Okta Showcase 2024 Updates

Product / Feature	Description	Importance
Okta AI	• Okta AI is a comprehensive set of AI features and capabilities that blend the latest AI models with Okta's unique crowdsourced threat intelligence and Identity data to power real-time Identity actions • Embedded across both Workforce Identity Cloud (WIC) and Customer Identity Cloud (CIC), Okta AI reinforces Okta's position as the most trusted Identity partner	• Okta AI lets organizations harness the power of AI to build better experiences and protect against cyberattacks • A smarter, faster, and more seamless experience when building, deploying, managing and using Identity with Okta • Empower security teams with technology that learns and evolves to tackle any Identity-based attacks • Developers can build apps with auto-generated Identity code and embedded actions, while IT can streamline and automate operations for admins and reduce headaches

Identity Threat Protection with Okta AI
 	
New WIC product with per user pricing
 	
Early Access (EA) now Generally Available (GA) Q3 2024
	• Identity Threat Protection with Okta AI delivers real-time detection and remediation for Identity-based threats by leveraging shared signals throughout a user's active session
	
	• This is Identity threat detection and response (ITDR) for Okta
	
	• Companies no longer need to buy another ITDR solution for a single, actionable view
	
	• This is not extended detection and response (XDR); Identity Threat Protection will integrate with XDR platforms
	
	• Empowers organizations to mitigate risk with richer threat detection and response capabilities with three critical capabilities:
	  ○ Continuous Risk Evaluation leverages AI to enforce security policies both at login and during an active user session, reducing the potential for unauthorized access and post authentication threats like session hijacking.
	  ○ Shared Signals Pipeline amplifies threat visibility across the tech ecosystem, enabling security teams to detect and respond to emerging threats between various security technologies, including Mobile Device Management (MDM), Cloud Access Security Broker (CASB), network security, Endpoint Detection & Response solutions, and more
	  ○ Adaptive Actions responds to real-time threats by enabling targeted actions such as Universal Logout from supported applications with the feature enabled, prompting users for on-demand multi-factor authentication, and executing automated workflows to address emerging risks
		• Because Identity is universally deployed across an organization's tech stack, with Okta's massive ecosystem of partners and SaaS apps, Okta is uniquely positioned to assess risk across security domains and throughout active user sessions
		
		• Extends Identity-powered security capabilities beyond the point of authentication to address the growing risk of post-authentication threats, such as session hijacking, Adversary-in-the-Middle (AiTM), and MFA bypass attacks via phishing
		
		• Addresses the issue of a fragmented cybersecurity landscape where security teams are adopting an increasing number of tools and navigating multiple consoles, which makes threat observability and risk assessment difficult to track
		
		• Strengthens best-of-breed approach to security by facilitating risk signal sharing at scale across the Okta ecosystem
		
		• Overcomes limitation of platform providers, which share signals mainly from first-party components, by providing customers the flexibility to consume signals from any security vendor they own or may choose in the future

Product / Feature	Description	Importance
Universal Logout New feature of Identity Threat Protection EA now GA Q3 2024	• Possible for the first time in the Identity industry, automatically log users out of their apps when there's a security issue, based on customer policies • Will support leading applications including Box, Google Workspace, Salesforce, Slack, Tableau, Zendesk, and Zoom, and will expand with more support across resources over time	• Makes Workforce Identity Cloud even more secure by proactively addressing security events, reducing the potential impact of a security incident for customers • Extends logout protection beyond platform provider workloads that includes the ecosystem of third-party apps and resources to ensure a comprehensive logout

Identity Security Posture Management
 	
New WIC product
 	
Available to select customers in North America Q2 2024
	• Identity Security Posture Management (ISPM) proactively identifies vulnerabilities and security gaps before they can even be exploited
	
	• Provides unparalleled visibility into identity posture across Okta, third-party Identity providers such as AWS and Azure AD, and cloud and SaaS environments like Salesforce, O365, and Github
	
	• Built to help discover and prioritize Identity issues based on real-world impact so users can focus their efforts where they matter most
	
