Zero Trust Advisory Service

Organizations worldwide are undergoing a significant transformation to secure their most valuable assets. Leaders within organizations are increasingly looking to leverage Zero Trust as a strategy to secure their enterprise resources. However, determining how and where to start their Zero Trust journey may be daunting, but we are here to help.

The Zero Trust Advisory Service offers a **holistic** approach to help your organization **design**, **implement**, and **maintain** its Zero Trust security posture.

Palo Alto Networks is a leader in cybersecurity technology, and we have leveraged our expertise to create a vision of how to deliver Zero Trust everywhere. The Zero Trust Advisory Service is our way of partnering with our customers for an aligned vision that ultimately enables us to succeed together. As a trusted partner, we seek to protect all of your users, applications, and infrastructure everywhere. We provide a consistent set of capabilities and validation criteria to ensure that blind spots are reduced within your enterprise environment. We leverage the principles of validating identity, verifying device/workload integrity, enforcing least-privileged access, and scanning digital transactions for malicious activity to provide peace of mind.

	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 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

Figure 1: Palo Alto Networks Zero Trust vision to protect all enterprise resources everywhere

With the Zero Trust implementation methodology, we take a holistic and vendor-agnostic approach to understand where the organization is in its Zero Trust journey. In the short term, we focus on the security architecture to make sure all required security capabilities are in place. In the long term, there is a continuous focus to implement and optimize a Zero Trust security posture per enterprise resource.

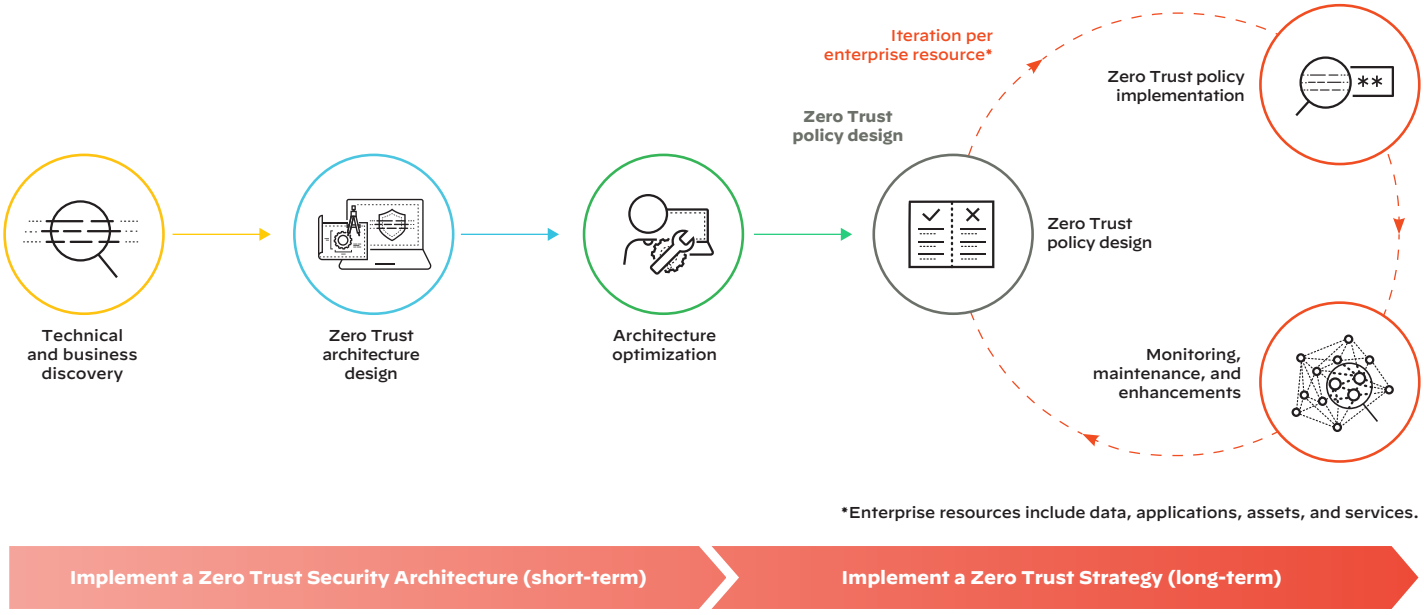

Figure 2: Palo Alto Networks Zero Trust implementation methodology

Technical and Business Discovery

In this phase, the objective is to create a baseline of your existing security posture. Our experts collect data from key stakeholders across your organization, and this data is assessed to create a baseline of your current security posture. At the same time, we also collect business-related information to understand the organization's operations and priorities as well as identify the critical assets or enterprise resources the organization is looking to protect under a Zero Trust architecture.

