Whitepaper

Okta Secure Identity Commitment

Last updated: Dec 31, 2025

Contents

Executive Summary

Identity is the primary enterprise security entry point for all workforce and consumer applications. Unfortunately, the volume and complexity of attacks against entities large and small continues to accelerate. Detecting and protecting against these attacks is mission critical.

As a leading independent identity company, Okta is at the forefront of dealing with attacks. As a result, we have launched the Okta Secure Identity Commitment to:

- Provide market-leading identity products and services
- Harden our corporate infrastructure
- Champion customer best practices
- Elevate our industry

Under this initiative, we have already delivered or announced a number of important features and upgrades within both our corporate infrastructure and our product portfolio. A summary of these updates is detailed below.

We know that our work is never complete, and we will continue to invest as needed in proactive anticipation of, and in response to, the dynamic cyber threat landscape.

Introduction

When we founded Okta in 2009, we focused primarily on IT management and — in particular — on using identity as a means of connecting people with technology.

Since then, two major trends have driven a dramatic change both in how identity is regarded and, by extension, in the demand for identity solutions:

1. **Identity is now the primary enterprise security entry point** for all workforce and consumer applications.
2. **The volume and complexity of cyber attacks has grown**, with a range of threat actors, including ransomware groups, nation-state actors, and malicious insiders, developing advanced tactics, techniques, and procedures (TTPs) to bypass defenses and evade detection.

These trends have driven a significant shift for the industry and imposed on us the responsibility to evolve from connecting people with technology to serving as a critical entry point to protect every organization's important data. This responsibility is captured in **our vision to free everyone to safely use any technology.**

Okta Secure Identity Commitment

Identity has become mission-critical security infrastructure.

As a leading independent identity company, Okta is at the forefront of the fight against identity attacks. Our product, engineering, security, and business technology teams continually innovate our technology platform to protect our nearly 20,000 customers.

We are committed to continue leading the industry forward and to protect our customers and their most sensitive assets. As a result, we have launched the Okta Secure Identity Commitment. This commitment is built upon four pillars, shown below. The remainder of this document explains how we are delivering on our commitments.

Provide market-leading secure identity products and services	Harden our corporate infrastructure	Champion customer best practices to help ensure our customers are best protected	Elevate our industry to be more protected against identity attacks

Market-leading identity products and services

We relentlessly invest in keeping our platform secure—because the most trusted brands in the world rely on Okta to protect their people, partners, and data. Our security is their security.

Through this continuous focus, we help ensure that the trust invested in us is met with the strongest and most innovative protection measures. We've built and continue to enhance market-leading protections into our identity platform. For example:

- Okta, based on internal reporting from August 1st through October 31st, 2025, has **detected and blocked more than 1.5 billion identity-based attacks** using ThreatInsight, spanning credential stuffing, bot activity, and other identity-based threats.
- Over the same time period, our Enhanced Dynamic Zones (EDNZ) **blocked over 290 million malicious or risky access attempts**, including attacks via residential proxies and VPNs.

We also back this innovation with operational excellence, including:

- 99.99% uptime
- 24x7 global support
- Support for 10B+ logins per month

At Oktane 2025, we announced a host of customer security boosting advancements, including leading the introduction of how Okta brings the identity security fabric to life.

Since then, we have been steadily executing on a few key themes to further strengthen our products and services, including:

- **Govern AI agents through a unified control plane -** Okta for AI Agents (Early Access in Q1 CY26) provides an identity layer for the agentic era — to help bring AI agents into your identity security fabric to deliver visibility, control, and governance across your organization.
- **Trusted Digital Experiences for Okta Customer Identity -** Bring customers and partners into a unified identity security fabric that delivers end-to-end protection for all identities, bringing together phishing-resistant authenticators with real-time threat protection, and automated governance to enable continuous compliance and reduce risk.

- **Building the future of secure federal identity governance -** Okta recently reached significant compliance milestones. Okta Identity Governance and Workflows are now FedRAMP High authorized for Okta for Government High, and eligible Okta for Government Moderate customers, and DoD IL4 authorized for US Military customers. Identity Threat Protection is FedRAMP High and FedRAMP Moderate authorized and is supported for DoD IL4. (Last updated in February 2026).
- **Secure production-ready AI Agents -** Auth0 provides the identity foundation to secure AI agents and make your products AI-ready. WIth Auth0 for AI agents, you can get identity right from day one, leverage the full power of identity to scale your AI initiatives and the smart, tailored experiences your customers demand.
- **Enhancements to Auth0 for B2B -** A suite of new features to help B2B customers deliver a smoother, faster and secure onboarding experience across the identity lifecycle—from initial setup to secure offboarding. This includes automated inbound user and group provisioning, delegated admin capabilities, and automated session termination.

Launched since September 2025

Okta

Generally Available

- Okta Identity Governance
  - Security Access Review
  - Universal Logout for Access Requests
  - Continuous Access Evaluation (CAE) for Access Requests
  - Access Requests for AD Groups
  - Governance Delegates
  - Entitlement History
  - Resource Owners
  - Governance Labels
  - Approval Escalations
  - Unified Audit Reports in Access Certification
  - Redesigned Approver Experience for Access Requests
  - Export Reports as PDF
  - Authorized for Okta for Government High (FedRAMP High)
- Okta Privileged Access
  - Geographic expansion in EMEA
  - Password Character Exclusions
  - Access Certifications for Service Accounts
  - Tripled Coverage of SaaS apps that can be managed in OPA
  - Coarse-grain permissions for Active Directory and RDP
- Identity Security Posture Management (ISPM)
  - MFA and SSO analysis - Dashboard and graph
  - ISPM Visibility of Active Directory
- Identity Threat Protection (ITP)
  - Custom Admin Roles for ITP
  - ITP Landing Page
  - Improved Session Protection Controls
  - Suspicious Login From An IP Flagged By FastPass
  - Suspicious Login From an IP Flagged In Credential Based Attack
  - Breached Credential Detected

Auth0

Generally Available

- Auth0 for AI Agents
- Advanced Filtering in Security Center
- Enhanced Signup Bot Detection for Stronger Security and Seamless User Experience
- New Management API Endpoints to Configure Bot Detection Settings
- FGA Logging API
- Native to Web SSO
- Customizable Device Remembrance for Adaptive MFA
- Advanced Customization for Universal Login
- Native Passkey Enrollment with My Account
- Express Configuration
- Tenant Access Control List
- Docs & API Explorers
- Forms - Flows Auth0 Send Email Action
- New Private Cloud AWS Region in Thailand
- Private Cloud Performance 30x and 30x Burst (3,000 RPS) offering on Azure
- Improved Accuracy for Security Center Metrics

Early Access

- Passkey Login for Custom Databases With Import Mode Off
- Self-Service Provisioning - GA by April 30, 2026
- Auth for MCP
- Actions - Transaction Metadata - GA by March 31, 2026
- Ephemeral Sessions with Actions - GA on January 19, 2026
- Akamai Supplemental Signals

- Okta Device Access
  - Desktop MFA Recovery for Windows
  - Platform SSO support in macOS Setup Assistant
- Adaptive MFA
  - Universal Logout support for AMFA customers
- Breached Credentials Protection
- Network Restrictions for Token Endpoint

Early Access

- Cross-App Access
- Okta Identity Governance
  - On-prem apps: JDBC connector (limited EA)
  - Access Certifications for Service Accounts
- Okta Privileged Access
  - Active Directory Account RDP Domain Controllers
- Okta Account Management Policy support for Password Expiry
- User Enumeration Prevention (UEP) Challenge
- Support for Higher Assurance Certificates in Custom Domains

Okta Customer Identity

Generally Available

- Breached Credentials Protection
- Okta Identity Governance
- Advanced Directory Management
- Claims Sharing between Okta and External IdP

Early Access

- Okta Account Management Policy support for Password Expiry

*Please note that all roadmap items are subject to change. We will update customers regularly on the status of previously communicated projects.

Launched since May 2024

Okta

- **Govern Okta admin roles**: Deliver zero standing privileges for your Okta administrator privileges with time-bound, ad-hoc access requests for individual access and access reviews for existing administrators.
- **Require MFA to access the Okta Admin Console**: Prevent administrators from creating authentication policies that only require a single factor. Opt-in to prevent any single factor access to the admin console.
- **Require MFA for protected actions in Admin Console**: Provide an additional layer of protection for critical actions in Okta by requiring step-up authentication for admins to perform high-impact actions.
- **Allow admins to detect and block requests from anonymizing services**: Provide administrators the ability to allow or deny access based on an evaluation of whether a source IP address is associated with anonymizers, to strengthen an organization's control against unauthorized access through such sources.
- **Apply IP and ASN binding to Admin Console**: To thwart potential session takeovers of critical (first party) resources, Okta automatically revokes an Okta Admin Console session if the ASN (Autonomous System Number) observed during an API or web request differs from the ASN recorded when the session was established. Customer administrators are also able to automatically revoke an administrative session if the IP address observed at session creation changes during an active session within the following Okta products: Workflows Admin, Okta Access Requests (Inbox), Okta Privileged Access (OPA), Okta Admin Console.
- **Enforce an Allow-listed Network Zone for APIs**: Restrict attackers and malware from stealing SSWS tokens, and from replaying them outside of the specified IP range in order to gain unauthorized access.
- **Enforce token binding for M2M application service integrations**: Okta has enhanced the security of automated transactions by enforcing, by default, token binding in machine-to-machine (M2M) integrations using proof of possession to help ensure that only authenticated applications can use tokens to access Okta APIs.

- **Prevent account lockout for Okta users**: Okta has provided a feature to block suspicious sign-in attempts from unknown devices. When the feature is enabled, it prevents legitimate users (including admins) from being locked out if another device that is unknown to Okta causes a lockout.

