Whitepaper

Okta Secure Identity Commitment

Table of 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 secure Identity products and services
- Champion customer best practices to help ensure our customers are best protected
- Elevate our industry to be more protected from Identity attacks
- Harden our corporate infrastructure

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 19,450+ customers.

For example, based on internal reporting through January 31, 2025, we found that Okta **detects and blocks around 8 billion attacks** each month through ThreatInsights, spanning credential stuffing, malicious bot activity, and other Identity-based threats. Continued investment in threat intelligence and mitigation has further increased the volume of blocked attacks, strengthening our ability to protect customers at scale.

Additionally, Okta's Enhanced Dynamic Zones (EDNZ) feature **blocked over 782 million malicious (or risky) access attempts** in January 2025 alone, expanding protection against residential proxies and VPN-based attacks, which are known vectors for adversaries.

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

Champion customer best practices to help ensure our customers are best protected

Elevate our industry to be more protected against Identity attacks

Harden our corporate infrastructure

Provide market-leading secure Identity products and services

We recognize that our security offerings are your security posture, which is why we are dedicated to advancing and prioritizing security features within our Identity products and services.

Through this continuous focus, we help ensure that the trust invested in us by globally recognized brands is met with the strongest and most innovative protection measures.

At Oktane 2024, we announced a host of customer security boosting advancements—including leading the formation of a new OpenID Foundation working group chartered to create a new Identity security standard: Interoperability Profiling for Secure Identity in the Enterprise (IPSIE).

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

- **Enhancing Identity security posture with AI-driven insights** – Strengthening risk detection with Okta AI-powered solutions like Identity Threat Protection or Log Investigator.
- **Expanding authentication and Zero Trust controls** – Introducing device-bound SSO, adaptive posture checks, and FIDO2 security keys to improve secure access.
- **Strengthening privileged access and compliance** – Adding automated entitlement reviews and role-based access controls.
- **Broadening integrations and security automation** – Supporting new SSF integrations, Google Credential Manager, and identity verification enhancements with Incode and CLEAR.

Launched since January 2025

Okta

Generally Available

- Okta Personal for Workforce
- Smart card just-in-time provisioning
- Yubico FIDO Pre-reg
- Okta Account Management Policy
- Okta Identity Security Posture Management
  - Enhanced MFA Insights and Graphs
- Workflows Post-Audit for FedRAMP High

Coming soon in April 2025*

Okta

Generally Available

- Device Assurance
  - Android Zero Trust Integration
- Desktop MFA Recovery for macOS
- Okta Identity Security Posture Management
  - Enhanced Non-Human Identity Analytics

Role-Based Access Control Capabilities

Launched since January 2025

Okta

Generally Available

- Workflows Post-Audit for FedRAMP High
- Identity Threat Protection with Okta AI
    - New SSF integration with Omnissa (Workspace One UEM)
    - Universal Logout support for SURF Security
    - Universal Logout support for Auth0-powered applications
- Out-of-the-box integrations for Identity Verification
    - Persona integration
- Device Assurance
    - Grace Period for Policy Compliance
    - Dynamic OS Version Policy Option
- Okta Device Access
    - Just-in-time Local Account Creation for macOS
    - FIDO2 Security Keys for Desktop MFA for Windows

Early Access

- Collections with Entitlement Management
- Secure Partner Access
- Authentication method chain
- On-prem Connector (for SAP)
- Enhanced Group Remediation for Access Certs
- Preconfigured Access Certification campaigns

Auth0

Generally Available

- Bot Detection upgraded with user agent and tenant-specific signals
- Tenant Logs for Action Failures
- Credential Guard on Azure
- OTP passwordless authentication for email and SMS
- Guardian App & SDK - Mobile Enrollment for Push
- Auth0 Integration with Okta Universal Logout
- Machine-to-Machine Access for Organizations
- Custom Email Provider
- Email OTP Verification

Early Access

- Tiered Alerting on Anomalies in Security Center
- Improve onboarding and integrations with Custom Token Exchange External Tokens
- Client Initiated Backchannel Authentication (CIBA)
- Verify Mobile Driver's License (mDL)

Coming soon in April 2025*

Okta

Early Access

- Active Directory Accounts in Okta Privileged Access
- Device-Bound Single Sign-On
- Advanced Posture Checks
- Enhanced Dynamic Network Zones (Residential Proxy / Blockchain Support)
- Out-of-the-box integrations for Identity Verification
    - Incode integration
    - CLEAR integration

Okta Customer Identity Solution

Early Access

- IdP single logout
- Network restrictions for OpenID Connect Token Endpoints

Auth0

Generally Available

- Active Session Management for Dashboard users
- Breached Password Detection on Password Reset Flow
- FAPI 2 Security Profile conformance testing and certification (Financial Grade APIs by the OpenID foundation)
- Teams support for Security Policies with *SSO Enforcement in Private Cloud
- Google Credential Manager support using Google Token Exchange

Early Access

- Auth for GenAI
- Tenant Security Manager with Okta AI
- Client Assertion JWT for the OIDC Enterprise Connection
- Customer-Provided Signature Public Keys
- Self-Service Domain Verification/HRD
- Passkey login for custom databases with import mode off
- Secure Tenant-level Access Control list
- Federated logout for OIDC and Okta Connections
- Limit M2M Usage Per Client & Organisation
- Native to Web SSO
- Step-up authentication for sensitive account/tenant flows
- Client Initiated Backchannel Authentication (CIBA) updated with Rich Authorization Requests (RAR)

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

Launched in 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**

  Prevent administrators from creating authentication policies that only require a single factor. Opt-in to prevent any single factor access to the admin console.

