

Highlights Across The Okta Platform

Identity is the number one attack vector¹, and we're dedicated to delivering comprehensive security for all identities — human and non-human — with solutions that are seamlessly interconnected and fully integrated across your business.

The screenshot displays the 'Non human identities dashboard' with several key components:

- Types & segments:** Non human Identities (77K), Service accounts (77K), Access Keys (77K), API Tokens (77K), AWS roles (77K), Resource (77K).
- Top risks:** Three donut charts showing risk levels: Super Admins (20%), Admins (17%), and Service accounts (42%).
- Prioritized issue list:** A list of security issues such as 'Unused Global Admin Service Account' (3), 'Unrotated Active Access Keys - Admin' (12), 'Old Password, No MFA, Unused Service Accounts' (21), 'Unused access keys' (12), and 'Unrotated active access keys - Account' (11).
- Service accounts with issues per source:** A horizontal bar chart showing issue counts for sources like 'Yourco Workspace' (50%), 'Google Workspace', 'yourco-okta.com', 'Yourco-PROD', 'AWS Organization', and 'yourco.my.salesforce.com'.
- Keys rotation and utilization:** A donut chart showing 20% unrotated keys, with a breakdown of 6% unrotated & unused, 42% rotated & unused, and 38% rotated and used.

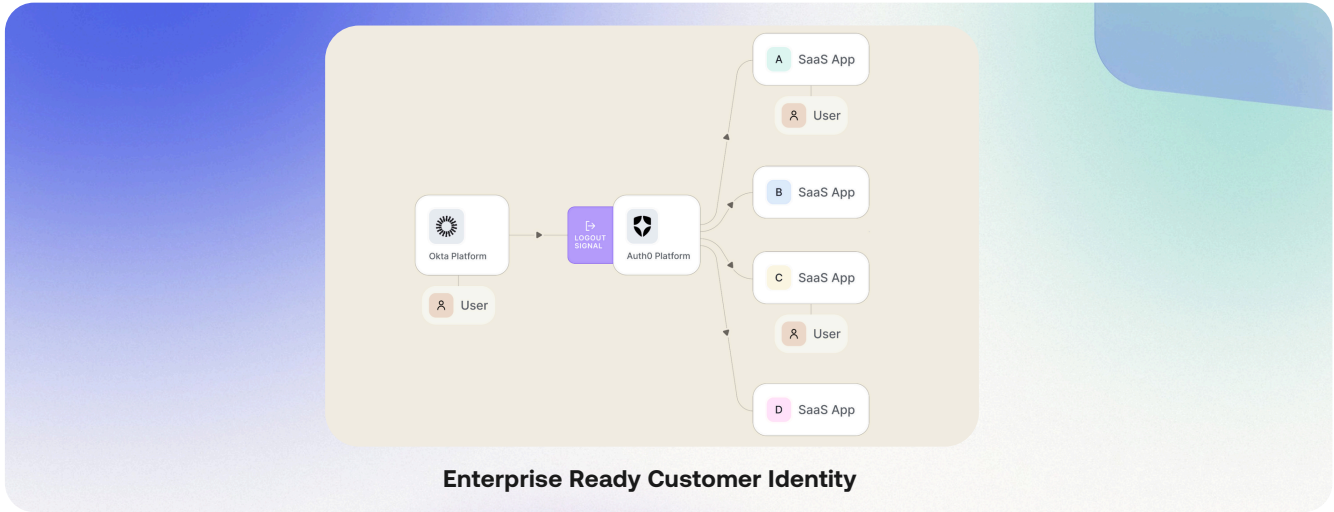
Protecting Non-Human Identities (ISPM)

