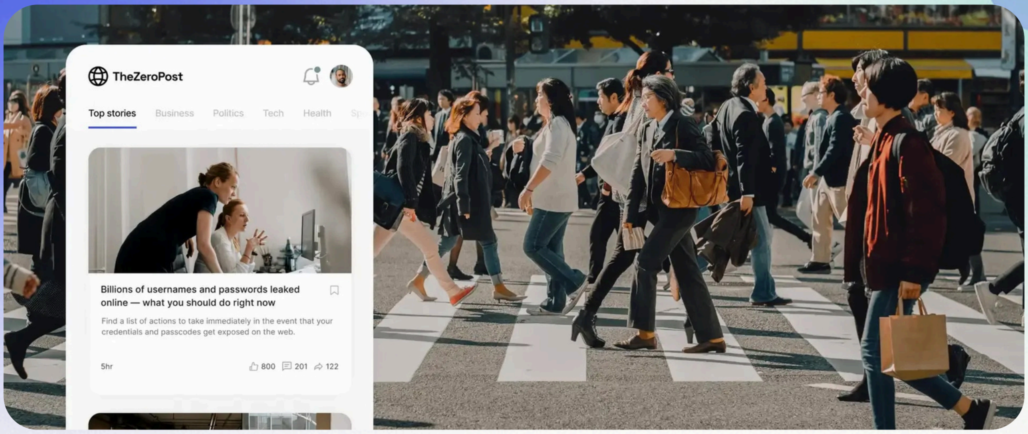
Highlights Across Okta – Workforce Identity Cloud and Customer Identity Cloud


TheZeroPost
Top stories
Business
Politics
Tech
Health
Billions of usernames and passwords leaked online — what you should do right now
Find a list of actions to take immediately in the event that your credentials and passcodes get exposed on the web.
5hr
800
201
122

