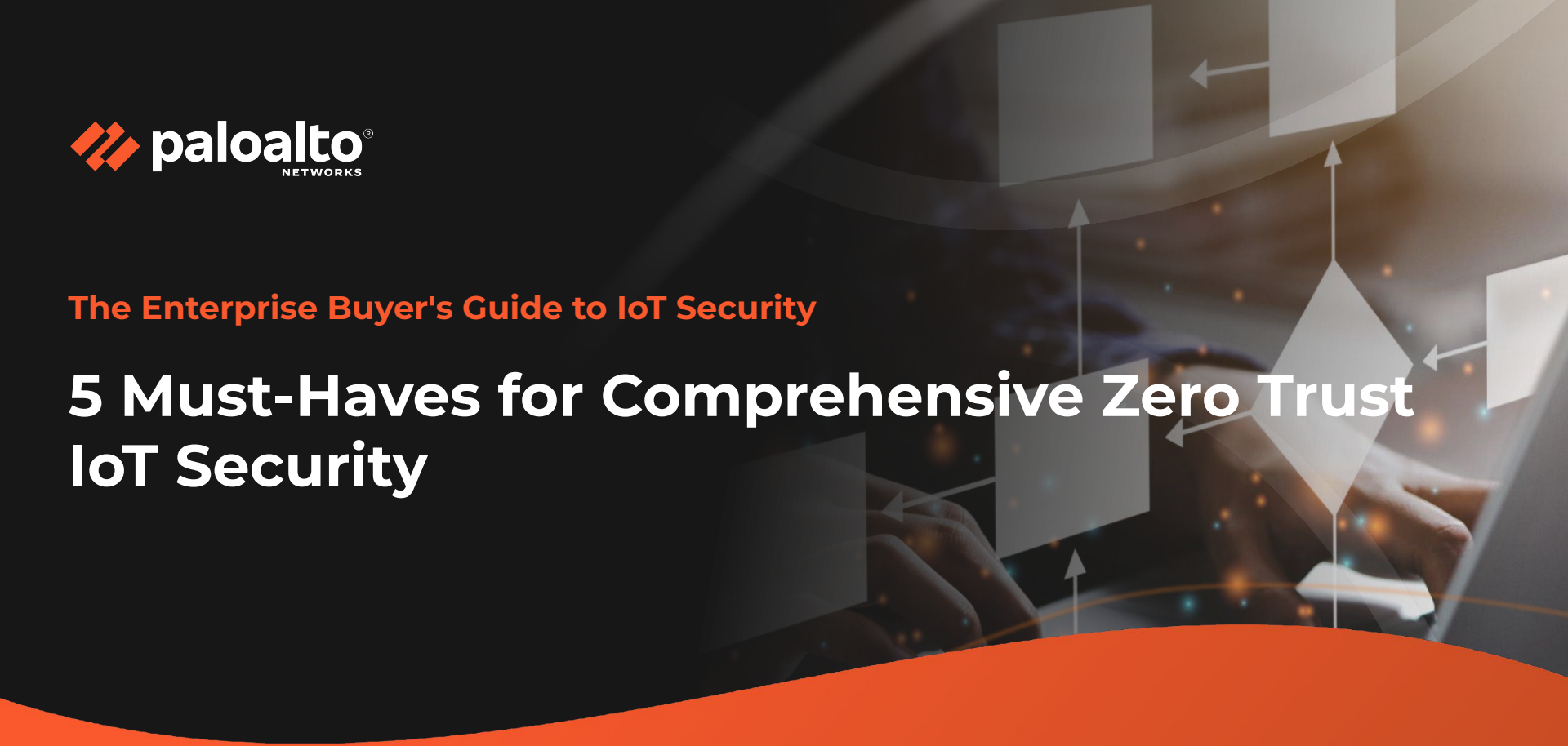


paloalto NETWORKS

The Enterprise Buyer's Guide to IoT Security

5 Must-Haves for Comprehensive Zero Trust IoT Security

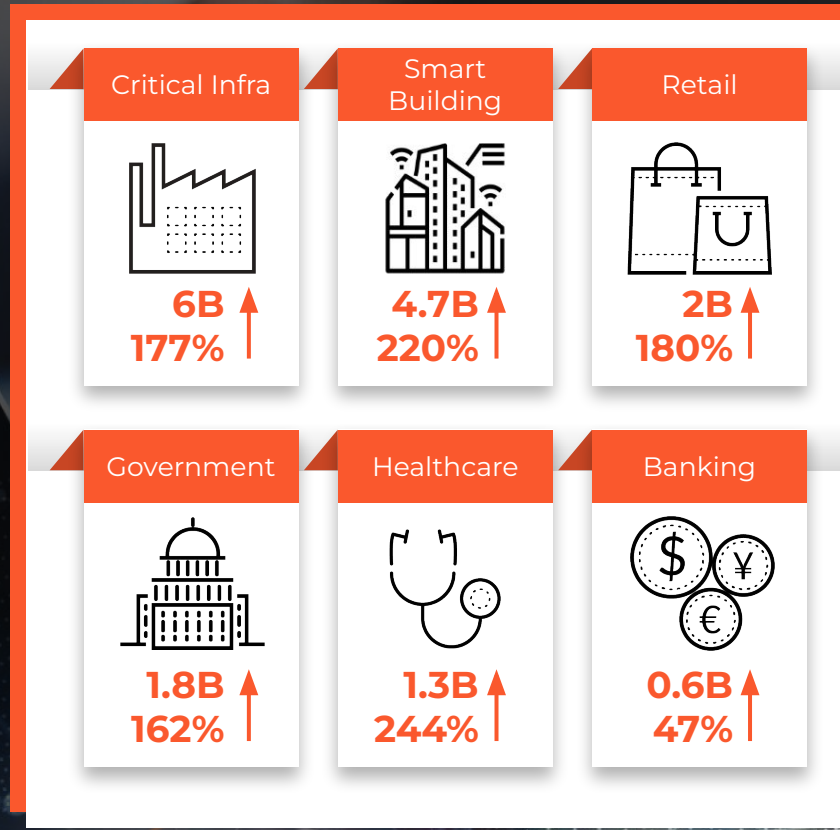
Table of Contents

The Adoption of Connected Devices Across Enterprises Continues to Surge

Gaining momentum during the pandemic, the expanded use of connected devices has become a fundamental part of the enterprise ecosystem.

10M
new smart devices added to the network every day*

4x
the number of enterprise IoT devices than users



*Expected number of devices in 2030 and % increase from 2020 to 2030

Trust-Based Security Is the Weakest Link

IoT devices provide a tremendously expanded attack surface with a remarkably low barrier to entry for cyberattackers. Enterprises must adopt a new security paradigm to combat these threats.

Several of the many factors that put connected devices at elevated risk include:

- Legacy operating systems
- Unsegmented networks
- Preexisting vulnerabilities
- Elusive device discovery and identification
- Authentication challenges

Network-connected IoT devices are targets for attackers because they are **shipped with vulnerabilities** and **remain vulnerable** when they are deployed.

More than half of connected devices are considered highly vulnerable.

98% of all connected device traffic is not encrypted.

83% of network-connected devices run an unsupported OS and are difficult to patch.

Most existing security systems depend on trusting the connected users, applications, and devices. Because of this, application traffic can flow unrestricted—including that generated from connected devices. With the rise of network-connected devices and other changes, such as cloud migration and hybrid work, the traditional network perimeter is no longer a circle of trust.

Our Unit 42 IoT threat report found that **57%** of all IoT devices are vulnerable to medium- or high-severity attacks and **40%** of CISOs are still struggling with IoT visibility and understanding.

Implicit Trust
Must Be Eliminated

There were 3B attacks on network-connected devices in 2021.
That's 2X more than in 2020

Security approaches historically employed by networking and security teams cannot effectively protect the sprawling and often unmanaged ecosystem of millions of network-connected IoT devices.

