Palo Alto Networks Enterprise Device Security

Discover, Assess, and Protect Every Device in Your Enterprise

Given today's rapidly evolving threat landscape, a fragmented approach to security is no longer an option. Digital transformation, increased M&A activity, and a distributed workforce drive the proliferation of devices—from traditional IT endpoints to unmanaged bring your own devices (BYODs) and specialized IoT/OT systems. This fragmented approach results in siloed risk information and visibility blind spots that AI-powered attackers can quickly exploit.

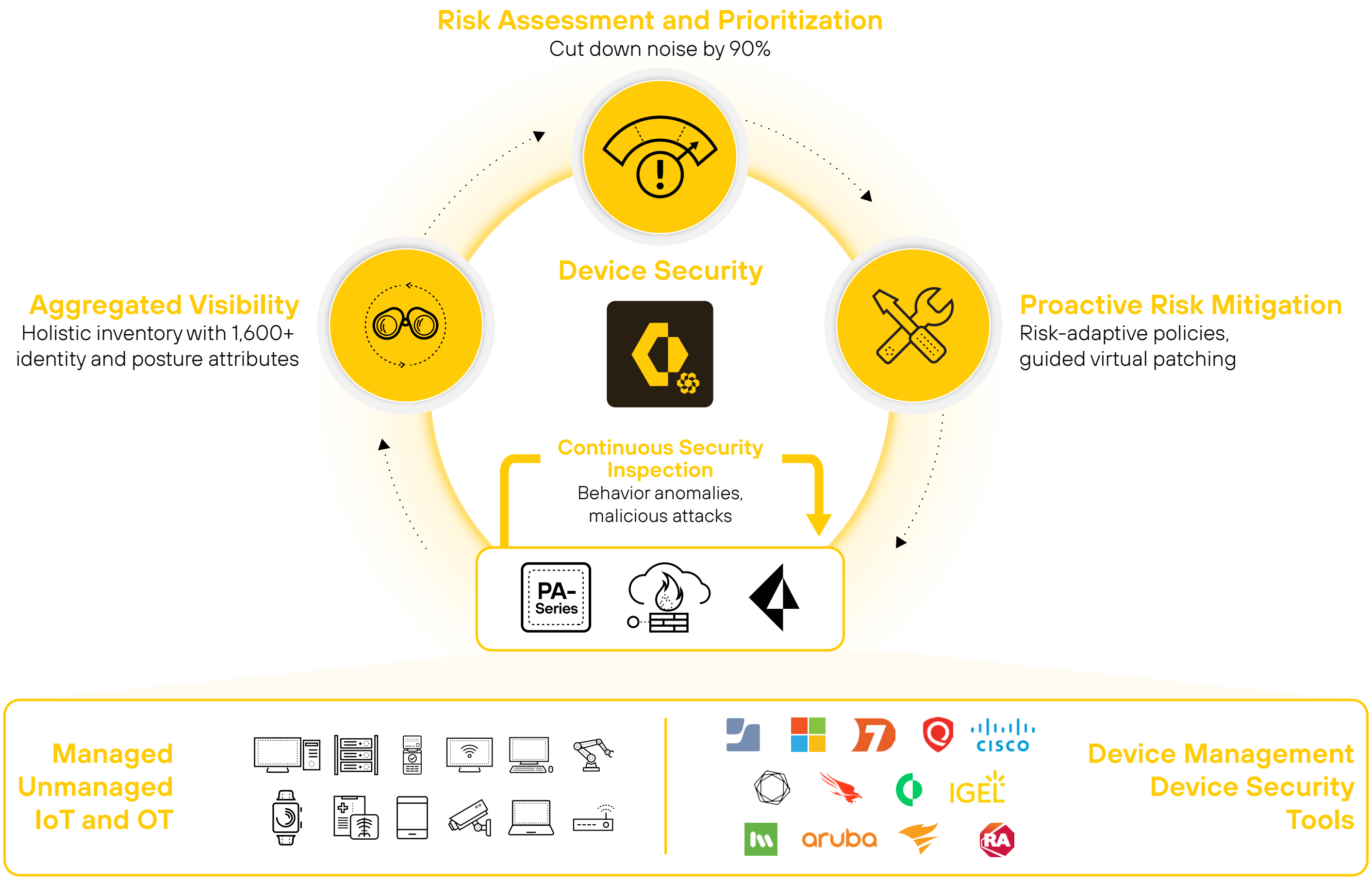
But now that every connected device is a potential entry point for cyberthreats, the real challenges are both seeing potential threats and having the ability to respond to them instantly. As the Muddled Libra attacks have highlighted, attackers are using unmanaged assets for network persistence and defense evasion. Organizations need complete visibility into all managed, unmanaged, and IoT assets, as well as the behaviors of these assets to identify anomalous behaviors and other indicators of compromise.

