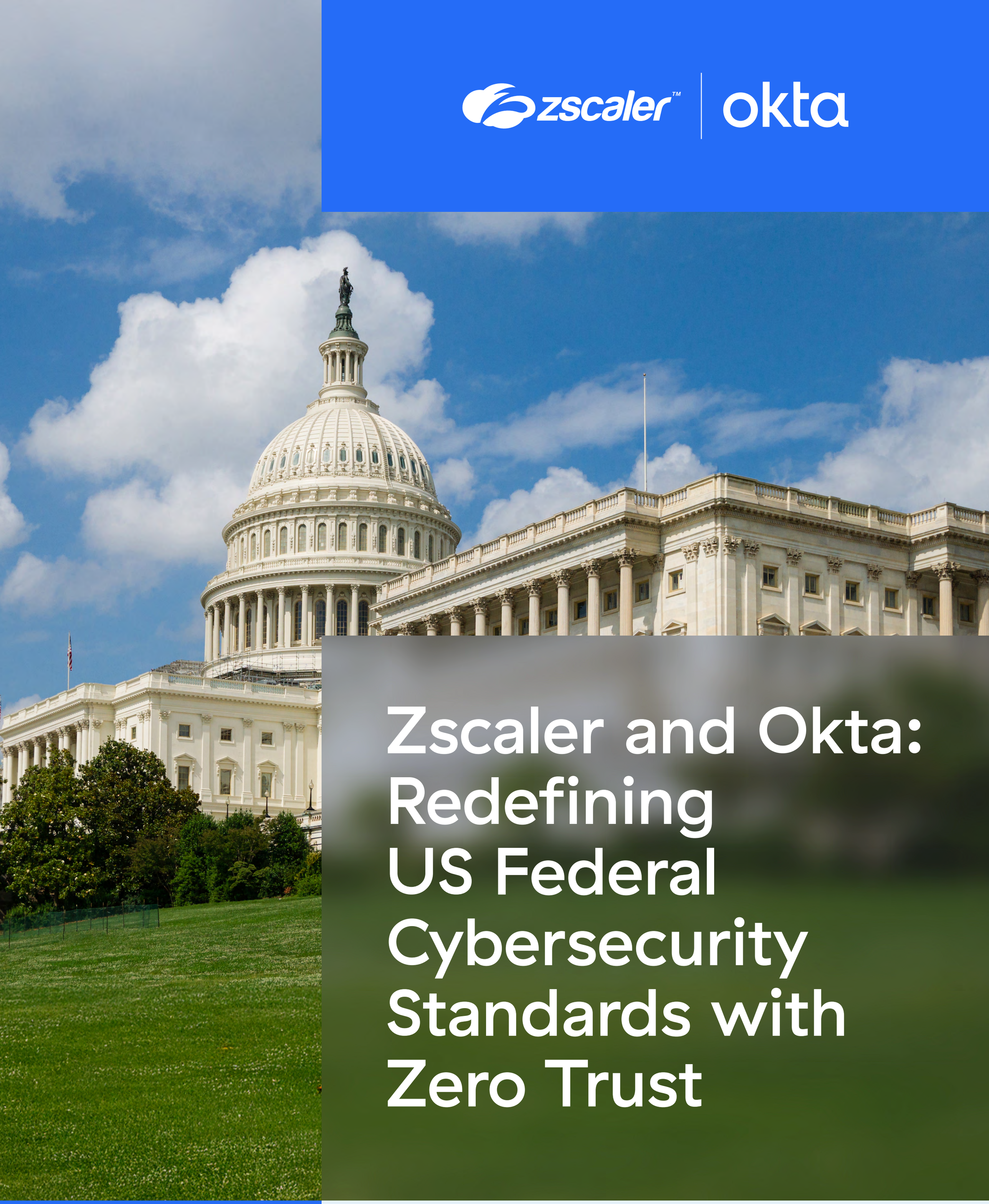

Zscaler and Okta: Redefining US Federal Cybersecurity Standards with Zero Trust

SOLUTION BRIEF

Introduction

US Federal agencies face growing pressure to modernize their IT infrastructure while meeting strict government regulations and budgetary constraints. The integration of Zscaler and Okta provides a robust security framework designed to support IT modernization efforts, ensure compliance with stringent federal standards, and align with cost-cutting measures.