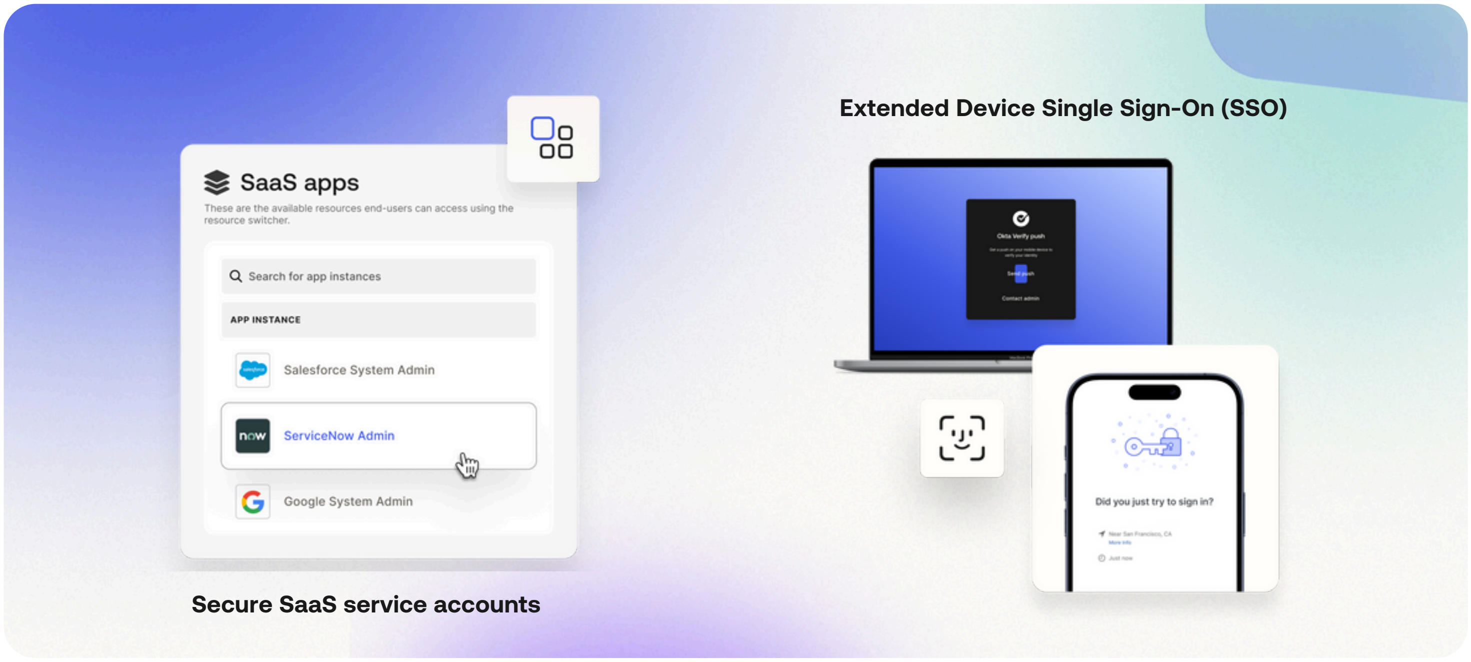
Secure Identity Assessment

Announcement	Description	Importance
Interoperability Profile for Secure Identity in the Enterprise (IPSIE) Announcement	Okta led the formation of an OpenID Foundation working group with Ping Identity, Microsoft, SGNL, and Beyond Identity as the first step toward establishing a new Identity security standard. The Interoperability Profile for Secure Identity in the Enterprise (IPSIE) is an open industry standard that will enhance the end-to-end security of enterprise SaaS products and provide a framework for SaaS builders to more easily meet evolving enterprise security needs. • It will encompass key aspects of identity security, including centralized authentication (SSO), automated user lifecycle management, privileged access control, security information sharing, and rapid session termination in response to threats, leveraging protocols like OIDC, SCIM, and CAEP/SSF to enable these capabilities across enterprise applications. • Okta led the formation of a working group within the OpenID Foundation to create this first ever unified Identity security standard for enterprise apps, resources, and workloads The IPSIE standard will bring together a set of existing and new standards, covering a wide range of proposed use cases, including: • **Single Sign-On** to centralize login, policies and enforcement (OIDC) • **Lifecycle Management** to secure user on/offboarding and prevent security risks like orphaned accounts and shadow directories, avoiding unauthorized access (SCIM) • **Entitlements** (Governance/Privileged Access) to enforce least privilege access and move toward zero standing privileges (SCIM) • **Risk Signal Sharing** to get seamless security insights and share them across the entire security ecosystem (CAEP/SSF) • **Session Termination** to immediately terminate all user sessions in response to detected threats • **Token Revocation** to disable access across apps and services The IPSIE standard will provide the framework for any enterprise apps to be discoverable, governable, and support SSO, SCIM, and continuous authentication through a variety of use cases.	• In February 2024 Okta announced the Secure Identity Commitment – our long-term pledge to lead the industry in the fight against Identity attacks. One way we aim to achieve this is by helping to standardize Identity security across the Industry so we can foster an open ecosystem where it is seamless and efficient to build and use enterprise apps that are secure by default. • Enterprises face fragmented identity security implementations, making it difficult to ensure consistent security and efficient integration across various SaaS applications. This fragmentation leads to increased vulnerability, complex management, and potential gaps in security coverage. • By standardizing Identity security, organizations can maintain a uniform level of protection across all their SaaS tools, reducing weak points and simplifying security management. • With clear guidelines, SaaS developers can more easily implement robust security features, while users benefit from a more secure and user-friendly experience across different applications. • Organizations can select the best-fit SaaS solutions without compromising on security, as the standard helps ensure compatibility and consistent security practices across different identity providers. • A standardized approach makes it easier for organizations to meet regulatory requirements and streamlines the process of integrating new SaaS tools into existing security frameworks.

Announcement	Description	Importance
Secure Identity Assessment New services offering Available now	Secure Identity Assessment (SIA) is Okta's end-to-end approach to help reduce customers' technical debt. In helping track security maturity progress, providing expert guidance for security best practices, and identifying vulnerabilities like admin sprawl, SIA helps close security gaps and build a stronger security foundation. SIA empowers organizations to proactively assess and address these vulnerabilities, and offers a clear remediation path to support regulatory compliance and an enhanced overall security posture. Continuous risk evaluation: • **Comprehensive Identity Evaluation:** Quickly pinpoint any identity misconfigurations, orphaned accounts, and permission anomalies. • **Tailored Remediation Plans:** Provides specific, actionable insights based on organizational needs, ensuring a customized path to resolve security debt. • **Multi-Tiered Approach:** Customizable assessments for large enterprises, mid-sized organizations, and partner-led or self-paced options.	Organizations often face tough decisions when prioritizing security resources. Companies will often stretch the value of existing systems instead of modernizing them. This creates technical debt in security, particularly identity debt: orphaned accounts, shadow IT, ghost accounts, and misconfigured identities. These issues cause vulnerabilities, making identity management more difficult over time. SIA will help customers remain secure-by-default, with end-to-end expert support during the following phases: • **Diagnose:** Okta helps customers track progress on their security maturity with tools like the IMM or security checklist to establish a roadmap to stay secure. • **Tailor:** Customers receive expert advice with Okta Expert Assist, helping get set up, achieve certifications to implement Okta, and work towards best practices on an ongoing basis. • **Fix:** Okta can pinpoint security gaps (e.g. orphaned accounts, shadow IT, admin sprawl) and customers can address immediate risks and work towards ongoing adherence.
Secure Identity Integrations New pre-built integrations Generally Available now	To enable customers to adhere to modern standards, Okta is launching 125+ new SaaS application integrations that bring advanced security and automation to some of the biggest SaaS applications. Customers can enhance their security and reduce operational burden by quickly integrating with apps that adhere to a common Identity security standard – from single sign-on and lifecycle management, to Identity automation, security posture visibility, and remediation. 125 + integrations are available now on the Okta Integration Network, and many more will be available by March 2025.	Modern enterprises with complex heterogeneous stacks need end-to-end Identity security standards that include deeper security posture visibility with real-time identity threat assessment and automated remediation and they need standardized integrations that are out-of-the-box and do not require resources for regular support. Value: • **Enhance security posture** - Integrate with SaaS apps that offer deep granularity and/or adhere to major industry standards • **Increased flexibility with a platform agnostic solution** - Customers get the same rich feature set as platforms, but get to quickly and securely integrate their apps of choice • **Reduce operational burden with standards based integrations** - Customers can quickly embed security capabilities with standards-based integrations from the Okta Integration Network

