Whitepaper

Okta Secure Identity Commitment

Last updated: Dec 3, 2024

Provide market-leading secure Identity products and services

Champion customer best practices to help ensure they are best protected

Elevate our industry to be more protected against Identity attacks

Harden our corporate infrastructure

okta

Contents

Executive Summary

Identity is the primary enterprise security entry point for all workforce and consumer applications. Meanwhile, 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 upon us the responsibility to evolve from connecting people with technology to serving as a critical entry point for protecting every organization's important data.

And this responsibility is captured within **our vision to free everyone to safely use any technology.**

Okta Secure Identity Commitment

Identity has become mission-critical security infrastructure.

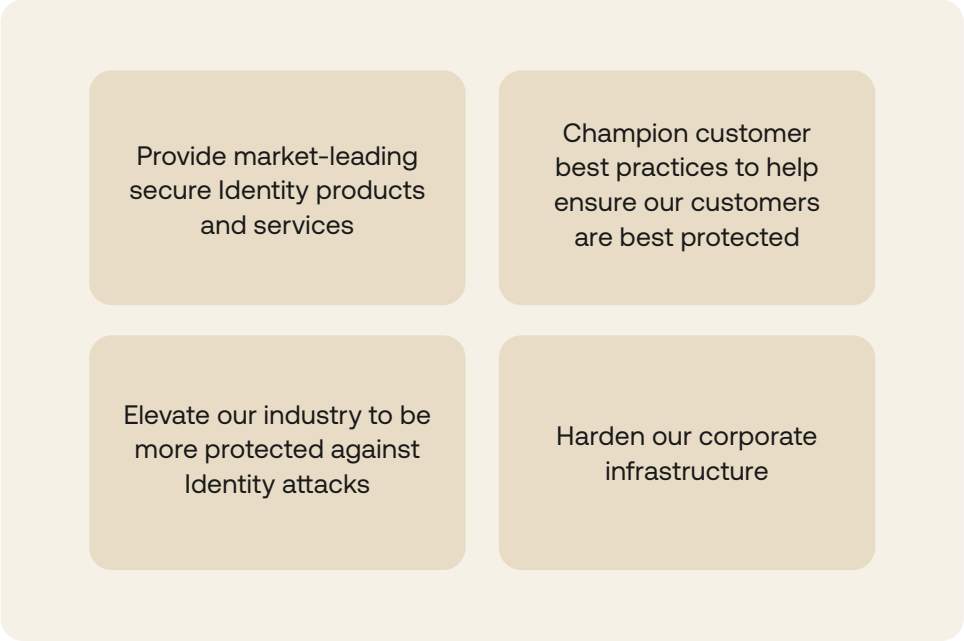
As a leading independent Identity company, Okta is at the forefront of the fight against Identity attacks. Our product, engineering, security, and business technology teams continually innovate our technology platform to protect our 19,450+ customers. For example:

- Okta **detects and blocks over 3 billion attacks** each month, from credential stuffing to malicious bots on the Internet (Based on internal reporting through October 16, 2024)
- We've **reduced credential stuffing attempts and malicious bot traffic by more than 90%** for some of our largest customers over a 90-day period (Based on internal reporting of anonymized data from Enterprise Customers over the period of October 5, 2023 to January 4, 2024)

- We're shaping industry best practices - 100% of **Okta Employees use Okta FastPass with device assurance and Adaptive MFA (AMFA) for phishing resistant factors** (Based on internal reporting as of February 2024)

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

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 Profile 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:

- Hardening administrative access to customer administration consoles
- Strengthening session, user, application, and device security
- Enhancing support for security best practices

