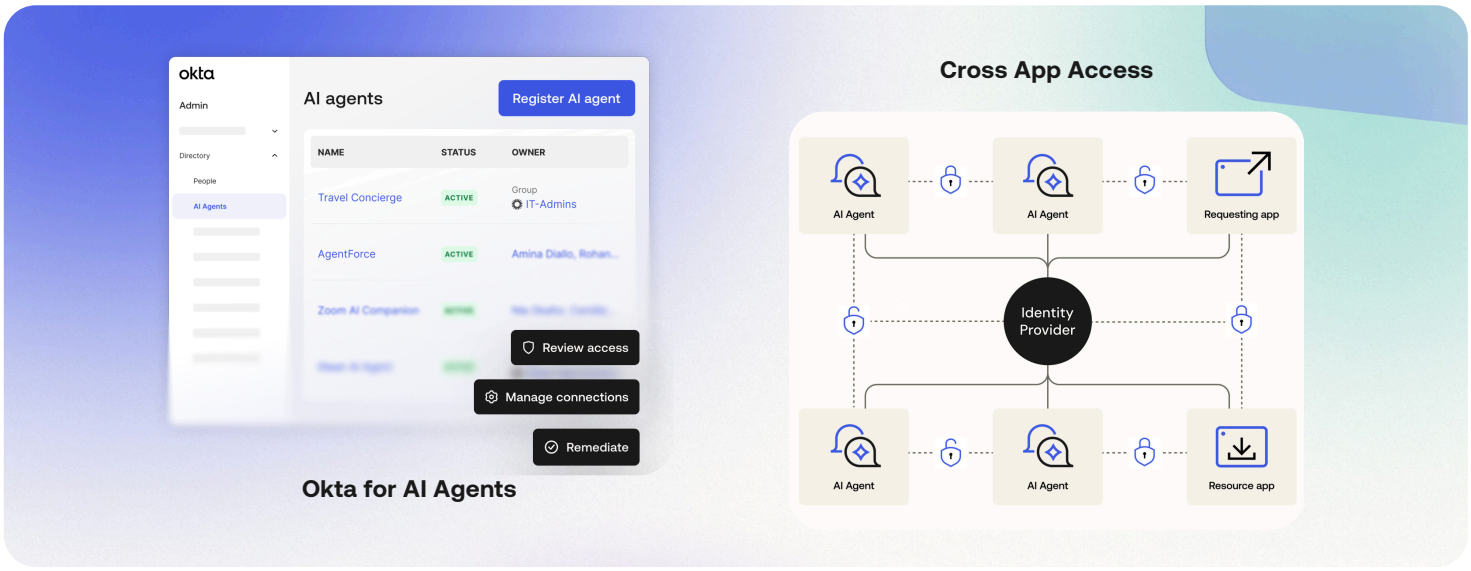
Highlights Across the Okta Platform

Whether you're securing your workforce, customers, or AI agents, our newest updates help you secure every user, every use case, and every resource.



