okta

How identity sprawl hides threats (and how to fix it)

With a modern, identity-first security strategy

Your organization is growing and changing. Your risk profile is too.

To drive agility and remote collaboration, competitive organizations like yours now depend on an ecosystem of best-in-breed solutions. These carefully constructed tech stacks deliver better results across the organization, customers and business partners. They can also put you at risk.

The rise of AI agents and agentic systems is adding fuel to the fire. While these agents open new doors for efficiency and service delivery, they also expand the attack surface and create a group of new risks that require new security approaches.

Fragmented IT environments that leave human and non-human identities scattered across different systems and infrastructure result in poor visibility into your organization's security posture and elevated risk of a costly breach.

Turn identity sprawl into actionable insights by gaining real-time, end-to-end visibility into all identity threats and strengthening your ability to remediate them in real time. Protecting your organization's sensitive information and positioning yourself for an AI-enabled future begins with visibility.

You didn't interview your AI agents. They're working for you anyway.

When it comes to AI agents, many organizations are dealing with the wild west. Agents are being created and deployed at a pace that IT and security teams simply can't keep up with. As a result, many organizations don't have any way of knowing which agents are active, what they can access, or how they behave. From a security standpoint, the AI agent revolution has created a growing number of blind spots.

AI adoption is outpacing security and governance

91% of organizations are already using AI agents*

But only **44%** of those organizations have a governance strategy in place**

*Okta AI at Work 2025: Securing the AI-powered workforce

**The Times, 2025

Unified identity security drives better visibility into both human and non-human identities

Fragmented technology and security stacks generate a mountain of data on risks and potential threats. But this setup leaves your team sifting through logs and piecing together an understanding of what really demands attention — making real-time remediation all but impossible.

In other words, identity fragmentation makes it impossible to identify where your organization's biggest vulnerabilities lie. It slows down threat detection and response, giving bad actors ample opportunity to inflict major damage using stolen credentials. To make matters worse, poorly secured AI agents run the risk of inadvertently exposing or sharing sensitive information. Without full visibility into what agents can access and how those access privileges are set up, organizations are left with ungovernable risk in a threat landscape that is becoming more sophisticated every day.

To manage this risk effectively, identity systems and processes must be unified on a single, AI-ready platform for better efficiency and control. Modern identity platforms make this unified approach to security possible. By extending this unified approach beyond employees to customers and business partners, organizations can eliminate silos between workforce and consumer data, ensuring a seamless, secure login experience that builds brand trust.

Enabling critical outcomes with Okta

The Okta Platform enables a robust and vastly simplified approach to identity-first security. Through a diverse suite of products and features, Okta provides end-to-end, real-time protection from sophisticated threats without burdening your workflows or customer experiences with excessive friction.

How to achieve full visibility into all identity threats

(And enable real-time remediation)

Effective risk remediation starts with a centralized view of your risk profile that synthesizes security signals into real-time, actionable insights. For customer identity management, this protects sensitive data by enabling rapid detection and response to account takeovers, fraud, and compromised credentials.

Furthermore, remediating risk cannot rely on slow, manual actions. Your identity solution must tie real-time insights into automated remediation workflows that can be tailored to suit the specific needs of your organization — including its accelerating adoption of AI agents, if applicable.

Unifying identity security makes this possible. By integrating phishing-resistant measures with a modern, identity-first risk engine, you gain real-time visibility into emerging threats. Whether safeguarding your workforce, customers, or business partners, this level of protection is essential in today's threat landscape — and only a unified identity approach can deliver it.

Leverage full visibility across core use cases:

- Secure workforce onboarding
- Ongoing protection across user groups
- Secure hybrid and on-prem environments

Secure workforce onboarding

Legacy approaches to identity often burden IT teams with manual onboarding and offboarding processes that are time-consuming and prone to human error.

Modern, unified identity platforms make it easy for new users — whether employees, contractors, partners, or other external identities — to get secure, frictionless access to the tools they need without delays or security gaps.

Automate secure provisioning and deprovisioning to save IT teams' time

Equip workers with MFA that helps ensure secure identity verification during onboarding

Manage access to every app and system for every employee through a centralized dashboard

Simplify onboarding without compromising on security:

HEALTHCARE: Provision traveling nurses and other contingent workers without delays or risk of excessive privileges

RETAIL: Simplify the onboarding of seasonal workers and other high-turnover positions to flesh out your staff quickly and securely

EDUCATION: Equip new students, faculty members, and staff with secure, role-based access from day one

GOVERNMENT: Drive mission continuity by securely onboarding contractors, inter-agency partners, and temporary staff with attribute-based, policy-driven access controls

Enforce ongoing protection across user groups

When identity is fragmented across the organization, a lack of centralized visibility makes detecting and responding to potential threats in real time essentially impossible.

With Okta, organizations can detect, respond to, and mitigate identity threats across all managed user groups — including employees, customers, and business partners as well as both human and non-human — through strong, risk-based authentication policies and intelligent threat response tools.

Unify identity systems while securely separating users into distinct populations

Isolate and remediate compromised accounts or devices in real time

Securely manage AI agents and revoke their access in real time in the event of risky behavior

Ensure consistent protections for humans and non-humans alike:

HEALTHCARE: Easily assign and enforce group-based access controls across key user groups and remediate potential breaches in real time

RETAIL: Securely deploy AI shopping assistants without the risk of putting customer privacy (or sensitive information) at risk

GOVERNMENT: Manage privacy and security risks when deploying AI agents widely for operational efficiency and service delivery

Secure hybrid and on-premise environments

Complicated hybrid environments demand an approach to IAM that simplifies the distributed management of identities and security policies while also extending modern identity security to on-prem identities and resources.

Extend risk-based authentication policies from the cloud to on-prem apps and infrastructure for adaptive security everywhere

Unify access control and enforce zero standing privilege across distributed environments

Detect, respond to, and mitigate identity threats across all managed devices

Simplify and strengthen identity security:

HEALTHCARE: Protect PHI while making critical information and resources available to healthcare professionals anywhere through cloud-based IAM

RETAIL: Extend modern, cloud-based identity security principles to highly specialized on-prem systems to strengthen on-site security

GOVERNMENT: Unify identity security, from cloud-native to edge use cases, to safeguard critical workloads and secure every mission, everywhere

Okta makes it possible

By unifying identity, Okta enables new levels of visibility into signals and policies across your IT, security, and customer environments, arming your teams with powerful, real-time threat detection and response capabilities.

Okta brings the identity security fabric to life by delivering end-to-end, orchestrated identity security before, during, and after authentication for every identity—human, non-human, and AI agents—across all environments.

Identity Security Posture Management

Continuously discover and remediate identity risks and misconfigurations.

Explore Identity Security Posture Management

Identity Governance

Enforce least privilege by automating user access reviews and provisioning.

Explore Identity Governance

Okta Privileged Access

Unify governance and access control for all of your critical infrastructure.

Explore Okta Privileged Access

Device Access

Extend highly secure, passwordless Okta authentication to desktops and devices—from first login.

Explore Device Access

Identity Threat Protection

Use Okta AI to automatically detect and respond to identity-based threats in real time.

Explore Identity Threat Protection

Ready to learn more?

In a risk landscape defined by increasingly sophisticated threats, the surest approach to a resilient and secure organizational future is a unified, identity-first approach to security.

Strengthening your security posture requires turning identity sprawl into actionable insights to close security gaps and preempt risk.

See the platform in action:

Watch the demo

Visit website