Launched in July and August 2024	Launched since October 2024	Coming soon in January 2025*
Workforce Identity Cloud Generally Available • Okta Identity Security Posture Management (ISPM) (GA in North America) • Identity Threat Protection with Okta AI • Expand in-product best practice guides • Enforce MFA for first-party administrator app access • Secure agent deployment for Active Directory • Yubico Enterprise Onboarding • Trusted App Filters for FastPass • Dynamic OS Version Compliance • Authentication Method Chain	**Workforce Identity Cloud** Generally Available • Secure Identity Integrations • Okta ISPM: Improved detections (SSO bypass) Early Access • Secure SaaS Service Accounts • Out-of-the-box integrations for Identity Verification (Persona) • Governance Analyzer with Okta AI • Enhanced Dynamic Network Zones • Step-up authentication for sensitive tenant flows • Expanding phishing-resistant policies across onboarding and recovery	**Workforce Identity Cloud** Generally Available • Okta Personal for Workforce • Smart card just-in-time provisioning • Yubico FIDO Pre-reg • Okta Account Management Policy • Okta ISPM – SSO integration and updated UI – Enhanced reporting – Better support for non-human identities – Remediation automation with OIG & Workflows • Workflows Post-Audit for FedRAMP High Early Access • Collections with Entitlement Management

Customer Identity Cloud

Generally Available

- Enhance Bot Detection on password recovery
- Log Service: Prioritized Logs and SIEM integration
- Thresholds within Security Center Dashboard
- Enhanced Sign-Up Attack Detection for Bot Detection V4
- Account Level Audit Logs
- Define organization level session timeouts
- Detect and Mitigate IP Rotation Attack

Customer Identity Cloud

Generally Available

- Forms
- Customize sessions with extensibility

Early Access

- Self-Service SSO
- Universal Logout
- Advanced Customization for Universal Login

Workforce & Customer Identity

Generally Available

- Secure Identity Assessment

Customer Identity Solution

Early Access

- Passkey autofill

- Secure Partner Access
- Authenticator sequencing
- Local account support for Desktop MFA for Windows
- Device Logout for macOS
- New Identity Threat Protection Integrations
- OEM On-prem Connector (for SAP)
- Enhanced Group Remediation for Access Certs
- Preconfigured Access Certification campaigns
- Enhanced Dynamic Network Zones: Residential Proxy/ Blockchain support

Customer Identity Cloud

Generally Available

- Customer-Managed Keys
- Bot Detection upgraded with user agent and tenant-specific signals
- OTP passwordless authentication for email and SMS
- Guardian App & SDK - Mobile Enrollment for Push
- Active Session Management for Dashboard users

Early Access

- Federated logout for OIDC and Okta Connections
- Native login with passkey for Android and iOS
- Secure tenant level access control list
- Tenant Security Manager with Okta AI
- Tiered Alerting on Anomalies in Security Center
- Client Initiated Backchannel Authentication (CIBA)
- FAPI 2 Security Profile conformance testing and certification (Financial Grade APIs by the OpenID foundation)
- Verify Mobile Driver's License (mDL)

*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

Workforce Identity Cloud

- **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.

Customer Identity Cloud

- **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

Workforce Identity Cloud

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.

Customer Identity Cloud

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

Workforce Identity Cloud

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.
- **Enhanced Dynamic Network Zones**: Define IP service categories, locations, and Autonomous System Numbers (ASNs) to block or allow specific traffic before authentication, enhancing security by preventing access from risky IPs and network zones.

- **Step-up authentication for sensitive tenant flows**: Get an additional layer of security and control for user's authentication processes.
- **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.

Customer Identity Cloud

Generally Available

- **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.

Workforce & Customer Identity

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.

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.

Coming soon by January 2025

Workforce Identity Cloud

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**
  - **SSO integration and updated UI**: Configure SSO access to Okta ISPM using the Okta OIDC app integration to enable a seamless, one-click SSO access setup without complex configurations. In addition, overall product UI enhancements for consistency across the Okta portfolio.
  - **Enhanced reporting**: Quickly generate detailed, executive-level reports, providing valuable insights for companies focused on data-driven decision-making at the highest levels. Furthermore, reports for specific risk categories (MFA coverage for example) can be generated for in-depth analysis of specific risks.
  - **Better support for non-human identities**: Adding support for secrets and tokens related security risks detections and remediations.
  - **Remediation automation with OIG & Workflows**: Automatically remediate detected risks to efficiently improve your security posture. Okta Workflows allows for a full automation and OIG Campaigns empower customers to create even more sophisticated remediations that can include human-in-the loop.
- **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.