Announcement	Description	Importance
<p>Secure Identity Integrations</p> <p>New pre-built integrations</p> <p>Generally Available</p> <p>Region Availability: Global</p>	<p>Okta Secure Identity Integrations (SII) provide powerful protection for top enterprise SaaS apps like Google Workspace, Microsoft 365, and Salesforce. Customers can quickly configure deep integrations within the OIN that go beyond SSO and MFA with out-of-the-box capabilities to simplify access, achieve compliance goals, and enable rapid response to security threats with built-in remediation.</p> <p>View our 150-plus Secure Identity Integrations</p>	<ul style="list-style-type: none"> • Extends security beyond basic SSO and provisioning for critical SaaS applications. • Reduces vendor lock-in, allowing customers to securely use best-of-breed apps. • Simplifies deployment and reduces operational burden with pre-built, out-of-the-box integrations. • Enhances security posture via features like Entitlements Management, Universal Logout, Workflows, and Posture Management integrations.
<p>Advanced Posture Checks</p> <p>New feature of Adaptive MFA</p> <p>Early Access</p> <p>Region Availability: Global</p>	<p>Advanced Posture Checks empower you to collect and assess device context—on any Windows or macOS device attribute or security setting—to further strengthen Zero Trust security during authentication.</p> <p>This feature seamlessly connects with your technology ecosystem to gather signals that inform access policies and continuous risk assessment.</p>	<ul style="list-style-type: none"> • Strengthens Zero Trust security by incorporating detailed device context into access decisions. • Allows granular assessment of device posture using any Windows or macOS attribute via OSquery. • Enables customizable compliance rules within Okta's policy framework. • Improves user experience with guidance for self-remediation if a device fails checks.
<p>Protecting Non-Human Identities</p> <p>New solution bundle</p> <p>Generally Available</p> <p>Region Availability: Okta Privileged Access is GA globally; Identity Security Posture Management is GA in North America</p>	<p>Non-human identities (NHIs) — including service accounts, shared accounts, break-glass identities, and AI agents — often operate outside traditional Identity governance frameworks, leaving organizations vulnerable to security risks.</p> <p>Okta provides a comprehensive, end-to-end solution for securing human identities and NHIs by unifying visibility, remediation, and vaulting in a single system.</p> <p>Eliminate standing privileges for privileged accounts by combining Okta Privileged Access with Identity Security Posture Management. This integrated approach secures non-federated privileged identities (service accounts, shared accounts, break-glass, AI Agent identities) while continuously monitoring Non-Human Identity risks and vulnerabilities across your critical enterprise ecosystem.</p> <p>Learn more about Okta's future vision for NHIs.</p>	<ul style="list-style-type: none"> • By adopting a unified identity strategy, customers can centralize, manage, and execute a principle of least privilege approach across both human and non-human identities, including AI Agent identities that interact with enterprise applications. • Provides unified visibility and control over human and non-human identities. • Enables discovery, vaulting, management, and governance of privileged/shared/service accounts. • Continuously monitors NHI risks (e.g., unrotated credentials, excessive privileges) via ISPM. • Reduces attack surface and enforces least privilege for NHIs, including AI Agents.

Announcement	Description	Importance
<p>On-Prem Connector</p> <p>New feature of Okta Identity Governance</p> <p>Early Access</p> <p>Region Availability: Global</p>	<p>Okta On-prem Connector is a new out-of-the-box connector allowing customers to integrate their on-premises apps with Okta Identity Governance, enabling discovery, visibility, and management of fine-grained application entitlements within Okta.</p>	<ul style="list-style-type: none"> • Extends modern Okta Identity Governance (OIG) to legacy on-premises apps (starting with SAP). • Eliminates manual, error-prone governance processes for on-prem apps. • Provides unified visibility and consistent policy enforcement across cloud and on-prem. • Automates provisioning, deprovisioning, entitlement management, and access reviews for connected on-prem systems. • Helps meet compliance requirements with audit-ready reporting for hybrid environments.
<p>Separation of Duties</p> <p>New feature of Okta Identity Governance</p> <p>Generally Available: April 2025</p> <p>Region Availability: Global</p>	<p>Separation of Duties (SOD) in Okta Identity Governance (OIG) ensures users do not accumulate conflicting access permissions that could introduce security risks or compliance violations. It enforces SOD policies based on pre-defined business rules to prevent fraud, maintain compliance, and reduce insider threats.</p>	<ul style="list-style-type: none"> • Proactively prevents users from accumulating conflicting ("toxic") access permissions. • Enforces SOD policies automatically at time of request or during certifications, preventing violations before they occur. • Reduces IT bottlenecks via an app-centric model allowing app owners to manage rules. • Helps meet regulatory compliance requirements (e.g., SOX) by systematically preventing risky access combinations. • Improves governance efficiency compared to manual checks or reactive detection.
<p>Okta Identity Governance for US Public Sector</p> <p>Audit-Ready for Okta for U.S. Military (Q2 2025) and for Okta for Government High (Q3 2025)</p>	<p>A US federally compliant Identity governance access solution that unlocks end-to-end security for mission owners to make informed access decisions. The unified Identity platform automates policy enforcement across the government's tech stack with minimal friction.</p>	<ul style="list-style-type: none"> • Provides a federally compliant version of Okta Identity Governance for US Public Sector (Military, Gov High). • Helps public sector organizations meet stringent compliance requirements for IGA. • Reduces implementation time and costs associated with customizing non-compliant solutions. • Increases adoption of modern IGA practices within government agencies. • Empowers mission owners with tools for informed access decisions and automated policy enforcement.

Highlights Across The Auth0 Platform

Leading businesses recognize that Customer Identity is key to delivering seamless experiences and driving revenue growth. They take a developer-first approach to Customer Identity, helping to ensure security at every stage of the customer journey without adding friction. With Auth0, developers can easily enable features, extend capabilities, and integrate Identity using no-code, low-code, and pro-code options. This flexibility empowers them to orchestrate Identity, meet evolving security demands, and scale with confidence.