Device Security for Visibility into Assets and Potential Risks

Palo Alto Networks Device Security delivers a unified, AI-first solution that provides comprehensive protection and monitoring across your entire attack surface. To achieve this, it discovers all connected devices, as well as identifies and mitigates hidden risks that would otherwise remain invisible or elusive to even the most seasoned InfoSec professionals.

Device Security is the single source of truth for all your device and risk data. It gathers weeks of toggling between dozens of tools, managing multiple spreadsheets, manually tagging and correlating assets, creating custom scripts to extract or cleanse data, and collecting endless meeting notes. Then, it turns all of this data into instantaneous insights that can be resolved within minutes of automated, proactive protection.

Security teams are able to see their full environment and proactively take actions on their most critical risks through automation. Device Security can use existing Palo Alto Networks Next-Generation Firewalls (NGFWs), Prisma® Access, and SD-WAN security infrastructure or standalone virtual metadata collectors to instantly begin monitoring and discovering 98% of assets within 48 hours. Third-party systems can easily integrate with Device Security via Cortex XSOAR® using one of our more than 35 prebuilt integration playbooks.



Risk Assessment and Prioritization
Cut down noise by 90%
Device Security
Aggregated Visibility
Holistic inventory with 1,600+ identity and posture attributes
Proactive Risk Mitigation
Risk-adaptive policies, guided virtual patching
Continuous Security Inspection
Behavior anomalies, malicious attacks
PA-Series
Managed
Unmanaged
IoT and OT
cisco
IGEL
aruba
RA
Device Management
Device Security
Tools

Figure 1. Device Security workflow

Device Security Delivers Aggregated Visibility, Risk Prioritization, and Proactive Mitigation for All Assets

To enable teams to move faster, make smarter decisions, and do more with less, Device Security provides a comprehensive, actionable approach to help organizations gain visibility and secure their entire attack surface. Our AI-first security platform enables security teams to improve security outcomes with simplified operations and a reduced total cost of ownership.

Aggregated Device Visibility

Device Security goes beyond mere discovery to provide aggregated visibility with over 1,600 identity and posture attributes for all connected devices—including managed IT, unmanaged BYOD, and IoT/OT. Asset discovery is powered by a three-tier machine learning model that both passively processes and actively collects network traffic. Device Security also enriches asset data from a diverse set of sources, including a large language model knowledge base and telemetry from leading endpoint detection, mobile device management (MDM), and vulnerability management systems. This comprehensive dataset eliminates blind spots and provides a single, unified view for comprehensive security posture insights.

Risk Assessment and Prioritization

Without effective prioritization, critical risks can become buried. Device Security reduces time spent triaging risks by 90% with multifactor risk scoring. It considers factors like severity (Common Vulnerability Scoring System [CVSS] or Exploit Prediction Scoring System [EPSS]), asset criticality, business impact, exploitation status, compensating control, and user-defined custom factors. This way, security teams can focus on the highest-priority risks that matter within their business context.

Proactive Risk Mitigation

Seeing the problem isn't enough. Teams need the ability to act. Device Security enables and recommends risk-adaptive Layer 7 policies based on a device's unique identity, risk posture, and unique behaviors relative to crowdsourced baselines from over 17 million devices. For unpatchable vulnerabilities—for example, due to a lack of vendor support, operational downtime, or system compatibility—Device Security provides guided virtual patching in Strata™ Cloud Manager using Palo Alto Networks industry-leading Advanced Threat Prevention signatures.

Continuous Monitoring

To keep pace with the rapidly evolving threat landscape, organizations need the ability to catch threats in real time. Device Security continuously monitors all device traffic and uses machine learning to develop and continuously reevaluate device behavioral baselines against both context-specific and crowdsourced (across more than 3,500 customers) baselines. When malicious, anomalous, or high-risk behaviors are observed, Device Security generates alerts, providing 24/7 monitoring across the entire network.

Use Cases: Identify and Mitigate Risks Across Devices

Today's enterprise environments include a mix of managed, unmanaged, and special purpose IoT/OT assets. These assets include company-issued laptops, unmanaged shadow-IT servers, legacy routers, and devices for which security was never seriously considered, such as an IoT air quality monitor. Each presents its own unique security challenges, and requires a unique approach to managing risk. The following use cases show how Device Security helps teams reduce risk, increase control, and respond faster across all of these environments.