Auth0

- **Fine Grained Authorization**: Enables user collaboration and access control with unmatched granularity and easy-to-use APIs, while being fast, scalable, and flexible.
- **Fourth-generation Bot Detection with Okta AI**: Incorporating third-party risk signals and an updated Machine Learning (ML) model, the new version of Bot Detection will have fine-tuned models specifically designed to protect against fraudulent registrations.
- **Highly Regulated Identity (HRI)**: Elevated security, privacy, and UX controls for sensitive customer interactions beyond login. Navigate security and compliance for high-risk customer scenarios like updating account information, accessing open banking payment, and sending money – while meeting end-users' experience expectations.
- **Auth challenge**: Reduce bot activity with Auth Challenge, which uses browser and device signals to make it more challenging for bots compared to traditional CAPTCHAs.
- **Require MFA for all dashboard admins**: Previously, MFA was an optional requirement for Auth0 administrators; MFA is now mandatory for all admins with a username/password-based login or third-party social login.
- **Extend OIDC Back-Channel Logout with Initiators**: Adds Account Deleted and Email Changed events to the existing list of logout initiators (Password Changed, Session Expired, and various Logout events), which hook up to session termination events to request applications log out users whenever that session is invalidated.
- **Enforce ASN binding for Auth0 admin sessions**: Okta will automatically revoke an Okta Admin Console session if the ASN (Autonomous System Number) observed during an API or web request differs from the ASN recorded when the session was established.

- **Manage session and refresh token management API**: Gives centralized access to the list, management, and revocation of user permissions across applications. In the event that a business suspects a session has been hijacked, they can preemptively revoke the session — protecting their customers and organization.
- **Define progressive factor enrollment for end-users**: Using a Post-Login Action, businesses can define the secondary factors their end-users must enroll into MFA, enabling customers to exert greater control over authentication policies that align with their security objectives.

Launched since July 2024

Okta

Generally Available

- **Okta Identity Security Posture Management (ISPM) (GA, North America)**: Proactively reduce your identity attack surface by identifying and prioritizing risks like excessive permissions, misconfigurations, and MFA gaps across your identity infrastructure, cloud, and SaaS apps.
- **Identity Threat Protection with Okta AI**: Enhance your identity's resilience post-authentication by continuously assessing risks on your identities. Leverage integrated signals from first-party and third-party partners to proactively counter emerging threats from any origin post-authentication.
- **Expand in-product best practice guides**: Okta will provide additional in-product guides to help customers implement best practices to protect their Okta tenants.
- **Enforce MFA for first-party administrator app access**: The admin console policy is now applied to first-party admin apps across Okta access certifications, Okta entitlement management, Okta Access Requests Admin. Access to these apps will require MFA. This is an opt-in feature.
- **Secure agent deployment for Active Directory**: Upgrading AD Agent to leverage an OIDC Proof of Possession-based approach to communicate with Okta and prevent unauthorized parties from accessing sensitive information.

- **Yubico Enterprise Onboarding**: Enhance your organization's security with Okta and Yubico by automating seamless phishing-resistant onboarding and FIDO2 Yubikeys for new and existing employees.
- **Trusted App Filters for FastPass**: Control which binaries may invoke FastPass in the language expression field within the authentication policy to help protect your org from local attack vectors, which include malicious binaries that invoke the Okta Verify loopback server.
- **Authentication Method Chain**: When you add an authentication policy rule, you can create an authentication method chain. This requires users to verify with multiple authentication methods in a specified sequence.

Auth0

Generally Available

- **Enhance Bot Detection on password recovery**: Introduce the option for customers to enable Bot Detection on password recovery flows (in addition to sign-up and sign-in, which already exist) to add an extra defense against account takeover attempts.
- **Log Service: Prioritized Logs and SIEM integration**: Enables streaming of important security events without interruption. Stream out security events to third parties with higher confidence and integrate with SIEM tools seamlessly.
- **Thresholds within Security Center Dashboard**: Baseline trend and anomaly monitoring on existing attack vectors in Security Center.
- **Enhanced Sign-Up Attack Detection for Bot Detection with Okta AI**: Incorporates third-party risk-scoring to further improve the ability to detect bots. Fine-tuned models are now specifically designed to combat sign-up fraud.
- **Account Level Audit Logs**: Provide visibility for customers to monitor at the account level for audit purposes rather than just at the tenant level.
- **Define organization session timeouts**: Customize session timeouts using additional logic, including Organization.
- **Detect and Mitigate IP Rotation Attack**: Leverage Bot Detection to trigger mitigation when it detects patterns of IP rotation from an attacker.

Launched since October 2024

Okta

Generally Available

- **Secure Identity Integrations**: Enhance security and reduce development time with 125+ new SaaS application integrations that bring advanced security to some of the biggest SaaS applications.
- **Okta ISPM**: Improved detections (SSO bypass): Strengthen security with enhanced detection capabilities to identify and block SSO bypass attempts, reducing unauthorized access risks.
- **Workflows authorized for Okta for Government High (FedRAMP High)**: Okta Workflows is designed to deliver significant value by automating and orchestrating processes to free up time and save costs across your agency.

Early Access

- **Secure SaaS Service Accounts**: Discover, vault, and control service accounts across your SaaS ecosystem to help reduce risk and eliminate standing privileges.
- **Out-of-the-box integrations for Identity Verification (Persona)**: Accurate Identity Verification to minimize risk of social engineering and deepfake attacks.
- **Governance Analyzer with Okta AI**: Drive better governance outcomes by leveraging signals from across Okta's unified platform.
- **Expanding phishing-resistant policies across onboarding and recovery**: Expand the same authentication policies typically applied to applications to the process of factor recovery to protect against phishing attacks.

Okta Customer Identity

Early Access

- **Passkey autofill**: Offer users a seamless, one-step login experience with passkeys directly from their autofill prompt—no extra clicks—to combine secure, phishing-resistant authentication with a streamlined user experience.

Auth0

Generally Available

- **Customer-Managed Keys**: Provide customers with the ability to securely replace and manage their tenant's top-level encryption keys, including BYOK (Bring Your Own Keys) and CYOK (Control Your Own Keys).
- **Forms**: Empower developers and marketers with a no-code visual editor to orchestrate, customize, and better secure signup and login flows to meet their unique needs.
- **Customize sessions with extensibility**: Define custom behaviors based on risk signals to revoke suspicious sessions, and set policies to detect and respond to hacking by leveraging the Session Management API with our Actions Extensibility platform.

Early Access

- **Self-Service SSO**: Provide your business customers with a hosted workflow to configure single sign-on (SSO) access to your SaaS app that works with most major identity providers.
- **Universal Logout**: Instantly terminate sessions across all devices and supported apps to mitigate session hijacking risks and improve security standing.

Okta & Auth0

Generally Available

- **Secure Identity Assessment**: Work directly with Okta experts to take control over your identity debt and close security gaps—like admin sprawl, misconfigured permissions, or shadow IT—before they become a security threat.

Launched since January 2025

Okta

Generally Available

- **Okta Personal for Workforce**: Provide free password manager as a perk for employees and maintain security hygiene by separating employees' personal apps from work apps.
- **Smart card just-in-time provisioning**: Pre-configure smart card attributes, allowing users to freely join other organizations without admins having to go through additional steps.
- **Yubico FIDO Pre-reg**: Protect your organization from modern identity attacks by implementing advanced phishing resistance across the organization with pre-enrolled FIDO2 Yubikeys.
- **Okta Account Management Policy**: Leverage the Authentication Policy (ASoP) to define the assurance requirements a user must meet to perform authenticator enrollment, password reset or unlock account operations.
- **Okta Identity Security Posture Management (ISPM) Enhancements**
  - **Enhanced MFA Insights and Graphs:** We've expanded our existing MFA monitoring with new unique, identity-focused insights, including app-level MFA coverage detection, login path analysis between direct and SSO access, enhanced visualization of authentication methods, and context-aware MFA requirement tracking. These additions provide deeper visibility into your authentication security posture and help identify potential MFA gaps more effectively.
- **Workflows Post-Audit for FedRAMP High**: Authorization expected for Workflows, which offers U.S. public sector organizations low- and no-code ways to build and manage complex functions, maintain compliance standards, and improve experience management.
- **Identity Threat Protection with Okta AI**
  - **New Identity Threat Protection Integrations**: Leverage new Shared Signals Framework (SSF) integration with Omnissa (Workspace One UEM). Plus, a new Universal Logout integration with SURF Security.
  - **Universal logout support for Auth0-powered applications**: Automatically log users out of their Auth0-powered apps when a logout or de-provisioning event occurs in Okta Workforce Identity.

- **Out-of-the-box integrations for Identity Verification**
- **Persona integration**: Trigger Persona identity verification flows at key points in the employee lifecycle—such as onboarding, authentication, and account recovery–to minimize the risk of social engineering and deepfake attacks.
- **Okta Device Access**
  - **Just-in-time Local Account Creation for macOS**: Enable users to create local macOS accounts with standard or administrator privileges to facilitate low-touch account management, especially for shared devices.
  - **FIDO2 Security Keys for Desktop MFA for Windows**: Secure the Windows login experience by allowing end users to use a FIDO2 security key, a high security assurance authenticator, to meet their Desktop MFA challenge.

Early Access

- **Collections with Entitlement Management**: Package multiple apps and groups together, simplify requestor and approver experience, and onboard new partners and special projects in a fraction of the time.
- **Secure Partner Access**: Enable business partners to securely and seamlessly access shared resources without requiring significant development, customization, and management tasks from IT.
- **Authentication method chain**: Enhance security and reduce the risk of account compromise by requiring a specific order of authentication methods for application access..
- **On-prem Connector**: An out-of-the-box connector that allows customers to integrate their on-prem apps with Entitlement Management, enabling the discovery, visibility, and management of fine grained application entitlements within Okta.
- **Enhanced Group Remediation for Access Certs**: A feature update to Access Certifications that provides OIG customers with the ability to automatically remediate user access to group assigned apps.
- **Preconfigured Access Certification campaigns**: provides OIG customers with the ability to easily initiate use case specific access review campaigns with just one click. Two preconfigured campaigns are available during EA: Discover and remediate inactive users, and Okta Administrator Review.