Announcement	Description	Importance
<p>Auth0 Platform: Innovations for Secure Experiences</p> <p>Platform enhancements</p> <p>Availability: Multiple launches included</p> <p>Regional Availability: Global</p>	<p>Auth0 is the secure Identity platform powering seamless, trusted customer experiences before, at, and after login. Recent innovations include Tenant Access Control, Advanced Customization for Universal Login, FAPI 2 Certification GA, CIBA GA, and Native to Web SSO.</p> <p>Secure experiences help ensure security at every stage of the customer journey while maintaining trust and convenience to protect customers before, during, and after login — without adding unnecessary friction.</p> <p>Businesses must adapt to evolving customer expectations to stay competitive. Our latest Auth0 innovations simplify authentication while ensuring security and compliance at every stage — before, during, and after login.</p> <p>Before login:</p> <ul style="list-style-type: none"> Tenant Access Control (Available March 2025) strengthens security by managing access at the tenant level, ensuring only authorized users can initiate authentication <p>During login:</p> <ul style="list-style-type: none"> Advanced Customization for Universal Login (Available March 2025) delivers a personalized, on-brand authentication experience with deeper customization options for Universal Login. <p>After login:</p> <ul style="list-style-type: none"> Client-Initiated Backchannel Authentication (Available March 2025) is now available in enterprise, enabling secure, user-initiated authentication flows for decoupled client interactions. Native to Web SSO (Available March 2025) simplifies authentication by extending session continuity between native and web apps, reducing friction for users. FAPI 2 Certification (Expected Q2 2025) ensures strong security and compliance with the latest Financial-grade API (FAPI) 2.0 standards, as part of the Highly Regulated Identity add-on. 	<ul style="list-style-type: none"> Addresses rising customer expectations for seamless, secure, and personalized digital experiences. Enhances security and UX before (Tenant Access Control), during (ACUL), and after login (FAPI 2, CIBA, Native-to-Web SSO). Provides tools for regulated industries needing financial-grade security (FAPI 2, CIBA). Offers flexibility for deep customization (ACUL) and improved cross-channel continuity (Native-to-Web SSO, CIBA). Simplifies identity management, allowing focus on innovation.

Announcement	Description	Importance
<p>Enterprise Ready Customer Identity</p> <p>New capabilities</p> <p>Availability: Multiple launches included</p> <p>Integration with Okta Universal Logout: GA: Jan 31, 2025 SS-SSO: GA Nov 28, 2024 SS- SCIM: EA Q2 2025 SS-Domain Verification: EA Mar 31, 2025 Multiple custom domains per tenant: EA Q2 2025</p> <p>Regional Availability: Global</p>	<p>Auth0 provides enterprise-grade Customer Identity solutions that streamline authentication, authorization, and security — delivering the efficiency, cost savings, and flexibility enterprises need to win big deals.</p> <p>Key capabilities include integration with Okta Universal Logout and self-service features, including Single Sign-On, SCIM, and Domain Verification. Additionally, organizations can now also support multiple custom domains within a single Auth0 tenant, streamlining authentication and management flows.</p>	<ul style="list-style-type: none"> • Helps B2B SaaS vendors meet complex identity requirements of large enterprise customers (IdP federation, SCIM, etc.). • Enables vendors to move upmarket without diverting significant engineering resources. • Provides capabilities like Organizations, FGA, and self-service features (SSO, SCIM) to streamline onboarding/management. • Enhances security via integrations like Okta Universal Logout (ULO). • Improves developer efficiency and accelerates time-to-value for enterprise-grade identity.
<p>Auth for GenAI</p> <p>New solution bundle</p> <p>Developer Preview available now</p> <p>Regional Availability: Global</p>	<p>Many organizations are building AI agents, but securing them remains uncharted territory. Auth for GenAI presents four key Identity challenges: user authentication, API access, asynchronous workflows, and authorization for Retrieval Augmented Generation. Auth for GenAI secures AI agents at every step without slowing them down, providing developers with the trusted tools and flexibility they need.</p>	<ul style="list-style-type: none"> • Addresses unique security challenges of authenticating/authorizing GenAI agents. • Provides purpose-built tools for AI agents to securely authenticate users, call APIs, and access data per permissions (e.g., for RAG). • Reduces security risks associated with granting AI agents access without proper controls. • Enables developers to build secure GenAI apps faster with ready-made solutions. • Helps businesses innovate with AI confidently, knowing security is handled.

All dates are calendar year unless otherwise indicated.

Disclaimer: Any products, features, functionalities, certifications, authorizations, or attestations referenced in this material that are not currently generally available or have not yet been obtained or are not currently maintained may not be delivered or obtained on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature, functionality, certification or attestation and you should not rely on them to make your purchase decisions.

¹[Verizon.com, 2024](https://www.verizon.com/2024)

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 why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.