okta

A Zero Trust Architecture for Government Agencies

How Okta, CrowdStrike, Zscaler, and AWS work together to implement secure, compliant, easy-to-use Zero Trust environments.

Federal agencies are required to develop a modern approach to cybersecurity known as Zero Trust Architecture (per NIST SP 800-207) by the end of fiscal year 2024.[1] That includes using automation, orchestration, and cloud migration. As a result, agencies need to work with vendors that can help them achieve this stronger security stance against evolving cyber threats.

However, with old, perimeter-based approaches to security, most agencies are struggling to begin the transition.

In collaboration with

aws

CROWDSTRIKE

zscaler™

Invest in a Zero Trust Architecture

Okta, CrowdStrike, Zscaler, and AWS provide integrated best-of-breed security solutions for government agencies to enable:

- A scalable, cloud-based platform to manage Identity, devices, secure connectivity, applications, and data.
- Advanced cyber capabilities
- Cross-platform visibility for a better and more diverse view of the threat landscape
- Improved user experiences for employees and citizens

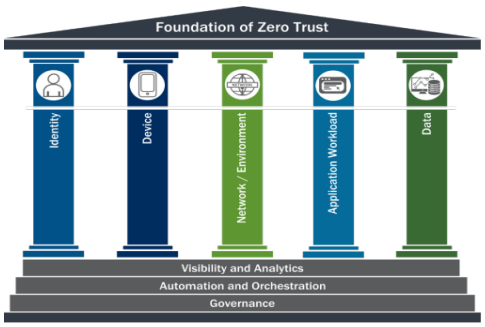
Strong, reliable pillars of protection

Federal agencies need a modern, Identity-centric strategy that can help them fast-track their Zero Trust Architecture (ZTA) implementation. The solution must meet the requirements in President Biden's Executive Order on Improving the Nation's Cybersecurity (EO 14028). It is possible to leverage modern cloud services to create an IT infrastructure that is secure, agile, scalable, and frictionless with improved customer experience.

Okta, CrowdStrike, Zscaler, and Amazon Web Services (AWS) together offer an integrated and proven solution that can quickly support governmental compliance requirements. The solution supports the US Cybersecurity and Infrastructure Security Agency's (CISA) five pillars of a ZTA: Identity, device, network and environment, application workload, and data.

[1] Zero Trust Executive Order

okta



CISA Zero Trust Maturity Model

The CISA Zero Trust Maturity Model provides a foundation of five pillars and three cross-cutting capabilities. Together, Okta, CrowdStrike, Zscaler, and AWS help agencies to complete their Zero Trust journey.

An integrated security solution, trusted by thousands

To address the five Zero Trust pillars, Okta, CrowdStrike, Zscaler, and AWS offer an integrated, cloud-native, flexible security solution to provide least privileged access control anywhere without compromising user experience. Agencies gain endpoint security, Identity and access management, and network security—all on a secure cloud network adaptive to hybrid working environments. The integration of these technologies accelerates Zero Trust Architectures, addressing these pillars together to help each agency take a scalable and least disruptive approach. It is an ideal collaboration for government agencies to successfully transition to Zero Trust and meet the demands of EO 14028.

Pillar 1: Identity security

Okta delivers an Identity management service that enables agencies to securely connect the right people to the right technologies at the right time. Using its own context-based policy engine, Okta makes authentication decisions to enable unified, automated, and Identity-driven security for the workforce and public.

Pillar 2: Device security

CrowdStrike secures devices with the CrowdStrike Falcon® platform, which provides endpoint threat detection and response, Identity protection, and device posture. The solution secures the modern enterprise with its cloud-native approach to stop breaches in real time for any endpoint and cloud workload, wherever users are.

Pillar 3: Network/environment security

Zscaler provides the Zero Trust Exchange™ (ZTE), which is a cloud native platform that powers a complete security service edge (SSE) to connect users, workloads, and devices without putting them on a legacy network. The ZTE reduces the security risks and complexity associated with perimeter-based security solutions that extend the network, expand the attack surface, increase the risk of lateral threat movement, and fail to prevent data loss. Zscaler enables fast, direct, and secure connections based on the Zero Trust principle of least-privileged access, which greatly reduces business risk.

Pillars 4 and 5: Application workload and data security

AWS provides public sector agencies with flexible cloud solutions to empower secure, scalable work. AWS offers AWS Verified Access, which validates every application request before granting access. Verified Access removes the need for a VPN, reducing management complexity for IT administrators. AWS also offers AWS Security Lake, which automatically centralizes security data from cloud, on-premises, and custom sources into a purpose-built data lake stored in your account. And lastly, AWS provides AWS GovCloud (US), which gives government customers and their partners the flexibility to architect secure cloud solutions that meet the demands of applicable US government regulations.

Learn more

Okta, CrowdStrike, Zscaler, and AWS together can help your agency implement a true **Zero Trust environment.**