Auth0

Generally Available

- **Bot Detection upgraded with user agent and tenant-specific signals**: Integrates user agent and tenant-specific signals into Okta's proprietary ML model, enhancing Bot Detection accuracy and effectiveness without adding friction for legitimate users.
- **Tenant Logs for Action Failures**: Monitor tenant action failures via audit and provisioning logs
- **Credential Guard on Azure**: Detect stolen credentials fast to prevent takeovers now available on Azure Private Cloud.
- **OTP passwordless authentication for email and SMS**: Enable end users to verify their email account on sign-up using a one-time password (OTP) code, and to reset their password using an email-delivered OTP instead of a link.
- **Guardian App & SDK — Mobile Enrollment for Push**: Provide ways for end users to register the Guardian App push notification factor without having to scan the QR code with their device.
- **Auth0 Integration with Okta Universal Logout**: Enable organizations using Okta as their IdP to automatically log users out of their Auth0-powered apps whenever a logout or de-provisioning event occurs in Okta Workforce identity.
- **Machine-to-Machine Access for Organizations**: Allows B2B SaaS providers to open up their APIs, enabling machine-to-machine (M2M) use cases while allowing access to sensitive data and operations of each Organization to be restricted to authorized parties.
- **Custom Email Provider**: Configure custom email providers and customize emails so they can have full control of the email delivery process.
- **Email OTP Verification**: Send users a one-time password via email for secure authentication.

Early Access

- **Tiered Alerting on Anomalies in Security Center**: Set thresholds on important security metrics, and configure when and how to get alerted based on these thresholds, so that you can take action in the event of a potential security anomaly or attack.
- **Improve onboarding and integrations with Custom Token Exchange External Tokens**: Provides a flexible solution using Actions that allows customers to provide their custom logic to control Token exchange (an Oauth grant-type).
- **Client Initiated Backchannel Authentication (CIBA)**: Provide the means to proactively reach out to users via a notification for them to authenticate and authorize access.
- **Verify Mobile Driver's License (mDL)**: Present mobile driver's license (mDL) verification request to end-users and verify mDL within your application.

Launched since March 2025

Okta

Generally Available

- **Desktop MFA Recovery for macOS**: Prevent productivity disruption by securely enabling admins to provide end users with time-limited recovery codes to login to their devices in the event of a lost phone or security key.
- **Identity Security Posture Management**
  - **Enhanced Non-Human Identity Analytics**: Expands monitoring capabilities with advanced visualizations and insights for non-human identities across your enterprise platforms. This comprehensive view unifies visibility into service accounts from Azure Active Directory and Salesforce, along with AWS API keys, helping security teams quickly identify and remediate potential risks in automated system access.

  - **Role-Based Access Control Capabilities**: Introduces granular role-based access controls designed specifically for complex, multi-org environments. This enhancement enables large enterprises to efficiently delegate detection management and remediation workflows across business units while maintaining centralized security oversight, aligning with hub-and-spoke governance models.
  - **Support for risky misconfigurations for AI Agents**: Gain comprehensive visibility into AI agent security posture, enabling secure, large-scale deployment of the digital workforce while maintaining robust identity security controls.

- **Identity Threat Protection with Okta AI**
  - **ITP Detections for Adaptive MFA Super Admins**: Instantly detect IP and device context changes for super admin roles, so you can act fast before threats escalate.
  - **SSF Receiver Integrations for Adaptive MFA SKU**: Leverage event signals from across your tech stack to dynamically adjust authentication requirements.
  - **Expanded SSF Partner Support**: Okta now supports event signals from SquareX and Widefield Security, enhancing threat detection with broader coverage across third-party security tools.
- Okta Identity Governance, Workflows, and Identity Threat Protection with Okta AI audit-ready for Okta for US Military (DoD Impact Level 4). Identity Threat Protection with Okta AI also audit-ready for Okta for Government High (FedRAMP High) and authorized for Okta for Government Moderate (FedRAMP Moderate).

Early Access

- **Device Assurance**
  - **Android Device Trust**: Enforce an extensive array of device signals on Android via Device Assurance policies.
- **Active Directory Accounts in Okta Privileged Access**: Reduce risks associated with undermanaged privileged Active Directory accounts. Okta Privileged Access will discover accounts and manage the passwords, enforce access controls such as RBAC, MFA, Access Requests and Check-Out with time-based-limits, while also providing an audit trail for monitoring and compliance.

- **Advanced Posture Checks**: Collect and assess the device context that you require—on any Windows or macOS device attribute or security setting—so you can further strengthen Zero Trust security during authentication.
- **Enhanced Dynamic Network Zones (Residential Proxy / Blockchain Support)**: Extended IP Enrichment support for such things as Residential Proxies to prevent unwanted traffic from accessing Okta resources.
- **Out-of-the-box integrations for Identity Verification**
  - **Incode & CLEAR integrations**: Trigger identity verification flows at key points in the employee lifecycle—such as onboarding, authentication, and account recovery–to minimize the risk of social engineering and deepfake attacks.
- **Okta Identity Security Posture Management**
  - **Self serve add connectors**: Empower security teams to independently expand ISPM coverage across multiple tenants and integrations without vendor assistance, accelerating time-to-value.
  - **Role Based Access Control - App admin and source integrator**: Delegate targeted remediation capabilities to application owners using role-based access controls that limit visibility to only relevant security findings, improving cross-team collaboration.
  - **MFA and SSO deep analysis dashboard and org graph**: Consolidate authentication security metrics across your entire identity landscape with granular per-app reporting on MFA adoption, phishing-resistant factors, and SSO validation.

Okta Customer Identity

Early Access

- **IdP single logout**: Allow end users to log out of multiple apps and external identity providers simultaneously with one click for a secure and seamless experience.
- **Network restrictions for OpenID Connect Token Endpoints**: Prevent token stealing and replay attacks by enforcing network restrictions on the token refresh endpoint.

Auth0

Generally Available

- **Active Session Management for Dashboard users**: Allows the developer to reject any unknown sessions and have full control over their account and logged-in sessions in both public and private cloud.
- **Breached Password Detection on Password Reset Flow**: Detect and block compromised passwords during reset to prevent account takeovers.
- **FAPI 2 Security Profile conformance testing and certification (Financial Grade APIs by the OpenID foundation)**: Deliver advanced API protections to protect privacy and prevent transaction tampering.
- **Teams support for Security Policies with SSO Enforcement in Private Cloud**: Manage security policies and enforce SSO for teams in Private Cloud.
- **Google Credential Manager support using Google Token Exchange**: Enable seamless authentication with Google Credential Manager using Google Token Exchange for secure access.

Early Access

- **Client Assertion JWT for the OIDC Enterprise Connection**: Enable more secure single sign-on (SSO) for business customers by using asymmetric cryptography (private/public key encryption) in which Auth0 stores the secret as opposed to it being transferred in the authentication request.
- **Customer-Provided Signature Public Keys**: Facilitate migrating from legacy identity providers to Auth0 by allowing customers to import their legacy public signature keys to their Auth0 tenant.
- **Self-Service Domain Verification/HRD**: Provides your business customers with a hosted workflow to independently manage their Home Realm Discovery and domain verification process.
- **Passkey login for custom databases with import mode off**: Customers using external custom databases where identities are not being imported to Auth0 will be able to offer passkey authentication for the digital identities in those custom databases.

- **Secure Tenant-level Access Control list**: Provide the ability for customers to block traffic from specific IPs, Classless Inter-Domain Routing (CIDR) blocks, and geographies to help combat DDOS attacks by blocking requests at the edge.
- **Federated logout for OIDC and Okta Connections**: Make use of simplified Federated Logout integrations with Okta Workforce identity Cloud and OpenID Connect identity providers.
- **Limit M2M Usage Per Client & Organisation**: Applies M2M token quota per App/Client to stop ill-behaving Apps to consume the tenant quota. This will provide more control especially for scenarios where 3rd Party M2M Apps access our customer APIs.
- **Native to Web SSO**: Streamline the customer experience by eliminating the need to re-login when moving from a mobile app to a web app. Leverage Auth0's built-in security features—including DPoP and App Attestation (for GA)—to enable a more seamless and secure Native to Web SSO experience.
- **Step-up authentication for sensitive tenant flows**: Get an additional layer of security and control for user's authentication processes.
- **Tenant Access Control List:** Create and manage rules that control access to your app. When a request matches a rule, it can allow, block, or redirect the request. Helps reduce risk by blocking or redirecting traffic based on customer-defined, self-serve rules using signals such as IP, CIDR ranges, Geography, User Agent, and TLS fingerprints (JA3/ JA4).

Developer Preview

- **Auth for GenAI**: Build your GenAI applications securely. Auth for GenAI is a suite of features that allows you to ensure that your AI agents can securely call APIs on behalf of your users, both interactively and asynchronously, by requesting for the right and least privileged access to users' sensitive information.

Launched since July 2025

Okta

Generally Available

- **Okta Identity Governance**
  - **Separation of Duties:** Help organizations spot and stop risky combinations of access in critical applications, reducing fraud and risk
  - **Resource Collections:** Provide a package of all the resources and access that a user needs to perform a role or project
  - **Govern Okta Admin Roles:** Apply the principle of least privilege access to Okta admin roles by requiring a request-and-approval process before granting time-bound admin permissions. Regularly review and certify any standing access to admin roles.
  - **Authorized for Okta for Government High (FedRAMP High)**
- **Okta Identity Security Posture Management**
  - **Geographic Expansion across EMEA and APJ**: Global availability across EMEA and APJ region.
- **Adaptive MFA**
  - **Integration with Palo Alto Networks Prisma Access Browser**: The native integration creates a new conditional access method to restrict access to SSO apps by using only the secure browser.
- **Identity Threat Protection with Okta AI (ITP)**
  - **Shared Signals Framework (SSF) Transmitter**: Use Okta's identity signals to trigger automated actions (e.g., session revocation, MFA challenge) in third-party tools, like Apple Business Manager, accelerating incident response workflows.
  - **ITP Workflows Connector**: Take real time, automated actions in response to ITP detections, with rich context and detailed insights about the event. Responses include, but are not limited to, suspending users or sending detailed notifications to security teams.
  - **Authorized for Okta for Government Moderate (FedRAMP Moderate):** ITP has achieved FedRAMP Moderate Authorization, marking a significant milestone for the public sector and reinforcing Okta's commitment to security and compliance

- **Okta Access Gateway (OAG)**
  - **OAG Secure-By-Design Changes**: The OAG admin console is only accessible on the local network by default and requires an admin password change for both the console and Command Line Interface (CLI).
- **Granular Admin Permissions to Access Identity Providers**: Admins can now assign specific IdPs to other admins using granular permissions, enhancing security by limiting access to IdP configurations for only authorized users.s
- **Policy Updates as Protected Actions**: When App Sign-On, Global Sign-On, ITP, or Account Management policies are updated in the admin console, admins must complete step-up authentication. This prevents unauthorized changes by bad actors with access to an admin session.

