Zero Trust Guidance for the US Federal Government

Numerous technology companies and systems integrators have recently jumped onto the Zero Trust bandwagon. With differing messages, many federal customers are struggling with how to use Zero Trust methodologies in a meaningful, valuable way to accomplish their missions. As agencies seek to implement Zero Trust, we recommend looking past the marketing and instead focusing on partners who have established themselves as leaders in the space and have a strong record of past performance. Palo Alto Networks is proud to be one of the first technology companies to adopt this methodology, and our solutions make us an ideal enforcement point for a scalable, proven Zero Trust architecture.

Introduction

Here at Palo Alto Networks, we believe so strongly in the need for a Zero Trust approach to security architecture that we went so far as to hire the subject matter expert who is widely accepted as its originator: John Kindervag. Back in 2009, when he was still an analyst at Forrester Research, Kindervag defined Zero Trust as "the critical cybersecurity strategy for protecting critical data, applications, systems, and services." Palo Alto Networks agreed with the Zero Trust strategy and began incorporating key Zero Trust capabilities into our Next-Generation Firewalls, allowing clients to deploy Zero Trust across their on-premises and cloud environments.

After many years of close coordination on the continued evolution of the Zero Trust strategy, Palo Alto Networks leadership and John Kindervag concluded that a closer working relationship was needed to drive faster and wider adoption of Zero Trust across industry and government customers. As a result, the originator of Zero Trust and the market leader in Zero Trust officially joined forces when, in 2016, John Kindervag joined Palo Alto Networks as our field chief technology officer. In this role, John meets with clients worldwide to provide counsel as they transform their environments and implement Zero Trust.

Since 2016, John has advised federal clients across the Department of Defense (DoD), civilian agencies, and the Intelligence community on how to implement Zero Trust across their varied environments. He has briefed senior SES/flag officer personnel and supported detailed technical pilots at DreamPort, the Library of Congress, and the NIST National Cybersecurity Center of Excellence (NCCoE), among others. These efforts and the associated lessons learned as well as best practices are reflected in this US government-focused white paper.

What Is Zero Trust?

Zero Trust Is Not About Making a System Trusted; It Is About Eliminating Trust

Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user access control.

Created by John during his tenure as a vice president and principal analyst for Forrester Research, Zero Trust is based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted. Under this broken trust model, it is assumed that a user's identity is not compromised and that all users act responsibly and can be trusted. The Zero Trust model recognizes that trust is a vulnerability. Once on the network, users—including threat actors and malicious insiders—are free to move laterally and access or exfiltrate whatever data they are not limited from accessing. Remember, the point of infiltration of an attack is often not the target location.

Attacks on sensitive data rarely use a single exploit or compromised credential. Attackers use exploits, malware, compromised credentials, and other methods together to work their way from their beachhead in an organization to the data. Often attackers use one method after another repeatedly. Malware may provide a user's credentials, which, in turn, provides limited access to their organization's network. Network access allows the attacker to move around the private network and place additional malware on privileged devices that are closer to the data. Then, the cycle repeats. The common thread in all these attack methods is that they take advantage of the trust inherent in the security posture of most enterprises. Trust has become a vulnerability as dangerous as any other.

Federal Government Challenges

The federal government faces unique challenges regarding Zero Trust that commercial entities do not. While cybersecurity programs within the federal government are more mature and provide significant capability, many do not address the issue of inherit trust. Due to this, Zero Trust has gained momentum across the federal government.

The following section outlines challenges that should be recognized by agencies or departments when planning their Zero Trust journeys. To address these challenges, we recommend our federal government customers integrate the Zero Trust architecture into existing SOC monitoring, develop automation frameworks that can be used to offload some of the manual efforts, integrate a SOAR solution into the monitoring platform, build correlation between endpoint and network data, gain visibility into encrypted traffic (inbound and outbound), and consolidate management platforms to increase operational efficiencies.

Classification Increases Complexity

Unlike commercial organizations, many federal agencies are forced to deal with multiple classification levels, which naturally creates some level of compartmentalization. This, in some sense, aids in adopting Zero Trust, but it also increases complexity due to separated network deployments, strict compliance requirements for technology, and lack of network visibility.

Additionally, separate network deployments increase the operational burden. This also results in the need to maintain independent security deployments and may require that multiple Zero Trust architectures be deployed within a single organization.

Numerous "Protect Surfaces"

The mission of the federal government differs greatly from that of a commercial organization. The distinct mission of federal agencies and departments causes them to have significantly more "protection surfaces" or "protect surfaces" as Kindervag refers to them. These mission-critical DAAS elements (i.e., data, applications, assets, services) become the focus of Zero Trust architecture designs. Within the DoD, these protect surfaces transform even more when dealing with tactical systems and critical mission systems. The sheer number of critical DAAS elements presents a challenge in deciding where to start and in which order to proceed. In the following, we address how to identify and classify DAAS elements in order to choose which should be addressed first.