Traditional security models target the protection of the entire attack surface, which is difficult to identify and constantly evolving—especially when it includes IoT devices. In addition, this requires opening broad access and creates vulnerabilities.

To effectively defend against persistent threats, organizations need to eliminate implicit trust in all systems and people granted network access. Limiting access to resources and continually evaluating anyone or anything with authorization can protect the vast enterprise attack surfaces.

Use Zero Trust as a Foundation for IoT Security

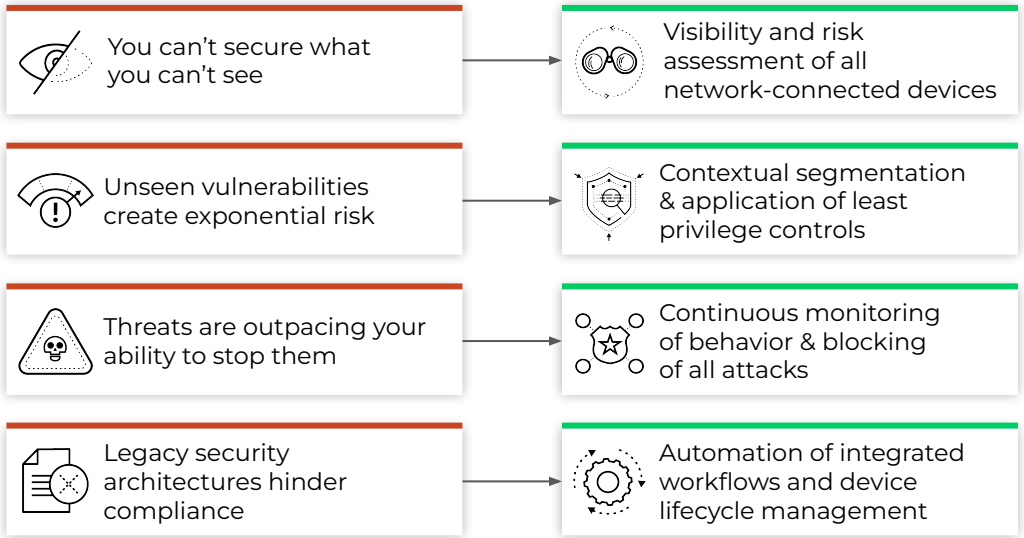
Zero Trust enforces least-privileged access for IoT devices, limiting exposure of data and applications.

Zero Trust provides a security framework for connected devices that continuously validates their integrity.

With a Zero Trust approach, IoT device transactions are secure and validated to thwart cyberthreats and protect data.

Areas of focus when applying a Zero Trust strategy to protect IoT devices include:

- Identify all IoT devices and workloads and assess risk.
- Limit access by applying least-privileged access and network segmentation policies.
- Continuously monitor all IoT devices and block any that show signs of anomalous behavior.

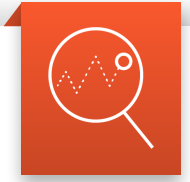


Current Solutions Don’t Address IoT Security Challenges

Prevailing security mechanisms are not adequate—or effective—when it comes to securing IoT in the enterprise.

A growing number of virtually invisible IoT devices are becoming invariable constituents in enterprise networks. From building and street light sensors, flow monitors, surveillance cameras to IP phones, point-of-sale systems, conference room technology, medical devices, and so much more, IoT, IoMT, and OT are on the network and in the organization. These devices significantly expand an organization’s attack surface. Prevailing network perimeter defenses are poorly equipped to address the security challenges arising out of this inflow.

Current Solutions That Fall Short



Vulnerability Assessment
for IoT devices are inherently more complicated because of the diversity of hardware, software, and communication protocols involved. While helpful to a degree in identifying potential weaknesses, they don’t actually solve the problem.

NAC or Network Access Control
solutions and methodologies just don’t scale well for IoT. They lack the sophistication required to identify and provide adequate security to IoT devices in the context of today’s threat landscape and can merely be used for enforcement only after an issue is identified.

