ZERO TRUST | paloalto NETWORKS

Palo Alto Networks Zero Trust Maturity Model

As with any strategic initiative, it's important to benchmark where you are as you begin your Zero Trust journey. It's also important to measure your maturity as you improve your Zero Trust environment over time. Designed using the Capability Maturity Model, the Zero Trust Maturity Model mirrors the five-step methodology for implementing Zero Trust and should be used to measure the maturity of a single protect surface.

The below legend details the various stages in the Maturity Model as it applies to each step in the 5-step methodology. On the second page, circle the number that aligns to the appropriate maturity stage for each of the 5-steps. As your Zero Trust environment evolves, continue to reevaluate your protect surfaces so you can identify the progress that has been made as well as what needs to be done to reach full maturity.

STEP	INITIAL (1 pt.)	REPEATABLE (2 pts.)	DEFINED (3 pts.)	MANAGED (4 pts.)	OPTIMIZED (5 pts.)
1. Define Your Protect Surface Determine which single DAAS element will be placed inside of your protect surface.	*Discovery is done manually. Only a small percentage of DAAS is discovered and classified.*	*Application and user identification capabilities are starting to be used. This includes automated tools and pilot projects with those tools to discover and classify data.*	*Team is trained on how to classify data as it is used. Processes are introduced to continuously mature protect surface discovery.*	*Immediate visibility into newly online DAAS elements (including updates to existing DAAS elements) is established, and DAAS elements are automatically classified into the correct or new protect surface.*	*Discovery and classification are fully automated.*
2. Map the Transaction Flows Map transaction flows based on how the DAAS element identified in Step 1 interact to understand the interdependencies between the sensitive data, application infrastructure (i.e. web, application, and database servers), network services, and users.	*Flows are conceptualized only based on what is already known.*	*Traditional scanning tools are used.*	*Flows are validated with system owners.*	*Visibility into what goes in and out of the system is maintained.*	*Transaction flows are automatically mapped across all locations.*
3. Architect a Zero Trust Environment Build a Zero Trust architecture to leverage network segmentation, enable granular access to sensitive data, and provide robust Layer 7 policy enforcement for threat prevention.	*With little visibility and an undefined protect surface, the architecture cannot be properly designed.*	*The protect surface is established based on current resources and priorities.*	*The basics of protect surface enforcement are complete, including placing segmentation gateways in the appropriate places.*	*Additional controls are added to evaluate multiple variables (i.e., endpoint controls, SAAS and API controls).*	*Controls are enforced using a combination of hardware and software capabilities.*
4. Create Zero Trust Policy Create Zero Trust policy following the Kipling Method: Who, What, When, Where, Why, and How.	*Policy is written at Layer 3.*	*Additional "who" statements are identified to address business needs. User-IDs of applications and resources are known, but access rights are unknown.*	*Team works with the business to determine who or what should have access to the protect surface.*	*Custom user-specific elements defined by policy are created, reducing policy space and the number of users with access.*	*Layer 7 policy is written for granular enforcement. Only known allowed traffic or legitimate application communication are permitted.*
5. Monitor and Maintain Analyze telemetry from the network, endpoint, and cloud while leveraging machine learning and behavioral analytics to provide greater insight into your Zero Trust environment and allow you to quickly adapt and respond.	*Visibility into what's happening on the network is low.*	*A traditional SIEM or log repositories are available, but processes are still highly manual.*	*Telemetry is gathered from all controls and sent to a central data lake.*	*Machine learning tools are applied to the data lake for context into how traffic is used in the environment.*	*Data is incorporated from multiple sources and used to refine Steps 1–4. Alerts and analysis are automated.*

Palo Alto Networks Zero Trust Maturity Model

Name of Protect Surface _____

DAAS Element Protected _____

Circle the number that aligns to the appropriate maturity stage for each of the 5-steps.

STEP	INITIAL (1 pt.)	REPEATABLE (2 pts.)	DEFINED (3 pts.)	MANAGED (4 pts.)	OPTIMIZED (5 pts.)
1. Define Your Protect Surface Determine which single DAAS element will be placed inside of your protect surface.	1	2	3	4	5
2. Map the Transaction Flows Map transaction flows based on how the DAAS element identified in Step 1 interact to understand the interdependencies between the sensitive data, application infrastructure (i.e. web, application, and database servers), network services, and users.	1	2	3	4	5
3. Architect a Zero Trust Environment Build a Zero Trust architecture to leverage network segmentation, enable granular access to sensitive data, and provide robust Layer 7 policy enforcement for threat prevention.	1	2	3	4	5
4. Create Zero Trust Policy Create Zero Trust policy following the Kipling Method: Who, What, When, Where, Why, and How.	1	2	3	4	5
5. Monitor and Maintain Analyze telemetry from the network, endpoint, and cloud while leveraging machine learning and behavioral analytics to provide greater insight into your Zero Trust environment and allow you to quickly adapt and respond.	1	2	3	4	5

TOTAL SCORE: ____ / 25 PTS.