Announcement	Description	Importance
Trusted digital experiences for Okta Customer Identity *Availability:* Multiple launches included, see below: • Passkeys EA Sept 2025 • Okta Identity Governance (OIG) GA Oct 2025 • Advanced Directory Management (part of OIG) GA Oct 2025 • Identity Threat Protection (ITP) EA Feb 2026	Build your brand's trust with new products on Okta Customer Identity. We're announcing powerful new capabilities to help solve your biggest challenges: Passkeys to facilitate eliminating phishing, Okta Identity Governance to automate ongoing governance and help securely delegate B2B users, and Identity Threat Protection to help stop attacks in their tracks. • **Passkeys:** Passkeys are a modern replacement for passwords that use public key cryptography for a phishing-resistant, user-friendly, and always-available authentication experience. Instead of remembering complex passwords, customers authenticate with a familiar biometric unlock like Face ID or Touch ID, or a device PIN. • **Okta Identity Governance (OIG):** Okta Identity Governance (OIG) for Okta Customer Identity (OCI) automates access policies and reviews to reduce privilege sprawl for external users. This helps with compliance and streamlines operations. A key part of this offering is Advanced Directory Management, which enables secure, delegated administration so external partners can manage their own users and access rights within a single governance framework. • **Identity Threat Protection (ITP):** Bot Detection and Remediation, Blocking New Account Fraud, Defending Against Credential Stuffing & Password Spray Attacks, Suspicious IP Throttling Resources: • Passkey Management • Help Documentation	• **Simple & Fast:** Customers can log in with a simple biometric scan or PIN, leading to a higher login success rate and faster login times compared to passwords. • **Phishing-Resistant:** Passkeys are cryptographically bound to a specific website, meaning they cannot be used on fake sites, making them inherently resistant to phishing attacks. • **No Password to Steal:** With passkeys, there is no password to be stolen in a data breach or to be guessed by attackers, providing a more secure and resilient identity for the customer. • **Reduces Security Risks:** It helps prevent privilege sprawl and unauthorized access by automating access policies and reviews, ensuring external users only have the permissions they need. • **Improves Compliance:** It streamlines operations and provides an auditable trail of who has access to what, making it easier for organizations to demonstrate compliance with industry regulations. • **Enables Business at Scale:** The inclusion of Advanced Directory Management allows for secure, delegated administration, which empowers partners and customers to manage their own users. This scales business operations without overwhelming central IT teams.
Enhancements to Okta for Government High and Okta for Government Moderate	Okta Identity Governance: Audit-Ready for Okta for Government High (FedRAMP High), supported for eligible Okta for Government Moderate (FedRAMP Moderate), and available with a signed BAA for HIPAA customers. OIDC ID Token Encryption is audit-ready for the full Okta US Public Sector portfolio.	• **Enforce least privileged access and simplify audits with Okta Identity Governance**, giving mission app owners smart, context-rich insights, automatically highlighting unusual access or policy outliers.

Announcement	Description	Importance
Availability: • Okta Identity Governance: Audit-ready for Okta for Government High (FedRAMP High), supported for eligible Okta for Government Moderate (FedRAMP Moderate), post-audit for Okta for US Military (DoD Impact Level 4), and available with a signed BAA for HIPAA customers. • OIDC ID Token Encryption: Audit-ready for the full Okta US Public Sector portfolio. • Workflows, Identity Threat Protection with Okta AI: Post-audit for Okta for US Military (DoD Impact Level 4).	**Customer Challenge:** Mission app owners manually identify and remediate inappropriate user access to enforce least privilege and prepare for audits. This process consumes valuable resources and diverts focus from mission-critical objectives. Agencies that need to embed highly sensitive PII in OIDC tokens or have compliance mandates (like NIST SP 800-63C FAL3) cannot do so securely. Resources: • Announcement blog	• **Implement JSON Web Encryption (JWE) with OIDC ID Token Encryption,** helping agencies to secure highly sensitive PII so that only a trusted Relying Party can decrypt and consume the token.
Okta for AI Agents New SKU Priced per workload principal per month *Availability:* Multiple launches included, see below: • Cross App Access (XAA) (Early Access available January 2026): XAA is a new, open protocol that brings app-to-app and AI agent connections under Okta's identity control, giving you centralized visibility, policy-driven security, and safer integrations as ISV partners start to build with it.	Okta will bring AI agents into your identity security fabric providing visibility to discover and identify risky agents with ISPM, control and management of their access with Universal Directory, and automated governance with access certifications to enforce security policies and manage the end-to-end lifecycle. AI agents are rapidly transforming how businesses operate — and how attackers exploit gaps. Over half of companies are already deploying AI agents, yet considering security as an afterthought. Unlike humans, AI agents: • Don't have a fixed owner • Can't complete traditional MFA • Spin up and down quickly • Often reuse or share credentials You can't secure what you can't see, manage, or govern. As AI agents become more autonomous and influential, they need identity-first security — just like human users. As agents scale, Okta helps prevent them from becoming attack vectors by embedding them into your identity security fabric. Once in the fabric, you will get these four use cases: 1. **Detect and discover:** Actively find every agent in your environment, understand their patterns, and assess the risk they pose.	AI agents are increasingly augmenting enterprise operations, autonomously executing tasks ranging from customer service interactions to financial process automation. Unlike human identities, these digital assistants operate at machine speed with ephemeral lifecycles and dynamic permissions that traditional IAM systems weren't designed to handle. Without proper identity security, AI agents introduce new vulnerabilities through their non deterministic behavior, privileged access requirements, and agent-to-agent communication patterns.

