Whitepaper

Setting the Bar for Enterprise Identity in the Age of AI

Contents

Introduction

75%

of enterprise buyers now prioritize advanced identity security
(Okta Buyer Survey 2025)

AI is accelerating SaaS—and enterprise expectations. Apps are being built and adopted faster than ever, but buyers want more: intelligent automation, seamless integration, and security by design. While 82% of organizations plan to increase AI investments, the overall AI maturity has declined by 9 points year over year, revealing a growing gap between rapid innovation and secure execution (ServiceNow Enterprise AI Maturity Index 2025).

While AI innovation is grabbing significant attention in the market, it's critical that vendors and enterprises alike don't lose sight of fundamental capabilities, including identity security. **75% of enterprise buyers now prioritize advanced identity security** (Okta Buyer Survey 2025), and leading SaaS builders are turning it into a **competitive edge**. Enterprise-grade capabilities like federated access, lifecycle management, entitlements, session control, risk monitoring, and automation remain essential for secure, real-time decisions at scale. But as AI begins acting autonomously across systems, **app-to-app authorization is the next critical frontier**.

- **Prioritize identity features to unlock growth**, closing critical gaps when it matters most.
- **Accelerate adoption** by gaining exposure to enterprise IT and security teams, delivering identity solutions trusted by around 17,000 customers.
- **Help to future-proof your product with standards that plug into any enterprise**—build once and deploy anywhere.

Let’s raise the bar, so you can build with confidence, scale faster, and win more enterprise deals.

Cross App Access for AI Agents

Okta's New Focus for SaaS Builders

Cross App Access for AI Agents (CAA) is a new protocol that governs how AI agents and applications connect by shifting control to the identity layer. It gives enterprises control over how AI agents and apps connect, enabling centralized policies, visibility, and lifecycle management for interactions that were previously ungoverned.

CAA is like applying a user's Single Sign-On (SSO) context to an agent accessing an API. It lets applications, and the AI agents, bots, and services within them, securely access data and perform actions across other apps on a user's behalf. It delivers trusted, governed access between apps without exposing credentials or expanding your attack surface.

Why it matters

As enterprises embrace AI automation, apps are increasingly acting on users' behalfs—triggering workflows, sharing data, and making decisions. But most identity models were built for humans, not software agents, creating friction in managing the web of app-to-app connections AI depends on. Without identity-based, cross-app authorization, it's difficult to efficiently manage access, enforce least privilege, or gain visibility into which agents are accessing what systems and why.

To stay secure, scalable, and compliant, SaaS apps need standards-based, machine-to-machine identity that can verify, authorize, and revoke access—just like it does for human users.

Federated Identity with Single Sign-On

Single Sign-On (SSO) gives enterprise users fast, secure access to approved apps. It centralizes identity management and lets IT enforce access policies from one place. By streamlining user access and lifecycle management, and factoring in device, network, risk, and compliance signals, SSO strengthens security and builds trust.without exposing credentials or expanding your attack surface.

Why it matters

SSO is essential to enterprise security, helping reduce credential sprawl and shrink attack surfaces. But traditional protocols like SAML have limitations, especially when it comes to securing backend services. That's where modern protocols like OpenID Connect (OIDC) come in. By leveraging OIDC along with contextual signals such as device, network, risk, and compliance, developers can strengthen security, reduce IT friction, and accelerate adoption.

Identity Directory and Authorization Lifecycle Management

Lifecycle Management automates access as employees join, change roles, or leave. With a unified directory, enterprises manage identities and entitlements from one source of truth, granting the right access instantly and revoking it the moment it's no longer needed. The result: stronger security, less manual effort, and complete visibility.

Why it matters

Enterprise provisioning often involves complex onboarding and offboarding. Different user groups need different levels of access, and IT must revoke access immediately when users leave. Aligning access with roles is critical to maintaining security and meeting compliance requirements.

Fine-Grained Entitlements Management

Entitlements Management defines what users—and now AI copilots and agents—can access after authentication. It enforces roles, permissions, and resource-level access through a clear, governed process. As AI adoption grows, managing agent access with the same precision as human users is essential. Fine-grained controls ensure everyone and everything gets only the access they need—and nothing more—helping enterprises stay secure, compliant, and in control.

Why it matters

Enterprises increasingly follow the principle of least privilege, granting users only the access they need. Without entitlements management, enforcing this at scale becomes nearly impossible. Manual permissions lead to excessive access, orphaned roles, and audit failures. Enterprises expect SaaS apps to provide entitlement visibility, delegated access reviews, and governance tool integration. Without it, your app becomes harder to manage.

