Strengthening identity security in the age of agentic AI

Okta, in association with Accenture

Accelerate agent adoption (without outpacing security)

In a few short years, AI transformation has, itself, transformed. Across industries, the request-response model of early AI tools has evolved into a sprawling web of autonomous AI agents capable of reasoning, continuous learning, and inference in the independent pursuit of an end goal.

It's an era of vast opportunity — and risk. AI agents manipulate a gargantuan amount of data to run efficiently and effectively. Without the right identity controls and strategic frameworks, this access becomes a liability.

91% of organizations are already using AI agents ...

Okta AI at Work, 2025

77% of executives agree that AI agents will reinvent how their organization builds digital systems

Accenture Tech Vision 2025

But only 10% feel like they have a well-developed strategy for governing them

CSA Report, 2025

Turn sprawl into a foundation

Okta's powerful identity security + Accenture's unmatched strategic insights can give you better visibility into and control over AI agents, at scale.

Build
Empower developers to build AI agents that are secure by design with intuitive tools and built-in protections

Connect
Enable agents to securely connect to systems and applications without granting unlimited standing access

Manage
Establish full lifecycle management for agents: visibility, access control, governance, and remediation

Detect
Minimize the attack surface with real-time detection and remediation of AI identity configuration risk

Build trust into AI's DNA

To stay secure and competitive, companies need to establish comprehensive AI governance frameworks that encompass fairness, accountability, risk management, security, and data integrity. Accenture can help develop and deploy these frameworks, beginning with modern identity built for the AI era.

Without the right identity controls, agents create and exacerbate risk

New vulnerabilities: Prompt injections and other AI-specific attacks can put sensitive access tokens in the hands of bad actors

Shorter lifespans: Agents have ephemeral and dynamic lifecycles, which makes traditional provisioning and de-provisioning frameworks obsolete

Lack of accountability: Agents often lack traceable ownership and consistent logging, making it difficult to understand or justify their actions

Compliance challenges: Without consistent, documented approvals of AI agent behavior, compliance with standards like GDPR, SOX, and DORA is at risk

Low visibility: Neglecting over-privileged agents and long-lived credentials heightens the risk of data exposure

Okta unites agents within a trusted, comprehensive identity security fabric

- Standards-first, policy-driven security protocols at the identity layer: OAuth/OIDC, JWT, mTLS
- Clear audit trails that resolve explainability and accountability blind spots
- Centralized logging, governance, and policy controls that simplify compliance, strengthen incident response, and can help mitigate impact in the event of an attempted breach
- Unified governance across human and non-human identities: visibility, least privilege, zero standing privileges, auditability

Tailored rollouts, built for your next step

Securing AI agents is complex but essential. Accenture can help you get it right — the first time.

1. Co-Create

2. Pilot

3. Scale

okta | accenture

Govern non-human identities through one pane of glass

Okta extends identity security principles to all kinds of AI agents, whether third-party or homegrown, so you can scale confidently and responsibly. Unlike point solutions, which only address a fraction of the issues unique to AI agents, Okta establishes a secure, standards-first identity security foundation that enterprises can use to manage agents throughout their lifecycle.

Auth0 for AI Agents

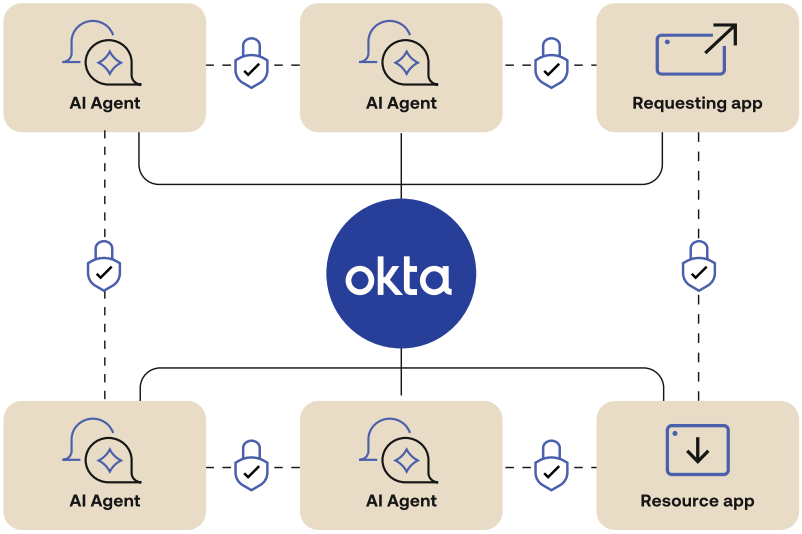
- Equip AI agents with secure login experiences on behalf of their users
- Use secure standards to retrieve, store, and automatically refresh API tokens
- Enable autonomous agent work while maintaining user control: Agents will prompt users for approval for critical actions
- Enable granular permissions to help ensure agents only access authorized content

Lifecycle management

- Centralize AI lifecycle management, from visibility and access control to governance and remediation
- Detect and remediate AI identity configuration risk to minimize attack surface
- Vault and protect credentials for human-in-the-loop interactions

Cross App Access (XAA) for AI agents

XAA is an open protocol that allows Auth0 apps to securely expose APIs and enable secure agent or app connections through centralized identity controls. XAA lets your enterprise customers govern access with greater control and visibility, while their end users benefit from a smoother experience without repetitive consent prompts.



Ready to accelerate and secure your innovations?

Learn more at Okta.com

Resources:

POV: okta.com/resources/whitepaper-accenture-securing-ai-agents