Security Challenges Facing the Federal Government

Federal IT environments face increasing cybersecurity threats due to a combination of inadequate security investments, bureaucratic hurdles slowing modernization, and a sprawling attack surface made worse by outdated systems. The scale and complexity of these environments, coupled with reliance on numerous interconnected systems, make them prime targets for cybercriminals. Insider threats and credential risks add to the danger, as identity-based attacks like phishing and credential stuffing enable adversaries to steal sensitive government data and move laterally through networks undetected.

Compounding these challenges are mounting compliance pressures from regulations like Executive Order 14028, OMB M-22-09, and TIC 3.0, which coincide with mandates by the Department of Government Efficiency (DOGE). These financial and policy constraints inhibit modernization efforts, leaving agencies more vulnerable to breaches and increasing the risk of non-compliance.

Outdated infrastructure intensifies these issues. Many agencies continue to depend on legacy systems such as MTIPS/MPLS networks and traditional VPNs, which fail to align with Zero Trust Architecture (ZTA) principles outlined in Executive Order 14028. These antiquated systems grant overly broad access privileges, introducing critical vulnerabilities and exposing agencies to breaches. Additionally, they impair workforce productivity with slow, inefficient access to applications and data, lack modern capabilities to inspect encrypted traffic, and are ill-equipped to combat sophisticated cyber threats.

The financial inefficiencies of legacy systems also place a significant burden on federal budgets. Federal agencies spend an estimated $90 million annually on MPLS circuit costs alone, with these expenses steadily rising. Over the past 12 years, $306 million has been poured into maintaining outdated enterprise infrastructure. In a broader context, $50 billion has been allocated over 15 years toward traditional government-wide connectivity solutions.

These challenges highlight a vital opportunity for transformation. By replacing obsolete systems, agencies can strengthen their cybersecurity posture while simultaneously reducing costs.

Zscaler and Okta Modernize Federal IT with Integrated Zero Trust

Zscaler and Okta form a powerful partnership for modernizing federal IT environments, helping agencies implement a Zero Trust framework that prioritizes security, drives cost efficiency, and supports compliance with federal mandates—all while addressing evolving cybersecurity threats.

Zero Trust, guided by the principle of "never trust, always verify," ensures every access request—whether internal or external—is authenticated, authorized, and continuously monitored before access is granted. Okta provides advanced user authentication and adaptive identity controls, while Zscaler's Zero Trust Exchange (ZTE) platform enforces identity-aware, least-privilege access to prevent unauthorized access and lateral movement across government networks.

As cloud-native and commercially-available platforms, Zscaler and Okta deliver integrated solutions that eliminate the need for legacy access technologies like MTIPS and VPNs, as well as on-premises or fragmented identity management systems. This makes them ideal for federal agencies aiming to modernize IT infrastructure and accelerate digital transformation, all while balancing budgetary constraints and adhering to cost-cutting mandates from the Department of Government Efficiency (DOGE).

A Closer Look at Key Integrations

Okta and Zscaler integrate to implement standard authentication methods like Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) to provide smooth, secure login experiences through Single Sign-On (SSO) and Multi-Factor Authentication (MFA). These features improve convenience for users while reinforcing security by verifying their identities. The integrated platforms also leverage System for Cross-domain Identity Management (SCIM), which simplifies user management by automatically updating roles and permissions in real time. This automation ensures that access rights are consistent (e.g., when users join, change roles, or leave) and reduces the need for manual adjustments—while ensuring that only approved individuals can access sensitive resources.