The following outcomes are produced:

- Detailed stakeholder reports
- Current security architecture and enterprise resource overview
- Baseline security posture

Zero Trust Architecture & Strategy

In this phase, the first objective is to design a vendor-agnostic security architecture and a roadmap for your organization to get from its current standing to where it needs to be. We utilize key data points from the previous phase to optimize the architecture and close any gaps discovered in your security posture. This ideal future state will address current cybersecurity challenges, support future cybersecurity needs, and offer all the required controls to implement a Zero Trust strategy going forward.

The second objective is to create a holistic Zero Trust maturity baseline for the organization and a Zero Trust strategy specific for your use cases.

The following outcomes are produced:

- Gap analysis reporting
- Vision of an optimized security architecture
- Strategic roadmap
- Zero Trust strategy

Zero Trust Policy Design & Implementation

In this phase, the objective is to design and implement a Zero Trust security policy. The optimized security architecture will be utilized to identify legitimate traffic flows for the enterprise resources based on the collected data. Next to the technical information, the organization needs to provide input on who can access what resource, when, and where. The combination of the technical and business input allows us to design a least-privilege security policy. This policy will be translated into a configuration for specific technical controls that will then be applied to the associated policy enforcement points applicable for a specific use case.

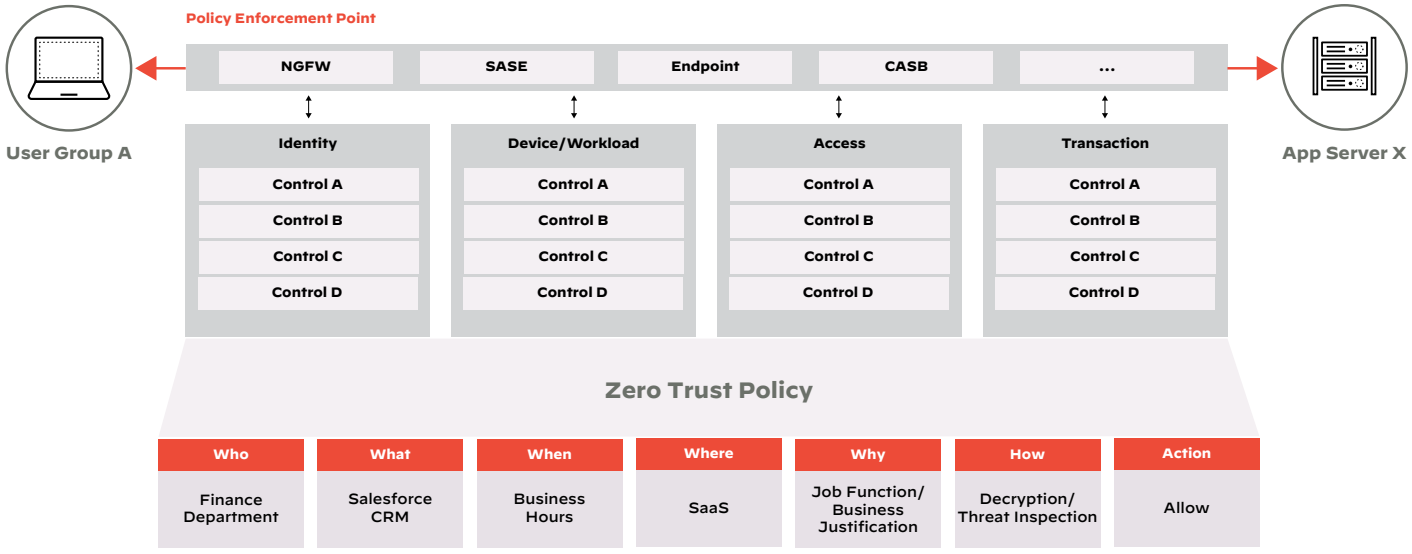

Figure 3: Palo Alto Networks Zero Trust policy framework

Over time, implementing Zero Trust policies will help increase the Zero Trust enforcement posture of the enterprise resources. As part of the implementation process, a Zero Trust maturity baseline will be created for each enterprise resource, and this will help track the posture improvements over time.

The following outcomes are produced:

- Zero Trust maturity per enterprise resource
- Zero Trust policy per enterprise resource

Monitoring, Maintenance & Enhancements

In this phase, the objective is to continuously evaluate if the implemented Zero Trust security policies still meet the technical and business requirements. Over time, enterprise resource access requirements may change. That's why it's essential for your organization to develop the people and implement the processes to continuously monitor and validate your Zero Trust security posture.

This iterative process will be used to ensure that the best possible Zero Trust policy is implemented based on available security controls, technical, and business information for an enterprise resource.

The following outcome is produced:

- Technology, people, and processes overview per enterprise resource

Benefits of the Service

- Deep insight into your organization's Zero Trust strengths and areas of improvement
- Development of a comprehensive cybersecurity strategy that aligns with business and cybersecurity outcomes
- A roadmap with short-term and long-term projects to implement your Zero Trust strategy
- Best practice recommendations to maximize the efficiency and effectiveness of your cybersecurity investments

To order the Zero Trust Advisory Service, please contact your local Palo Alto Networks partner or sales representative.

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