Comparing Zero Trust Approaches to Security for IoT Devices

With the expansion of work-from-home policies, BYOD (bring your own device) policies, corporate resources shifting to the cloud, the pervasive growth of Internet of Things (IoT) technology, and the increase in cyberthreats, the traditional network perimeter is dissipating. The need to adopt a Zero Trust approach as a core strategy to enterprise security has become undeniable in the face of these trends in technology and resources.

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, cloud adoption, and security operations.

Palo Alto Networks has outlined the Zero Trust framework with guiding principles for IoT devices that encompass security for infrastructure within an enterprise. The three key pillars are Device/Workload, Access, and Transaction, as outlined in the following diagram:

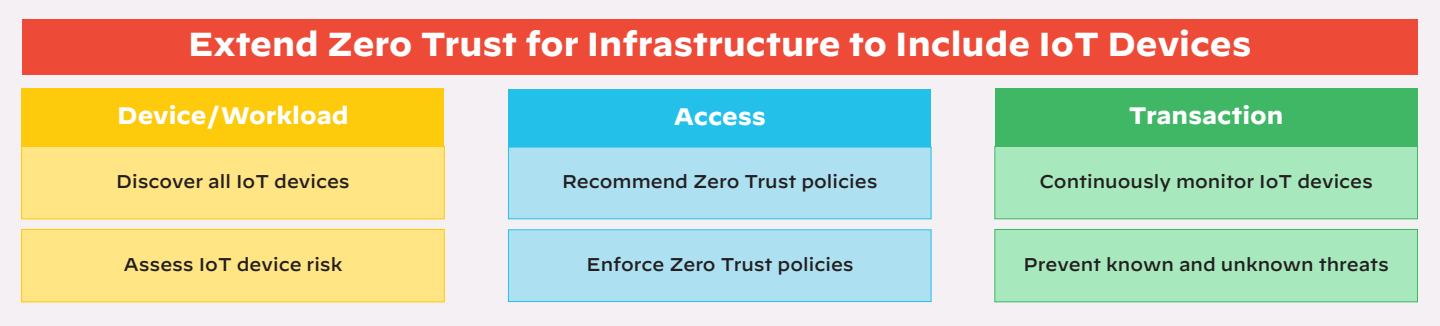

Figure 1: Key Zero Trust capabilities and continuous validation for IoT devices

While many solutions in the market tout Zero Trust for IoT devices, they fail to meet the complex needs of IoT security. Here is the comparison at a glance:

Table 1: Comparison of IoT Security Solutions

Zero Trust Principle	Palo Alto Networks	Other IoT Security Vendors
Discover all IoT devices	Yes **ML + DPI + Crowdsourced** Uses ML-driven discovery coupled with deep packet inspection and crowdsourced device knowledge to discover and classify all IoT devices in no time across multiple verticals.	Partial **DPI** Employ a signature-based approach to device discovery that cannot keep up with new and never-seen-before devices.
Assess IoT device risk	Yes **Across Five Vectors** Covers behavior anomaly, device noncompliance (e.g., missing agents, patches), static device intelligence (e.g., MDS2), vulnerabilities, exploits, and threats.	Partial **Across Four Vectors** Cover behavior anomaly, device noncompliance, vulnerabilities, and threats.
Recommend Zero Trust policies	Yes **Automated** Automatically defines and recommends high confidence policy options based on ML-behavior verdicts across local and crowdsourced IoT device insights.	No **Manual** No policy recommendations.
Enforce Zero Trust policies	Yes **Native** Natively implements policy enforcement using the Palo Alto Networks NGFW or built-in integration with NAC and Wi-Fi solutions.	No **Not Native** No native implementation. Need external integrations.
Continuously monitor IoT devices	Yes **Ongoing Baseline Audit and Trend Visualization** Compares baselines over time, monitors connections/anomalies/connection requests/amount of data transmission, policy violation and provides visualization for reporting and easy assessment.	Partial **Limited Baseline Audit and No Trend Visualization** Compares baselines over time, but limited device behavior and policy violation.
Prevent known and unknown threats	Yes **Built-in Prevention** Monitors IoT devices at all times to prevent known and advanced threats, and detects unknown threats.	No **No Built-in Prevention** Only monitors IoT devices and their risks.

Read our white paper to learn more about the right approach to Zero Trust for 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