Early Access

- **Okta Identity Governance**
  - **On-prem Connector for Oracle EBS**
    On-prem Connector for Oracle EBS connects Oracle EBS on-premises apps with Okta Identity Governance. It helps admins discover, view, and manage Oracle EBS entitlements directly in Okta.
  - **Unified Requestor Experience**
    Unified Requestor Experience for requesting access in Slack, Teams and the end user dashboard catalogue for both Access Request conditions and Request Types.
- **Okta Privileged Access**
  - **Support for RDP w/ Active Directory accounts**: Launch RDP sessions using Active Directory accounts without exposing passwords, with built-in policy controls for MFA and access requests.
  - **On-demand credential rotation**: Allow authorized users to rotate credentials immediately in response to risk, without waiting for scheduled changes.
- **Identity Threat Protection with Okta AI (ITP)**
  - **Custom Admin Roles for ITP**: Enforce least-privilege access with precise, scoped admin permissions for managing ITP configurations, such as who can manage user sessions, configure risk policies, or set up Shared Signals Framework (SSF) integrations.
- **Breached Credentials Protection (Phase 2)**: Customizable responses

to breached credential events with the ability for admins to validate the breached credential flow using a test account.

- **Network Restrictions for Token Endpoint**: Enhance security by allowlisting network zones per client to restrict token requests to trusted IPs and defend against replay attacks, token theft, DoS, and rate limit abuse.

Okta Customer Identity

Early Access

- **Network Restrictions for Token Endpoint**: Enforce network restrictions thereby enhancing security to protect customers from token relay attacks and theft.
- **Universal Logout for Okta Customer Identity Apps**: An out-of-the box solution that automatically logs users out without having to build anything additional thus improving security and user experience.
- **Cascading of the Single Logout Request to External IdP**: Automatically log users out of external identity providers when they log out of an Okta-connected application configured for Single Logout, improving security for shared devices.
- **Claims Sharing between Okta and External IdP**: Simplify the user login experience by potentially removing the need for users to enroll extra security steps in Okta if those steps have already been completed with their primary identity provider, all while ensuring a secure connection.
- **Overlapping IdP Signing Certificate**: Allows multiple active signing certificates for each external identity provider, making certificate updates seamless and preventing downtime for federated logins, improving security and reliability.
- **OIDC Token Encryption**: Safeguards data from unauthorized access during transmission by allowing Okta to encrypt sensitive user information within OIDC tokens using industry-standard methods when communicating with other trusted apps.

Auth0

Generally Available

- **Client-Initiated Backchannel Authentication (CIBA)**: Also known as a

decoupled authentication flow, CIBA enables a client application to initiate the authentication process on behalf of the customer.

- **Ephemeral Sessions in Actions**: Dynamically configure whether a session should expire when the browser is closed. Define ephemeral sessions per client, organization, connection, or by any custom business logic within Actions.
- **Session and Refresh Token Metadata**: Attach and persist metadata within a user's session or refresh token. This metadata can be used across authentication flows to provide additional context and flexibility in session management.
- **Passkey Enhancements**: Support on Custom DB Connections with Import Mode Off: Auth0 customers using custom database connections with import mode set to off will be able to allow end-users to sign up with and log in with passkeys.
- **Enhanced Bot Detection Accuracy and Reduced Friction:** Enhanced bot detection to reduce false positives for VPN users, improving accuracy and minimizing friction even on shared IPs or anonymized networks.
- **FAPI v2 Certification:** Provide support for Financial Grade Identity beyond standard OAuth2 and OpenID Connect protocols. Our FAPI v2 certification makes it easier to better secure your APIs to support compliance for Financial Services' transactions and other sensitive, high-risk scenarios.

Early Access

- **Enhanced Security Incident Management through Auth0 Guide**: Enrich Attack Protection capabilities with "intelligent" security summaries and insights from Auth0 Guide – ask about Security Center data and investigate the cause of alert notifications received.
- **DPoP (Demonstrate Proof of Possession)**: Protect access and refresh tokens by constraining them cryptographically to the application that they are issued to.
- **Advanced Customization for Universal Login (ACUL)**: Customize the sign-up and sign-in experience across every app, device, and digital journey, and leverage application and user information to deliver the best user experience.
- **Multiple Custom Domains**: Enable multiple B2C brands and white-labling B2B brands to have different tailored and branded user experiences across channels (UL, email, etc.).

- **Passkey Enhancements**: Enrollment API: Add support for Native Passkeys to API-driven flows, enabling easy-to-use, phishing-resistant authentication into native mobile experiences. Expands the native passkey signup and login capabilities to include ad hoc enrollment, enables developers to implement enrollment methods, and prompts at different points in their applications.
- **Non-Unique (Shared) Email Addresses for Identities**: Allow multiple user accounts to share the same email address within a database connection. Instead of using email as a unique identifier, accounts must be distinguished by either a username or phone number.
- **Native Passkey Management using My Account API:** The enhancements are designed to give you granular control and flexibility over passkey implementation. This enables even more seamless and secure authentication experiences within your custom applications.
- **Right-to-Left Language Support with additional language translations in UL and Guardian:** End-user authentication interfaces (Universal Login and Guardian) will support right-to-left language support along with several new right-to-left languages including Arabic, Hebrew, and more.

Launched since September 2025

Okta

Generally Available

- **Okta Identity Governance**
  - **Security Access Review:** Examines user access to sensitive resources manually or automatically via admins using the Admin Console or APIs. Prioritizes reviews based on criticality and anomalies to investigate, confirm, or revoke access in response to security incidents.
  - **Universal Logout for Access Requests:** Supports Universal Logout within the Okta Access Requests web app. Allows admins to automatically sign users out of the application when a Universal Logout event is triggered.

- **Continuous Access Evaluation (CAE) for Access Requests:** Refreshes user sessions periodically to invoke sign-on policy evaluations. Prompts users to re-authenticate if the current policy requirements are no longer met.
- **Access Requests for AD Groups:** Enables users to request access to AD groups directly through Request Conditions. Uses bi-directional sync to automatically add or remove users, facilitating efficient and time-bound access management.
- **Governance Delegates:** Enables super admins and users to assign a delegate to manage tasks like access certification reviews and access request approvals. Provides process continuity for Request Types, Request Conditions, and Access Certifications by assigning future tasks to the delegate when the original approver is unavailable.
- **Entitlement History:** Provides a chronological timeline of user entitlement assignments and unassignments for enabled applications. Offers a clear audit trail to track historical access for specific users and timeframes.
- **Resource Owners:** Automates Okta Identity Governance (OIG) configuration by assigning owners to apps, groups, and entitlements. Enables the automatic assignment of reviewers for Access Certifications and approvers for Request Conditions based on owner-assigned resources.
- **Governance Labels:** Categorizes resources like apps, groups, entitlements, and collections using the Labels API. Uses key-value labels to automate and simplify the management of Access Certifications.
- **Approval Escalations:** Allows end users to escalate requests to an approver's manager if the primary approver is unavailable. Helps ensure users are not blocked from accessing critical resources for Request Types and Request Conditions.
- **Unified Audit Reports in Access Certification:** Simplifies the generation of compliance audit data by providing a single location for all reporting needs. Reduces the time required for audit readiness within Access Certifications.
- **Redesigned Approver Experience for Access Requests:** Streamlines the approval process by presenting critical information and calls-to-action upfront. Enhances visibility for Request Types and Request Conditions by providing direct access to request details, emails, and integrated Slack messages.

  - **Export Reports as PDF:** Allows OIG-specific reports to be exported in PDF and CSV formats with customizable columns. Includes a cover page on PDF exports with metadata such as report type, organization name, and timestamps for internal audit stakeholders.

- **Okta Privileged Access**
  - **Geographic expansion in EMEA:** A new preview environment powered by the OP2 cell, offering the EMEA region the ability to test implementations and gain confidence before going live.
  - **Password Character Exclusions:** Gives administrators control to prevent password rotation failures by configuring the system password generator to exclude specific symbols that are not supported by target systems.
  - **Access Certifications for Service Accounts:** Okta Identity Governance can run certification campaigns for service accounts stored in the OPA vault.
  - **Tripled coverage of SaaS apps that can be managed in OPA:** There are now 45 validated applications for OPA. Here is the full list of supported apps.
  - **Coarse-grain permissions for Active Directory + RDP:** Control local server permissions for AD accounts just-in-time when a user is accessing a domain-joined server with RDP.
- **Identity Security Posture Management (ISPM)**
  - **MFA and SSO analysis - Dashboard and graph:** Security leaders gain granular MFA and SSO analysis in an exportable dashboard to identify top trends and risks.
  - **ISPM Visibility of Active Directory:** Security teams gain visibility into Active Directory identities, groups, and their risks to reduce attack surface.
- **Identity Threat Protection (ITP)**
  - **Custom Admin Roles for ITP:** Enforce least-privilege access with precise, scoped admin permissions for managing ITP configurations, such as who can manage user sessions, configure risk policies, or set up Shared Signals Framework (SSF) integrations.
  - **ITP Landing Page:** A converged experience to easily navigate to all features in ITP. Easily discover new features, understand configurations, and tune controls to streamline your deployment and strengthen security posture.

