



# Accelerating Your Zero Trust Journey in State and Local Government

## A Holistic Approach to Zero Trust: Reduced Complexity and Risk

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction. It's a way for state and local governments to build resilience into their IT environments. With the volume of cyberattacks against government agencies at an all time high, and in light of recent federal mandates, the Zero Trust Model has become increasingly important for state and local government IT leaders who need to keep up with digital transformation and adapt to the ever-changing security landscape.

Unfortunately, many states and localities are still struggling with a poorly integrated, loose assembly of point products that do not align to a strategic approach. Deployed properly, Zero Trust is a strategic approach to cybersecurity that simplifies and unifies risk management under one important goal: to remove all implicit trust in every digital transaction. This means regardless of the situation, user, user location, device, source of connection or access method, cybersecurity must be built in by design in every network, connection and endpoint to address the modern threat landscape. By adopting a true Zero Trust architecture, state and local agencies will benefit from more consistent, improved security and simplified security operations that effectively lower costs.

Palo Alto Networks has been helping governments move toward Zero Trust for several years through direct agency work and as part of the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence. We were selected as one of 20 vendors that are actively collaborating with the NIST on making Zero Trust actionable.

---

## Zero Trust Today: A Modern Security Approach for State and Local Government

In today's environment, state and local governments have reached a tipping point: many users and applications now reside outside of the traditional perimeter. A hybrid workforce is a new reality. Agencies must provide employees access from anywhere and deliver an optimal user experience. The days of managing implied trust by relying on a static, on-premises workforce are gone. At the same time, application delivery has firmly tilted in favor of the cloud – public or private – and has enabled development teams to deliver at an unprecedented pace. However, new architectures as well as new delivery and consumption models create more instances of implied trust, an expanding catalog of apps creates a broader attack surface and implied trust granted to microservices yields new opportunities for attackers to move laterally. Infrastructure can be anywhere, and everything is increasingly interconnected, making the elimination of implicit trust even more critical. You can no longer simply trust IT equipment, such as printers or vendor-supplied hardware and software, because IT and workplace infrastructure are increasingly connected to internet-facing apps that centrally command and orchestrate them. Anything internet-facing is a risk to your agency. Physical locations are increasingly run by internet-connected devices, which typically have more access than they need.

### The Zero Trust Enterprise: Making Zero Trust Actionable

The biggest challenge to adopting a Zero Trust approach is not a lack of specific security tools but rather a simple lack of resources (talent, budget, interoperability, time, etc.). Running the most current security controls against a moving target – a dynamic threat landscape – has been a privilege reserved for a few well-resourced organizations. So why would Zero Trust work this time for the masses? Through Palo Alto Networks extensive experience and comprehensive set of security capabilities, the Zero Trust Enterprise introduces consistent Zero Trust controls across the entire organization. As Forrester noted, “Palo Alto Networks has essentially either procured, acquired or built every tool or capability an organization could need to operate a Zero Trust infrastructure. Palo Alto Networks is assembling a robust portfolio to deliver Zero Trust everywhere – on premises, in the data center and in cloud environments.”<sup>1</sup>

Instead of testing, running and fixing multiple nonintegrated security controls across all your security domains, such as malware or data loss prevention, you can rely on one single control that can be deployed across your entire institution or department. Security by design becomes a reality as the time and cost of deployment and operations all decrease. Moreover, leveraging the network effect of telemetry from the entire organization and not just from one specific area means that the time to respond to and prevent cyberthreats decreases as well, leading to more resilient cybersecurity.

### A Trusted Partner: More Than a Decade of Zero Trust Experience

With thousands of customers and deployments, Palo Alto Networks is a Zero Trust pioneer with experience across the entire security ecosystem, including network, endpoint, Internet of Things (IoT), critical infrastructure and more. We know that security is never a one-size-fits-all approach. Here's what makes our Zero Trust Enterprise approach different:

- **Comprehensive:** Zero Trust is a methodology and should never focus on a narrow technology. Instead, it should consider the full ecosystem of controls that many agencies rely on for protection.
- **Actionable:** Comprehensive Zero Trust isn't easy, but getting started shouldn't be hard. For example, begin with what you have. Think about what current set of controls can be implemented using the security tools you have in place today.
- **Intelligible:** Your Zero Trust approach should be easy to convey to both nontechnical and technical leaders in a concise, easy-to-understand summary.
- **Ecosystem friendly:** In addition to having one of the most comprehensive portfolios in the market, Palo Alto Networks and its broad ecosystem of security partners have an unparalleled ability to make your Zero Trust journey a reality.