	• With ISPM, customers can:
	  ○ Proactively assess identity risk posture
	  ○ Continuously uncover critical misconfigurations and gaps, such as inconsistent MFA enforcement, and account sprawl
	  ○ Prioritize and remediate the most pressing issues based on risk severity
		• As organizations embrace multi-cloud and SaaS environments, security teams often struggle to maintain visibility and control over their identity landscape and identity security posture
		
		• New challenges result in an increased attack surface and higher exposure to security breaches:
		  ○ Fragmented identity data across multiple systems creates blind spots, making it difficult to identify and mitigate potential risks
		  ○ The proliferation of dormant accounts and/or the failure to deprovision accounts contributes to potential vulnerabilities
		  ○ Modern IAM solutions offer effective tools such as MFA and compliance frameworks to protect access, but customers lack the confidence that these are deployed properly
		
		• ISPM empowers organizations to take a proactive stance in reducing their identity attack surface and addresses these challenges by providing:
		  ○ 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

Govern Okta Admin Roles New WIC product enhancement EA now GA Q4 2024	• Govern Okta Admin Roles covers the complete governance lifecycle, from workflows to access requests to certifications, for admin permissions inside Okta • Available as a standard feature across all Okta Workforce products without requiring the purchase of Okta Identity Governance	• Okta itself is at the top of the list of the most critical resources that organizations need to govern access to • When thinking about how to build products with security top of mind, governing Okta admin roles is key

Product / Feature	Description	Importance
Bot Detection Enhancements New CIC product enhancement GA Q2 2024	• This fourth-generation Bot Detection with Okta AI leverages machine learning models to stay ahead of adversaries and their tactics • Incorporates third-party bot scoring data to significantly enhance its ability to identify and thwart bots more effectively 　○ Compared to previous iterations, this new model is 25% more effective at catching bots all while maintaining minimal impact on the user experience • Fine-tuned models designed to combat specific types of bot attacks at different parts of the user journey, such as account creation will also be released	• Bots make up nearly 50% of all internet traffic today; enhanced bot detection capabilities help identify and mitigate fraudulent registrations more effectively • By distinguishing between legitimate users and automated bot activity, customers can reduce the risk of unauthorized access and account takeover • Bot Detection enhancements help companies minimize wastage by ensuring their marketing dollars are spent acquiring real, valuable customers who are more likely to generate revenue and contribute to business growth
Auth Challenge New CIC product enhancement GA Q2 2024	• Auth Challenge is Okta's new default response to bots that uses browser and device signals to make it nearly four times as challenging for bots compared to traditional CAPTCHAs (a type of challenge–response test used in computing to determine whether the user is human in order to deter bot attacks and spam) • Customers can stop more bots with virtually zero friction for their customers	• Auth Challenge increases the cost for bad actors to deploy an attack by draining additional compute resources • Unlike traditional CAPTCHA challenges, Auth Challenge operates transparently in the background, which means that users can seamlessly authenticate without being prompted to solve complex CAPTCHA puzzles, leading to a smoother and more user–friendly login experience • By bolstering security without compromising usability, Auth Challenge helps to reduce the risk of account takeover incidents • Malicious actors are less likely to successfully bypass authentication mechanisms, protecting users' accounts • Improves latency, reliability, and resilience against DDoS attacks, ensuring a consistently smooth authentication experience for users worldwide