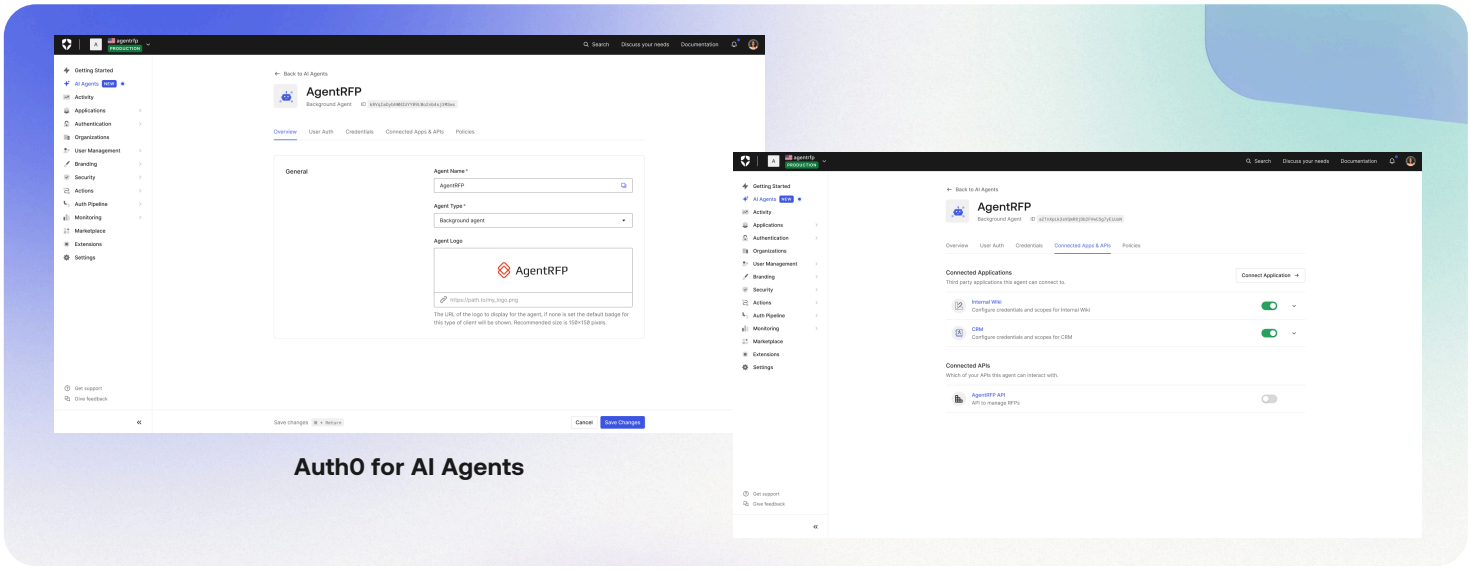
Announcement	Description	Importance
• Phase 1 Use Case Launch (Early Access available January 2026): Identity Security Posture Management (ISPM), Universal Directory, Identity Access Management, and Okta Privileged Access (OPA) • Phase 2 Use Case Launch (Generally Available FY27): Access Certifications, Extended Universal Logout	2. **Provision and register:** Treat agents as you would human identities. Each one should have a unique identity linked to a human owner who is accountable for its actions. 3. **Authorize and protect:** Agents should operate with only the access they need, for the time they need it, through recently introduced Cross App Access (XAA), a new open protocol that helps standardize how users, AI agents, and applications connect securely. 4. **Govern and monitor:** You must constantly monitor agent activity, looking for any unusual behavior that could signal a threat through automated access requests and periodic certifications to facilitate ongoing compliance with a clear audit trail. **Packaging information:** • **Auth0 for AI Agents** (Auth0 tenant, Token vault, 4 E.Cs., FGA)* • **ISPM for AI Agents & Non-human identities (NHI):** Discovery for AI Agents & associated NHI • **IDaaS & AMP** Policy, Scopes for AI Agents + **XAA*** • **OPA:** Workload Identity Resource Unit (to access vaulted creds) • **OIG:** Access Requests and Certs for AI Agents • **ITP:** Universal Logout for AI Agents Resources: • Learn more • See the blog * Potential for add'l connectors, RPS, Token monetization via Agent Tiers; Design principle to offer fully solutioned bundle for most use cases	
Okta Privileged Access with Axiom Priced per resource unit Early Access Q1 CY 2026	Okta acquired Axiom Security, a Privileged Access Management (PAM) product that helps organizations eliminate standing privileges and secure access to critical infrastructure. Axiom's technology will be integrated in Okta Privileged Access, expanding access controls to more sensitive resources that Okta customers can use to further strengthen their identity security fabric. Okta Privileged Access is and will continue to be the single control plane for all of our customers' privileged resources, whether on-premises or in the cloud, streamlining access and governance while eliminating standing privileges. **Customer Challenge:** • Disparate solutions for controlling access to servers, infrastructure, Kubernetes, and databases • Lack of traceability to tie access back to an individual Resources: • Blog	• This acquisition will help Okta customers extend their identity security fabric to more privileged access and resources • This acquisition allows Okta to accelerate our roadmap for expanded functionality around JIT access for databases and Kubernetes • Okta Privileged Access is and will continue to be the single control plane for customers privileged resources