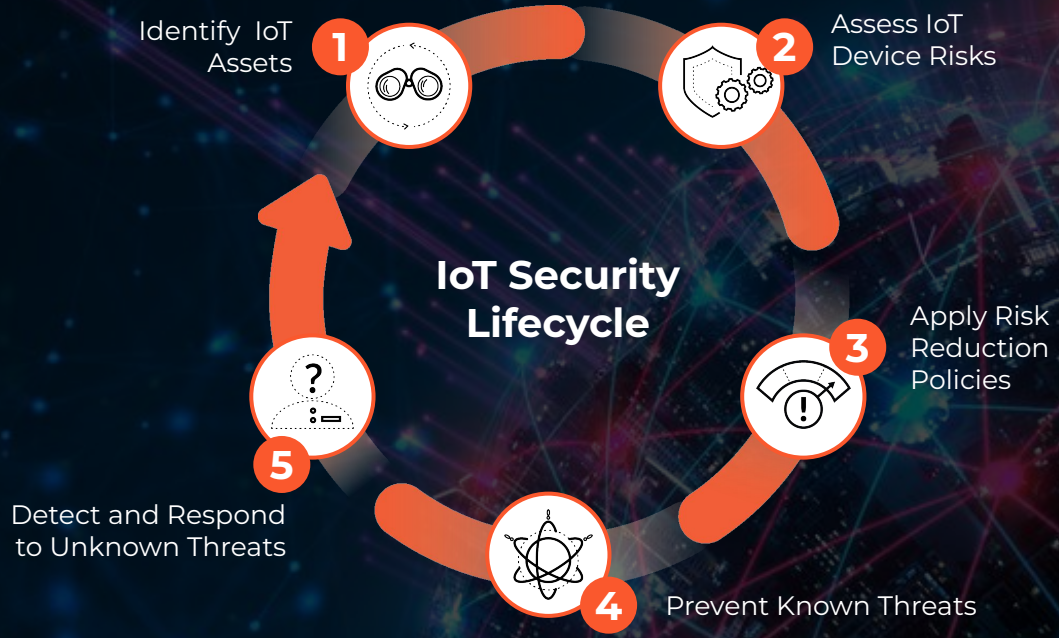
Point Solutions for IoT Security
require too much effort for security teams—implementing single-purpose sensors, integrating with existing systems, and enduring a high learning curve.

CISOs must consider a “lifecycle approach” to level up their IoT security strategy.

Implement a Proven Process to Secure and Manage IoT Devices

Secure network-connected IoT device workflows in five steps that cover the entire device lifecycle and support a Zero Trust security framework.

Network-connected IoT devices need to be understood in the context of a complete device management methodology to minimize risk to the network. The ideal methodology relieves both network security and IT teams from the day-to-day operational burdens of securing and managing these devices across all stages of the IoT lifecycle—from discovery of IoT devices and their associated risks to security actions that enforce protections and defend these devices from known and unknown threats.



To implement the IoT security lifecycle, look for **5 must-haves** in your IoT security solution.

1. Identify IoT Assets

Get complete visibility into all network-connected devices across the enterprise.

The enterprise IoT security lifecycle begins with determining the state of your security posture by gaining complete visibility into the attack surface. Collect an up-to-date inventory of all known and unknown network-connected devices. During this device discovery process, the solution should capture essential attributes to provide full context on each device.

Employing this discovery process allows all IT and business stakeholders to get a complete picture of what the IoT device landscape looks like in your organization.

An ideal IoT security solution should do the following:

- Identify at least 90%+ of devices in visible segments within 48 hours.
- Detect new, never-seen-before devices with ML-based device classification to categorize devices by a variety of classifications, including vendor, make, model, type, operating system, firmware, location, subnet, risk score, PII type, and MDS2.
- Perform detection of newly plugged-in devices within minutes—not hours or weeks.
- Differentiate unmanaged network-connected devices from managed IT assets.
- Log all connected devices to help IT and security teams identify unmanaged devices.
- Be able to automatically update your asset management solutions, such as CMMS, ITSM, and CMDB, with rich information, gathered from network-connected devices.
- Leverage multipurpose sensors that integrate into existing infrastructure.

