World Wide Technology

Google Cloud

Top Five Takeaways:

Moving to a Zero Trust Architecture

How government agencies can adhere to the Cyber EO

As the threat landscape continues to evolve, government agencies cannot simply add another tool to their security stack as a method of protection. The Cyber Executive Order (EO) calls on agencies to adopt a Zero Trust framework, one that requires more than a simple point product, but a comprehensive strategy and overarching view of an agency's cyber posture. In a cloud first world, how can agencies accelerate their journey to Zero Trust given the current and evolving cyberspace environment?

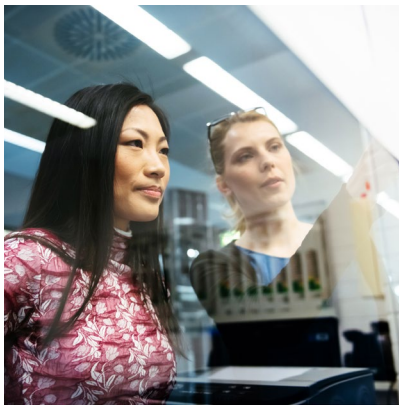
To enable a more streamlined pathway to Zero Trust, agencies should consider the following:

Assessment and Planning

Zero Trust assessment and planning is a critical component to initiate an effective Zero Trust program. This should be designed to help an agency reach its security goals through Zero Trust architecture planning for core applications and data. Working with a third-party to take an unbiased look at an agency's IT environment and advising the organization on the culture change, policies and technology needed to achieve a Zero Trust framework is step one. This can be delivered in phases to ensure success within the agency's infrastructure and will help identify what tools are actually needed to support existing assets and infrastructure in cloud-based, on-premises, or hybrid environments.

Secure Application Access

A Zero Trust framework requires the ability to identify, access and manage applications across an agency network. This should include implementing a container-based offering for secure application access and monitoring. A secure application access solution can serve as a scalable, highly responsive alternative to government network boundary systems by deploying and managing containers that provide secure access and monitoring for applications in cloud or on-premises environments. The result of implementing this type of solution includes fast secure and controlled access by users to software-as-a-service (SaaS) apps directly over the internet.



Active Cyber Threat Detection

Active cyber threat detection capabilities can help government agencies quickly determine if they may have been compromised by cyberattacks that they have not yet detected. Ideally delivered through a cloud-native solution, an active cyber threat detection solution leverages threat hunting, detection and investigation capabilities to ensure fast and effective incident response and remediation. This will also allow government organizations of all sizes to readily analyze their historic and current log data to detect threats confidently and quickly.

Integrated Threat and Data Protection

Agencies need a Zero Trust solution that enables secure access with integrated threat and data protection. This should include features such as:

Identity and context-aware access controls: easily configure policies based on user identity, device health and other contextual factors to enforce granular access controls to applications, VMs and APIs. Implement strong authentication and authorization policies to ensure users have access to the resources they need.

Integrated threat and data protection: prevent data loss and thwart threats such as malware and phishing with real-time alerts and detailed reports.

Support for cloud, on-premises or hybrid environments: access SaaS apps, web apps and cloud resources no matter where they are hosted.

Easy adoption with agentless approach: capability delivered as a non-disruptive overlay to an agency's existing architecture, with no need to install additional agents, for a seamless, familiar, easy-to-use experience.

Outcomes-based Approach

Ultimately, successful implementation of Zero Trust is not about the individual technology components and inputs themselves. Instead, what matters most is how security components are integrated and orchestrated to achieve and enforce a simple set of core principles, including:

- Connecting from a particular network must not determine which services an agency can access.
- Access to services and data is granted based on what we know about the end user and the device.
- All access to services must be authenticated, authorized and encrypted.

Google – A Case Study in Zero Trust

Google began its Zero Trust journey over a decade ago, under similar circumstances to those driving today's government cybersecurity efforts. To improve the company's security posture and user experience, Google had to reimagine its infrastructure and production networks. This ultimately drove innovations in how the company protected its supply chains and resulted in a complete rethinking of the scale, analytics and visibility needed to fully modernize and transform enterprise security. This also resulted in a baseline and framework for a structured and effective Zero Trust architecture, one that government agencies can emulate for a successful transition.

About World Wide Technology

World Wide Technology (WWT), a global technology solutions provider with $13.4 billion in annual revenue, combines the power of strategy, execution and partnership to accelerate transformational outcomes for large public and private organizations around the world. Through its Advanced Technology Center, a collaborative ecosystem of the world's most advanced hardware and software solutions, WWT helps customers and partners conceptualize, test and validate innovative technology solutions for the best business outcomes and then deploys them at scale through its 4 million square feet of global warehousing, distribution and integration space. For more information, visit **wwt.com.**

About Google Cloud

Google Cloud is helping federal, state, and local governments empower their workforce and improve the lives of their constituents with our secure, interoperable, intelligent platform. Whether your organization is looking to build new applications in the cloud or transform your current infrastructure, we can help modernize service delivery to focus on your mission. For more information, visit our government **webpage** or **www.cloud.google.com**