Secure Managed Devices: Close the Gaps in Your Device Coverage

Even in well-managed environments, gaps often emerge when endpoint tools are inconsistently deployed or policies drift across business units. Devices might be missing EDR agents, running outdated configurations, or excluded from vulnerability scans. These issues are hard to catch when asset and risk data are siloed across dozens of systems. Device Security builds a comprehensive profile for every connected device using over 1,600 identity and posture attributes. It continuously monitors assets and aggregates telemetry from integrated endpoint detection, MDM, and vulnerability management systems. Multifactor risk prioritization factors in CVSS, EPSS, asset criticality, business impact, and compensating controls, highlighting the risks that matter most.

Through aggregated asset visibility and comprehensive risk prioritization, security teams can quickly identify the most impactful compliance gaps and take immediate action through risk-adaptive Device-ID policies or trigger enforcement directly within existing tools via Cortex XSOAR or the NGFW. Device Security saves teams weeks of manual effort in identifying gaps. It also automates the process of triaging and remediating risks, enabling security teams to spend less time tracking down risk instances and more time on strategic security initiatives.

Managed Asset Use Cases

- Incomplete or Outdated Asset Inventory
- Inconsistent Security Tool Deployment
- Unauthorized Software Installed
- Not Scanned for Vulnerabilities

Secure Unmanaged Devices: Discover and Control Shadow IT

Unmanaged or unauthorized devices, such as personal laptops, rogue access points, and contractor-owned systems, often connect to enterprise networks without visibility or control. These assets bypass standard security controls and introduce hidden risks.

Device Security uses machine learning-based discovery and enriched metadata from multiple data sources to uncover every device connected to the network, including those outside formal IT management. It also builds a behavioral and risk profile for each device and recommends identity-aware segmentation policies that can be enabled on our NGFWs using Device-ID. Continuous traffic monitoring detects anomalous or high-risk behavior, with alerts generated in real time. Teams can quickly identify and contain risks from unmanaged devices with risk-adaptive Device-ID policies until they are secured or removed, eliminating shadow IT exposure risks.

Unmanaged Asset Use Cases

- Visibility Blind Spots from Third-Party Systems
- Unauthorized Network Access
- Shadow IT
- Unpatched Exploitable Vulnerabilities

Secure IoT/OT Devices: Protect Devices Using Insecure Protocols or Unsupported Systems

Many operational environments rely on specialized devices that use insecure protocols, like the Server Message Block (SMB) protocol, or run outdated, unsupported operating systems. These systems often cannot be patched due to vendor limitations, operational constraints, or the risk of disruption. Without proper controls in place, these assets introduce persistent exposure risks.

Device Security identifies these devices and continuously monitors their traffic to establish and refine behavioral baselines. It alerts security teams when deviations or malicious patterns are observed, using both local context and crowdsourced baselines across more than 16 million devices. Layer 7 Device-ID policies enable organizations to define least-privilege policies based on App-ID™ and destination. Guided virtual patching enables organizations to natively mitigate risks from unpatchable vulnerabilities. Both controls help teams contain threats without costly or disruptive device updates.

IoT/OT Asset Use Cases

- Visibility Blind Spots
- Poor Segmentation
- End-of-Life Systems
- Unsecure Protocols/Weak Credentials
- Unpatchable Vulnerabilities

Why Palo Alto Networks

Palo Alto Networks is the cybersecurity partner trusted by organizations worldwide. We combine deep industry experience with advanced security technologies to protect your operations in real time, even as threats evolve and environments grow more connected.

Our Device Security solution stands apart by delivering:

- **Unified protection across managed, unmanaged, and IoT/OT devices:** Our AI-first platform spans physical and digital environments, eliminating gaps and reducing complexity. Device Security is built into our product portfolio so you don't need separate enforcement hardware or custom integrations.
- **Adaptive device identity and risk-based policy enforcement:** Granular control through dynamic Device-ID enables context-aware segmentation and enforcement that aligns with operational priorities, from managed IT endpoints to specialized unmanaged systems.
- **AI-powered threat prevention:** Inline controls stop known and unknown threats in real time, reducing dwell time and minimizing impact across all device types.
- **Proactive risk mitigation:** Beyond detection, Device Security offers guided virtual patching and risk-adaptive policies to actively remediate risks, even on unpatchable or legacy systems.
- **Built for ease of deployment:** Device Security uses the existing network infrastructure without needing to deploy and manage single-purpose hardware. Your team can quickly access Device Security with minimal configuration and get access into comprehensive visibility and enforcement of over 98% of your devices within 48 hours.

Learn more about how Device Security can protect your rapidly expanding attack surface. Contact us for a free trial.

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

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.