lack built-in prevention of threats and enforcement of security policies.

Achieving Zero Trust for IoT Devices

Palo Alto Networks IoT Security brings IoT devices into the fold of the Zero Trust security model based on the three pillars of device/workload, access, and transaction and the principles thereof to minimize IoT security risks and keep your network safe from cyberattacks. Palo Alto Networks has made it exceedingly easy to achieve Zero Trust for IoT devices, thus elevating organizations' overall security posture. Here is the practical approach to how organizations can achieve Zero Trust with IoT Security from Palo Alto Networks.

Zero Trust Principle One: Device/Workload

Identify all devices, including IoT

1. Discovery

You can't secure what you can't see. To extend the principles of Zero Trust, it is essential to go beyond users and standard IT devices to include all unmanaged IoT devices in the network. IoT Security from Palo Alto Networks is the only agentless IoT security solution that uses machine learning (ML) and deep packet inspection with crowdsourced telemetry to discover and classify every connected IoT device in the network, including the never-seen-before ones. ML is a superior approach as compared to the reactive, traditional, signature-based methods of device discovery. As newer IoT device types get added to the network fueled by newer wireless protocols such as 5G or by a hybrid work-from-home model, the ML-powered device discovery approach ensures that the new devices are quickly and accurately discovered and classified in real time.

Our IoT Security analyses 200 parameters to accurately match each device's IP address accurately with its type, vendor, and model to surface 50+ essential device attributes that completely profile the device. Accurate and granular device classification is a necessary prerequisite to differentiating unmanaged IoT devices from managed IT assets. Doing that enables enforcement of Zero Trust-driven security policies that only allow approved traffic in your IoT environment.

Here are the top categories of contextual information that IoT Security provides.

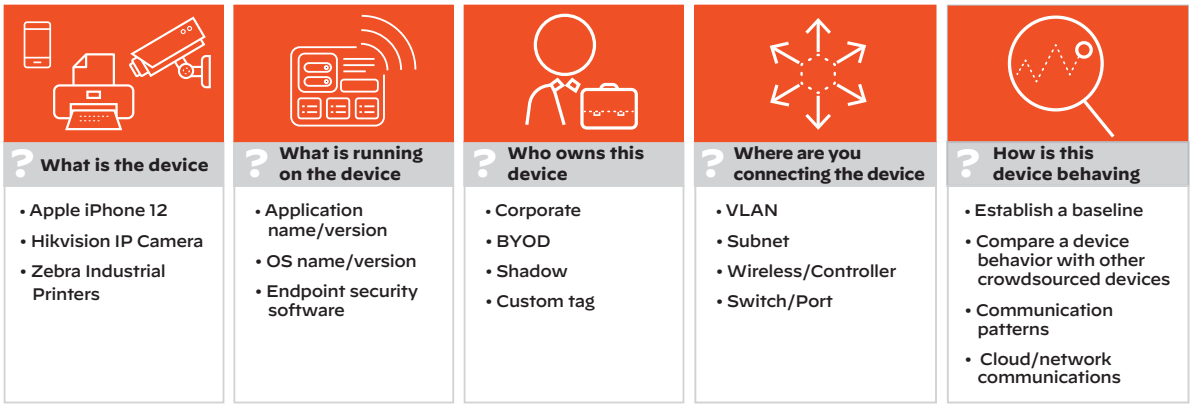


Figure 4: IoT Security can discover 90% of the devices within 48 hours—and more after that

2. Risk Assessment

The next step in applying the Zero Trust framework is to assess the risk with high confidence and determine the level of risk for IoT devices. "Risk" has become a nebulous term and has been used interchangeably with "threat" and "vulnerability." To really understand risk, one needs to know what it truly means. Risk is a function of threats exploiting vulnerabilities in order to compromise or damage assets (IoTs in this case). Therefore, IoT device risk is measured based on three vectors: threats, vulnerabilities, and asset context. IoT Security from Palo Alto Networks detects and assesses risk across all three vectors. This is done leveraging crowdsourced device data, machine learning-powered device behavior anomaly assessment, proprietary Unit 42 Threat research, CVEs, third-party vulnerability management information, and more.