2. Assess IoT Device Risks

Proactively reduce risk with continuous risk assessment and monitoring of IoT devices.

In the risk assessment stage, you must monitor IoT devices at all times. Real-time risk monitoring, reporting, and alerting are crucial for organizations to reduce risks proactively. Signature-based solutions lack accuracy and speed, which limits your ability to protect these assets.

Accurate risk assessment in the IoT security lifecycle lets you take a better approach. It allows your IT security teams to continuously scrutinize devices and monitor their traffic patterns to drive proactive NAC segmentation and reduce the threat surface. Risk assessment also prompts IT teams to proactively consider microsegmenting the network by different device types and classes to forestall the possibility of lateral movement of threats.

An ideal IoT security solution should do the following:

- Integrate with multiple threat feeds, such as CVE, MDS2, and RSSI, to accurately map vulnerabilities with the network-connected device inventory.
- Detect and report anomalies in connected devices that may affect risk scores—in real time.
- Calculate risk scores on network-connected devices and device categories.
- Track changes to risk scores and store complete connected device risk history for compliance purposes.
- Integrate with vulnerability management systems and connected device vendors for centralized enterprise risk management and to deliver information to security teams.

3. Apply Risk Reduction Policies

Leverage automated risk-based security policy recommendations and enforcement.

An ideal IoT security solution will not burden you with additional infrastructure or investment. Look for a solution that will allow your IT security teams to simply leverage your existing next-generation firewall investment for comprehensive and integrated security posturing. With this, least-privileged access policies can be automatically recommended and natively enforced based on the level of risk, and, the extent of untrusted behavior detected in your network-connected devices.

Taking into account that trust is nothing but a vulnerability, your IoT security solution must directly align with the principles of Zero Trust to enforce policies for least-privileged access control. This significantly reduces the pathways for adversaries, whether they are inside or outside your organization, to access your critical network-connected assets.

An ideal IoT security solution should do the following:

- Provide mechanisms to convert connected device behavior baseline into policies that only allow trusted behaviors.
- Automate enforcement with network-connected device and application identification.
- Support both allow lists and block lists.
- Track connected devices and applications to enforce policies regardless of where they reside within the network.
- Update policies automatically to limit manual updates every time a change occurs.
- Integrate into NAC and automatically share connected device information to enforce controls and context-aware segmentation.

4. Prevent Known Threats

Take swift action to mitigate risks as soon as the threat is made known.

The diverse nature of IoT devices creates a highly distributed environment in your network with numerous points of compromise. Successful outcomes of your security posturing in stage four of the IoT security lifecycle will require actionable insights. It is important to have information related to the detection and prevention of known threats that impact your connected devices to enable a swift response for threat mitigation.

Look for a threat prevention mechanism that uses payload-based signatures to block advanced threats. This will ensure the most up-to-date security posture and enable defense against known threats for rapid responses to anomalous connected device vulnerabilities and weaknesses across your network. In addition, this type of solution will not overburden security teams with detection alerts that could be stopped.

An ideal IoT security solution should do the following:

- Selectively enable security threat protections based on the IoT device group's risk posture.
- Detect and prevent known threats from IoT device exploits.
- Block connected device malware attacks that stem from malicious websites.
- Prevent attacks on network-connected devices that use DNS for command and control to steal data.
- Prohibit unknown threats to connected devices that are delivered via payloads.

5. Detect and Respond to Unknown Threats

Quickly detect and respond to zero-day vulnerabilities.

When it comes to detecting and preventing truly unknown threats, legacy approaches isolate the threat data that each organization receives and generates. The result of these legacy approaches is silos, which reduce the possibility of prevention. To meet the requirements of the last step in the IoT security lifecycle, your solution should be capable of leveraging a new approach.