  - **Improved Session Protection Controls:** Admins can configure which session context changes initiate policy re-evaluation, providing granular control based on organizational risk tolerance.
  - **Suspicious Login From An IP Flagged By FastPass:** This detection indicates that a sign-in event occurred from an IP address that Okta FastPass flagged in a phishing event.
  - **Suspicious Login From an IP Flagged In Credential Based Attack:** This detection indicates that a successful sign-in event occurred from an IP address where multiple sign-in failures also occurred.
  - **Breached Credential Detected:** This detection indicates that a username-password combination in your org appears in a third-party list of public data breaches.
- **Okta Device Access**
  - **Desktop MFA Recovery for Windows:** Prevent productivity disruption by securely enabling admins to provide end users with time-limited recovery codes to login to their devices in the event of a lost phone, security key, etc.
  - **Platform SSO support in macOS Setup Assistant:** Deliver an enhanced device onboarding experience that automatically creates a local macOS account enrolled in Desktop Password Sync, leveraging Okta user profile attributes and credentials.
- **Adaptive MFA**
  - **Universal Logout support for AMFA customers:** Universal Logout allows admins to sign users out of all federated apps and devices if suspicious activity is detected.
- **Breached Credentials Protection:** Customizable responses to breached credential events with the ability for admins to validate the breached credential flow using a test account.
- **Network Restrictions for Token Endpoint:** Enhance security by allowlisting network zones per client to restrict token requests to trusted IPs and defend against replay attacks, token theft, DoS, and rate limit abuse.

Early Access

- **Cross-App Access:** New, open protocol to securely manage how AI agents and apps connect to each other by shifting access control from the app to the IdP.

- **Okta Identity Governance**
  - **On-prem apps: JDBC connector (limited EA):** Out-of-the-box connector for LCM provisioning and Entitlement Management for generic databasesDBs. via a "JDBC connector."
  - **Access Certifications for Service Accounts:** Certify whether users should retain access rights to SaaS/Okta/AD service accounts managed in Okta Privileged Access using Okta Access Certifications.
- **Okta Privileged Access**
  - **Active Directory Account RDP Domain Controllers:** Officially support the OPA Agent on Domain Controller hosts, so RDP access to Domain Controllers can be protected with OPA
- **Okta Account Management Policy support for Password Expiry:** Expanded protection for password expiry flows in the OAMP policy. Enable greater control over assurance requirements when the end-user's password expires or is compromised.
- **User Enumeration Prevention (UEP) Challenge:** Admins can now select stronger factors for UEP challenges (e.g. OV push, FastPass) – beyond the password.
- **Support for Higher Assurance Certificates in Custom Domains:** Use of Custom Domains requires that customers configure a certificate provided via Okta or Certificate Authority - this will allow for SHA-384 and SHA-512 certificates. Gain assurance of authenticity and integrity with enhanced security certificate encryption options.

Okta Customer Identity

Generally Available

- **Breached Credentials Protection:** Let admin tailor user experiences and verify workflows using test accounts, improving both security and operational confidence.
- **Okta Identity Governance:** Enable secure onboarding and governance for customer identities with Okta. Help ensure compliance and audit requirements are met to so only the right identities have the right level of access.
- **Advanced Directory Management:** Securely manage B2B customers' access to shared applications at scale. Extend strong security controls like passwordless authentication to protect customer access and delegate user management and app assignments to optimize IT operations.

- **Claims Sharing between Okta and External IdP:** Enhance identity federation by enabling secure, seamless access to resources across Okta and third-party IDPs without compromising security.

Early Access

- **Okta Account Management Policy support for Password Expiry:** Provides greater control over your customers' password security. This feature expands the Okta Account Management Policy (OAMP) to include password expiration, allowing you to enforce stronger security requirements when a password expires or is compromised.

Auth0

Generally Available

- **Auth0 for AI Agents:** Auth0 for AI Agents provides a single plane to manage user authentication, fine-grained permissions and human-in-the-loop workflows. With Cross-App Access available out of the box, executives can have confidence and security in AI agents.
- **Advanced Filtering in Security Center:** Anomaly monitoring on expanded attack vectors in the Security Center dashboard through filter categories, list groupings of events by multiple categories for incident analysis. Provides more granularity to existing metric so customers can better troubleshoot and triage incidents.
- **Enhanced Signup Bot Detection for Stronger Security and Seamless User Experience:** improved machine learning (ML) model for signup to deliver stronger protection against automated account creation while keeping friction low for legitimate users. Includes expanded detection signals, smarter traffic classification, and optimized sensitivity settings.
- **New Management API Endpoints to Configure Bot Detection Settings:** Auth0 now provides Management API endpoints to manage Bot Detection configuration, configure bot detection controls, challenge policies, and CAPTCHA management.
- **FGA Logging API:** The Auth0 Fine-Grained Authorization (FGA) Logging API enables users to query access logs that capture all operations across five FGA endpoints - Write(), Check(), BatchCheck(), ListUsers() and ListObjects().
- **Native to Web SSO:** Enables seamless authentication between native mobile apps and web apps, eliminating the need for users to re-enter credentials when switching between them.

- **Customizable Device Remembrance for Adaptive MFA:** Adaptive MFA now allows administrators to configure device remembrance durations (TTL) for the New Device assessor; the default can be customized to any value between 1–365 days.
- **Advanced Customization for Universal Login:** Advanced Customization for Universal Login enables you to build custom, client-rendered interfaces for Universal Login screens, allowing you to control all aspects of your Universal Login experience.
- **Native Passkey Enrollment with My Account:** Native Passkey Enrollment enables users to add a passkey to their account using APIs; applications can fully manage user onboarding of passkeys. This feature is the first of many capabilities being added to My Account.
- **Express Configuration:** Express Configuration enables enterprise customers to securely configure identity integrations with SaaS applications without the need to copy and paste protocol-specific configuration values.
- **Tenant Access Control List:** Create and manage rules that control access to your app. When a request matches a rule, it can allow, block, or redirect the request. Helps reduce risk by blocking or redirecting traffic based on customer-defined, self-serve rules using signals such as IP, CIDR ranges, Geography, User Agent, and TLS fingerprints (JA3/ JA4).
- **Docs & API Explorers:** Refreshed Docs & API explorer experience with a host of new benefits for developers. This feature improves search and discoverability, provides AI native capabilities (eg. LLMx.txt) and better align code snippets to our SDKs for more specific implementation examples.
- **Forms - Flows Auth0 Send Email Action:** Allows you to send emails from Flows using the customized Email Provider at your Auth0 Tenant.
- **New Private Cloud AWS Region in Thailand:** Customers in the region can now leverage this new presence for significantly reduced latency and enhanced performance. It also provides a robust, in-country solution for organizations managing their data governance and sovereignty objectives.
- **Private Cloud Performance 30x and 30x Burst (3,000 RPS) offering on Azure:** The 3,000 RPS Private Performance and 3,000 RPS Private Performance Burst offerings on Azure enable enterprise organizations to leverage high-scale, dedicated identity infrastructure while maintaining commitment to the Azure ecosystem.

- **Improved Accuracy for Security Center Metrics:** Refined logic behind how Security Center metrics are calculated to provide more accurate and actionable insights. When an IP address triggers more than 10 relevant events for a given metric within a single hour, it will now be counted toward that metric. This update helps ensure greater consistency and reliability across event-based metrics within the Security Center.

Early Access

- **Passkey Login for Custom Databases With Import Mode Off:** Enables customers to use passkeys as the primary authentication mechanism without having to import users into the Auth0 database. Auth0 Databases and Auth0 Custom Databases with import mode ON are already supported.
- **Self-Service Provisioning - GA by April 30, 2026:** A ticket-based, user-friendly workflow that enables your business customers to quickly and confidently set up user provisioning on their own.
- **Auth for MCP:** Authenticate and authorize MCP client calls to protect resources in the growing Model Context Protocol ecosystem.
- **Actions - Transaction Metadata - GA by March 31, 2026:** Allows developers to define and share metadata between Actions during their execution. It Enables developers to define and re-use cross Action variables improving their Actions implementation, resources management and performance.
- **Ephemeral Sessions with Actions - GA on January 19, 2026:** Dynamically configure whether a session should expire when the browser is closed. Define ephemeral sessions per client, organization, connection, or by any custom business logic within Actions.
- **Akamai Supplemental Signals:** Allows Auth0 Enterprise customers who have Akamai configured as a reverse proxy in front of Auth0 to forward signals from Akamai Bot Manager and Akamai Account Protector into Auth0.

Harden our corporate infrastructure

We hold all of our internal people, processes, and technology to the same rigorous cyber threat profile as our customer-facing environment — emphasizing a holistic, inside-out approach to security. Additionally, we are accelerating our investments to further harden our ancillary (i.e., production-adjacent) and corporate systems.

Launched since September 2025

- **CheckMate for Auth0**
  A free utility for Auth0 customers that assesses the configuration of their Auth0 tenant against security best practices.
- **New notification type**
  Suspected Targeted Threat Actor Activity Notification
- **Threat Research launch at Oktane: Uncloaking VoidProxy**
  Okta uncovers security methods to secure organizations against an actively deployed Phishing-as-a-Service (PhaaS) platform
- **Okta joined the World Economic Forum's Partnership Against Cybercrime**
  Okta contributed insights to the World Economic Forum's Partnership against Cybercrime initiative
- **Enhanced scanning of open source software (OSS)**
  Okta has released an open source software policy to identify third-party software in use

*Please note that all roadmap items are subject to change.
We will update customers regularly on the status of previously communicated projects.

Launched since May 2024

- **Extend phishing resistance for all employees**: We've long deployed Okta FastPass for Phishing resistant MFA; we have recently added additional phishing resistance via Yubikeys for all employees — for whom the whole employee lifecycle, from account activation to recovery, is 100% passwordless.
- **Conduct an internal security assessment**: In partnership with a leading global advisory firm, we conducted a comprehensive security review of our products, infrastructure, and corporate systems, including completed security assessments of our internal financial, sales, data warehouse, marketing, infrastructure as a service (IaaS) & integration systems.

- **Standardized and centralized reporting for security risk management**: We deployed a single-vendor solution to centralize risk and issue management related to our governance, risk and compliance program, including third-party risk management.
- **Conduct a SaaS application security assessment**: In partnership with third-party security experts, we conducted security assessments of our critical SaaS applications, including the Okta Help Center, and our financial, customer relationship management (CRM), human capital management (HCM), sales, data warehouse, marketing, IaaS, and integration systems.