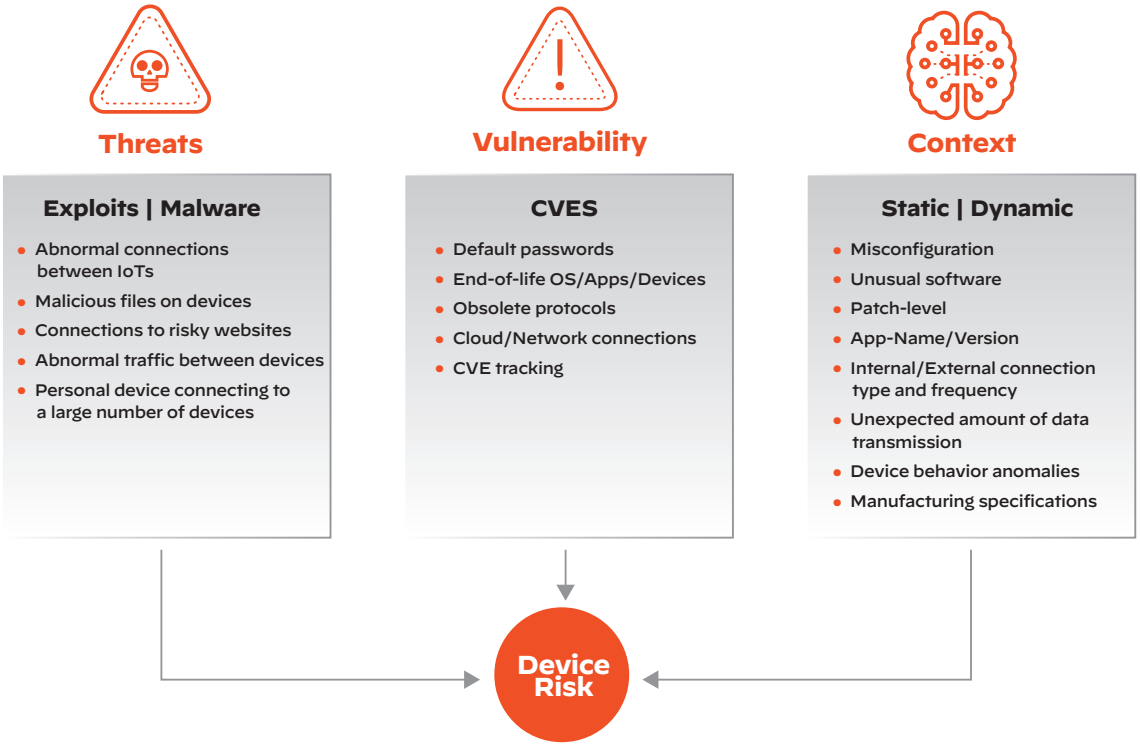


Figure 5: Comprehensive risk framework and assessment

IoT Security measures risk and assigns a score for the amount of risk it observes at four levels:

1. Individual IoT devices
2. Device profile
3. Site
4. Organization

When calculating the risk scores of device profiles, sites, and organizations, IoT Security considers not only the scores of individual devices within a particular group but also the percent of risky devices in relation to all devices in the group. The different scores provide a simple means to check the risk posed at various points and areas of your network.

Read how you can cut down from three-plus weeks to a few hours to discover IoT device vulnerabilities in your network.

Zero Trust Principle Two: Access

Least-privileged access segmentation for native and third-party infrastructure

3. The Least Access Policy

The least access as a policy is a key tenet of Zero Trust. The least access as an IoT security policy is intended to offer a minimum level of access by an IoT device to the network. Since most IoT devices are "purpose-built" and have predictive behavior, this allows for the application of the least access policy, which can be used in the following scenarios:

- **Virtual patching to keep IoT devices operational:** The least access policy can allow even vulnerable devices to operate by blocking or restricting their access to certain resources. This policy comes in handy where IoT/OT devices are business drivers and need to be operational, for example, critical IoT devices in healthcare delivery organizations or on manufacturing floors. This is a temporary strategy to limit the exploitation risk of a vulnerability while the vulnerability is remedied.
- **Network access control policy:** The least access policy is also used to limit or restrict the access of IoT devices to certain resources to carry out their required task. For example, a security camera only needs to communicate with video storage and the vendor website for firmware updates.

Today, one has to go through multiple labor-intensive steps to define and develop risk reduction policies per device profile. The manual steps include inventorying IoT devices, defining device profiles by device type or function, establishing behavioral baselines, defining policies that do not disrupt the business operations, and integrating with other enforcement technologies to enforce those policies.

IoT Security from Palo Alto Networks is the only solution in the market today that goes a step further from risk assessment to automatically provide risk reducing Zero Trust least-privileged access policies. 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 updated automatically, keeping your administration overhead to a minimum.

Read how you can have 20X time savings from the automated policy creation of IoT Security.

Network Segmentation Policy

To follow "never trust, always verify" as a guiding principle to Zero Trust, segmenting the IoT devices can be viewed as a step toward Zero Trust. For instance, housing mission-critical heart rate monitors in the same network as imaging systems would not be a sound practice in healthcare organizations. A device profile-based segmentation approach that considers many factors, including device type, function, mission criticality, and threat level, provides an isolation approach that significantly reduces the potential impact of cross-infection.

IoT Security enabled on the Palo Alto Networks Next-Generation Firewall takes a device profile-based fine-grained segmentation approach that takes those factors into consideration to enable sequestration. This significantly reduces the potential impact of cross-infection between IT and IoT devices. The use of Palo Alto Networks Next-Generation Firewall (NGFW) as a segmentation gateway leverages its inherent networking capabilities for seamless deployment into an existing environment and allows for controlled introduction of security controls over unmanaged IoT devices within a network.

Suppose customers prefer to choose a network access control (NAC) solution to segment their network. In that case, IoT Security provides built-in integration with Cisco ISE, Forescout®, and Aruba ClearPass® to implement segmentation; however, since NAC only has visibility in devices that can be authenticated, it has blind spots to IoT devices that cannot be authenticated as they do not have users associated with them. Therefore, IoT Security provides discovered unmanaged device information to the NAC solution and provides additional device context to segment them intelligently. Here is a sample of one of our live customers showcasing how IoT Security plugs in the NAC solution's visibility and context blind spots.

