Strengthen Security with Zero Trust

Industry

Federal Government

Use Case

Strengthen security with Zero Trust

Mission Benefits

- Greater cyber resilience, contributing to the availability of essential functions that enable the mission.
- Improved network visibility, which helps close the gap between threat detection and decision-making, enhancing situational awareness and increasing confidence to operate safely in cyberspace.
- Insider threat deterrence by recognizing and limiting opportunities to exploit trust.

Operational Benefits

- Increased command and control over enterprise computing activities.
- Simplified compliance with applicable standards and regulations, using zone boundaries to segment sensitive resources.
- Simplified management operations through automation and standardized rule sets.
- Immediate flagging of unexpected or anomalous traffic by Zero Trust segmentation gateways.

Security Benefits

- Limited potential for data exposure through a reduction in the attack surface.
- Strict enforcement of a least-privileged network access policy.
- Enhancement of the organization's ability to prevent exfiltration of sensitive data.
- Visibility into and control over applications and services throughout the environment.

Mission Drivers

Governments around the world are managing data more broadly and rapidly than ever, enabling critical missions that underpin our national security, economic stability, and public safety. Partnerships with the private sector to safeguard these valuable systems and data are critical to executing these missions. Whether data is stored, in-transit, or shared, all systems that handle data—wherever they are—must be able to ensure its confidentiality, integrity, and availability.

Government departments and agencies simply can't afford to have cybersecurity incidents disrupt their normal operations, and "trust" has proven to be an exploitable vulnerability. One effective strategy for ensuring cybersecurity resilience is to pursue a Zero Trust architecture.

Mission Problem

Today's cyberthreat landscape is complex, and digital transformation is moving quickly. Competing priorities and initiatives can often distract departments and agencies from their primary mission: ensuring the continuation of government Mission Essential Functions (MEF) enabled by a secure digital operating environment.

As agencies transition to Zero Trust, the top concerns include:

- Preventing unauthorized lateral movement
- Preventing unverified network activity
- Ensuring only legitimate users have access to authorized network resources

Traditional Approach

In a traditional model, agencies rarely spend time understanding what they are trying to protect. Most efforts center around system functionality, while security has traditionally been implemented from the network perimeter, in the network's endpoints, and overlaid on top. As new threats emerged, discrete point products were added to this model to address them. For example, security vendors countered application-level attacks with intrusion prevention systems (IPS). As computer viruses became more prevalent, governments added antivirus to endpoints. When phishing email attacks increased, so did the deployment of content filtering to counter that threat.

This approach, known to many as "defense in depth," has resulted in a string of disjointed products that do not holistically interoperate to address the scope and breadth of all potential threats. The principle drawbacks of this security model are:

- **Reduced situational awareness**: With multiple non-integrated security products, it's difficult to get a comprehensive view of network traffic and threats.
- **Lack of access management**: Minimizing the risks of unauthorized access is a fundamental security principle. This is best achieved by implementing integrated security from the inside out—the opposite of the defense-in-depth approach.
- **Diminished security with complex management**: When each point product is separately managed and not integrated, agencies get less effective security and greater overhead.

These drawbacks are also confirmed by key findings outlined in the Federal Cybersecurity Risk Determination Report and Action Plan published by the Office of Management and Budget (OMB) in May 2018.

In 2013 and 2014, the United States experienced two of the largest breaches of government data in its history. The 2013 incident at the National Security Agency (NSA) involved an IT administrator who had access to all information on the classified network, while the 2014 breach at the Office of Personnel Management (OPM) involved an attacker who obtained valid user credentials. Both incidents exploited trust, further demonstrating the need for Zero Trust.

Palo Alto Networks Approach: Zero Trust

Zero Trust is a cybersecurity strategy designed around the concept that users, applications, and data should never be inherently trusted—their actions should always be verified, in every environment. The strategy involves limiting the scope of an attack and blocking lateral movement by leveraging microsegmentation based on users, data, and location.

We present the concept of a Zero Trust architecture to help form a security strategy that supports continuity of government operations by only allowing communications that are essential, validated, and approved. Palo Alto Networks secures governments globally by helping them adopt three cybersecurity principles that increase the efficacy of protection and reduce the workloads on network and security teams:

1. Implement a Zero Trust approach
2. Apply consistent security regardless of location
3. Adopt security automation

We've helped government agencies establish effective Zero Trust outcomes in a wide range of urgent situations and attack-related emergencies. To execute on Zero Trust, we use the five-step methodology depicted in figure 1. This method helps senior agency officials, mission owners, and engineers implement a robust security framework based on prioritizing the protection of MEFs.