Additional Announcements for Workforce Identity Cloud

Powers identity for all employee, contractor, and business partner use cases



Extended Device Single Sign-On (SSO)

Secure SaaS service accounts

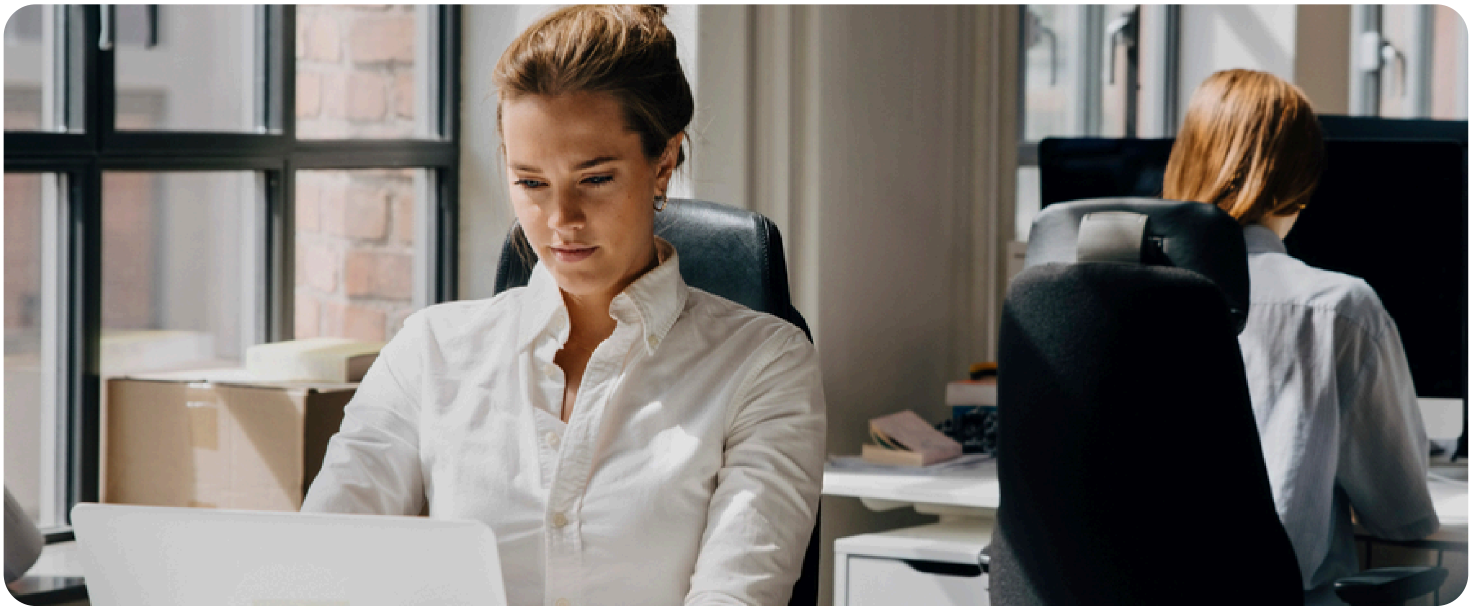
Announcement	Description	Importance
Secure SaaS service accounts New feature of Okta Privileged Access Early Access available in Q4 2024	• Secure access to non-federated service accounts for top enterprise applications. • Eliminate standing privileges for SaaS service accounts across your organization. Use Okta Privileged Access to discover and secure access to non-federated privileged SaaS accounts (e.g., service accounts, shared accounts, break-glass accounts) for top enterprise applications. Key Capabilities: • Achieve zero standing privileges for service, shared, and break-glass SaaS accounts. • Enforce individual accountability to shared accounts. • Configure flexible policy options, such as time-bound approvals tied to specific accounts.	• Enterprises today use hundreds of SaaS applications and every application has service accounts that are not federated. These shared/service/privileged accounts for applications are a rapidly growing and often an under-managed risk vector for organizations, presenting a massive security and visibility problem. • Leveraging Okta's extensive integration network, customers will be able to discover, manage, and govern shared/service/privileged accounts across their enterprise applications for stronger security. This speeds implementation while also centralizing and extending visibility into more resources. • Similarly, Okta's unified approach enables admins to centrally manage policies for these privileged accounts alongside applications and entitlements, eliminating silos and standardizing secure-by-design authentication and enforcement, including use of high assurance, phishing-resistant factors and transactional MFA.
Governance Analyzer with Okta AI New feature of Okta Identity Governance Early Access available in 2025	• Governance Analyzer with Okta AI analyzes the vast amount of user and resource insights Okta has specific to an organization to deliver risk scores and recommendations that drive better decision-making and lower risk–all within the same experience and interface end users and identity teams are already using. • Unleash higher-quality governance decisions by leveraging risk insights across Okta's unified platform. Insights include usage data, previous governance decisions, and the relationships between a given user and a resource. • Intelligently predicts access risk while also equipping approvers with key insights, such as past risk events associated with the user.	Drive better governance outcomes by empowering decision makers with the necessary context to make an informed decision, leveraging signals from across Okta's unified identity platform.