Announcement	Description	Importance
RDP Click to connect for Active Directory accounts *Availability:* • RDP Click to connect for Active Directory: EA Q3 CY25 • Access certifications for service accounts: EA Q4 CY25 • On-demand credential rotation: EA Q3 CY25	A modern, passwordless SSO experience for accessing Windows Remote Desktop Protocol (RDP) sessions via Okta Privileged Access. Protect RDP flows with better security, choosing when AD passwords can be revealed or connections restricted to RDP-only sessions. What's coming: • **SSO for AD:** This feature enables users to 1-click SSO into Windows Domain-Joined Server using Active Directory accounts. • **Enhanced security for AD:** Security Admins are able to granularly control which accounts can be used and on which servers while also having the option to enforce step-up MFA or require an Access Request Approval before the session is established. • **Less AD set up:** This feature utilizes the AD Agent for account discovery and password management and can be used in conjunction with already available AD Account password vaulting features and Check-Out/Check-In.	• **Simplifies and secures access to Windows RDP sessions:** This new passwordless single sign-on (SSO) experience allows users to connect to Windows servers with a single click while enforcing strong security measures like MFA and access requests. • **Enhances security for Active Directory:** Admins can now enforce granular policies to control which accounts can access specific domain-joined servers, ensuring that only authorized users can connect to sensitive systems and minimizing risk exposure. • **Reduces administrative burden:** The new feature leverages your existing Okta Active Directory agent for easy setup and can be used with current password vaulting features, streamlining the process for IT teams.
Identity security fabric use cases • Protect non-human identities: EA Q1 CY26 • Secure hybrid & on-premises environments: GA Q1 CY26 (OAG in LEA Q1 CY26) • Enable security-driven governance: GA Q4 CY25 • Secure workforce onboarding: GA Q1 CY26	Modern security demands a unified identity security fabric. Okta brings this fabric to life through interconnected use cases—our threads—that address the most critical challenges facing security teams. By weaving the threads into a cohesive fabric, Okta delivers end-to-end, orchestrated identity security before, during, and after authentication for every identity —human, non-human, and AI agents—across all environments. **Customer Challenge:** • Cyberattacks are getting more frequent and sophisticated, especially from non-human identities like AI agents. • Fragmented point solutions create security gaps and complexity. • Integrating disparate systems drains resources and distracts security and IT teams from strategic initiatives. Resources: • Blog	• **Drive broader, deeper security outcomes:** Okta delivers end-to-end identity security before, during, and after authentication. • **Enhance efficiency and reduce operational cost:** A unified identity platform helps eliminate fragmented tools, simplifying operations for security and IT teams. • **Confidently secure every identity at scale:** Okta secures every identity—human, non-human, and AI—across all environments with consistent, scalable controls.
Verifiable Digital Credentials *Availability:* • Digital ID verification: Early Access Q1 CY26 • Verifiable digital credentials platform: Early Access CY26	Okta's Verifiable Digital Credentials platform enables organizations to verify and issue tamper-proof, reusable identity data — like government IDs, employment, or certifications. Reduce fraud and onboarding friction while enabling secure, privacy-preserving credentials that work across systems and partners. Built on open standards for maximum control and future interoperability. What's coming: • **Digital ID verification:** Allows businesses to verify government issued digital IDs natively, starting with mobile drivers license (mDL) and expanding to more ID types. It will fast-track onboarding, reduce manual review costs, and decrease fraud risks. • **Verifiable digital credential platform:** Infrastructure for businesses to issue, verify, reuse, and trust tamper-proof credentials. Built on open standards and future interoperability, the platform will offer both SDKs and integrations. Resources: • Learn more	• **Reduce costs associated with identity verification:** Time is money. Simply reuse trusted VDCs instead of re-verifying each time to combat your rising vendor and help desk-related costs. • **Decrease onboarding time and drop-off with VDCs:** Enhance your existing Okta/Auth0 identity layer by adding VDC flows. Faster more accurate verification makes for improved success rates, decreased processing time — an overall smoother user experience. • **Reduce fraud and compliance risk:** Eliminate manual document review in favor of tamper-proof data verification checks with cryptographic credentials — safer and more compliant. A big win!

