

Security and Resilience for AI-Powered Work in State and Local Government and Education

Okta + Google Workspace

AI adoption is accelerating faster than governance can keep up. According to Deloitte's State of AI in the Enterprise 2026, 74% of companies plan to deploy agentic AI within two years, yet only 21% have mature governance models for autonomous agents. ^[1]

As government agencies, colleges, and universities race to adopt AI and support distributed workforces across an expanding ecosystem of SaaS apps and devices, they face urgent security and flexibility challenges. The path forward starts with a fundamental truth: to get AI right, you have to get identity right.

Securing modern work and AI without losing flexibility

As organizations embrace AI-powered ways of working and cloud-first collaboration, identity has become the front line of security and the most common point of compromise.

Organizations want the productivity gains of AI-assisted work, but they also recognize the risk: AI introduces new pathways to sensitive data, new governance requirements, and greater exposure if identity and access controls aren't strong enough.

At the same time, work now spans SaaS apps and multiple devices distributed across staff, faculty, contractors, and partners. This makes it

harder to ensure the right people have the right access at the right time, increasing exposure to credential theft, unauthorized access, inconsistent policy enforcement, and shadow AI usage that can put sensitive data at risk.

Many organizations also feel pressure from platform lock-in, which can limit choice, slow modernization, and increase long-term commercial and operational risk.



Common challenges

- Granting agents unmanaged “keys to the kingdom,” which creates shadow AI outside of IT view
- Keeping up with identity-centered threats and unauthorized data access
- Managing fragmented identity across multi-agency and multi-campus environments
- Securing access without slowing the workforce down

[1] Source: [Deloitte: The State of AI in the Enterprise, 2026](#)

What you gain: secure productivity across every agency and campus

The joint solution is designed for organizations that want to modernize collaboration, accelerate AI adoption, and improve resilience without compromising user experience or flexibility.



Built for AI-driven work

Organizations can safely harness the power of Gemini by combining smarter workflows with adaptive security. While Gemini accelerates content creation and information synthesis, Okta ensures these AI agents have the keys, not the kingdom. By leveraging risk-based authentication and granular policies based on device, network, and location, Okta provides a unified control plane to govern the entire agent lifecycle. This prevents shadow AI and stops credential-based breaches that put resident and student data at risk.



Reduced friction for service delivery

Security should not slow service delivery. Okta and Google Workspace support seamless access to the tools staff, faculty, and students use every day while reducing password fatigue and login disruption.



Open and flexible by design

Modern work requires choice. Okta and Google Workspace enable organizations to modernize collaboration while maintaining the flexibility to integrate best-in-breed tools across the broader ecosystem, without being constrained by a closed platform. Organizations can scale securely as workforce models change and as new applications, devices, and AI workflows are introduced.

Collaboration and AI, secured by identity

Okta and Google Workspace solve this challenge by bringing together modern collaboration and best-in-class identity to enable productivity that's secure by design. Together we keep identity, access, and collaboration protected across the entire ecosystem.

Okta secures access to Workspace and extends the same protection across 8,000+ applications for fast and secure Single Sign-On (SSO) and user provisioning, while automating the identity lifecycle to reduce IT friction and risk. With adaptive, condition-based access controls and stronger protections against modern threats, organizations can move faster and adopt AI with confidence, without being locked into a rigid, single-vendor stack.

Okta + Google Workspace is ideal for organizations that want to:

- Modernize collaboration with AI-powered productivity
- Reduce identity risk while improving resilience and control
- Support hybrid work and distributed teams securely
- Avoid vendor lock-in while providing best-in-breed tools

Together, we provide an open, Zero Trust foundation that enables people to work faster and smarter, wherever work happens, without lock-in or compromise.

How Okta + Google Workspace Work Together

Okta delivers deep integration capabilities that enhance security, automation, and operational efficiency across Google Workspace deployments. Organizations can choose how they manage users and licenses by leveraging Okta Universal Directory, or Google master accounts as the authoritative user source.

- **Master from any authoritative source** to simplify identity management across HRIS, SIS, and AD
- **Automate license provisioning and workflows** to streamline onboarding / offboarding and optimize budgets
- **Control access with condition-based policies** for precise security and compliance enforcement.
- **Mitigate threats proactively** with visibility, remediation guidance, and real-time session termination

Empower AI with identity-first security

With the integrated solution, organizations can increase productivity, strengthen identity security, and preserve the flexibility to evolve without compromise. When it comes to AI agents, identity matters. Together with Google Workspace, Okta secures AI by empowering it with identity-first security. The result is scalable AI innovation with security built in.



Work Transformation Set: Break free from legacy tech to unlock AI-first work

For organizations ready to migrate off legacy solutions and consolidate procurement, the Work Transformation Set offers Google Workspace with Gemini, Okta identity, and Omnisia device management through a unified Google Cloud price, plan, and contract to streamline planning, procurement, and adoption.

Built for the AI era and open by design, it helps customers modernize collaboration while reducing the risks of growing cybersecurity attacks and simplifying change management

For more information on this integration, visit okta.com/partners/google

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables agencies and institutions to securely connect the right people to the right technologies at the right time. We provide simple and secure access to people and organizations everywhere, giving them the confidence to deliver on their mission. To learn more, visit okta.com