Announcement	Description	Importance
Advanced Posture Checks New feature of Adaptive Multi-factor Authentication (AMFA) Early Access available in Q1 2025	With Advanced Posture Checks, you have a robust device compliance solution that allows you to collect any device posture signal via OSquery– from any Windows or macOS device, managed or unmanaged – and customize sets of rules and conditions within Okta's application policy framework. This enables you to tailor compliance checks to meet your unique security needs and centrally reinforce MDM policies across the organization to support MDM compliance for all devices before allowing access to downstream resources.	• Organizations must maintain a strong security posture across workforce devices, including personal, unmanaged machines and external devices from business partners, contractors, and others. Non-compliant devices with access to organizational data and resources are targets for bad actors trying to gain access. • However, businesses that support BYOD are limited in their ability to enforce MDM compliance, and even fully managed devices are prone to MDM configuration drift due to delays in policy enforcement and stale views of device compliance states. To add to the complexity, ensuring compliance across an enterprise with multiple departments with their own MDM solution is next to impossible. These challenges, if not resolved quickly, result in elevated security risk for the entire organization. • Okta is delivering extensible posture management to help organizations address security gaps and secure access more efficiently.
Extended Device Single Sign-On (SSO) New feature of Okta Device Access Early Access available in Q1 2025	With Extended Device Single Sign-On, SSO starts when you're first verified at device login, which means you can leverage a successfully completed desktop MFA challenge to gain access to downstream resources that require the same level of security assurance. Not only does this decrease how often you are asked to authenticate, but it initiates a session that is cryptographically bound to a secure hardware-backed key on the device, which helps make user context-based exploits much less possible. Access is tied not only to the user but also to their device, so if a bad actor is able to steal an active session, they won't be able to leverage it from a different device. Extended Device SSO can mitigate the risk of phishing attacks along all access touchpoints and strengthen your organization's security posture.	• Each new device or application adds to a business's ever-expanding attack surface. With employees accessing resources from personal, unmanaged or corporate-issued devices – from more locations than before – many organizations are simply overwhelmed by how to manage the evolving challenge of securing access. One thing is clear though, traditional MFA is no longer enough. • At the same time, organizations need their employees to have a simple yet secure experience when working on corporate devices in order to sustain a productive workforce. This means reducing the number of authentication prompts to minimize friction while maintaining the highest security standards.
Out-of-the-box integrations for Identity Verification New feature of Adaptive Multi-Factor Authentication Early Access available now with Persona integration	Out-of-the-box integrations with third-party identity verification providers allows admins to trigger ID verification flows via Okta's authentication policies to verify that the user on the other side is who they say they are. • Enable Identity verification throughout the employee lifecycle using out-of-the-box integrations with third-party Identity verification providers. • Enforce Identity verification for sensitive actions using Okta's robust authentication policy framework. • Redirect users to a third-party vendor for identity verification – no custom configuration required. • Mitigate social engineering attacks with real-time document verification and liveness detection. Identity Verification with Persona: • Use an Identity Verification vendor such as Persona as an Identity Provider (IdP) within Okta. Performing an identity verification request allows you to confirm a user's identity. It verifies their government-issued identity document and asks them to take a selfie to satisfy a liveness check. • Integration with Persona is available in Early Access now, and will be expanding to other leading identity verification providers soon.	• The rise of social engineering and deep fake attacks allows malicious actors to bypass traditional security measures, posing serious risks to organizations. A stronger approach to identity validation is crucial to safeguarding against these evolving threats. • Identity Verification adds an extra layer of phishing resistance in your org. It allows you to ensure that the right user is onboarding or resetting their account.

