A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER | PALO ALTO AND AT&T

Modernizing Zero-Trust Network Access

How building on existing success increases security

It's time for a second generation of Zero-Trust Network Access.

The first generation of ZTNA deployed critical cyber defense capabilities for public agencies at a time when they were rapidly adapting to remote work and depending more on cloud-native applications. But legacy ZTNA solutions have fundamental flaws cybercriminals can exploit.

With an advanced ZTNA 2.0 strategy, agencies can make it more difficult for intruders to gain access.

Upgrading to ZTNA 2.0

The bedrock of ZTNA is least-privilege access, which prevents people from visiting network areas unrelated to their work. ZTNA is a key step to stopping invaders from infiltrating trust-based networks. But legacy ZTNA isn't perfect.

"It doesn't protect all your data and all your apps simply because it doesn't have the mechanisms to recognize all those applications or all the data," says Carlos Valarezo, North American sales leader with Palo Alto Networks.

The next generation of ZTNA can overcome these shortcomings by providing:

Comprehensive least-privilege access. Legacy ZTNA tools can't fully enforce least-privilege access, but the new generation of protection solves this problem.

Continuous trust verifications and security inspections. While legacy ZTNA solutions operate with "allow and ignore" connections, which do not protect information after access has been granted, ZTNA 2.0 always verifies users and inspects connections.

Protection across the board. Unlike the first generation of ZTNA, which provides no data visibility for cloud-native apps, ZTNA 2.0 helps protect all data and apps, securing the cloud-native microservices architectures that most software-as-a-service (SaaS) solutions rely on.

"ZTNA 2.0 isn't just another marketing term," says Paul Gilbert, head of public sector product with AT&T Cybersecurity. "It's a robust improvement over the limitations of legacy ZTNA solutions."

Driving the Need for Change

The same work and communication changes that called for first-generation ZTNA have prompted a reassessment of security strategies. Both constituents and agencies have advanced expectations for the services available and how quickly they can be delivered. As public sector operations embrace the cloud and other modern technologies, they require increasingly robust protection. ZTNA 2.0 is the solution.

As public sector operations embrace the cloud and other modern technologies, they require increasingly robust protection.

ZTNA 2.0 is the solution.

"We're at a pivot point — particularly in government — where cloud is here to stay," Valarezo says. "Applications are everywhere now. The workforce is accessing those applications from everywhere."

For example, remote work and digital SaaS applications undermined the traditional network perimeter defense and drove the need for ZTNA. But now, ZTNA 2.0 is critical to help agencies beef up their monitoring and inspection of cloud-based applications and data, and fold these protections in with on-premises technologies.

ZTNA 2.0 allows agencies to integrate multiple security solutions to provide comprehensive, continuous least-privilege access across the whole environment. This advanced approach is necessary for agencies as they seek to address any gaps in their security strategy.

Now is the time to assess quickly deployed security strategies and determine if they're still working as envisioned. The shortfalls that exist in legacy ZTNA solutions will only become magnified with time.

Finding Effective Partnerships

Upgrading to ZTNA 2.0 requires cybersecurity practitioners who understand the constantly-evolving threat landscape. Recruiting and retaining this kind of talent can be daunting for agencies. Most public organizations can gain access to far more talent at a lower cost through managed services rather than trying to fill those skills gaps in-house.

The challenge for many agencies is finding the best fit for their organizations. That requires asking tough, pointed questions of potential partners:

- **How does your service deliver value and differ from that of your competition**
- **What kind of service-level agreements can you deliver?**
- **What's your track record with public sector agencies?**
- **How will you integrate your solution with an existing technology stack?**

"It's very important that your partner understands what you currently have and can help you get to the point where you want to be," Gilbert says.

Keep in mind ZTNA 2.0 will most likely be delivered via a technology platform. The platform partner must show how they can dovetail their tech with your entire IT ecosystem.

This piece was written and produced by the Government Technology Content Studio, with information and input from Palo Alto and AT&T.

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Sponsored by:

paloalto® NETWORKS

For more information, visit
www.paloaltonetworks.com/about-us

AT&T Cybersecurity

AT&T Cybersecurity is one of the world's leading managed security services providers. Our experienced cybersecurity consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

ADOBESTOCK