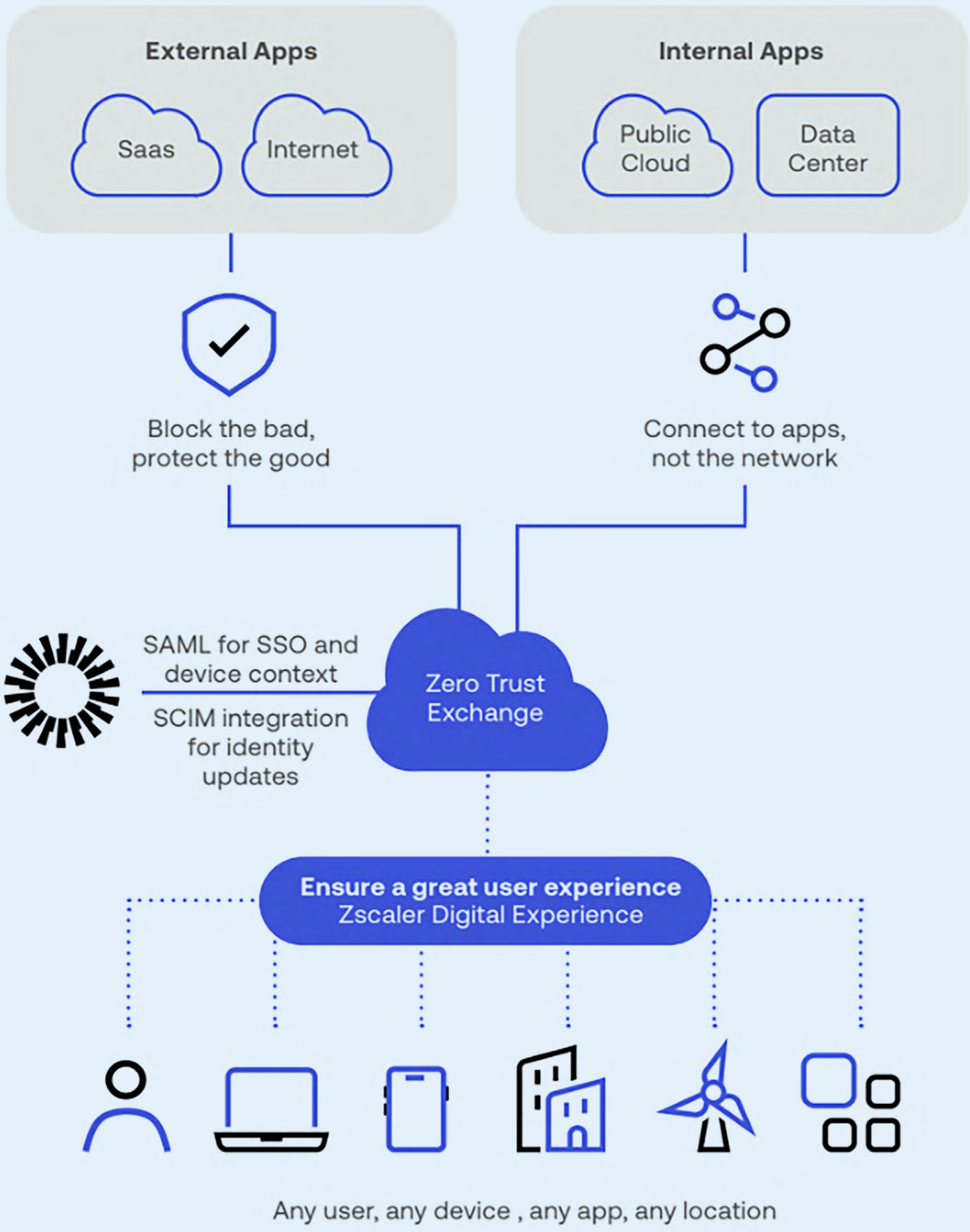

FIGURE 1

Zscaler and Okta enable robust authentication to verify user identities and enforce Zero Trust access, ensuring users are granted access only to the specific resources they need—no matter where they are located.

Beyond foundational integrations, the partnership drives advanced security measures at every level:

- **Bi-Directional Risk Alert Sharing and Threat Containment:** Zscaler Deception works with Identity Threat Protection with Okta AI (ITP) to strengthen defenses against insider threats and external cyberattacks. This integration provides adaptive security and continuous authentication to enforce Zero Trust policies in real time. Zscaler uses decoy systems to detect risks and send precise alerts to Okta through the Shared Signals Framework (SSF). These alerts help Okta take action, for example, logging out compromised accounts, to reduce the risk of breaches.

- **Context-Aware Access Controls with Dynamic Step-Up Authentication:** Zscaler's Adaptive Access Engine connects with Okta Workforce Identity to apply dynamic security policies based on changing context of the user. If a user's online behavior or activities show signs of higher risk, Zscaler's Adaptive Access Engine can require extra verification using Okta's step-up authentication before allowing access, adding an extra layer of security.

- **Proactive Vulnerability Management:** Zscaler Unified Vulnerability Management combines data from Okta logs—such as user logins, device details, activities, and risk levels—with insights from over 150 other data streams through Zscaler's Security Data Fabric. This integration gives security teams the tools they need to quickly detect and resolve vulnerabilities.

- **Secure External User Access with Universal Logout:** Zscaler's Zero Trust Exchange uses Cloud Browser Isolation (CBI) to provide external users with safe, agentless access to web apps from unmanaged devices. It guards sensitive data and secures app interactions without requiring any endpoint installation. Okta enhances this process by allowing IT teams to efficiently manage identity and access through Okta Universal Directory. This includes quickly onboarding users, assigning applications, applying security policies, and scaling operations as needed.