Enhanced detection and response capabilities, including:

- **New security incident case management tool**: Our new tooling has improved response time, automation, and accuracy.
- **New threat intelligence platform**: Our new platform will enable automation and correlation of threat intelligence to enhance our threat detection and response capabilities.
- **Additional dark web monitoring capabilities**: We are now proactively identifying potential threats by regularly scanning the dark web for content related to Okta.

Launched since August 2024

- **Enhanced laptop protections**: We have further limited and restricted how Okta laptops can be used, continuing to emphasize least privilege and granularly scoped roles.
- **Automate discovery and reporting of M2M service accounts in SaaS applications**: We have implemented a tool that provides visibility into local service accounts created within SaaS applications, improving our ability to manage and rotate the secrets used for authentication.
- **Enhanced mobile device protections**: We have improved our overall mobile device management (MDM) security posture through additional restrictions on privileged access.

Launched since October 2024

- **Standardized and centralized reporting for vulnerability management, asset management, and cloud security posture management (CSPM)**: We will centralize all vulnerability-related information across our production and corporate environments.
- **Improved logging ingestion and analysis tooling**: We will improve our logging capabilities to enable more relevant alerts. This will allow us to investigate an incident across our logging environment in a more timely manner.
- **Enhanced scanning of open source software (OSS)**: We have made additional improvements to OSS component vulnerability scanning in order to detect operational risks and malware in third-party libraries. This tooling has been operationalized within Okta's development and release workflows.
- **All feasible applications behind Single Sign-on (SSO)**: SSO helps prevent unauthorized devices and users by requiring inherence at login. Okta has implemented SSO internally across various applications, enabling MFA at scale while improving the user experience.
- **Full deployment of local administrator rights lockdown**: In the event of a system compromise, restricting administrator rights across the network helps restrict the movement of threat actors. This is a key component of security that doesn't rely on any one perimeter.
- **Mobile Device Management (MDM) software enforced for any device requesting corporate access**: All devices, including personal devices, requesting corporate access will be managed under MDM. This security control helps restrict the installation of unauthorized software and reduces any potential attack surface.

Launched since January 2025

- **Additional security controls established for third-party libraries**: Mitigating the risks associated with external dependencies is a key component of a robust security program. Okta has taken steps to help reduce the risk of vulnerabilities via third-party libraries with additional security controls and monitoring.
- **Backup verification process established for account recovery**: Okta partners with Persona for identity verification (IDV), verifying not just credentials, but identities, to ensure that users are who they claim to be during account unlocks and password resets.
- **How Okta embraces identity verification using Persona**: Okta has introduced ID verification as a compulsory component of our evolving onboarding process and secure account recovery activities, to improve our security posture assurance—including context on Okta's unique use cases.

Launched since March 2025

- **Additional detections on production changes:** Okta's enhanced detections on code changes in production will assist in prohibiting unauthorized modifications and/or potentially malicious insertions.
- **Vulnerability Management Automation:** By automating vulnerability management, Okta can continuously identify, prioritize, and remediate security risks without manual effort.
- **Expanded log collection for SaaS Apps:** An enhanced data footprint will streamline Okta's troubleshooting and root-cause analysis while bolstering security monitoring and compliance efforts.

Launched since July 2025

- **Okta Threat Intelligence**: Okta now publishes threat advisories on the latest identity-based attacks we have observed at security.okta.com - these observations are available exclusively for the security contacts of Okta customers. Ask your CSM for how to access these resources.

- **Threat Research: The Secrets Agentic AI Leaves Behind**: Okta Threat Intelligence published a preliminary analysis of authentication methods used for agentic AI access to protected applications.
- **Auth0 Detection Library**: Okta has published a library of common detections for suspicious activity in an Auth0 tenant to the open source community.
- **Confidence in Support Comms with Caller Verify at Okta**: Age-old security questions are inefficient, dated and, even worse, answers can be stolen. In this post, we'll outline how seamless and secure authentication prompts are leveraged in Support Comms use cases using Caller Verify.

Launched since September 2025

- **CheckMate for Auth0:** Okta has released a free, open-source tool designed to empower developers and security personnel to proactively assess and strengthen the security posture of your Auth0 tenant environment. Learn more about CheckMate for Auth0 from our blog announcement.
- **New notification type:** Okta has expanded the range of suspicious activity notifications sent to customers based on a growing set of intelligence priorities.
- **Threat Research launch at Oktane:** Uncloaking VoidProxy: Okta has uncovered a Phishing-as-a-Service (PhaaS) platform targeting Microsoft 365 and Google Workspace accounts in multiple industry sectors, tracking as VoidProxy or O-TA-083. This advisory enables organizations to understand and mitigate the risks posed by this threat. Learn more about VoidProxy from our threat intelligence blog announcement.
- **Okta joined the World Economic Forum's Partnership Against Cybercrime:** Okta's Chief Security Officer and VP of Threat Intelligence contributed expert insights to "Elevating Cybersecurity: Ensuring Strategic and Sustainable Impact for CISOs" and "Fighting Cyber-Enabled Fraud: A Systemic Defence Approach" respectively.
- **Enhanced scanning of open source software (OSS):** Okta has released an open source software policy and source code scanning to identify third-party software in use. This enables Okta to readily address security vulnerabilities in its products, services, and systems.

Champion customer best practices

Misconfigured identity is just another entry point for a threat actor or malicious insider. With 16 years of experience, we have the unique expertise to help our customers have the right identity configuration.

To make sure our customers benefit from our depth of experience, we are further strengthening our customer policies.

Moreover, we are committed to deploying our products with Okta's security best practices, and our modernized Okta Learning experience is just one way we help customers grow their own skillsets to stay aligned to these standards. The cyber-threat landscape is becoming more complex, with the surge of AI enabling a greater variety of threat actors. We are striving to equip our customers and the wider industry with best-practice guides and other education resources to stay in lockstep with the threat landscape.

Launched since September 2025

- From phishing to AI agents: Solving the authorization crisis
- Why attackers keep winning with consent phishing
- Threat actors: "Please do not use Okta FastPass"
- Addressing the growing threat of ransomware with Druva CTO Stephen Manley
- North Korea's IT Workers expand beyond US big tech
- How to transform shadow AI into innovation and empowerment
- First Drift, now Gainsight: Closing the gaps in SaaS hygiene
- The Secure Sign-in Trends Report 2025
- Payroll pirates target help desks to siphon employee paychecks
- Secure Sign-in Trends 2025: Okta published an anonymized study on user adoption of various sign-in methods to access Okta-protected resources in the workforce.

*Please note that all roadmap items are subject to change. We will update customers regularly on the status of previously communicated projects.

Completed since May 2024

- **Customer Identity Cloud Enhancements to Prevent Account Takeover**: Examines and explains the importance of new features that bolster defenses against account takeovers (ATOs).
- **Actions Template Implementation Guides**: Facilitates best practices by giving Customer Identity Cloud customers a secure configuration template to start their implementation.
- **Protecting Administrative Sessions in Okta**: Learn recommended configurations in Okta to protect administrative sessions and privileged access, reduce the attack surface, prevent ATOs, and limit the blast radius of stolen sessions.
- **Apply IP or ASN binding to Admin Console (WIC, on by default)**: Secure by default is an industry best practice, and we've made IP Binding protection the default setting for customers. Which means that if an admin suddenly appears at a different IP than they logged in initially, they will be automatically logged out and asked to re-authenticate.

Completed since August 2024

- **Win over the board: CISO strategies for proving security's ROI:** Learn how CISOs can demonstrate tangible business value without compromising key performance indicators and effectively communicate the value of their security programs to gain necessary support from the board.
- **How Okta fosters a security culture:** Discover how Okta has created a culture of security—such that security becomes implicit within an organization's DNA and second-nature to its team.
- **Identity Security Checklist:** Helps you adopt a strong identity posture and discover how to protect your organization from identity-based cyberattacks with this detailed checklist.
- **The Ultimate Guide to Phishing:** Learn how to protect yourself, your workforce, your business, and your customers from phishing attacks with this definitive guide.

- **Standards whitepaper: Okta + NIST 800-63B:** Learn how to align NIST's Digital Identity Guidelines (800-63B) with Okta's Secure Identity Commitment, including session duration, inactivity, and app classification.
- **Identity Threat Level assessment:** Unlock valuable insights into your industry's identity threat level with Okta's new tool, leveraging real-time data on bot activity to compare your score against other industries, regions, and time frames.

Completed since October 2024

- **Secure Sign-In Trends Report 2024:** In the newest edition of our report designed for IT and security professionals, uncover key insights and practical recommendations to help future-proof your authentication strategy.
- **Phishing-resistant MFA shows great momentum:** Delve further into key takeaways from our newest Secure Sign-In Trends report, including steady growth in MFA adoption, with phishing-resistant MFA on the rise.
- **Introducing Okta's Secure Identity Assessment:** Discover Okta's new professional services offering designed to help reduce your identity debt and improve your overall security posture.
- **5 tips to enhance security without sacrificing productivity or user experience:** Learn how CISOs can enhance security posture while improving productivity and enabling seamless UX.
- **Five reasons to upgrade your org to the Okta Identity Engine:** Explore why thousands of organizations are upgrading from Okta Classic to the modern Okta identity Engine. This guide highlights key benefits like enhanced authentication, passwordless sign-ins, device assurance, and improved admin experiences to help secure your identity posture and streamline user access.
- **Zero Trust and the Identity Imperative: Building resilience against emerging threats:** Explore how organizations can benefit from industry guidelines and best practices, like those outlined by NIST, to strengthen their Zero Trust approaches—and learn about current threats and trends companies are facing, including phishing, shadow IT, misconfigured identity, and more.

- **Verifying the identity of your remote workforce:** With deepfakes on the rise and increasingly hard to distinguish from reality, remote identity verification is growing in importance — and difficulty. How do you verify an employee is who they say they are when you can't physically see them? This article outlines best practices for identity verification during the hiring process and beyond.
- **The weakest link: Securing your extended workforce:** Organizations lean on third parties to expand their business capabilities, from call centers to vendors and acquired companies. But rarely do these third parties have the same security standards and protocols, making them a target since attackers know they're the weakest links into the core organization.

