Whitepaper

Okta Secure Identity Commitment

Last updated: Aug 28, 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 they 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.

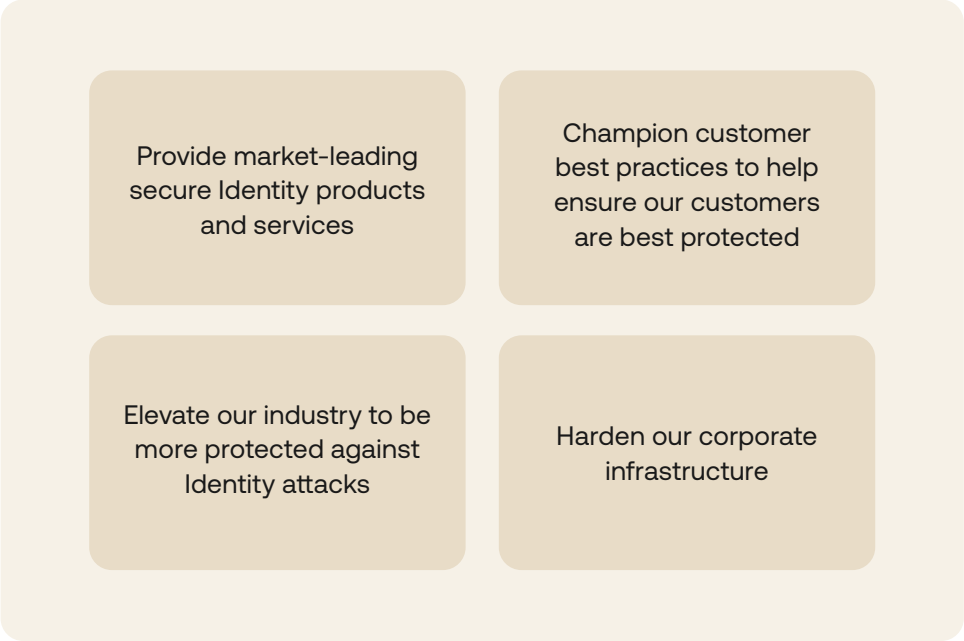
As a leading independent Identity company, Okta is at the forefront of the fight against Identity attacks. Our product, engineering, security, and business technology teams continually innovate our technology platform to protect our 19,000+ customers. For example:

- Okta ThreatInsight **detects and prevents ~2B+ malicious requests** within a 30-day period (Based on internal reporting over the period of December 5, 2023 to January 4, 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** (Base d 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 2023, we announced a host of customer security boosting capabilities — including many with Okta AI.

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
- Supporting security best practices across our customer base

Features announced in May 2024	Features launched by September 2024	Coming soon in October 2024
Workforce Identity Cloud • Govern Okta admin roles • Require MFA to access the Okta Admin Console • Require MFA for protected actions in Admin Console • Allow admins to detect and block requests from anonymizing services • Apply IP and ASN binding to Admin Console • Enforce an allow-listed network Zone for APIs • Enforce token binding for M2M application service integrations • Prevent account lockout for Okta users	**Workforce Identity Cloud** • Identity Security Posture Management (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 • Granular Authenticator Enrollment + Recovery with ASoP • Dynamic OS Version Compliance • Authentication method chain	**Workforce Identity Cloud** • Step-up authentication for sensitive tenant flows • Secure SaaS Privileged Accounts • Expanding phishing-resistant policies across onboarding and recovery

Customer Identity Cloud

- Fine-Grained Authorization
- Fourth-generation Bot Detection with Okta AI
- Highly Regulated Identity (GA)
- Auth challenge
- Require MFA for all dashboard admins
- Extend OIDC Back-Channel Logout with Initiators
- Enforce ASN binding for Auth0 admin sessions
- Manage session and refresh token management API
- Define progressive factor enrollment for end-users

Customer Identity Cloud

- Enhance Bot Detection on password recovery
- Control Your Own Key
- 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

- Concurrent-sessions control
- Customize sessions with extensibility
- Secure tenant-level access control
- Breached password detection on password reset flow
- Tiered Alerting on Anomalies in Security Center

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

Features announced 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:** Empower developers to define authorization logic with greater scalability, availability, and auditability than traditional access control methods. Available on both Workforce and Customer Identity Clouds.

- **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.

Features launched by September 2024

Workforce Identity Cloud

- **Identity Security Posture Management (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.
- **Granular Authenticator Enrollment + Recovery with ASoP**: Implement and extend a single policy to control authentication, recovery, and enrollment. Reduce social engineering attacks with granular control over enrollment and recovery auth flows.

- **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

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

Coming soon in October 2024

Workforce Identity Cloud

- **Step-up authentication for sensitive tenant flows**: Get an additional layer of security and control for user's authentication processes.
- **More secure SaaS Privileged Accounts**: Deliver zero standing privileges for shared SaaS accounts, enforce individual accountability to shared accounts, and enable flexibility in policy options like MFA and approvals to balance security with efficiency.
- **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

- **Concurrent-sessions control:** Introducing concurrent session control capabilities allows your tenants to keep the number of active devices for your users under control. Either as a cap to shared credentials or as a risk signal, concurrent session control allows you to reject new logins above limits defined by your business.
- **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.
- **Secure tenant-level access control**: 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.
- **Breached password detection on password reset flow**: Protect your password reset flow—help prevent the use of known breached credential combinations during the recovery flow.
- **Tiered Alerting on Anomalies in Security Center**: Receive proactive alerts when an anomaly is detected so you can stay ahead of attacks in real-time.

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:

- **Identity Security Checklist**: 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**: Learn how to align NIST's Digital Identity Guidelines (899-63Bb) 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.
- **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.

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 shaping 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:

- **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 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.
- **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.

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 May 2024	Launched in August 2024	Coming soon in October 2024
• Extend phishing resistance for new and existing employees • Conduct an internal security assessment • Standardized and centralized reporting for security risk management • Conduct a SaaS application security assessment **Enhanced detection and response capabilities, including:** • New security incident case management tool • New threat intelligence platform • Additional dark web monitoring capabilities	• 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)

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

Recently delivered in May 2024

- **Extend phishing resistance for new employees:** We've long deployed Okta FastPass for Phishing resistant MFA; we have recently implemented phishing resistance via Yubikeys for all new employees — for whom the whole employee lifecycle, from onboarding 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, 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, infrastructure as a service (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.

Coming soon 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):** To improve security hygiene, all security libraries will be scanned against supply chain attacks.
- **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.

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 they 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.