Whether you're implementing a Zero Trust strategy on a private network or in the cloud, and regardless of infrastructure, the five-step methodology takes you through:

Step 1: Define your protect surface

Step 2: Map the protect surface transaction flows

Step 3: Architect a Zero Trust network

Step 4: Create the Zero Trust policy

Step 5: Monitor and maintain the network

Zero Trust Methodology

Figure 1: Five-step methodology

Palo Alto Networks Next-Generation Firewalls are designed to deny all and permit by exception. Combining this with the five-step methodology, a system inherently includes Zero Trust by design, resulting in:

- Closed-loop process for establishing least-privileged network access policies for any use case.
- Enhanced command and control (C2) over MEFs and network connectivity.
- Process integration between network and security operations.
- Positive control over a range of threats (e.g., passive, active, insider, integrator).
- Complete understanding of expected communications and easy spotting of unusual patterns.

Monitoring and maintaining the Zero Trust lifecycle is an integral part of IT service management (ITSM). The ITSM process will help administrators answer the questions of "why" and "how" before approving changes that will modify the defined protect surface. For example, making changes to an existing application or introducing a new application will trigger a change management process supported by ITSM. This helps agencies quickly shift their mindset to standardizing cyber defense capabilities and automating processes since security is built into the operating framework.

Customer Implementation

Zero Trust was first introduced to one of our government customers as part of a briefing we provided ahead of their network re-accreditation. This agency, a large joint service organization that serves a strategically important user base, has numerous facilities and operates on a multimillion-dollar cybersecurity budget. It also manages separate private networks that service several branches of government as well as data centers that connect to a joint information system environment.

During the briefing, the stakeholders quickly realized several benefits of our Zero Trust approach with regard to gaps they had previously identified in their network: gaining more visibility into internal network activity and recognizing abuse of privilege instances. Recognizing that our technology would bridge these gaps and help the agency achieve its desired outcomes, the stakeholders asked our team to help them execute.

As a part of our Transformation Services package, we helped the agency develop and deliver a Zero Trust architecture with microsegmentation that included advanced threat prevention. In consultation with the key stakeholders, we defined and inserted strict network security policies to permit by exception, and approved network traffic using the Kipling Method. Figure 2 shows the agency's MEF and endpoints protected with end-to-end policy enforcement points (PEPs) that are centrally managed and locally enforced.