Announcement	Description	Importance
Okta's Global Expansion *Availability:* • Canada and India cells will launch in Q1 2026. • French language support will launch in Q1 2026.	The Okta Platform is expanding its regional availability to include Canada and India to help customers support data residency and compliance requirements. We're also extending admin console and help documentation to support French language translations.	• **Regional Data Storage:** Customers will have additional regional options to store production data for both their primary and disaster recovery deployments of the Okta Platform. • **Improved Performance:** Customers may experience lower latency and improved performance by connecting to local data centers, leading to a better user experience for their employees and customers. • **Support French language admins:** Enable customers to use Okta in their preferred language.
Okta Private Cloud New SKU Priced as fixed fee Early Access available now for Okta Workforce and Customer Identity	Single-tenant, dedicated Okta instance purpose built for security-conscious, performance-sensitive, and high-growth enterprise environments.	Okta Private Cloud eliminates multi-tenant risks for our most security-conscious and performance-driven customers, delivering the ultimate in data isolation and guaranteed performance. • **Data Isolation:** Safeguard your identity data with physical and logical isolation, minimizing multi-tenant risks while meeting the most stringent security and compliance requirements. • **Dedicated Infrastructure:** Performance on demand with sustained, reserved capacity to handle your most intense write-heavy operations. • **Scale:** Future-proof identity platform designed to scale with your long-term growth.

Highlights Across the Auth0 Platform

Build a more secure and seamless customer identity experience.



Announcement	Description	Importance
Tenant Access Control List Early Access Now Expected General Availability September 2025	Create rules to allow, block, or redirect traffic based on risk signals like IPs, CIDR ranges, JA3/JA4 fingerprints, ASN, user agent, or geo. Resources: • Tenant Access Control List docs	• Tenant Access Control Lists give you self-serve controls to stop threats earlier in the flow. • This reduces risk and helps conserve rate limits by preventing bad traffic—like IPs linked to denial-of-service attacks—from ever reaching your app.
Enhanced Security Incident Management with Guide Early Access Now Generally Available in 2027	Security Center data is now available in Guide. Use the AI-powered chatbot to explain alerts, identify root causes, and access AI-driven insights and attack playbooks—all in one place.	By integrating with Security Center data, Guide now gives you a faster and simpler way to detect, analyze, and respond to identity threats. Instead of relying on manual investigation or support tickets, you can use the AI-powered chatbot to: • Explore your tenant's data • Understand the cause of alerts, • Receive actionable recommendations and attack playbooks —all in one spot. This helps reduce investigation time and enables proactive threat prevention.
Auth0 for AI Agents New SKU Priced as a percent of total based on MAU tier *Availability:* Multiple launches included, see below:	Auth0 for AI Agents is the complete auth solution for building AI agents more securely. With just a few lines of code, developers can move faster while embedding: • **Authentication:** Implement secure login experiences so that AI agents (from interactive chatbots to background workers) can identify your users. • **Token Vault:** Secure an Agent's interaction with other apps: We keep security tokens locked up so agents don't access things they shouldn't.	The complete auth solution for building your AI agents more securely. • Companies need a way to build AI agents securely and seamlessly. Developers build risky, one-off solutions to control what agents can access inside their own apps.