Contractor/DIB Access

For a majority of government agencies, mission accomplishment involves allowing access to contractors and other non-agency personnel. Sometimes, this is internal staff augmenting the government labor force with agency-issued accounts and permissions; other times, it is contractors working on contractor sites with non-GFE equipment. All of these things present a challenge to providing the appropriate level of application and data access.

The primary challenge is to develop a strategy around identity management that includes personnel who are potentially outside of your IdAM solution. If the outside personnel have CAC or PIV credentials, this can be significantly easier; however, if they are using an internal directory, there may need to be an abstraction layer to integrate or pull specific account information. Even if the integration partner is using AD, if they are not adhering to a standard on account creations and fields that are utilized as part of their access strategy, direct federation may not be possible.

In addition to identity management, contractor and DIB staff access needs to be addressed. Traditionally, staff have been given GFE laptops with VPN capability in order to allow remote work capability. As federal IT needs evolve, this is no longer a one-size-fits-all solution. Traditional VPNs tended to give access equivalent to being on site. Working under the premise that the best approach is to grant the right amount of access at the right time to the right person may no longer be the most prudent solution. Determining the right level of access for agency staff, contractors, and other personnel is critical when designing a remote access capability. Ideally, access is only given for the specific need of that employee at that time. For example, a senior agency staff member could be allowed access to financial data while connected remotely from GFE at home, whereas a contractor on a personal device at a coffee shop could be allowed access to email only.

Multi-Cloud Deployments

Multi-cloud is a reality within the federal government. Agencies and departments are leveraging cloud IaaS, PaaS, SaaS, and FaaS from numerous providers. Zero Trust approaches need to address a multi-cloud deployment across multiple authorization levels.

Commercial companies were able to take an iterative approach to developing a cloud strategy. They were able to move some trivial data first, then start migrating less important applications to a single cloud, and then start consuming software as a service before moving to a full multi-cloud and cloud native application development strategy. Cloud implementation within the federal government has not been afforded this walk-then-run ability. With the “push to cloud” coming from governance bodies, agencies are having to develop fairly advanced cloud strategies from the onset, as there isn’t a single cloud provider that can meet all requirements. Zero Trust approaches center around security policy, and the consistent application of that policy in a multi-cloud environment is a non-trivial undertaking.

The primary step in securing for multi-cloud deployments is gaining visibility. This includes visibility from the on-premises (or shared) data center to a cloud provider, SaaS application, cloud native, and inter-cloud visibility. This is a rapid shift in responsibility, especially in parts of the federal government that were struggling with unifying a visibility solution for only on-premises. Our visibility recommendation starts with the Next-Generation Firewall within the data center, expands to VM-Series virtual firewalls within cloud environments, and covers SaaS visibility for applications utilized.

Lessons Learned

Through deployment experience within commercial and federal government customers, Palo Alto Networks has gathered relevant lessons learned that can be used to streamline Zero Trust deployments. The following are key findings and suggestions that should be evaluated before beginning a Zero Trust journey.

The Methodology Matters

Zero Trust policy determines who can traverse the microperimeter at any point in time, preventing access from unauthorized users to your protect surface, and prevents the exfiltration of sensitive data. True Zero Trust can only be done at Layer 7. The Kipling Method of creating Zero Trust policy enables Layer 7 policy for granular enforcement so that only known, allowed traffic or legitimate application communication is allowed. This method reduces the attack surface while also significantly reducing the number of port-based firewall rules. With the Kipling Method, you can easily write Zero Trust policy by answering:

- Who should be accessing a resource? This defines the “asserted identity.”
- What application is the asserted identity of the packet used to access a resource inside the protect surface?
- When is the asserted identity trying to access the resource?
- Where is the packet destination? A packet’s destination is often automatically pulled from other systems that manage assets in an environment, such as from a load-balanced server via a virtual IP.
- Why is this packet trying to access this resource within the protect surface? This relates to data classification, where metadata automatically ingested from data classification tools helps make your policy more granular.
- How is the asserted identity of a packet accessing the protect surface via a specific application?