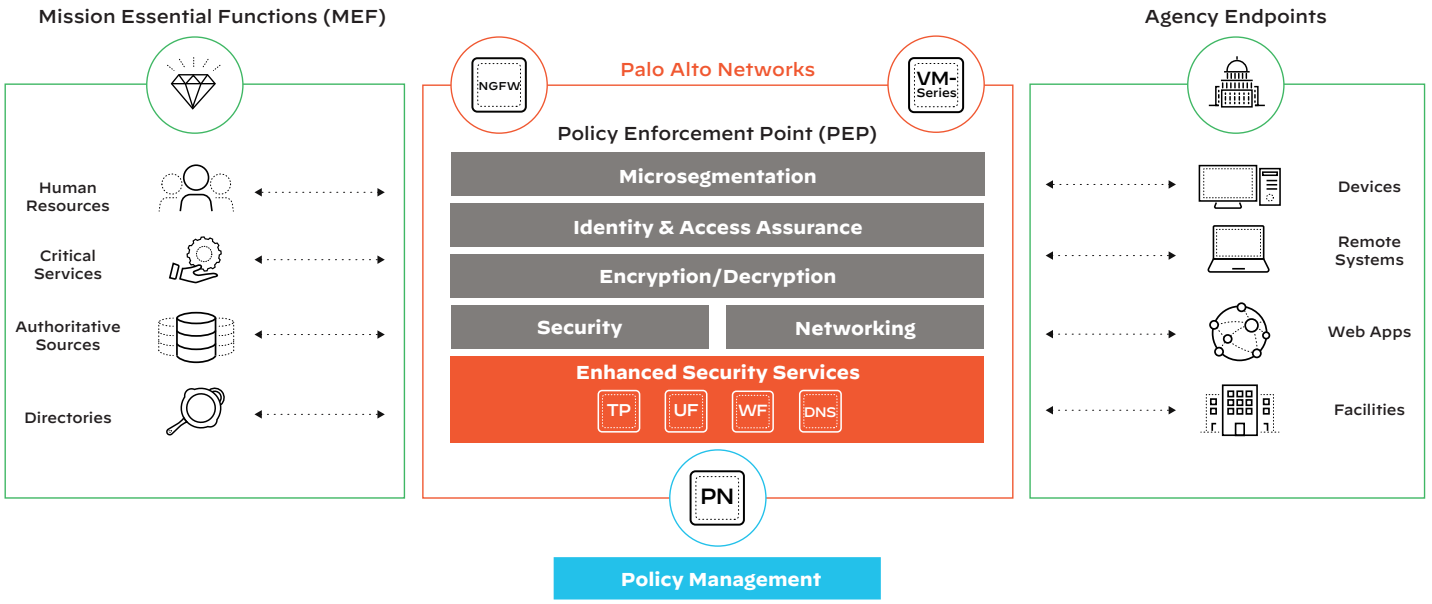

Figure 2: Microsegmentation architecture

Guided by the five-step methodology, the protect surfaces had been defined, and microsegmentation architecture had been selected as the Zero Trust approach for two of the agency's independent private networks. Next, stakeholders specified the Zero Trust policies they wanted to apply to those private networks. Consistent with designing security from the inside out, user access played an essential role in the architecture, supported by our Next-Generation Firewalls User-ID™ technology, which answered the question of who was seeking to access specified data or systems. The ability to identify all users on the network, ensured policy enforcement for authenticated users from an authoritative identity source (in this case, Active Directory®).

To answer "what" and "where," we enabled App-ID™ technology, which can uniquely classify critical services and accurately identify applications before establishing connectivity for privileged users at each endpoint. The agency was able to achieve its gap analysis objectives through closed-loop network security policies. Figure 3 shows where to find answers to help inform the creation of the agency's Zero Trust policies.

Figure 3: Creating a Zero Trust policy

Customer Benefits of a Zero Trust Architecture

By leveraging the Palo Alto Networks platform, any organization can reap numerous benefits like those presented in this use case.

Mission Benefits

- Greater cyber resilience, contributing to the availability of essential functions that enable the mission.
- Improved network visibility, which helps close the gap between threat detection and decision-making, enhancing situational awareness and increasing confidence to operate safely in cyberspace.
- Insider threat deterrence by recognizing and limiting opportunities to exploit trust.

Operational Benefits

- Increased command and control over enterprise computing activities.
- Simplified compliance with applicable standards and regulations, using zone boundaries to segment sensitive resources.
- Simplified management operations through automation and standardized rule sets.
- Immediate flagging of unexpected or anomalous traffic by Zero Trust segmentation gateways.

Security Benefits

- Limited potential for data exposure through a reduction in the attack surface.
- Strict enforcement of a least-privileged network access policy.
- Enhancement of the organization's ability to prevent exfiltration of sensitive data.
- Visibility into and control over applications and services throughout the environment.

Conclusion

With more data in more places, a government-wide Zero Trust strategy is critical to modern environments. With the help of automation and consistent security across defined networks, a Zero Trust architecture is possible. As your agency extends its mission to the cloud, our security-as-a-service capabilities—including our Prisma™ and Cortex™ product suites—will help expand your Zero Trust environment. For instance, Prisma Access is a comprehensive secure access service edge (SASE) solution that delivers networking and security, ideal for agency branch offices and remote users (two TIC 3.0 use cases).

Palo Alto Networks is a trusted partner of hundreds of national and federal departments, bureaus, and offices. Our enterprise and cloud offerings protect the mission for civilian and defense agencies in critical operating environments globally.

Additional Resources

To learn more about how Palo Alto Networks can help organizations improve cyber risk management, visit our website. Visit our Federal Government webpage to learn how to modernize your agency operations. We can also help you understand more about Zero Trust.

Services to Help You

Palo Alto Networks offers a number of services to help you maximize the value of your investment and protect your business. For more information on support services, Professional Services, and education and training opportunities, visit our Services Overview page.

- **Our global Customer Support** provides timely, expert assistance to keep you up and running safely. Our support organization has been rated outstanding by third-party assessments. All Customer Support plans include online case management, online support resources, and license keys and upgrades. Premium and Premium Plus support options offer additional resources.
- **Our Professional Services and Certified Professional Services Partners** deliver the tools, best practices, and assistance you need to define an effective strategy, simplify operations, and prevent successful cyberattacks.
- **Education and Training Services** help you expand knowledge and skills with world-class training, certification and accreditation, and digital learning options.
- **Cyber Range** is interactive cyber defense training that helps keep your IT network, infrastructure, OT, DevOps, and SecOps teams razor-sharp.

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

strengthen-security-with-zero-trust-uc-060420