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**: Securely manage identity and access to shared applications for business partners without requiring significant development, customization, and management tasks from IT.
- **Authenticator sequencing**: Get granular control over authenticator method order, implement a layered approach to authentication, and configure policies for specific organizational goals.
- **Local account support for Desktop MFA for Windows**: Admins will be able to install Desktop MFA without needing to be domain joined to Active Directory or Azure Active Directory.

- **Device Logout for MacOS**: Logs users out of their MacOS devices based on security events detected by Identity Threat Protection, with policies that admins can define when elevated risk is identified.
- **New Identity Threat Protection Integrations**: Take advantage of new SSF integrations with CrowdStrike, AppOmni, and Omnissa (Workspace One UEM) and Universal Logout integration with SURF Security.
- **OEM 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.
- **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.

Customer Identity Cloud

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).
- **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.
- **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.
- **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.

Early Access

- **Federated logout for OIDC and Okta Connections**: Make use of simplified Federated Logout integrations with Okta Workforce Identity Cloud and OpenID Connect identity providers.
- **Native login with passkey for Android and iOS**: Native login flows within your Android applications to provide a tailored experience for your end users.
- **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.
- **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.
- **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.
- **Client Initiated Backchannel Authentication (CIBA)**: Provide the means to proactively reach out to users via a notification for them to authenticate and authorize access.
- **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.
- **Verify Mobile Driver's License (mDL)**: Present mobile driver's license (mDL) verification request to end-users and verify mDL within your application.

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 15 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 ensuring our products are deployed with Okta's security best practices to directly contribute to fortifying customers' defenses against Identity-related breaches.

To those ends, 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 in August 2024	Launched in October 2024	Coming soon in January 2025*
• Win over the board: CISO strategies for proving security's ROI • How Okta fosters a security culture • Identity Security Checklist • The Ultimate Guide to Phishing • Standards whitepaper: Okta + NIST 800-63B • Identity Threat Level assessment	• Secure Sign-In Trends Report 2024 • Phishing-resistant MFA shows great momentum • Introducing Okta's Secure Identity Assessment • 5 tips to enhance security without sacrificing productivity or user experience • Five reasons to upgrade your org to Okta Identity Engine • Zero Trust and the Identity Imperative: Building resilience against emerging threats • Verifying identity of your remote workforce • The weakest link: Securing your extended workforce	• Guide to proving the ROI of cybersecurity • Threats I'm monitoring in 2025: From deepfakes to Scattered Spider

*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
- **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 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.

Coming soon in January 2025

- **Guide to proving 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.
- **Threats I'm monitoring in 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.

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 in August 2024	Launched in October 2024
• Identity Maturity Model Whitepaper • Tackling Admin Sprawl with Okta • CISA's Secure by Design pledge • $4.8M committed to Okta for Good out of a $50M commitment total	• Preparing for the New Identity Security Standard • Okta's Ongoing Commitment to Secure By Design • NetHope and Okta: Securing Digital Protection and Cybersecurity for Nonprofits Worldwide • $11.7M committed to Okta for Good out of a $50M commitment total • 3 ways Okta can help you improve your security posture and respect privacy-forward human rights • Help reshape Identity security: Join the IPSIE working group

*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.

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.

Recently delivered in August 2024	Launched in August 2024	Coming soon in October 2024
• Enhanced laptop protections • Automate discovery and reporting of M2M service accounts in SaaS applications • Enhanced mobile device protections	• Standardized and centralized reporting for vulnerability management, asset management, and cloud security posture management (CSPM) • Improved logging ingestion and analysis tooling • Enhanced scanning of open source software • All feasible applications behind Single Sign-On (SSO) • Full deployment of local administrator rights lockdown • Mobile Device Management (MDM) software enforced for any device requesting corporate access	• Additional security controls established for third-party libraries

*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.

Coming soon in 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 is taking steps to help reduce the risk of vulnerabilities via third-party libraries via additional security controls and monitoring.

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 re 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.