Supporting Federal Compliance Mandates

The integration of Zscaler and Okta tackles critical challenges faced by federal agencies and contractors, such as modernizing outdated infrastructure, adopting Zero Trust principles, and meeting increasingly stringent security mandates. By providing comprehensive identity management, access control, and threat protection, this partnership helps agencies align with key federal directives, including:

- **FedRAMP and DoD Compliance:** Zscaler and Okta are both FedRAMP Authorized, allowing seamless deployments in civilian and defense environments. Zscaler holds certifications for FedRAMP High and DoD Impact Level 5 (IL5), while Okta is certified at FedRAMP Moderate, FedRAMP High, and DoD IL4 with approval to support IL5 workloads. These certifications simplify the Authorization to Operate (ATO) process, streamline compliance audits, and reduce operational complexity—enabling agencies to securely adopt cloud-based solutions with greater efficiency.

- **Executive Order 14028—Improving the Nation's Cybersecurity:** Executive Order 14028 directs federal agencies to enhance their cybersecurity posture by adopting Zero Trust principles, implementing MFA, and encrypting sensitive data. Zscaler and Okta help agencies meet these requirements by providing integrated solutions for Zero Trust, Secure Access Service Edge (SASE), and identity and access management (IAM). Okta delivers adaptive identity access controls, such as MFA and context-aware authentication, while Zscaler ensures secure connectivity to private applications with adaptive access policy enforcement, inline TLS/SSL inspection to detect and block threats in encrypted traffic, and data loss protection (DLP). Together, they enable real-time access validation, granular application segmentation, and rapid incident response, aligning with EO 14028 priorities.

- **OMB M-22-09—Federal Zero Trust Strategy:** OMB M-22-09 outlines five core pillars for Zero Trust implementation: identity, device, network, application workload, and data. Okta and Zscaler provide a comprehensive solution addressing these pillars, helping agencies comply with M-22-09 mandates. Okta evaluates identity, device, location, and behavioral context to enforce secure authentication, while Zscaler applies risk-based conditional access policies, enables application-specific microsegmentation, and protects sensitive data through inline Data Loss Prevention (DLP) and advanced traffic inspection. Together, they accelerate the adoption of a unified, cloud-native Zero Trust architecture, delivering secure and scalable access across hybrid environments.

- **CISA Zero Trust Maturity Model:** The CISA Zero Trust Maturity Model offers a blueprint for agencies aiming to reach "Advanced" or "Optimal" levels of Zero Trust maturity. Zscaler and Okta support this modernization by delivering continuous, identity-focused access control tied to dynamic risk assessments. They enable granular, policy-driven segmentation while leveraging integrated threat intelligence and real-time telemetry to enhance decision-making and improve overall security posture.

- **TIC 3.0—Trusted Internet Connections Modernization:** Zscaler supports agencies in addressing Trusted Internet Connections (TIC) 3.0 requirements by providing secure direct-to-cloud connectivity along with advanced traffic inspection for cloud environments, remote users, and branch offices. Additionally, the use of identity federation and strong authentication solutions, such as those that enable users to log into applications with credentials from their organization's identity provider (e.g., Active Directory), can help facilitate TIC-compliant access. By leveraging tools like Zscaler with leading identity solutions such as Okta, agencies can modernize their network architectures efficiently while maintaining governance and visibility.

- **Cybersecurity Maturity Model Certification (CMMC):** The CMMC framework governs how federal contractors secure Controlled Unclassified Information (CUI). Zscaler and Okta help agencies and contractors meet critical CMMC requirements by delivering a Zero Trust, identity-centered architecture that streamlines compliance across multiple domains, ensuring robust protection of sensitive data.

Here's a breakdown of how Okta and Zscaler work together to ensure CMMC compliance across multiple domains.

CMMC Domain	Okta – Identity First Security	Zscaler – Zero Trust Access & Inline Protection
Access Control (AC)	Enforces least-privileged access based on user identity, MFA, and risk context. Supports PIV (Personal Identity Verification) and CAC (Common Access Card) authentication and role-based access for federal users.	Grants application-specific access without exposing the network; blocks lateral movement and unauthorized reach to critical business resources and sensitive data.
Identification & Authentication (IA)	Verifies user identity using adaptive MFA and integrates with federal credentialing systems.	Consumes Okta identity context to apply fine-grained access policies for private and internet-bound apps.
System & Communications Protection (SC)	Works with device posture signals to enforce access based on trusted endpoints.	Inspects all traffic inline (including TLS), blocks malware/phishing, and enforces DLP and secure app segmentation.
Audit & Accountability (AU)	Provides centralized identity logs and session data for audit, investigation, and reporting.	Delivers full visibility into user activity, application access, and policy enforcement; integrates with SIEMs.
Incident Response (IR)	Triggers step-up authentication or session termination based on risk signals or anomaly detection.	Revokes access dynamically in response to identity or threat triggers; helps contain breaches in real-time.
Configuration Management (CM)	Offers cloud-native identity services with managed baselines and centralized configuration.	Cloud-delivered service with minimal endpoint footprint; consistent, centrally managed policy updates.