Announcement	Description	Importance
Bring your own Identity verification provider New product enhancement Early Access available in 2025	Seamlessly integrate the Identity verification provider of your choice with Okta to protect against advanced threats – no custom configuration required.	• Okta provides customers with the choice and flexibility to leverage identity verification technologies to further reduce the risk of identity attacks. • In addition to a robust risk engine and phishing-resistant authenticators, Okta's integration with customers' identity provider of their choice allows organizations to enforce a multi-layered security approach, ensuring enhanced protection and trust throughout every stage of the employee lifecycle.
Enhanced Disaster Recovery with Self-Service Failover New feature of Enhanced Disaster Recovery, included as part of the Enhanced Disaster Recovery SKU Early Access in Q1 2025	• Enhanced Disaster Recovery allows for customer based failover (at the individual org level) as well as reduced Recovery Time for read-only access, to a guaranteed 5 minutes in the event of a regional outage with Okta's cloud providers. • Now with self-service failover for enhanced disaster recovery, customers can initiate and test failover on demand to a secondary site for read-only access in under 5 minutes, strengthening overall business continuity.	• Enhanced Disaster Recovery delivers enterprise-grade resilience and reliability in the event of a regional infrastructure-related outage. • Empowers customers to initiate and test failover on demand to a secondary site for read-only access in under 5 minutes, strengthening overall business continuity.
Workflows is Post-Audit for FedRAMP High Authorization expected in Q4 Available to FedRAMP High and eligible FedRAMP Moderate customers	Workflows is a low- and no-code Identity automation and orchestration platform for US Public Sector organizations to automate Identity processes at scale, maintain compliance standards, and improve experience management. Workflows help customers cut costs and speed up development time by replacing custom code and scripts with Identity automation. With simple "if this, then that" logic, templates, pre-built connectors, and the connector builder, almost any identity process can be automated.	US Public Sector organizations are racing against time to create better end-user experiences and replace outdated technology and practices. This transformation requires collaboration across all personnel and impacts a broad range of agency missions. While legislative and industry pressures play a role, many modern tools for efficiency are still lacking in government services. Catching up to core efficiency and productivity standards — including the adoption of tools that allow secure and easy access to essential resources — sets an agency apart. Okta's modern, Identity-centric automation tools offer Federal teams low- and no-code options for building and managing complex functions, maintaining compliance standards, and improving experience management. • **Centralized Identity-Led Experiences:** Okta centralizes workstreams around the user, helping agencies to develop personalized and protected experiences for everyone, be they a public servant, contractor, member of the public, or partner of an extended ecosystem – all within one centralized platform. • **Deep, Flexible Partnerships:** Okta Workflows has ready-to-integrate connectors and the ability to connect to any API, making Okta the leading partner in consolidating everything connected to your agency. • **Automation at Scale:** Agencies must develop their tech stack with and for their users to ensure it solves actual problems at scale. Okta's Identity automation boosts agencies' ability to act strategically.
Automated remediation in Identity Security Posture Management (ISPM) New capability of Identity Security Posture Management Generally Available in North America in Q4 2024	• Okta Identity Security Posture Management (ISPM) empowers enterprises to proactively take control of their identity sprawl and harden their identity security posture, reducing their attack surface and risk of being breached. • ISPM customers can now automatically remediate critical risks to efficiently improve their security posture.	Okta ISPM empowers organizations to take a proactive stance in reducing their identity attack surface and addresses critical identity security challenges by providing: • A bridge between Security and IT teams to regain control over their identity security posture. • A centralized view of identity security posture across their entire ecosystem. • A proactive approach to detect vulnerabilities, misconfigurations, and policy violations. • A fast path to prioritization and resolution of the most critical identity security issues, such as inconsistent MFA enforcement or excessive privileged access.