Product / Feature	Description	Importance
Passkeys New CIC feature GA now	• Provides a phishing-resistant sign-up, and sign-in experience for end users, making them less reliant on legacy credentials • Available as a no-code toggle to ease the implementation experience and increase adoption of phishing-resistant, passwordless authentication	• Provides comprehensive support beyond just the protocol level, covering signup, sign-in, and progressive enrollment — all accessible via a single toggle without requiring code modifications to the application • Other cloud platform vendors lack passkey support in their customer identity solutions • Legacy identity vendors offer limited, protocol-only passkey options, necessitating custom user journeys and manual handling of onboarding and resets, which can compromise security and cause account lockouts • Niche startups specializing in passkeys lack key functionality support for complex scenarios involving user onboarding, user migration, progressive profiling, connecting to CDP/CRMs, and enterprise service level agreements
Highly Regulated Identity New CIC product bundle GA Q2 2024	• A dedicated solution that raises the bar for security, privacy policy controls, and user experience • Built on financial industry regulations and standards to address the complex and nuanced fraud, compliance and user experience needs for the most sensitive of scenarios • Includes Financial-grade API (FAPI) Security Profile 1.0 Advanced • Utilizes cloud-native technology and CIC's advanced security system, which benefits from threat insights from tens of thousands of CIC customers across free, self-service, and enterprise plans	• Allows Okta to support customers who want to meet specific identity standards (e.g., Open Banking) and expand its position in highly regulated industries worldwide, such as banking, insurance, and healthcare • Improves security for any customer, even those outside of regulated environments, by making operations like Strong Customer Authentication (SCA) easy to implement through Actions and allowing them to bring their own encryption keys • Other cloud platform vendor identity offerings do not support the advanced security standards of OIDC and OAuth 2.0, which are required for highly regulated identity scenarios • Legacy identity vendor code bases are insufficient in meeting the required protocols and standards for OpenBanking and Financial Grade API
Continuous Session Protection New CIC product GA Q2 2024	• Helps developers and security teams address session hijacking and revoke suspicious sessions quickly • Adheres to geo and industry-specific compliance requirements by managing session times	• Reduces the risk of account takeover by detecting anomalous session behavior and triggering specific countermeasures • Increase revenue by limiting active sessions across applications • Improves UX by having control over session expiration limits

Other Product Roadmap Updates

New and upcoming Workforce Identity Cloud products and features		
Powers identity for all employee, contractor, and business partner use cases		
Product / Feature	**Description**	**Importance**
FastPass Context Re-Evaluation New feature of FastPass (passwordless) GA now	• Pulls security signals from a users device every time a new app is accessed, and prevents further access if the device or session gets compromised • After initial authentication is successful, Okta Verify re-checks device posture to ensure security remains as strong as at the time of authentication • If Okta Verify detects that anything looks different from the point of initial login, such as if the device disabled the local firewall or the Crowdstrike Zero Trust score changed, the user will be prompted for re-authentication.	• Extends secure device context checks beyond initial point of authentication versus stale checks from platform identity providers that can be many hours old, increasing the chances of non-compliant logins • Makes Workforce Identity Cloud even more secure • Further advances the journey to passwordless in a frictionless way • Strengthens best-of-breed approach to security by facilitating risk signal sharing at scale across the Okta ecosystem
Log Investigator with Okta AI New feature of WIC EA Q3 2024	• Log Investigator with Okta AI enables admins to ask questions about Okta data in plain English, and obtain insights on the historical context of their Identity posture • Together with Okta Identity Threat Protection, admins can easily trace back risk events, user activity, system anomalies, and more	• Helps customers rationalize the massive amount of data in their Okta system log • Makes it easier to investigate potential threats, troubleshoot end user issues, and work more efficiently • Significantly improves the speed at which customers can get the answers they need from the syslog and take timely actions
Policy Recommender with Okta AI New feature of WIC EA now	• Policy Recommender with Okta AI provides personalized recommendations and templates, streamlining the setup of secure authentication practices, including device posture checks and phishing-resistant authenticators • Provides recommendations based upon aggregated intelligence from across Okta's extensive ecosystem as well as best security practices	• Makes it simple to configure the most secure access policies for the most commonly used applications in the Okta Integration Network • Simplifies application of security policies across heterogeneous components, enabling customers to easily implement defense-in-depth architectures
Governance Analyzer with Okta AI New feature of Okta Identity Governance EA Q4 2024	• Governance Analyzer with Okta AI provides decision makers with valuable context and recommendations in reviews and requests, unlocking highest quality governance decisions without adding cognitive burden on them • Leverage data from other parts of Okta's unified platform, such as involvement in past identity threat events or potential risk of access • Intelligently predicts access risk and proactively launches an access certification campaign while also equipping approvers with key insights, such as past risk events associated with the user	• Drives better governance outcomes by empowering decision makers with the necessary context to make an informed decision, leveraging signal from across Okta's unified identity platform

okta

Product / Feature	Description	Importance
Okta Identity Governance Entitlement Management New feature of Okta Identity Governance GA now	• Organizations can discover and manage entitlements from a wide variety of applications all within a single platform • Detect and govern dormant entitlements, rightsize and provide recommendations for misconfigured entitlements for cloud and on-prem resources, hook entitlements for all applications	• Leverages Okta's massive amount of data and unique position as the neutral Identity partner • Provides cloud-native entitlement management of multi-cloud and on-prem resources by increasing the value of an existing powerful bundle