Completed since January 2025

- **CISOs' top threats for 2025, from deepfakes to Scattered Spider:** Cybercriminals are constantly evolving and refining their tactics. Find out what's keeping CISOs up at night, from increasingly sophisticated ransomware to supply chain vulnerabilities and AI-based cyber attacks.
- **Cyber-safety over the holidays:** A practical guide to staying safe during the holiday season, highlighting tips for protecting your identity and accounts from scams and cyber threats. Includes actionable advice such as monitoring accounts, securing devices, and practicing safe online shopping.
- **Five predictions for Identity-centric attacks in 2025:** Explore the evolving landscape of identity-based cyberattacks, including emerging threats like advanced phishing kits, a resurgence of device-based attacks, and exploitation of business processes through social engineering.
- **How to prove the ROI of cybersecurity:** Data breaches were up 72% in 2023 alone, but security professionals are still struggling to get the buy-in and resources they need to move key initiatives forward. This guide includes advice from CISOs and security leaders for demonstrating ROI and lays out the steps to showing that security isn't just a cost center, but a strategic driver of business growth and resilience.
- **The most targeted companies choose phishing-resistant MFA:** Learn how organizations targeted by advanced phishing campaigns are adopting phishing-resistant MFA methods like Okta FastPass and FIDO2 to reduce risk. Discover how phishing-resistant MFA helps prevent credential theft, enables passwordless security, and protects against evolving phishing tactics. More here.

- **How Okta mitigates OWASP's top 10 non-human identity risks:** Learn how to address OWASP's top 10 non-human identity (NHI) risks using Okta's platform — from securing sensitive credentials to enforcing least-privilege access and streamlining identity lifecycle management.
- **What a change of power in Washington means for cybersecurity:** With the new administration entering office in the U.S., what should security leaders expect and plan for? In this article, Okta Federal CSO Sean Frazier shares his predictions for the next presidential term, from deregulation to state-sponsored cyber attacks.
- **Okta Ventures highlights insights from CSO Survey:** Okta Ventures shares insights from CISO survey and details these trends are impacting security startups.
- **One trick finds the root of any Okta troubles:** Whether you're troubleshooting a technical issue or performing a forensic investigation into your Okta Workforce identity org, discover new queries that can help you get to the root of problems.

Completed since March 2025

- **The Okta Security Detection Catalog:** This repository contains a collection of detection rules for security monitoring and detailed descriptions of log fields used for threat analysis within Okta environments.
- **Empowering security with customer trust solutions:** Get a glimpse into efficiencies introduced in the Security Trust Center by the Assurance team, and why it's critical to update Okta contacts to stay informed.
- **Businesses at Work 2025 Report:** The past decade has seen dramatic changes in the business landscape, including more sophisticated cyber threats, the rise of distributed work, and smartphone saturation. Our Businesses at Work report has tracked how workforces have adapted and the new tools they've adopted. Learn more about the key trends and highlights in our blog.
- **How Okta Ventures support startups with integrations to drive Enterprise Readiness:** Blog highlighting Okta Ventures work supporting integrations on the Okta Integration Network that support enterprise readiness and security use cases for the startup ecosystem.

- **How AI services power the DPRK's IT contracting scams:** Learn how generative AI tools have been used by North Korean nationals to gain employment in remote technical roles around the globe, observations from the Okta Threat Intelligence team, and what mitigating controls we recommend.
- **How to measure the success of your security program:** Tracking the right metrics is key to demonstrating ROI, getting buy-in, and securing resources. In this article, CISOs share how to measure the success of your security program with practical qualitative and quantitative metrics that demonstrate value to your organization.
- **Nonprofits at Work 2025 report:** Deep dive on nonprofit customer data from the Businesses at Work report and beyond. The report highlights nonprofits as the second-most targeted sector, and shares security and app trends to help inform nonprofit strategies and convey the urgency of cybersecurity.
- **The hidden threat in your stack: Why non-human identity management is the next cybersecurity frontier:** NHIs are on the rise, and so are their risks. This article examines three challenges CISOs face—from gaining visibility to prioritizing risks—and how they're managing them.
- **From vulnerabilities to vendor trust: How CISOs build cyber resilience:** Business resilience has become a primary driver of security strategies across industries. In this article, CISOs share tactics to boost cyber resilience, strengthen disaster recovery plans, and reinforce trust in mission-critical vendors to the board.

Completed since July 2025

- **Deepfakes and deception:** Building a human firewall against AI-powered attacks: Explore how AI-driven deepfakes and sophisticated social engineering tactics are evolving to bypass traditional defenses. In this piece, we emphasize the importance of empowering users through awareness training — creating a "human firewall" — to recognize and resist AI-fueled deception schemes.
- **The 'superuser' blind spot: Why AI agents demand dedicated identity security:** Okta's CPO Arnab Bose highlights how AI agents can accumulate high-level access — effectively becoming hidden "superusers" — and why they require their own identity policies and controls. The article urges organizations to treat AI agents with the same rigor as human identities to close this critical security gap.

- **Navigating AI's impact on security with Guidewire CISO James Dolph:** In this video, Guidewire's CISO James Dolph discusses how AI is not only enhancing phishing via increased believability, but also transforming the CISO role. He emphasizes reframing security strategies to anticipate AI's dual role in both attacks and defense.
- **The password problem: Why we need a passwordless world:** Okta advocates for a move beyond passwords to seamless, passwordless authentication methods like biometrics and WebAuthn. This piece outlines the benefits — stronger security, improved user experience — and underscores the need for education and design to drive user adoption.
- **Sophisticated deception: Thoughtworks CISO Nitin Raina on a new era of social engineering attacks:** Thoughtworks' CISO Nitin Raina warns that cybercriminals are increasingly using AI to orchestrate highly convincing, context-aware phishing and social engineering campaigns. He stresses that this fast-moving threat requires new detection techniques and proactive response strategies from CISOs.
- **Third-party risk: 3 actions security leaders should take to safeguard their business:** Supply chain attacks are a growing concern, and one that can feel beyond your organization's control. In this article, we'll unpack the critical considerations for managing third-party relationships, from evaluating vendor security to mitigating threats across the supply chain.

Completed since September 2025

- **From phishing to AI agents: Solving the authorization crisis:** Webster Bank's CISO, Patricia Voight, joins Okta to discuss the authorization crisis with a focus on data exfiltration resulting from consent phishing, and how Okta's Cross-App Access and Fastpass can solve the fundamental authorization problem.
- **Why attackers keep winning with consent phishing:** Explore how sophisticated social engineering attacks are tricking users into authorizing attacker-controlled OAuth applications. In this piece, we emphasize the importance of adopting Cross-App Access to secure agent-to-app and app-to-app connections.

- **Threat actors: "Please do not use Okta FastPass":** VP of Okta Threat Intelligence Brett Winterford highlights evolving social engineering tactics attempting to evade security measures companies have established. He emphasizes organizations must not only adopt phishing-resistant authenticators, but also enforce phishing resistance in policy.
- **Addressing the growing threat of ransomware with Druva CTO Stephen Manley:** Ransomware attacks are surging, targeting organizations of all sizes, from school districts to hospitals. In this video, Druva CTO Stephen Manley shares a three-pronged approach to combatting these attacks.
- **North Korea's IT Workers expand beyond US big tech:** A large-scale analysis of North Korean IT Worker activity revealed this threat is much more expansive than previously known. Read the article to find out which industries and regions are most at risk — and what you can do to prepare.
- **How to transform shadow AI into innovation and empowerment:** As AI tools flood the market, employee adoption is inevitable, though adherence to approved tools is not. In this article, find out how organizations are gaining visibility and establishing effective AI governance.
- **First Drift, now Gainsight: Closing the gaps in SaaS hygiene:** The Salesloft Drift and Gainsight incidents are a stark reminder that a breach of a single service can have a ripple effect across today's interconnected SaaS ecosystem. Learn what steps your organization can take to stay secure and avoid being impacted, from enforcing inbound IP restrictions to calling on vendors to support security standards like IPSIE.
- **The Secure Sign-in Trends Report 2025:** Global workforce MFA adoption reached 70% this year. Read the report for an inside look at MFA adoption and to see how your organization stacks up against global authentication benchmarks.
- **Payroll pirates target help desks to siphon employee paychecks:** Okta Threat Intelligence has been monitoring a string of threat activity targeting payroll systems. Recently, these "payroll pirates" have begun targeting help desks to gain access to user accounts and ultimately defraud individuals of their paychecks. Learn how security leaders should prepare.
- **Secure Sign-in Trends 2025:** Okta shared our third annual Secure Sign-in Trends report. This report summarizes an anonymized study on user adoption of various sign-in methods to access Okta-protected resources in the workforce.

Elevate our industry

Identity has become the primary enterprise security entry point for all workforce and consumer applications. The volume and complexity of attacks against entities large and small continues to accelerate. Detecting and protecting against these attacks is a mission-critical requirement. Organizations need a neutral, and independent identity provider. Okta has a responsibility to lead the way

We also take a proactive role in helping shape the industry's approach to identity security — addressing the escalating complexity and volume of cyber threats with leading-edge prevention, detection, protection strategies, and setting a high standard for the industry.

Completed since September 2025

- Release of Okta for Good-funded research that reveals opportunities to close the cyber gap by hiring talent without a four-year degree
- Expanding Nonprofit Access to Okta Products
- Allocated $21.3M from the Okta for Good Fund

*Please note that all roadmap items are subject to change.
We will update customers regularly on the status of previously communicated projects.

Completed since May 2024

- **Beyond Compliance: Elevating Okta's ESG with Security and Trust:** Discover how Okta's comprehensive ESG strategy elevates trust and security, supporting industry standards and building a safer digital world for all.
- **How to Secure the SaaS Apps of the Future:** Learn the essential requirements for securing modern SaaS applications against post-authentication attacks and elevating cybersecurity standards across the tech industry by advocating for the adoption of advanced security features such as proof-of-possession, continuous access evaluation, and universal logout capabilities.