Customer Identity Solution (CIS) Announcements

Building secure, seamless experiences

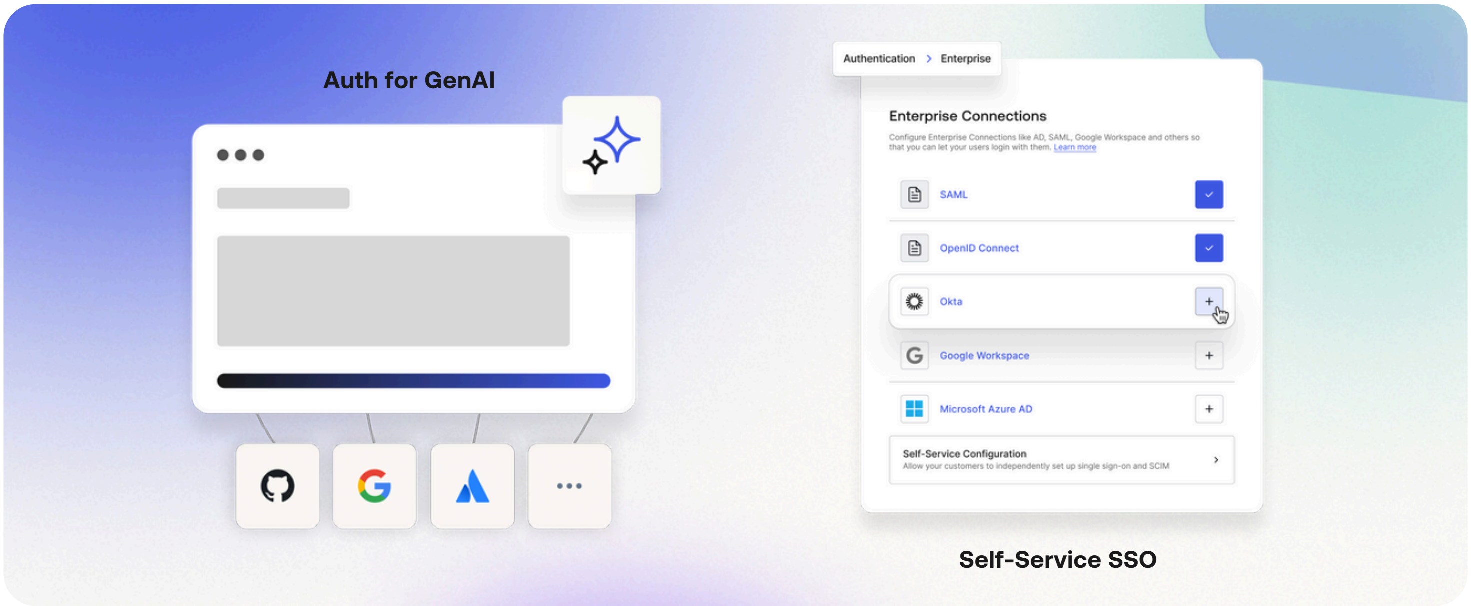


Announcement	Description	Importance
Revamped Roadmap for Customer Identity Solution (CIS) Announcement	• We're committed to thousands of customers who leverage Customer Identity Solution to deliver seamless, secure experiences. We've listened to customer feedback and delivered features like Multi-Brand, additional ThreatInsights capabilities, and Multiple identifiers over the past year. • To reflect on our active investment and commitment to continuous improvement, Okta is launching features like Passkeys, Identity Security Posture Management, and more to give more control over user experience and security.	• The CIS roadmap in response to customer feedback. This roadmap is designed for organizations with paramount security, regulatory compliance, and configurability. • CIS focuses on delivering security outcomes first with our platform differentiators: simple, out-of-the-box, easy-to-manage features and unique capabilities that enhance security posture and management. This approach allows us to capture a larger market by addressing security and user experience. • CIS prioritizes security outcomes, while CIC optimizes user experience without compromising security, providing organizations with comprehensive solutions tailored to their needs.
Passkey autofill New product within Customer Identity Solution Early Access available now	• The new passkey autofill user interface leverages browsers' native autofill functionality to streamline authentication. • Users can enjoy a seamless, one-step login experience with passkeys, directly from their autofill prompt—no extra clicks. • Combines secure, phishing-resistant authentication with a seamless user experience.	• Streamlined user experience for passkeys authentication using browser autofill. • Quickly and intuitively log in without extra prompts. • Combines secure, phishing resistant authentication with seamless user experience. • Eliminates the need for typing credentials. • Cross-device compatibility to login seamlessly from different devices
Identity Security Posture Management (ISPM) New product within Customer Identity Solution Available in 2025	• Identity Security Posture Management helps security teams better assess identity security risks and take control of their identity sprawl. • Okta is extending this capability to the Customer Identity Solution so our customers get a single source of truth for their Identity risk.	• Enables organizations to reduce risk and drive down fragmented enterprise IT and overhead costs • Proactively assess identity risk posture. • Continuously uncover critical misconfigurations and gaps, such as inconsistent MFA enforcement, and account sprawl. • Drive effective remediation by focusing on the most critical vulnerabilities first, making remediation more efficient and impactful.

Announcement	Description	Importance
Transactional MFA New product within Customer Identity Solution Available in 2025	• Transactional MFA enhances security by requiring an additional authentication factor during high-risk transactions, ensuring that only authorized users can complete sensitive actions. • Users receive real-time authentication prompts, making it straightforward to verify their identity without disrupting their workflow. • Integrates seamlessly into existing user journeys, balancing robust security measures with a user-friendly experience.	• Protects sensitive transactions, significantly reducing the risk of fraud and unauthorized access to accounts. • Enhances user confidence by providing an extra layer of security, assuring safeguarded transactions • Implementing Transactional MFA helps organizations comply with regulatory requirements. • Provides a tailored approach to risk management, optimizing both security and user convenience.