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 in July & August 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.

- **Dynamic OS Version Compliance**

  Stay up-to-date with major OS version releases and security patch updates with Device Assurance policy enhancements that allow dynamic compliance tracking.

- **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 in 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.

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 Solution
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.
- **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.

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.

- **Device Assurance**
    - Grace Period for Policy Compliance: Provide end users with uninterrupted access to essential resources during configurable timeframes to empower them to self-remediate any device compliance issues before being locked out.
    - Dynamic OS Version Policy Option: Require devices to have the latest OS updates through a more flexible, low-touch policy configuration that dynamically gates access based on minimum OS versions.

- **Device Assurance**
    - Grace Period for Policy Compliance: Provide end users with uninterrupted access to essential resources during configurable timeframes to empower them to self-remediate any device compliance issues before being locked out.
    - Dynamic OS Version Policy Option: Require devices to have the latest OS updates through a more flexible, low-touch policy configuration that dynamically gates access based on minimum OS versions.

- **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, with or without entering an OS account password.

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 (for SAP)**
  An out-of-the-box connector that allows customers to integrate their on-prem SAP 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.

Coming soon in April 2025

Okta
Generally Available

- **Device Assurance**
  Android Zero Trust Integration:
  Enforce an extensive array of device signals on Android via Device Assurance policies.
- **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.
- **Okta 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.

Early Access

- **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.
- **Device-Bound Single Sign-On**
  Initiate a hardware-protected SSO session for seamless admission to your downstream apps after device login.
- **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 Customer Identity Solution
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

- **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.
- **Tenant Security Manager with Okta AI**
  Enriches Attack Protection capabilities with “intelligent” security summaries and insights, and allows users to chat with a Customer Identity Cloud subject matter expert AI chatbot.
- **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.

- **Client Initiated Backchannel Authentication (CIBA) support for Rich Authorization Requests (RAR)**

  Allows CIBA requests to users to be enriched with transaction details that the user can review before authorizing.

Champion customer best practices to help ensure our customers are protected

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. 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 January 2025

- CISOs' top threats for 2025, from deepfakes to Scattered Spider
- Cyber-safety over the holidays
- Five predictions for Identity-centric attacks in 2025
- How to prove the ROI of cybersecurity
- The most targeted companies choose phishing-resistant MFA
- How Okta mitigates OWASP's top 10 non-human identity risks
- What a change of power in Washington means for cybersecurity

Coming soon in April 2025*

- How to measure the success of your security program
- Strategies to improve cyber resilience
- Secure governance of non-human identities

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

Launched in 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.

Launched in 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.

Launched in 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.

Launched 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-bassed 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.

Coming soon in April 2025

- **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.

- **Strategies to improve cyber resilience**

  Since the CrowdStrike outage, 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.

- **Secure governance of non-human identities**

  Discover effective strategies to enhance secure governance of non-human identities (such as service accounts and chatbots), including improving visibility, automating oversight, and safeguarding critical systems.

Help elevate our industry to be more protected against Identity attacks

Leading the way in Identity security is an imperative at Okta. We are focused on helping to detect and mitigate Identity attacks for our industry, and we work towards these goals by accelerating our capabilities and embracing new technology such as AI.

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.

Launched since January 2025

- CISA Secure by Design Technical Exchange
- Raising the bar for our industry with IPSIE
- Guidewire CISO chat: Identity at the core of security
- Building resilient Identity: Reducing security debt in 2025
- $15.7M committed to Okta for Good out of a $50M commitment total

Coming soon in April 2025*

- Okta for Good Global Impact Report

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

Launched in 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.

Launched in 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.

Launched in 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.

Launched 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 25+ companies to create a groundbreaking, 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 between James Dolph, CISO at Guidewire Software, and Chris Niggel, Regional CSO at Okta.
- **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”.

Coming soon in April 2025

- O4G will release its **2025 Impact Report**, sharing updates, successes, and learnings from the first year of our $50M philanthropy commitment.

Harden Okta's corporate infrastructure

We hold all of our internal people, processes, and technology to the same rigorous security standards as our customer-facing products — 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 January 2025

- Additional security controls established for third-party libraries
- Backup verification process established for account recovery
- Embracing Identity verification using Persona

Coming soon in April 2025*

- Biometric Authentication for High & Moderate Assurance Apps
- Additional detections on production changes
- Vulnerability Management Automation
- Expanded log collection for SaaS Apps

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

Launched in 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 in 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 in 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.

Coming soon in April 2025

- **Biometric Authentication for High & Moderate Assurance Apps**
  Biometric authentication simplifies the end user experience by eliminating the need to remember complex credentials, offering both enhanced protection and improved convenience
- **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.

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
- Champion customer best practices to help ensure our customers are best protected
- Elevate our industry to be more protected from Identity attacks
- Harden our corporate infrastructure

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