## Benefits

- Expert assistance in identifying critical assets
- Methodical approach to mapping the transaction flows to/from critical assets
- Zero Trust architecture designed by security experts
- Implementation roadmap to achieve the Zero Trust architecture developed during the engagement

# Zero Trust Design Service

## Translate your Zero Trust strategy into practical implementation

Adopting Zero Trust principles can greatly increase protection of your critical assets from exfiltration and threats. Knowing how to start your Zero Trust journey can be daunting, but we are here to help. Palo Alto Networks offers the Zero Trust Design Service to create a custom roadmap for how to implement Zero Trust in your network.

**If everything is critical, then nothing is critical.**

Fundamental to the Zero Trust model is accurate accounting for and visibility/security of all high-value assets in an enterprise network. A high-value asset is any data, be it personally identifiable information, intellectual property, or any other high-risk information that is of strategic value to an enterprise—and attackers.

The first step to implementing Zero Trust in your network is to select high-value assets. We will work with you to identify your highest value assets. From there, we will perform asset discovery and flow mapping to fully understand access to those high-value assets. Using that information, our expert consultant will create a targeted Zero Trust architecture, including a full implementation plan, to secure your high-value assets.

## How the Zero Trust Design Service Works

**Identify the critical assets**: We will work with you to review your current environment and select critical assets to be the focus of this design engagement. The selection will be based on business risk as well as knowledge of the network and applications surrounding the critical assets. Once the asset inventory is complete, it will be validated with your team.

**Complete asset discovery and flow mapping**: After the critical assets are identified, we will create an inventory of assets and the map flows to them. This step is often the most challenging and time consuming. We use different tools available for logging and analyzing network flows based on your network and access.

This includes:

- Categorize the flow type (e.g., user, IT, Admin, OPs)
- Identify the applications being used
- Identify the user information (requires User-ID™ integration)
- Identify when access is being attempted
- Identify where decryption is required

Then, we will step through the flows in the inventory to determine which ones are:

- Known and approved
- Known but unapproved
- Unknown (and require assessment of risk approval)

**Create targeted Zero Trust architecture**: The inventory information as well as your business goals will be used to create targeted architectural design to implement Zero Trust controls against the identified critical assets. We will work with your team to establish any architectural principles and environment/operational limitations. A design will be built on Zero Trust principles to include segmentation requirements, privileged access controls, endpoints controls, security analytics, and functional needs (e.g., third-party integration, decryption).

**Develop an implementation plan**: Finally, an implementation plan will be developed to achieve the architecture. This plan will work to minimize impact to production workflows. It will include consolidation of assets with similar security requirements and work to isolate high-value assets to the maximum extent and security benefit possible. The architecture and implementation plan will be reviewed with your team.

With the architecture design and implementation plan in hand, you will be empowered to choose from multiple options to execute the implementation. The range of possibilities includes using your internal teams, engaging with a partner, utilizing a Resident Engineer or engaging with Palo Alto Networks Professional Services for the Zero Trust roadmap implementation.

To order the Zero Trust Design 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