As the federal government looks to implement Zero Trust architecture, it can follow a five-step approach:

1. **Define the protect surface** by identifying critical DAAS.
2. **Map the transaction flows** by understanding where the resources reside and how they're accessed, ultimately gaining a deeper understanding of how traffic moves throughout the network.
3. **Build a Zero Trust Architecture** by using information from the previous steps to decide where and how to implement controls.
4. **Create a Zero Trust policy** by utilizing information from the Kipling Method to determine what contextual information is used to define an access policy.
5. **Monitor and maintain the network**. Inspecting and logging all traffic, all the way through Layer 7, will provide valuable insight into how to improve over time. This includes ways to make policies more secure and what should be included in a protect surface. Using tools to analyze telemetry from the network, cloud, and endpoints will help enhance and evolve your Zero Trust policy.

Categorizing Data and Application Sensitivity

A Zero Trust security model protects the data, applications, services, and systems whose loss, or loss of availability, would cause harm to an organization or its customers. Therefore, before segmenting the data, applications, services, and systems, you must understand their sensitivity. There are a significant number of industry standards and government regulations, such as GDPR, HIPAA, and PCI DSS, that help define how data and applications are categorized. However, because every organization's data requirements are unique, and standards differ based on industry and location, this guide uses the following example levels of data sensitivity:

- **Public**—public information or service.
- **Low sensitivity**—information that would cause limited harm to the organization. Examples include:
  - Non-critical data and applications with a limited user base.
- **Moderate sensitivity**—information that risks causing serious harm to the organization or its customers. Examples include:
  - Business data and applications, including email and voice and video communications.
  - Infrastructure, applications, and systems whose loss of integrity and availability would impact the organization.
- **High sensitivity**—information that will cause severe harm to the organization or its customers. Examples include:
  - Any information falling under statutory requirements for notification in the case of a breach.
  - Personally identifiable information (e.g., financial, health, legal).
  - Critical intellectual property (code, designs, etc.).
  - Critical infrastructure and systems whose loss of integrity and availability would severely harm the organization.
  - Public key infrastructure; Active Directory.

Design from the Inside Out

A common mistake made when deploying Zero Trust is attempting to transition the entire enterprise in a short period of time. Instead, we suggest defining the protect surface and then designing a Zero Trust architecture outward. This creates a natural workflow using the Kipling Method. This design method enables the proper place of Policy Enforcement Points (PEP) that can most efficiently secure the protect surface. To best implement the Zero Trust least-privileged access security model in the network, the PEP security platform must:

- Have visibility of and control over the application and application functionality in the traffic.

Traditional security infrastructure describes applications through port and protocol. Zero Trust's least-privileged access model requires precise control over application usage that a port and protocol definition cannot achieve.

- Be able to allow specific applications and block everything else. Allowing a specific set of applications through a whitelist and denying everything else significantly reduces the number of ways an organization can be attacked.
- Dynamically define access to sensitive data based on a user's group membership. Many traditional security policies define access based on the location of the endpoint in the network. Even if enterprise mobility didn't blur the traditional network boundaries, network location is a poor identifier for users and their assigned privileges.
- Be able to validate a user's identity through authentication. For access to the most sensitive data, the security platform should validate user information obtained from the organization's authentication servers with another authentication method before allowing access. This ensures the traffic is coming from the expected user and not from someone impersonating them.
- Dynamically define the resources that are associated with the sensitive data or application. Many data centers and platform-as-a-service (PaaS) environments dynamically allocate resources to applications. To ensure the security posture matches the current resource allocation, the security platform needs to adjust, along with the changing environment.
- Block data by file type and content. Blocking risky file types reduces the number of ways you can be attacked as well as the number of ways attackers can exfiltrate data.
- Log detailed information on the traffic so security analytics can process it and identify abnormal behaviors.

When sensitive data is stored in the public cloud or a SaaS application, Zero Trust requires the security platform to:

- Assess the appropriateness of the data stored in the SaaS application or storage service.
- Identify previously unknown malware, and mitigate known malware and spyware stored in the SaaS application or storage service.
- Evaluate the accessibility of the data and mitigate unsafe sharing.
- Log detailed information on the access of the data so security analytics can process it and identify abnormal behaviors.

Identity Considerations

Identity and access management (IdAM) not only underpins an effective Zero Trust strategy but is critical for any security policy success. Prior to developing an effective strategy for granting the right amount of access, the identity of the person requiring the access must be accurately and consistently determined. In addition to users with interactive logins, applications used frequently require account access at some level to execute on API calls and other required functions. Although Active Directory® has been the traditional standard, it can no longer completely meet all of the needs for identity management in an evolving IT landscape.

Commercial entities have started utilizing tools classified as IdAM to cover the gaps, but the use case in the federal government is more complex. Within a single organization, a user may have a number of identities, with associated CAC/PIV cards to manage. If a user has elevated and administrative access on more than one security enclave, there may be multiple certificates and authorizations for a single user.