- **Leveraging the Okta Identity Security Commitment to enable Zero Trust:** Learn how Okta security features support identity-powered Zero Trust strategies, placing each in the context of a Zero Trust theme from the NIST Cybersecurity Framework.
- **Learning grants address the tech industry skills gap:** Okta Learning grants support unemployed tech workers, including veterans and military spouses. They equip individuals with Okta's on-demand course catalog, 1 Premier Practice Exam, 1 Okta certification voucher, and more.

Completed since August 2024

- **Identity Maturity Model Whitepaper:** Learn how to help assess progress in your organization's identity maturity journey and understand how identity can help you achieve your business goals.
- **Tackling Admin Sprawl with Okta:** Discover how to efficiently manage admin privileges and enhance security with practical strategies for auditing admin usage and automating monitoring to facilitate compliance.
- **CISA's Secure by Design pledge:** Okta signed the CISA Secure by Design pledge, along with companies around the globe, to showcase our industry's commitment to taking meaningful steps in adopting secure by design principles.
- **Okta for Good (O4G) has committed $4.8M** towards its $50M philanthropy commitment, including two $1M, five-year commitments to long-time partners and known leaders advancing digital transformation for the nonprofit sector.

Completed since October 2024

- **Preparing for the New Identity Security Standard:** The OpenID Foundation's Interoperability Profiling for Secure Identity in the Enterprise (IPSIE) working group is in the process of creating an open industry standard to 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. Learn how developers can get their apps enterprise-ready using Auth0 tools.

- **Okta's Ongoing Commitment to Secure By Design:** In May 2024, Okta was one of the first technology providers to sign the CISA Secure by Design pledge. The pledge commits enterprise software companies to make a "good faith" effort to meet seven high-level Secure by Design goals within the course of a year. Learn how Okta has progressed against this pledge.
- **NetHope and Okta: Securing Digital Protection and Cybersecurity for Nonprofits Worldwide**: Okta and NetHope's partnership advances digital security for nonprofits, addressing the growing cyber threats these organizations face. With a $2.5M philanthropic commitment, this collaboration aims to strengthen nonprofit cybersecurity through initiatives like the Global Humanitarian ISAC and Dial-A-CISO program, fostering leadership, and accelerating digital transformation. Together, we are building a safer digital ecosystem to protect vulnerable populations and support mission-critical operations worldwide. NetHope members deliver more than 60% of all annual international, non-governmental aid, serving over 1.67 billion people in 190 countries.
- **O4G has allocated $11.7M** towards its $50M philanthropy commitment, including investments to address the 4M global cybersecurity talent gap. At Oktane, we announced our partnership with CodePath to build an open source cybersecurity lab that will reach 3,000 students annually with simulated real-world cybersecurity scenarios. Additionally, we were the funder in the launch of Canada's first university-based cybersecurity clinic at Toronto Metropolitan University. The clinic will provide free cybersecurity services to nonprofits, while equipping next gen cyber professionals with vital hands-on experience.
- **Help reshape identity security: Join the IPSIE working group:** Learn how the newly formed IPSIE working group aims to establish a unified enterprise identity security standard. This initiative focuses on reducing implementation challenges through standardization, fostering innovation, and ensuring consistent security practices across the ecosystem.
- **3 ways Okta can help you improve your security posture and respect privacy-forward human rights:** Discover how Okta helps organizations enhance security and champion privacy-forward human rights through principles like Secure by Design, support for vulnerable organizations, and a commitment to setting new industry standards. Learn how these efforts empower trust and innovation while safeguarding digital identities.

Completed since January 2025

- **CISA Secure by Design Technical Exchange:** Okta presented to the CISA Secure By Design technical exchange on our journey to reduce an entire vulnerability class. Our engineers showcased the actions taken over the past year to analyze and classify vulnerabilities, define the scope, implement process changes, which include performing deep reviews, education campaigns and implement initiatives and oversee the execution of an holistic approach involving several organizations through Okta.
- **Raising the bar for our industry with IPSIE:** Discover how Okta is working to advance security with the Interoperability Profiling for Secure Identity in the Enterprise (IPSIE), uniting more than 25 companies via the OpenID Foundation working group to create an industry-wide standard for secure SaaS integrations focused on all aspects of Identity, including single sign-on, lifecycle management, risk signal sharing, and more.
- **Guidewire CISO chat: Identity at the core of security:** Explore how you can achieve secure access to resources & maintain a Zero Trust model through a comprehensive, unified identity security strategy in this discussion with James Dolph, CISO at Guidewire Software.
- **Building Resilient Identity: Reducing Security Debt in 2025:** Okta's security team delves into the growing challenge of managing identity sprawl and technical debt, which leaves organizations vulnerable to attacks and operational inefficiencies—and how without a clear strategy, identity security gaps can lead to misaligned priorities, hinder business outcomes, or incur costly breaches.
- **O4G has allocated $15.7M** towards its $50M philanthropy commitment, completing the first year of our 5-year commitment to "Building a More Secure World".

Completed since March 2025

- **Okta's Secure by Design Pledge – One Year On:** Our latest post highlights one year's worth of progress on Okta's commitment to CISA's Secure by Design Pledge, including our default hardening achievements and detailed updates on our pledge progress across various themes such as MFA, vulnerabilities, and more.
- **Securing the Future of Identity with IPSIE: A New Industry Standard:**

Identity security is broken—threats are rising, systems are fragmented, and the stakes have never been higher. Without a unified industry standard providing full visibility into the technology stack, organizations remain vulnerable to breaches. Learn how the OpenID Foundation's IPSIE Working Group aims to change that by developing a standard the entire industry can support.

- **Okta for Good Impact Report:** For nearly a decade, Okta for Good has addressed critical societal issues that align with our business, including strengthening nonprofit cybersecurity, investing in the next generation of cyber talent, and advancing climate action. In this report, Okta shares updates, successes, and learnings from the first year of our $50M philanthropy commitment.
- **Okta Ventures Request for Builders: Five key focus areas in Identity and security:** Okta Ventures partners and invests in early-stage startups building identity-enabled platforms. Learn about five cutting-edge areas—from digital governance for agents to agentic payment rails—where Okta Ventures sees immense potential for innovation.
- **How Responsible Disclosures are Shaping a Safer Cyberspace:** Okta supports and actively participates in responsible disclosure practices including a Bug Bounty program, which contributes to a safer online community by reducing the number of active vulnerabilities that could be exploited by threat actors with malicious intent. Learn about the industry benefits of responsible disclosures, which continue to grow for software vendors and technology users alike.
- **The Identity 25:** A report highlighting key leaders and innovators in the identity and security industry, showcasing the community of builders who help to create a broad security ecosystem.
- **CISO Pitch for Charity Event at Okta HQ:** During RSA Week, Okta and SentinelOne hosted a cybersecurity startup pitch event in conjunction with the Security Tinkerers organization at Okta's HQ and donated $100,000 to 2 security education non-profits: Hack the Hood and Codepath. Over 80 CISOs confirmed in attendance.
- **Next Gen Workforce for Cyber & AI:** During RSA Week, O4G hosted the event "Next Gen Workforce for Cyber & AI'' at Okta SFHQ. The event had 125+ attendees including current and emerging cyber professionals to

discuss essential skills and competencies required for the next generation of cybersecurity and AI professionals. The attendees received access to free Okta training and certification resources through the "What's Next by Okta Learning" program.

- **Introducing the new Okta Security Technical Implementation Guide (STIG):** Following our partnership with The Defense Information Systems Agency (DISA), is the release of the new Okta Identity as a Service (IDaaS Security Technical Implementation Guide (STIG). This Okta Security article introduces the new STIG guidance with an important call to action for our customers in our ongoing pursuit — to free everyone to safely use any technology.
- **O4G has allocated $16M** towards its $50M philanthropy commitment.

Completed since July 2025

- **Security and sustainability through people, processes, and technology**: Securing critical infrastructure enables sustainable business practices and respect for human rights like privacy. Okta supports our B2B customers in securing their critical infrastructure. Effective identity management and ESG programs include aligning people, processes, and technology for a unified approach to security risk management.
- **New Okta for Good Technical Services for Nonprofits** expands our technical services offerings to nonprofits. This includes the Okta Quick Launch Guide, curated by the Okta for Good team for nonprofits & other organizations with few technical resources. This on demand resource includes content from Okta Learning.
- **New pro bono partner implementation services for Nonprofits through our partners Cloudworks and BeyondID**: Many nonprofits operate with small IT teams with limited skillsets. Nonprofits need more than a product donation to be secure—they need technical implementation support. This ensures the product is set up according to best practices. This new program expands our support offerings to customers in EMEA and beyond through partners.
- **O4G has allocated $19.5M** towards its $50M philanthropy commitment.

Completed since September 2025

- **Release of Okta for Good-funded research that reveals opportunities to close the cyber gap by hiring talent without a four-year degree:** To address the global cybersecurity talent gap of 4.8 million people, Okta for Good partnered with Opportunity@Work to research pathways for individuals without college degrees into cyber careers. This foundational research will provide insights on how to effectively tap into a robust talent pool — more than 70 million U.S. workers (over 50% of the workforce) — ultimately strengthening the cybersecurity profession.
- **Expanding Nonprofit Access to Okta Products:** As the second most targeted sector for cyberattacks, non-profits are in need of robust protection. Okta for Good aims to support organizations in securely delivering their mission through our latest expanded nonprofit offering. This offering features a tailored Okta for Good product bundle to help strengthen your security posture, secure access to sensitive apps and data. A powerful product is only part of the solution. Okta for Good Technical Services for nonprofits provides the technical guidance and support you need to get up and running on Okta quickly and securely.
- **O4G has allocated $21.3M** towards its $50M philanthropy commitment.

Conclusion

Okta is committed to being an industry leader in the fight against identity-based attacks. As a result, we launched the Okta Secure Identity Commitment, which is based on four pillars:

- Provide market-leading secure identity products and services
- Harden our corporate infrastructure
- Champion customer best practices to help ensure our customers are best protected
- Elevate our industry to be more protected from identity attacks

This is a long-term commitment and we will continue to evolve along with the technology and threat landscape.

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.