Confidently Segment Devices and Apply Zero Trust Policies with Enterprise IoT Security

Why Do You Need Network Segmentation?

Network segmentation is a tried and true technique used by security practitioners to address an assortment of issues in IT infrastructure environments. The main benefits of network segmentation include:

- Optimized network availability by localizing the impact of faults.
- Improved security hygiene by preventing the lateral movement of threats.
- Constrained scope of compliance audits (HIPAA, PCI, etc.) to a limited network segment.
- Limited data exfiltration by controlling access to critical data and intellectual property.
- Reduced attack surface for legacy or vulnerable systems performing crucial business functions.

How Enterprise IoT Security Delivers Network Segmentation

Enterprise IoT Security, powered by the Palo Alto Networks Next-Generation Firewall, delivers effective segmentation by discovering, profiling, assessing risk, continuous monitoring, and enforcing granular policy for all connected devices. Additionally, Enterprise IoT Security integrates with other Network Access Control (NAC) technologies to eliminate their unmanaged IoT device blind spots to deliver meaningful segmentation.

Challenges in Network Segmentation for IoT Devices

1. Effective network segmentation requires the complete visibility of network-connected devices. Traditional agent-based endpoint security solutions cannot discover and manage IoT devices.
2. Current technologies for connected device discovery only identify and classify the network-connected devices for which they have pre-populated signatures and cannot scale to find all IoT devices.
3. Current endpoint security and NAC solutions have limited visibility into IoT device context.
4. Existing firewall solutions lack granular policy enforcement capabilities within a VLAN or a subnet.
5. Today, multiple labor-intensive steps are required to define and develop risk reduction policies per device profile, causing delays and errors in IoT segmentation.

Table 1: Scenario Comparison

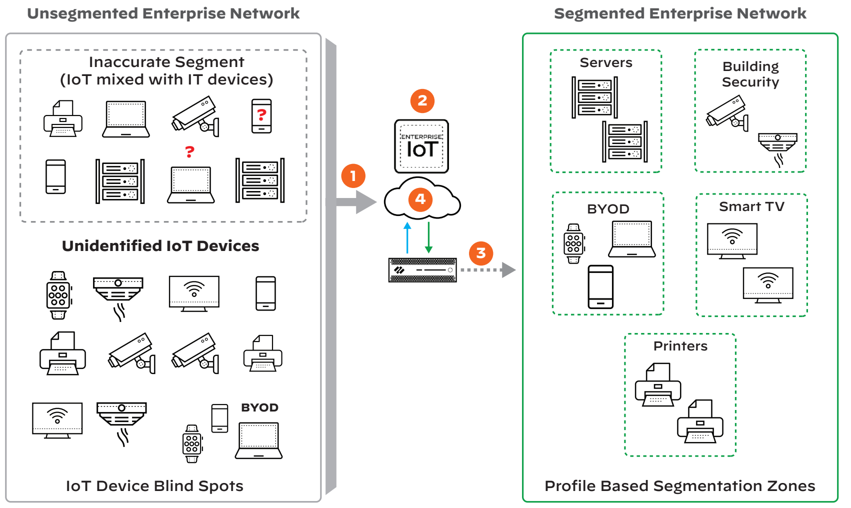
Without Enterprise IoT Security	With Enterprise IoT Security
• Connected devices blind spots • No security policy for connected devices • IT mixed with IoT	• ML-driven IoT, IT, and Bluetooth visibility • Automated Zero Trust policy recommendations • Segmentation of network-connected devices by device profile

Context-Aware Segmentation Natively with NGFW

The Enterprise IoT Security service on the Palo Alto Networks Next-Generation Firewall (NGFW) uses machine learning (ML) with our leading App-ID technology and crowdsourced telemetry to profile all devices for discovery, risk assessment, vulnerability analysis, and anomaly detection. Unlike any other solution in the market, Enterprise IoT Security analyzes the profiles, context, and device behavior to provide Zero Trust-based least privilege access and segmentation policy recommendations. These automated policy recommendations are then enforced by the NGFW for the secure segmentation of unmanaged devices. Segmentation policies remain linked to a device even if it moves within a network.

Palo Alto Networks Enterprise IoT Security considers several factors like device type, function, mission criticality, application behavior pattern, threat level, and more to enable segmentation for IoT devices based on Zero Trust principles. These context-aware segmentation zones significantly reduce the potential impact of the cross-infection of threats between IT and IoT devices. In addition, Enterprise IoT Security continuously monitors device behavior to find anomalies and refine security policies.

The use of Palo Alto Networks NGFW as a segmentation gateway offers deployment flexibility, allowing the controlled introduction of security policies over IoT devices without a network redesign. Traffic to and from IoT devices can be limited to required resources, allowing both north-south and east-west policy enforcement.



1. ML-Powered Enterprise IoT Security discovers and profiles all IoT and IT devices in the network.
2. Enterprise IoT Security provides Zero Trust segmentation policy recommendations for network-connected devices based on device profiles, risk posture, and behavioral baselines.
3. The Zero Trust segmentation policy recommendations are enforced with one click natively via the Palo Alto Networks NGFW.
4. Enterprise IoT Security continuously monitors device behavior to fine-tune polices.

Figure 1: Segmentation workflow through Palo Alto Networks Enterprise IoT Security

Eliminate IoT Blind Spots with Built-in NAC Integration

If you prefer a Network Access Control (NAC) solution to segment your network, Enterprise IoT Security provides built-in integration with Cisco ISE, Forescout, and Aruba ClearPass to implement segmentation. NAC technologies only have limited context for unmanaged IoT devices. Enterprise IoT Security augments NAC solutions by eliminating their discovery and contextual blind spots. Enterprise IoT Security provides discovery of IoT device information to the NAC solution and provides additional device context to segment them intelligently.

Automate Network Segmentation with Enterprise IoT Security

Capabilities at a glance:

- **IoT device discovery**: Discovers and classifies all devices connected to networks including those never seen before.
- **Agentless and passive**: Uses machine learning (ML), deep packet inspection (DPI), and crowdsourcing to identify and profile all network-connected devices.
- **Vulnerability analysis**: Finds vulnerability gaps by observing Software Bill of Materials (SBOM), OS, patch, default password, obsolete protocols, and more.
- **Threat and behavior analysis**: Assesses and monitors network behaviors of IoT devices for device context and threats.
- **Automated Zero Trust policy recommendations**: Creates policy recommendations for IoT devices based on their behavior baselining.
- **Continuous monitoring**: Monitors IoT devices at all times to fine-tune policies, prevent known threats, and detect unknown threats.
- **Automated segmentation**: Shares context and policy with enforcement solutions to implement segmentation. Provides one-click enforcement natively with NGFW for faster implementation. Automatically shares policies with the NAC solutions with built-in integrations.

Enterprise IoT Security helps organizations embrace a new yet simplified approach to IoT device segmentation modeled steadfastly on Zero Trust best practices.

To learn more, visit the website or request a demo of the industry's most comprehensive Zero Trust security for smart devices.

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