Announcement	Description	Importance
• Auth0 for AI Agents (Generally Available October 2025) • RDP Cross App Access (Early Access available January 2026) • Vertical Sample Apps (Generally Available September 2025)	• **Async Authorization:** Support lengthy, complex tasks driven by agents. As needed, Auth0 will enable AI agent to simply stop and ask for human approval before moving forward. • **Fine-Grained Authorization for RAG:** Set clear rules for the data AI agents can access to keep user documents data safe and prevent leaks. Precise controls ensure agents only pull information from authorized docs. Teams gain the freedom to innovate with persistent memory and human-in-the-loop workflows, while giving executives a high degree of confidence that every in-app action is protected, auditable, and compliant. From pilot to production, Auth0 facilitates the trust, compliance, and speed required to transform AI ideas into enterprise-ready solutions — all backed by the world's most trusted identity platform. Cross App Access: Cross App Access (XAA) is a new, open protocol that extends OAuth for agent-to-app and app-to-app access at scale. Built directly into Auth0, it provides out-of-the-box control and visibility for two key scenarios: • For B2B apps: Give your enterprise customers centralized IT control and visibility into which agents and apps can connect — no custom integrations required. • For internal agents: Use XAA to securely connect your own company's agents to apps when using a supported IdP like Okta. In both cases, Cross App Access eliminates long-lived tokens, replaces repetitive user consent flows with policy-driven approvals, and delivers smoother, more secure experiences. Vertical Sample Apps: As AI agents become a new type of identity, securing their access presents unique challenges across different industries. This is especially true in regulated sectors like healthcare or finance, and in high-volume sectors such as retail. The industry-specific sample applications help organizations understand how Auth0 can help securely manage and protect human identities today while also preparing them to safeguard emerging AI agent identities. Resources: • Blog Link: The 'Superuser' Blindspot • Landing Page Link: Cross App Access Landing Page • Healthcare Blog Link: The Future of Healthcare Is AI-Powered and Secure: How CIAM Builds Trust • Retail Blog Link: Securing AI Agents: Retail's Next Big Challenge	• Companies need to prioritize developer efficiency so they can focus on building innovative products, not auth.
Auth0 for B2B Enhancements *Availability:* Multiple launches included, see below: Comprehensive self-service capabilities: • Self-Service Provisioning (Early Access available Q3 2025)	A suite of new features to help B2B customers deliver a smoother, faster and more secure onboarding experience across the full identity lifecycle—from initial setup to more secure offboarding. This includes automated inbound user and group provisioning, delegated admin capabilities, and automated session termination. Comprehensive self-service capabilities: • **Self-Service Provisioning:** helps enable your customers to more securely configure inbound SCIM connections to manage identities at their pace. ‘	Faster, smarter, and more secure customer onboarding with Auth0. • Accelerate customer time to value with self-service capabilities and automated Okta Integration Network (OIN) app setup to easily onboard customers at scale with minimal support. • Seamless and more secure admin experience that gives privileged users control over management of their users. • Market leading inbound user lifecycle management with support for Google Workspace and Group Provisioning

Announcement	Description	Importance
• Self-Service Org Domain Verification for Discovery (Early Access available Q4 2025) • Self-Service SSO Template (Generally Available Q4 2025) • My Organizations API (Early Access available Q4 2025) Market-leading inbound user lifecycle management: • Group Sync with Inbound SCIM (Early Access available Q4 2025) • Directory Provisioning for Google Workspace (Early Access available Q4 2025) Gain enterprise traction via Okta ecosystem: • Universal Logout (Now Generally Available) • Express Configuration (Generally Available Q4 2025)	• **Self-Service Org Domain Verification for Discovery:** helps enable customers to verify and associate domains with specific Auth0 Orgs. Users are automatically directed to the correct login flow across all connected apps, no re-verification required. • **Self-Service SSO Template:** Add additional IdP support (Okta SAML and Auth0 SAML) • **My Organizations API:** Allows privileged end-users to modify their Orgs and perform common delegated admin tasks (e.g., Org member and access management, security policy configuration) Market-leading inbound user lifecycle management: • **Group Sync with Inbound SCIM:** Sync user groups in real-time with out-of-box support for Workforce directory services that implement outbound SCIM. • **Directory Provisioning for Google Workspace:** Automatically provision and deprovision users from organizations that use Google Workspace as their workforce IdP. Gain enterprise traction via Okta ecosystem: • **Universal Logout:** Delivers out-of-the-box session termination for Auth0 apps, completing the identity lifecycle with more secure offboarding and compliance — no engineering required. • **Express Configuration:** Automates setup of Auth0 apps in the OIN, streamlining onboarding facilitating fast, error-free deployment for nearly 17,000 Okta customers.	• Complete the lifecycle more securely: Out-of-the-box session termination delivers compliance-grade offboarding, eliminating custom code while strengthening security for your customers.

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.