It needs to draw from a collective threat intelligence engine that delivers real-time malware analysis and protections from zero-day attacks. Tapping into crowd-sourced data from a global community of subscribers provides collective immunity and saves your IT security team valuable time. This is achieved by leveraging information from connected devices, risk scores, vulnerability data, and behavioral analytics to investigate never-heard-before threats unique to your ecosystem of network-connected devices—right from the outset. This last step will also uncover potential threats missed in earlier stages and leads you into a cyclical process for continual improvement.

An ideal IoT security solution should do the following:

- Detect abnormal behaviors at different tiers—first at the device category level, then at the device vendor/model level, and last at the device instance level.
- Leverage crowdsourced intelligence using machine learning enhanced with threat modeling to detect unknown threats or attacks and provide proactive notifications or actions.
- Integrate into SIEM and SOAR using a simplified playbook-based approach to orchestrate incident response and threat prevention actions.
- Connect with active IoT device security researchers to discover any new threats as soon as information is available.

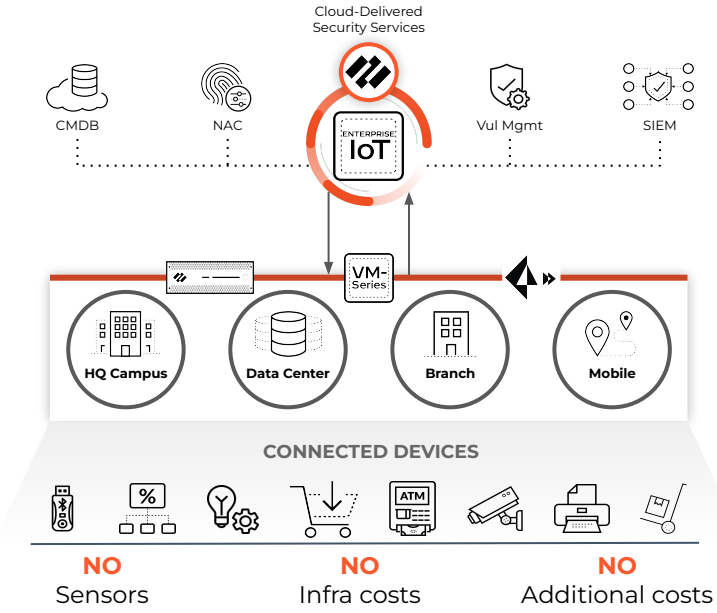
Enterprise IoT Security by Palo Alto Networks

The industry's the most comprehensive Zero Trust solution for IoT devices.

- Provides visibility, prevention, enforcement, and operational insights in a single platform powered by machine learning
- Uses machine learning (ML) with crowdsourcing to quickly and accurately discover all devices, even unknown ones
- Offers built-in prevention, instead of an alert-only approach, to keep unmanaged devices safe from all known/unknown threats and vulnerabilities by preventing threats and blocking vulnerabilities from entering your network
- Decreases the cost of enterprise security with operational insights for IT and security teams
- Automatically enforces least-privileged access policies directly or through integrations to help reduce the strain on your network and security operations teams, keep all connected devices safe, and increase their uptime and availability
- Delivers enterprise-class security for connected devices from a single platform that can be deployed effortlessly without requiring additional infrastructure

Palo Alto Networks Enterprise IoT Security, with its Zero Trust framework, is the only solution in the market today that enables maximum return on investment (ROI) and automated IoT device security. This unique solution provides deep visibility, focused operational insights, and enhanced security for network-connected devices all in one platform.