Shared Signals

Shared Signals enable your app to exchange real-time risk events with identity and security platforms, triggering actions like access revocation, step-up authentication, or session termination. As AI agents take on more responsibilities, it's crucial to spot and respond when any user misbehaves. Shared signals deliver the speed and coordination needed to shut down threats—human or AI—before they escalate.

Why it matters

Modern enterprise security depends on continuous risk evaluation—not just one-time authentication. As users change devices, locations, or behavior, risk levels shift. Apps that can share and respond to identity-related risk signals become part of the enterprise's active defense. Without this, your app becomes a security silo, slow to react and hard to trust in a zero trust model.

Shared signals unlock real-time threat response, especially when paired with actions like Session Termination. When a high-risk login or user deprovisioning occurs, your app can immediately revoke access and contain the threat—no manual steps required.

Session Termination

Session Termination lets users, identity providers, or automated systems instantly end active sessions. The moment a threat is detected, you can revoke access and shut down the session, even for an agent acting on behalf of a user. This real-time control keeps your app secure and aligned with zero trust principles.

Why it matters

SSO sessions often remain active long after login. If a session is compromised due to a stolen device, user deactivation, or flagged risk, enterprises need a way to revoke access instantly. Without it, users may retain access even after being removed from the identity provider, creating serious risk and compliance gaps. By connecting

Session Termination with Shared Signals, your app can respond automatically to real-time threats. A high-risk login or account compromise can trigger immediate session termination, enforcing zero trust policies and keeping your app secure.

Identity Automation and Workflows

Workflows let enterprises automate identity tasks, like onboarding, access changes, and deactivation, without manual effort or custom code. With pre-built connectors and templates, they go beyond provisioning to handle complex actions like triggering helpdesk tickets, sending alerts, or enforcing compliance reviews. By supporting workflows, your app integrates seamlessly into enterprise automation across IT, security, and governance.

Why it matters

Enterprise teams increasingly use no-code workflow platforms to manage identity and access at scale. These tools let IT and security teams automate tasks across systems, like provisioning access or reassigning ownership, without code or developer support. If your app can't connect to these flows, it creates friction, delays adoption, and adds risk. By supporting Workflows through a connector, your app becomes easier to manage, more secure, and better aligned with enterprise identity programs.

Risk Monitoring

Risk Monitoring gives enterprises real-time visibility into how human and non-human identities are configured and used. It flags threats, excessive permissions, and policy gaps, like missing MFA or incomplete deprovisioning, before they become incidents. With continuous insight, customers can tighten controls, reduce risk, and stay ahead of attacks.

Why it matters

Identity and access sprawl is one of today's fastest-growing attack surfaces. Over-provisioned roles, incomplete offboarding, and unused credentials expose organizations to phishing, account takeover, and human error. In fact, 82% of breaches involve the human element, including credential misuse and misconfiguration (Verizon Data Breach Investigation Report 2025). Enterprises now treat identity security posture as a core part of their zero trust strategy and expect SaaS vendors to help. If your app can't surface risks or respond to posture changes, it becomes a blind spot in the customer's security ecosystem.

Privileged Access Management

Privileged Access Management (PAM) secures high-risk accounts with elevated permissions, like admins, service accounts, and non-human identities, including local agents. These accounts hold powerful access, and if compromised, can cause serious security and compliance failures. PAM ensures they're tightly controlled, monitored, and used only when necessary.

Why it matters

While most enterprise users authenticate through a central identity provider, many SaaS apps still use local accounts for admin tasks, automation, or system-level access. These accounts often get overlooked during onboarding, offboarding, and audits, making them prime targets for attackers. Security-conscious customers expect more. Your app must not only manage standard access but also secure privileged accounts with oversight, credential protection, and usage tracking.

Get Started

Enterprise identity is evolving—and the opportunity for SaaS builders is now. Build on a strong identity foundation and deliver AI-ready features like app-to-app authorization to stay ahead.

Take Action

Ready to accelerate your path to enterprise success? Here's how Okta helps you **build, scale, and grow** with confidence:

- **Build with Okta**—Join our office hours to get live answers to your integration questions.
- Scale through the **Okta Integration Network**—Reach around 17,000 enterprise customers and accelerate adoption.
- Grow in **partnership with Okta**—Unlock go-to-market support, technical guidance, and new business opportunities.