* For an in-depth understanding of how Okta and Zscaler's platforms effectively address critical security and management domains within the CMMC framework, review the comprehensive documentation on Okta's approach to CMMC compliance and Zscaler's Zero Trust solution for CMMC.

Driving Cost Savings and Operational Efficiency

Federal agencies using Okta have achieved significant savings by replacing legacy identity systems, with one agency reporting a 6x cost reduction through the Okta Identity Cloud. Okta's automation capabilities, such as Okta Workflows authorized at FedRAMP High, have further reduced labor-intensive identity processes at scale—ensuring users quickly and securely access critical resources. Meanwhile, targeted identity governance has helped agencies cut up to 25% of SaaS waste*, optimizing budgets while maintaining compliance. With FedRAMP High certification and alignment with mandates like EO 14028, TIC 3.0, and CMMC, Okta ensures agencies adhere to the highest security and regulatory standards.

Zscaler complements these outcomes by helping agencies modernize network security and implement Zero Trust principles. By eliminating legacy perimeter tools and TIC stacks, agencies have realized 70% cost savings, streamlined 90% of infrastructure complexity, and reduced operational overhead by 30%, yielding an annual ROI of over $200,000. The financial impact has been equally impressive, with government agencies saving $306 million over 12 years by deploying scalable Zero Trust solutions. Additionally, tens of millions of dollars are saved annually by transitioning from expensive MPLS circuits to cost-effective ISP connections, reinforcing Zscaler's value in modernizing federal IT while staying within budgetary constraints.

On the security front, Zscaler's Zero Trust architecture has closed 85% of security gaps through encrypted traffic inspection and segmentation, ensuring sensitive data remains secure. With FedRAMP High and DoD IL5 certifications, Zscaler aligns with federal mandates such as EO 14028, TIC 3.0 use cases, and CMMC controls, delivering modern security while meeting compliance requirements. To learn more about how Zscaler supports federal agencies, explore our blog here.

* Savings are estimates based on customer reporting. Savings may vary and are not guaranteed.

Message to Federal Leaders

Federal IT leaders are being asked to do more with less — while ensuring airtight security in an increasingly distributed environment. Legacy infrastructure like MPLS/MTIPS networks, VPNs, firewalls, and monolithic identity systems are expensive, complex, and misaligned with modern threat models.

Zscaler and Okta offer a new path forward:

- **Zero Trust without compromise** — With Okta providing secure, adaptive identity access and Zscaler delivering inline, least-privileged access to apps, users, and workloads.
- **Massive cost savings** — Agencies have realized up to 6x savings in identity and 70% reduction in security infrastructure costs.
- **Operational agility** — Automation and cloud-native access have slashed provisioning timelines, onboarding delays, and investigation response cycles.
- **Full alignment with mandates** — Both platforms are FedRAMP and DoD authorized and help meet the requirements of EO 14028, OMB M-22-09, the CISA ZTMM 2.0, TIC 3.0, and CMMC readiness.

An Important Consideration: Zero Trust is an Ecosystem

While Zscaler and Okta deliver critical capabilities for Zero Trust identity and application access, they are only one part of the equation. To fully realize the potential of a comprehensive Zero Trust security strategy, federal agencies must adopt an ecosystem approach that integrates solutions such as Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and Configuration Management Database (CMDB) platforms to address the full scope of federal mandates. These tools work in tandem to enhance visibility, streamline investigations, accelerate response times, and ensure compliance with evolving security requirements. Federal agencies can unlock the full power of Zero Trust by integrating the right mix of technologies, creating a security posture capable of meeting modern challenges with confidence.

Call to Action

Now is the time to modernize. With Zscaler and Okta, agencies can replace outdated perimeter-based controls with a unified, Zero Trust model that is faster, more secure, and more cost-effective.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more about how Zscaler secures the federal government with the power and scale of the cloud here.

About Okta

Okta, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn how Okta accelerates agency missions with modern, zero trust identity to support the US Government's high impact workloads here.