Network effect of 85,000+ Palo Alto Networks customers turns unknown threats to prevention 180x faster and delivers over 4.3m updates/day



Palo Alto Networks Enterprise IoT Security Integrates with Third Parties

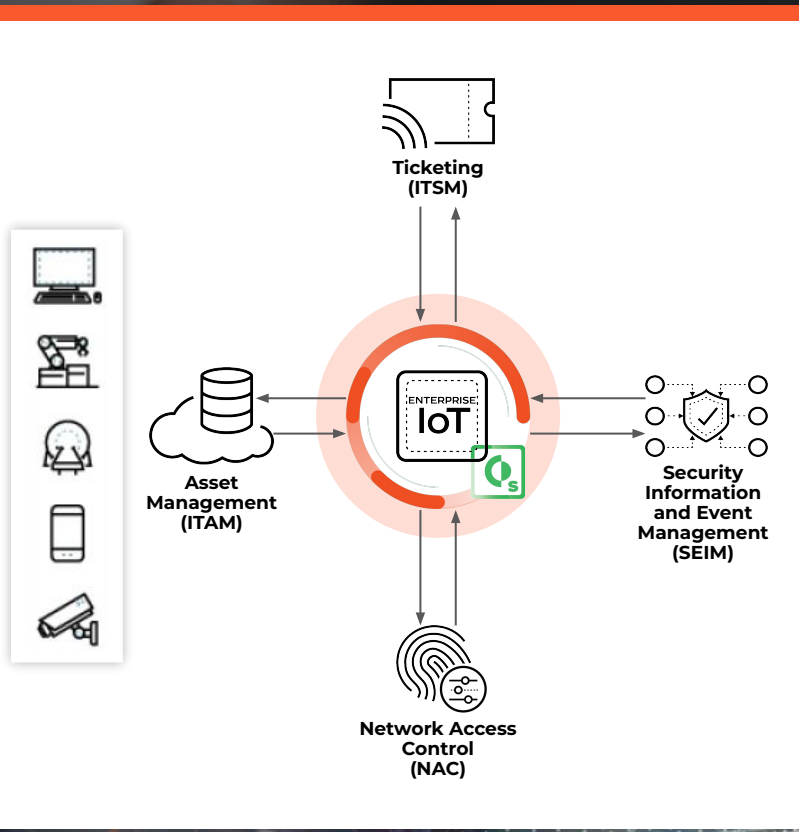
Powered by built-in XSOAR technology.

Leverage seamless integration into your existing workflows. This eliminates resource-intensive API-led integrations and reduces the burden on infrastructure and security teams.

By leveraging native integrations from Palo Alto Networks into your existing connected devices, IT, and security workflows, you can strengthen your current IT Service Management (ITSM), Network Access Control (NAC), security information and event management (SIEM), and other use cases.

Using a modular and customized playbook-driven orchestration, Palo Alto Networks lets your security team:

- Improve operational inefficiencies.
- Enrich asset inventories.
- Accurately onboard network-connected devices.
- Enforce device controls.
- Automate incident responses without having to build integrations from scratch.



Leverage Your Current IT Security Team

Without the need to form a new team, deploy new infrastructure, or change existing operational processes.

Unprecedented visibility and protection
- ML-based connected device discovery
- Automated risk assessment
- Native security policy enforcement
- Context-aware network segmentation

Easy deployment with flexible form factor options
- Hardware firewalls
- Software firewalls
- Cloud-delivered firewalls

Leverage leading prevention from other security services

Scale linearly as your business grows with elastic multitenant cloud infrastructure

Automate workflows with playbook-driven integrations

Full range of network-connected device coverage managed and unmanaged.

Think IoT Security. Think Palo Alto Networks.

Founded in 2005, Palo Alto Networks is based in Santa Clara, California, and serves customers globally with offices worldwide.

At Palo Alto Networks, our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We are at the forefront of protecting tens of thousands of organizations across clouds, networks, and devices and help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

Curious to learn more about Enterprise IoT Security? **Check out these resources.**

"As a CTO, I can easily manage known risk but what keeps me up at night is the unknown risk. Inherently we knew we had IoT devices on our network but couldn't easily identify, quantify, or classify the devices or risk associated with them. Having Palo Alto Networks IoT Security in place provides that visibility and affords us the ability to manage the risk appropriately."

Chief Technology Officer, NDIT

NORTH Dakota | Information Technology
Be Legendary.

Read the case study

www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087