Okta Privileged Access
 	
New product $14 per resource unit per month
 	
GA now
	• For all critical resources (servers, databases, infrastructure), both on-prem and in the cloud, including infrastructure and servers, customers will be able to:
	  ○ Implement zero standing privileges
	  ○ Extend passwordless to the most critical resources
	  ○ Democratize just in time access with self-service access requests and automation
		• Completes Okta's unified identity offering across identity access, governance, and now privileged access
		
		• Okta is the only vendor today to provide a comprehensive, modern identity management solution for workforce identity
		
		• Delivers privileged access to all critical resources without limitations due to platform

FastPass + Yubico New joint offering EA now	• With Yubico's FIDO Pre-reg, new employees can be created in Okta in advance of their first day, receive their pre-registered YubiKey, and follow two simple steps to establish user-presence and gain access • Drives end-to-end phishing resistance with pre-enrolled YubiKeys for passwordless in minutes	• Mitigates the risk of social engineering and unauthorized factor self-enrollment that can occur with platform identity solutions • Gives customers more choice to leverage a variety of authentication factors • Further advances the journey to passwordless and phishing resistance • New employees can be up and running within minutes of receiving their laptop
Secure Partner Access New solution bundle Beta now EA Q3 2024	• A comprehensive solution for business partner collaboration to enable secure and efficient interactions with supply chain and distribution partners • Build portals that set up users in one org isolated per partner or a company they need to collaborate with • Efficiently onboard business partner identities to reduce IT burden and accelerate business outcomes	• Provides a true, enforceable boundary regardless of entry point and avoids exposing an entire directory to partners, which can occur with platform identity vendors • Enables seamless collaboration while minimizing risk and operational overhead for partner users • Fills a critical gap in the identity market as an organization's employees and partners are typically managed separately, resulting in a better security posture • Expands Okta's Workforce Identity Cloud to cover even more use cases for organizations with extended workforces

Product / Feature	Description	Importance
Okta Personal New feature of WIC Beta now EA Q1 2024	• Users can see all of their apps in one place, save and autofill passwords and share passwords with the familiar experience that Okta users love to use for work • Decouples personal apps from a user's Okta enterprise account and migrates those apps into a free Okta Personal account that they can take with them even after they leave the organization	• Extends the Okta experience that customers love into personal identity • Advances the concept of identity belonging to the user • Provides a consistent user experience and flow regardless of platform or mobile device

New and upcoming Customer Identity Identity Cloud, powered by Auth0, products and features The enabler of amazing digital experiences across consumer and SaaS applications

Product / Feature	Description	Importance
Fine Grained Authorization New product with MAU based pricing GA now	• Provides authorization as a service that allows developers to design authorization models in a way that's centralized, flexible, scalable, and easy to use • Provides a centralized view into authorization policies, so customers can efficiently manage their compliance goals • Authorization as a service that eliminates authorization complexity across systems, users, and applications • Delivers scalable and fully flexible authorization: customers can now use Okta to build team collaboration, multi-tenancy, custom roles, IoT, and cloud entitlement management	• Speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business • Legacy identity vendors use traditional, role-based,methods of authorization that have limited granularity, are static, and are implemented at the application level, while Okta distinguishes itself with cloud-native, centralized authorization as a service • Other cloud platform vendors do not offer a comparable solution for customer identity • Compared to smaller identity providers focused on self-hosted solutions for startups, Okta stands out with mature, scalable, and enterprise-grade security, making it the leading choice for robust authorization
Verifiable Credentials with Mobile Drivers License (mDL) New feature of CIC EA Q3 2024	• Customer Identity Cloud will add support to easily perform online verification of Mobile Drivers licenses • Allows application builders to adopt this technology to build digital customer experiences that bypass physical credential proofing processes that exist today	• Okta CIC enables customers to easily streamline Know Your Customer (KYC) and compliance challenges, making onboarding and verification as straightforward as adding a social connection • Speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business