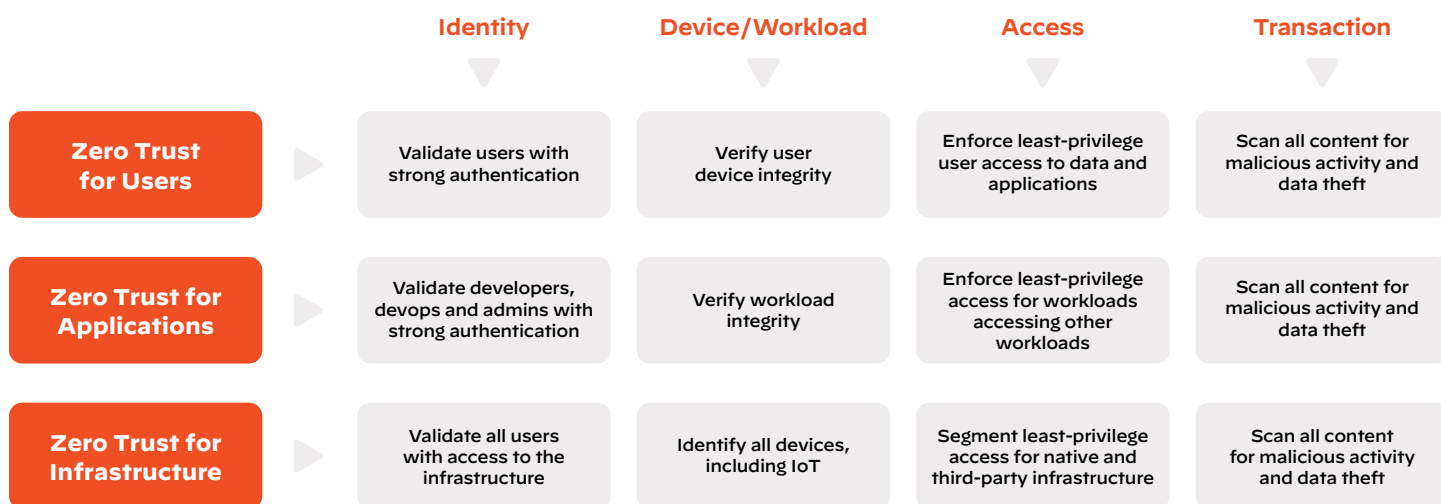
---

1. [The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers](#)

# A Comprehensive Zero Trust Approach: Users, Applications and Infrastructure

At its core, Zero Trust is about eliminating implicit trust across the organization. This means eliminating implicit trust related to users, applications and infrastructure.

- **Users:** Applying Zero Trust to users is a key step in any Zero Trust effort. It starts with strong identity controls that must be continually validated for every user, using best practices, such as multifactor authentication and just-in-time access, which is granting users access to applications or systems for a predetermined period of time, on an as-needed basis. Without strong identity management, Zero Trust policies and controls are much less effective and can be nearly impossible.
- **Applications:** Cloud transformation provides strategic advantages for state and local agencies. It enables new cloud native application development practices and faster application rollout. The right time to architect your security to fit your cloud transformation is while you're moving workloads to the cloud. Many organizations today are applying Zero Trust principles to modernize their cloud native security strategy. For cloud native environments, a Zero Trust architecture continuously runs cybersecurity checks at every stage of the software development lifecycle. From a development and DevOps perspective, this results in safe and frictionless application development.
- **Infrastructure:** Organizations often respond to each emerging threat with a new tool or technology. Research shows that on average, an organization runs 45 cybersecurity-related tools on their network.<sup>2</sup> This heterogeneous environment means that IT teams often have poor visibility and control over unmanaged resources, such as IoT devices and supply chain infrastructure, which have been major factors in recent high-severity security breaches. That means for everything infrastructure-related, including routers, switches, cloud and especially IoT and supply chain resources, eliminating implicit trust is even more critical and must be addressed with a Zero Trust approach.



**Figure 1:** Each pillar requires validation across identity, devices/workloads, access and transactions

For each of the three pillars – users, applications and infrastructure – it is critical to consistently take the following actions:

- **Establish identity using the strongest authentication possible.** The request is authenticated and authorized to verify identity before granting access. This identity is continuously monitored and validated throughout the transaction.

2. [The More Cybersecurity Tools an Enterprise Deploys, the Less Effective Their Defense Is](#)

- **Verify the device/workload.** Identifying laptops, servers, personal smartphones and mission-critical IoT devices that are requesting access, determining the device's identity and verifying its integrity are all integral to Zero Trust. The integrity of the device or host requesting access must be verified. This integrity is continuously monitored and validated for the lifetime of the transaction. In the case of applications, cloud and critical infrastructure, the requested device, microservice, storage or compute resource, as well as partner and third-party apps, must each be validated before granting access.
- **Secure the access.** Agencies must ensure that users only have access to the minimal amount of resources needed to conduct an activity. Even after authenticating and checking for a clean device, least-privilege access must still be ensured.
- **Secure all transactions.** To prevent malicious activity, all content exchanged must be continuously inspected to verify that it is legitimate, safe and secure. Data transactions must be fully examined to prevent data loss and attacks on the organization through malicious activity.

## The Security Operations Center: An Essential Function

The security operations center (SOC) continuously monitors all activity for signs of anomalous or malicious intent to provide an audit point for earlier trust decisions and potentially override them if necessary. Using broad agency data collected from network, endpoint, cloud and other access points, the SOC leverages user and entity behavior analytics, threat hunting, anomaly detection and correlation rules in the security information and event management tool to double-check all trust decisions. This is possible because the SOC has a wide view of the entire infrastructure versus a subset of information, such as separate firewalls or endpoint telemetry. When this information is examined across the entire infrastructure rather than in individual silos, the SOC has the ability to discover things that would normally go undetected.

## Palo Alto Networks: Your Partner for Zero Trust

State and local governments are managing data more broadly and rapidly than ever, enabling critical functions that underpin our local security, economic stability and public safety. More data in more places means institutions face an imperative to pursue a Zero Trust strategy. Palo Alto Networks is a trusted partner to states and localities. Our enterprise and cloud offerings can protect the mission while assisting you on your journey toward Zero Trust.

## Additional Resources

Find out more about how you can [strengthen security with Zero Trust](#). Visit the Palo Alto Networks [Services](#) resources to find out more about our support offerings to help you maximize the value of your investment and protect your state or locality. Contact the Palo Alto Networks team for additional information or visit the [Palo Alto Networks state and local government website](#).



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](http://www.paloaltonetworks.com)

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.  
panw\_wp\_ps\_zerotrust\_statelocal\_0422