Table 3: How IoT Security Plugs In NAC Blind Spots		
MAC	NAC Identity	IoT Security Identity
00:*0:7*:73:37:5*	AmbiCom-Device	Carefusion Infusion Pump Base Station
c8:2*:*4:56:27:06	Apple-Device	Medical Workstation
08:60:6*:*8:06:83	Asus-Device	Medical Workstation
00:08:74:*2:50:*5	Dell-Device	DICOM-Viewer
00:2*:5*:6*:06:72	HP-Device	DICOM-Imager
00:09:6*:*6:60:7*	IBM-Device	Medical Workstation
00:*0:*4:2*:*0:94	INSIDE-Technology-Device	Medical Workstation
Total Devices	**5,958**	**12,012**

Table 4: Discovered NAC and IoT Security Devices	
NAC	IoT Security
Discovered devices= 5,698	Discovered devices=12,012
NAC Context=	IoT Security Context=
AmbiCom-Device	AmbiCom Carefusion Infusion, base station

Context-aware partitioning of IoT devices ensures they have least-privileged access and connect only to required applications. In addition, It keeps them quarantined from guest and business networks and minimizes operational downtime in critical IoT infrastructures by mitigating incompatibility issues cropping up between systems.

4. Policy Implementation

IoT Security can implement the recommended Zero Trust security policies natively with its NGFW or via third-party enforcement points. The following outlines how the implementation is achieved:

- Enforce recommendations with one click via Palo Alto Networks NGFW. Our patented Device-ID™ policy construct tracks an individual device across the network, providing detailed information as a context within the ML-Powered NGFW for any alert or incident that may occur—regardless of changes to the device's IP address or location. In addition, policy rules and Layer 7 controls are automatically updated as the location and identified risks change. See table 5 on how Device-ID is more scalable and provides faster remediation and response to threats.
- Enforce the recommended policies using our NAC integrations with Cisco ISE, Forescout, or Aruba ClearPass.

Table 5: How Device-ID Helps Administrators Get Fast and Accurate Policy Implementation	
Without Device-ID	With Device-ID
Reliance on IP address as a proxy for device identity does not provide accurate device identity	Device identity is available within policy
Reliance on users, network, or device admins to properly address device issues is error-prone and creates an opportunity for exploitation	Consistent policy enforcement regardless of where the device is connected or how it is configured
Reliance on external systems such as NAC or asset management requires integrations to be built and maintained	Directly feed Device-ID using IoT Security, eliminating the need for complex integrations
Threat or incident investigation needs SOC to touch multiple systems to track down which specific device generated the alert.	Threats alert with device info received by SIEM

Zero Trust Principle Three: Transaction

Scan all content within the infrastructure for malicious activity and data theft

5. Continuous Monitoring

Continuous monitoring is the final and crucial step in closing the Zero Trust security loop for IoT devices. Even if a device has been profiled and placed in the correct segment, it could still get compromised during its course of connection to the network. If and when a device is found to be compromised, its access to the resources and the network should be blocked immediately.

Our ML-based IoT Security automatically ascertains the device's identity and verifies "normal behaviors." Once "normal behaviors" are determined, the solution kicks in anomaly detection to uncover and prioritize any potential deviation from the baseline. Our machine learning establishes a baseline of Layer 7 IoT device behaviors and provides two types of insights:

- IoT Security uses ML and compares the behaviors with similar crowdsourced devices to continually establish a behavior baseline and monitor deviation. This information helps automate Zero Trust policy creation.
- IoT Security also monitors device traffic and communication patterns and continually contrasts them against existing VLAN design to simulate the right microsegmentation design and, after that, enforcement.

IoT devices generate unique, identifiable patterns of network behavior. Using machine learning and AI, IoT Security recognizes these behaviors and identifies every device on the network, creating a rich context-aware inventory that's dynamically maintained and always up to date. After identifying a device and establishing a baseline of its normal network activities, it monitors its network activity to detect any unusual behavior indicative of an attack or breach. IoT Security notifies administrators through security alerts in the portal and, depending on each administrator's notification settings, through email and SMS notifications if it detects such behavior. It also blocks the device that is not compliant with the established security and compliance policy from accessing the network.

6. Built-in Prevention

IoT Security monitors all IoT devices and stops all threats with the industry's leading IPS, malware analysis, web, and DNS prevention technology. 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.

Zero Trust Throughout Your Infrastructure

In the past, securing users, applications, and devices identifiable inside the network perimeter was the obvious thing to do. However, the explosion of unmanaged IoT devices in enterprises with blurred, ever-expanding network security perimeter sets a new paradigm. As a result, enterprises must embrace a new yet simplified approach to IoT security modeled steadfastly on Zero Trust best practices.

Get a free product demo of the industry's most comprehensive IoT security solution and see for yourself how Palo Alto Networks IoT Security service significantly simplifies the adoption of the Zero Trust framework for unmanaged IoT 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