Product / Feature	Description	Importance
System for Cross-domain Identity Management (SCIM) New feature of Customer Identity Cloud Enterprise plan Beta now GA Q2 2024	• Okta Customer Identity Cloud will now support the standard System for Cross-domain Identity Management • Integrating SCIM in Customer Identity Cloud to Workforce Identity Cloud simplifies synchronization of user directories and allows customers to harness the power of both clouds by owning both ends of the connection • Allows customers to streamline user management by automating the provisioning and de-provisioning of user access across applications to reduce manual effort, increase security, and enable the organization to scale with ease	• Allows SaaS companies to sell to larger enterprises by streamlining provisioning and lifecycle management, thanks to seamless integration between workforce and customer identity—a capability unmatched by other identity providers • Other cloud platform vendor identity solutions are inadequate for SaaS application development, lacking Enterprise federation, role-based access control (RBAC), and SCIM support • Legacy identity vendors necessitate on-prem legacy systems and makeshift SCIM solutions with cloud support limited to workforce scenarios, requiring custom work for SaaS applications
Identity Flow Optimizer with Okta AI New feature of CIC EA Q4 2025	• Identity Flow Optimizer with Okta AI provides developers with inline recommendations on the identity configurations and actions they can add to boost conversions, improve security, and build their apps faster	• Makes identity configurations and actions simple to enable a more streamlined developer workflow • Speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business
Actions Navigator with Okta AI New feature of CIC EA Q2 2025	• Actions Navigator with Okta AI allows developers to discover and implement marketplace integrations or write an Action (function that is used to customize and extend CIC capabilities) by simply asking for it in a search prompt	• Helps make finding right marketplace integrations easier, showcases the power of Okta AI and Okta's commitment to making identity easy and intuitive for developers • Speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business

Tenant Security Manager with Okta AI
 	
New feature of CIC
 	
EA Q4 2024
	• Tenant Security Manager with Okta AI enriches Okta's Attack Protection capabilities with intelligent security recommendations through security snapshot alerts and dashboard notifications to improve the customer tenant's security posture	• Provides security professionals with configuration recommendations to detect and react to malicious attacks.
		
		• Examples include:
		  ○ Learning from a tenant's traffic and making security recommendations to speed reaction time
		
		  ○ Automating the analysis of normal and abnormal traffic patterns and recommending actions to effectively mitigate security events

Product / Feature	Description	Importance
Guide with Okta AI New feature of CIC EA Q3 2024	• Guide with Okta AI offers comprehensive onboarding assistance and intuitively maps out the best steps for users to take, seamlessly steering them toward the most valuable workflows from simple English prompts • Guide can explain any setting or jargon in the platform into easily understandable language and also enrich the experience with contextual assistance and curated links to relevant documentation	• Offers comprehensive onboarding assistance, by intuitively mapping out the best possible steps for users to take, seamlessly steering them toward the most valuable workflows—all from simple prompts written in plain English • Speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business
Workflows No-Code Automation New feature for joint customers of Okta WIC and Okta CIC GA now	• Workflows is Okta's no-code identity automation and orchestration platform that can enable anyone to innovate with its simple, drag and drop UI • With Workflows for Customer Identity Cloud, developers can use no-code to customize and extend custom logic	• Enables developers and digital teams to improve security posture, and drive stronger customer experience and retention • Speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business
Phone number as sole identifier New feature of CIC EA Q2 2024 GA Q3 2024	• A passwordless option that allows users to sign-up with just their phone number	• Makes it easier to support more users, in more countries where phone is an expected form of authentication, such as in Asia-Pacific or Latin America • Further advances the journey to passwordless, and enables customers to meet their users where they are
Custom sign-up prompts New feature of CIC GA now	• Enable developers to create personalized registration journeys directly within the new Universal Login • Sign-up prompts can be tailored to customer preferences, localization needs, privacy, consent, and beyond	• Enables developers and digital teams to improve security posture, and drive stronger customer experience and retention • Speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business

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.