Additional Announcements for Customer Identity Cloud

The enabler of amazing digital experiences across consumer and SaaS applications



Configure Enterprise Connections like AD, SAML, Google Workspace and others so that you can let your users login with them. Learn more

Allow your customers to independently set up single sign-on and SCIM

Announcement	Description	Importance
Authentication for Generative AI (Auth for GenAI) New solution bundle Available in 2025	Auth for GenAI makes it easier for customers to build their GenAI applications securely. This set of features allows builders/developers to ensure their AI agents have the right and least privileged access to sensitive information, can call APIs securely on behalf of users to integrate with other apps, and can securely implement on-demand user authentication when background/async AI agents need user confirmation for actions.	GenAI apps can introduce vulnerabilities because their behavior is non-deterministic. They also rely on UX patterns that are different than those of web/mobile apps. Auth for GenAI allows implementing those patterns easy, while helping protect from vulnerabilities. • **Call APIs on user's behalf** - As GenAI apps (e.g. chatbots) integrate user products to provide delightful experiences, calling APIs on behalf of users will become a commonplace need. Users need to do this securely to prevent vulnerabilities that can be caused by hallucinating LLMs and admin like agent credentials. • **Async User Confirmation** - As AI agents go mainstream, async agents (or agent running in the background) to perform processing or wait for conditions will become commonplace. Those agents will need to authenticate users on-demand, to avoid keeping user credentials around indefinitely.

Announcement	Description	Importance
Authentication for Generative AI (Auth for GenAI) *(cont.)*		• **Fine-grained authorization for Retrieval Augmented Generation (RAG)** - as RAG becomes prevalent in GenAI apps, it is paramount to ensure that the content used to generate answers is content each user can access. Fine-grained authorization enables retrieved content to be filtered at very granular levels (e.g. documents, studies, pages, etc.) so LLMs are only fed with content each user has permissions to. • **Chat sharing** - As GenAI apps make chatbots prevalent, sharing chat sessions with co-workers/friends will be common and help with organic product growth.
Developer Portal New solution bundle Available in 2025	Developer Portal offers a branded and secure developer portal for developers and partners instantly and helps make APIs AI-ready. This new solution makes it easy for you to securely expose your API, with your brand, to developers and partners.	• **Securely Expose Branded Portals for APIs:** Okta is working to make it extremely easy to securely expose your APs, with your brand, to developers and partners. • **Expand AI Agent API Access:** AI agents don't need user interfaces; they're better off talking to an API. To become "AI native," products that don't have an API will look to build one, and all new products will launch with one. This means that agent identity and securing how developers and partners access your API will become more critical than ever.
Self-Service Single Sign-On (SSO) Early Access available now Generally Available in Q4 2024	• This feature provides business-to-business customers with the tools needed to delegate SSO setup to their enterprise customers. By delegating this task, you can streamline your onboarding process and grant customers more autonomy over their sign-on experience. You can also reduce the time and costs associated with managing SSO across your customer base. • Self-Service SSO requires minimal configuration in your Auth0 tenant and provides your customers with a setup assistant that guides them through the enablement process. After a customer completes their setup, the SSO integration is automatically added to your tenant as an Enterprise connection. Self-Service SSO uses the following components to delegate setup to your customers: • **Self-service profile:** Defines key elements of customer SSO implementations, such as the identity providers they can use for SSO and which user attributes they must capture, such as email. • **Self-service access ticket:** Grants customer admins access to the SSO setup assistant and sets specific details for their resulting SSO integration. • **SSO setup assistant:** Guides customer admins through the SSO setup process.	• Delegate administration to business customers by enabling them to set up their own Single Sign-On (SSO) access to applications. As a result, business customers will have fast and secure SSO access, and your developers can focus on your core app.
Self-Service System for Cross-Domain Identity Management (SCIM) New feature Generally Available in Q3 2025	Offload SCIM configuration to your business customers for automated provisioning and de-provisioning of user access across applications.	• Streamline user management by automating the provisioning and de-provisioning of user access across applications. • Reduce manual effort, increase security, and enable your organization to scale with ease while enabling compliance & authentication.