Realizing these complexities, and understanding that a Zero Trust architecture has to take them all into account while maintaining a consistent security policy, Palo Alto Networks recommends the following actions in the IdAM space:

- Develop an identity sources hierarchy, with the source having the most fidelity prioritized (i.e., if you have a policy with specific users, prioritize this over a policy applied to Active Directory groups, followed by network segments).

> "Given that account takeover is one of the top attack vectors, SOCs need to know when credentials have been exposed so they can mitigate risks before an exposed credential becomes a breach. SOCs are the ideal watchdogs to know when high-value targets (such as executives or admins) are exposed due to third-party credential leaks. As the saying goes, attackers no longer need to break in. Now they just log in."
>
> **—Ted Ross, CEO and Co-Founder, SpyCloud**

- Separate user identification collection and distribution and policy enforcement in larger environments. A User-ID-specific firewall will lower the load on the security firewall, allow for quicker adoption of newer PAN-OS® versions, and ensure a redistribution architecture can be simplified for growth (see figure 1).
- Build and maintain a standard for username format across identity sources. Although User-ID is capable of ingesting and differentiating multi-username formats, planning at the onset will ensure that [jane.doe@domain.com], [DOMAIN\jdoe], and jdoe will all map to the same user.
- Create meaningful Active Directory groups and have a Zero Trust policy assigned to default groups, ensuring that there will always be a policy applied to a customer even in cases of misconfiguration.
- Identify service accounts used within the end user compute environment and add them to the ignored group within policy so service execution on a desktop does not impact identity policy assignment. Additionally, create a prefix for service accounts so they can be filtered based upon the prefix rather than individual assignment.
- Architect around existing strengths. If you have an existing IdAM solution, look at how you can shape your environment to utilize it. If an important application is web based and available externally, look at moving it behind a security perimeter and tying it into your identity management system, allowing for centralized logging and verification.
- Standardize and publish an Active Directory standard for your agency.
- Have an abstraction layer ready to provide proxy identity services.
- Structure application access in such a way as to be able to selectively give access (e.g., don't publish a critical app directly to the internet and attempt to restrict access via the client server authentication).
- Instead of segmenting application parts in areas based on type (all of the data bases are in the "mid-tier") segment based upon criticality and group access. This does not have to be physical separation via network segmentation; this can be done via firewall and other policy.
- Spend time classifying applications and data that need to be accessed remotely, and then build a strategy to secure them based on these access requirements.

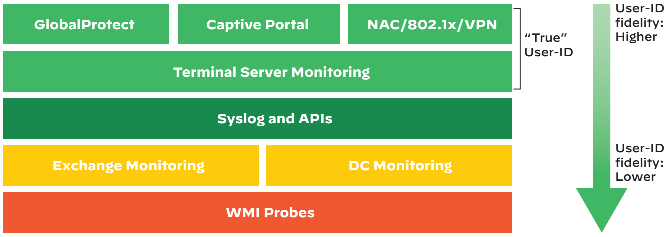

Figure 1: Palo Alto Networks User-ID

Agree to a Maturity Model and Track Improvement

As with any strategic initiative, it's important to benchmark where you are as you begin your Zero Trust journey as well as measure your maturity as time goes on and as improvements are made to your Zero Trust environment. 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.

It is our suggestion that a defined maturity model be adopted to ensure progress is tracked and aligned to an end-state goal.

Table 1 identifies the stages of the Maturity Model as it applies to each step in the five-step methodology.

Continuous Monitoring Is Crucial

One of the most common mistakes regarding Zero Trust is the lack of a continuous monitoring strategy. Environments constantly change, which means that a Zero Trust deployment will change as well. New users, systems, applications, and data are a given. It is crucial that a model is put in place to continuously monitor and evaluate the environment. Additionally, continuously monitoring provides a platform that can be used for additional innovation, such as behavioral analytics, automated responses, and integration into large analytic systems.

It should also be recognized that a Zero Trust deployment will include multiple security platforms, sensors, and vendor solutions. A common monitoring platform that can consolidate and correlate data from multiple systems is key to understanding the true status of the deployment.

Recommendations:

- Integrate the Zero Trust architecture into existing SOC monitoring.
- Develop automation frameworks to offload some of the manual effort.
- Integrate a security orchestration, automation, and response (SOAR) solution into the monitoring platform.
- Build correlation between endpoint and network data.
- Gain visibility into encrypted traffic, both inbound and outbound.
- Consolidate management platforms to increase operational efficiencies.

Table 1: Palo Alto Networks Zero Trust Maturity Model

Step	Initial (1 point)	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.
1. 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 user with access.	Layers 7 policy is written for granular enforcement. Only known allowed traffic or legitimate application communication is 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.

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