Announcement	Description	Importance
Universal Logout New feature Early Access available now Generally Available in Q4 2024	• Universal Logout is built for today's sprawling adoption of SaaS apps. It allows Security teams to detect risk changes and automatically terminate all user sessions across applications and devices. • Employee Identities are automatically signed out of SaaS apps managed by Okta CIC when a logout or de-provisioning event occurs in WIC. Not only does this boost Security, but it also adds a huge value to the businesses that use the apps you build. • Universal Logout is an Okta feature based on the Global Token Revocation specification. Apps that build an API supporting this specification can allow security management incident tools like Okta Identity Threat Protection in Okta Workforce Identity Cloud to send a request to revoke users' sessions and tokens when it identifies a change in risk. • SaaS apps that work with Universal Logout in Okta WIC today include: Google Workspace, Apple Business Manager, Microsoft Office 365, Salesforce, Slack, and Zoom.	• Securing sessions and users post-login is becoming even more important as attackers increasingly target stolen session cookies and post-login operations. Here's how Universal Logout benefits customers: • **Improve Enterprise Security Posture:** Enterprise customers demand quick access revocation during security incidents and employee termination scenarios. Supporting Universal Logout empowers customers to instantly mitigate risks across their ecosystem and improve security. • **Available Out-of-the-box:** Many businesses spend millions of dollars developing a response to a security incident. Universal Logout for WIC is an out-of-the-box solution ready for your application and your customers to use. No development work is required.
Forms Generally Available now	Forms is a feature of Okta Customer Identity Cloud's extensibility offerings that provides developers and UX teams with a no-code visual editor to easily and quickly build forms to customize the login and sign up experience. Some of the key capabilities of Forms include: • Pre-built components with frontend and backend validations. • Custom business logic with out-of-the-box integrations with third parties. • Controlled and secure experience within your tenant's domain. Not required to redirect users to external sites. • Consistent branding experience with Universal Login.	Frictionless sign-up and login experiences are crucial for winning over customers and staying competitive. Businesses today need tools that not only enable operations to be efficient and secure, but also help drive customer retention and growth, adapt to unique security needs, and unify and activate data across multiple apps and systems. Extensibility is key for every customer today, helping deliver frictionless end-user experiences and boost revenue. There are various use cases and customizations that require extending an Identity solution to deliver business outcomes. • **Accelerate time to market:** Easily build and edit forms with a no-code visual editor. • **Build frictionless customer experiences:** Simplify adding custom policies and terms to signup and login flows. • **Improve form conversion rates:** Collect and activate relevant customer data and enrich customer profiles over time with progressive profiling.
Advanced customization for universal login (ACUL) New feature Limited Early Access available in Q4 2024	Advanced Customizations for Universal Login, is a new pro-code capability for Universal Login that allows customer engineering teams to leverage the latest frontend technologies, internal design systems and component libraries, and 3rd party CSS and Javascript to build custom client-rendered interfaces for Universal Login.	Simplifying user authentication for businesses, Advanced Customization for Universal Login offers customizable options and advanced features without the need for manual updates. Some of the enhancements in EA and GA will be: • White-labeled SaaS • Multiple Brand per Tenant • Multiple Brands & Domains • Right to Left Languages • More and Custom Language Support
Client-Initiated Backchannel Authentication (CIBA) New feature of Highly Regulated Identity Early Access available in Q4 2024	Client-Initiated Backchannel Authentication (CIBA) allows users to initiate authentication prompts (like push notifications) from the application backend instead of the user device. In other words, customers can use CIBA to send push notification step-up prompts to users for in-person and over-the-phone interactions instead of costly and less secure SMS and knowledge-based questions.	• CIBA provides the means to proactively reach out to users via a notification for them to authenticate and authorize access. This can enable use cases where the interaction is triggered from backchannel applications and does not require the user to be redirected to the Authserver on the consumption device.

Announcement	Description	Importance
Client-Initiated Backchannel Authentication (CIBA) *(cont.)*	• CIBA is an “API first” integration to optimize UX and launch Transaction Authorization & User Validation from backend applications without requiring user redirection. • CIBA extends OIDC to define a decoupled flow where the authentication or transaction flow is initiated on one device and verified on another. The device on which the OIDC application initiates the transaction is called the consumption device and the device where the user verifies the transaction is called the authentication device.	• CIBA utilizes backend authentication, making this protocol much more secure from interference. • With CIBA, call center agents, for example, can send an authentication request right to a user's phone, allowing users to authenticate and authorize the agent to perform an action with just a single tap.
Auth0 Pricing & Packaging Update Free and Self-Serve Plans Generally Available now	Auth0 free and self-serve pricing plans (announced September 2024) have been expanded to make it easier to build, deploy, and scale apps no matter what the authentication needs are. • **New Free Plans include:** ○ 25,000 MAUs so our customers can scale. ○ Unlimited* Okta Connections & Unlimited* Social Connections so users can easily access your app. ○ A custom domain so our customers can fully brand your authentication. • **New Paid Plans include:** ○ 10 Organizations on B2C Plans and Unlimited* on B2B Plans so our customers can better manage their customers and partners. ○ Increased MFA offerings to mitigate the growing threat of AI-based attacks. ○ The ability to get up to 15 Enterprise Connections in B2B Pro via add-ons for more seamless integration across apps. ○ Unlimited* Admins across all paid plans *subject to system limitations	Our new free and self-serve plans tackle key customer challenges by simplifying complex identity management and enhancing security without significant costs. These plans offer scalable solutions that grow with your business, allowing you to focus on core development while ensuring robust, cost-effective authentication and authorization.

All dates are calendar year unless otherwise indicated.

Any products, features or functionality referenced in this material that are not currently generally available may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.

About Okta Okta 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.