Whitepaper

Okta Secure Identity Commitment

Provide market-leading secure Identity products and services

Harden our corporate infrastructure

Champion customer best practices to help ensure they are best protected

Elevate our industry to be more protected from Identity attacks

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

As part of 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

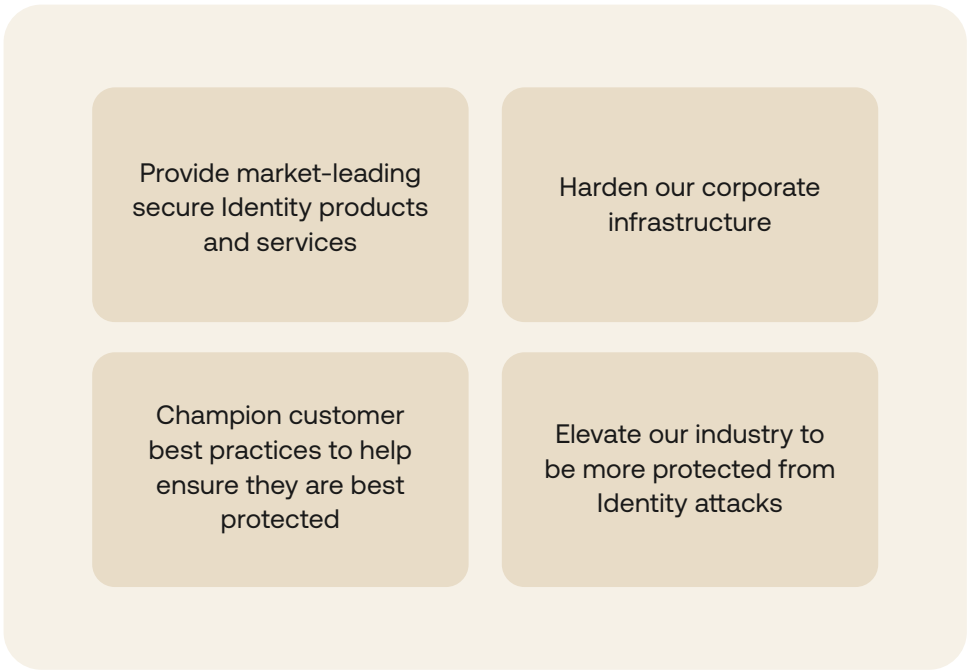
Identity has become mission-critical security infrastructure.

As a world-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 18,000+ customers. For example:

- Okta ThreatInsight ***detects and prevents ~2B+ malicious requests*** within a 30-day period (Source: Okta Internal Source - January 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 (Source: Okta's The State of Secure Identity Report 2023)
- We're shaping industry best practices - 100% of Okta Employees use ***Okta FastPass and Adaptive MFA (AMFA) for phishing resistant factors*** (Source: Okta Internal Source - February 2024)

We are committed to lead the industry in the fight against Identity attacks. As a result, we have launched the Okta Secure Identity Commitment.

This commitment is built upon four pillars:



Provide market-leading secure Identity products and services

We recognize that our security posture is 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.

Harden our 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.

Champion customer best practices to help ensure they are best protected

Misconfigured Identity is just another entry point for a bad actor or malicious insider. With 15 years of experience and 18,000+ customers, we have the unique expertise to help ensure 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.

Elevate our industry to be more protected from 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. We do this 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. This includes supporting Okta for Good to help fund the digital transformation of nonprofits and advance inclusive pathways into tech.

The remainder of this document will explain how we are delivering on our commitments.

Provide market-leading secure Identity products and services

At Oktane 2023, we announced a host of customer security boosting capabilities — including many with Okta AI.

Looking ahead, there are a few key themes for how we will further strengthen our products and services, including:

- Tightening administrator access in an Okta organization
- Strengthening session security
- Supporting security best practices across our customer base

Recently delivered	Features planned for February 2024	Features planned for July 2024
• Okta Privileged Access • Entitlement Management • Passkeys • Highly Regulated Identity • Okta Expert Assist • Spera acquisition • Change in case access on the Okta Help Center • Admin session authentication • Management APIs - Admin session required for Okta API calls • And more...	• Require MFA to access the Okta Admin Console • MFA required for protected actions in Admin Console • Allow admins to detect and block requests from any anonymizer • Apply IP binding to Okta Admin Console and IP or ASN binding to Admin Console • Enforce an Allow-listed Network Zone for APIs • Deliver Zero Standing Privileges for Okta admin roles • Enforce token binding for M2M application service integrations • Preventing account lockout for Okta users • Apply IP binding to Privileged Access Management (PAM) • And more...	• Device-bound session cookies for Okta applications • Enhance Bot Detection • Strengthen the default CAPTCHA • Extend session management control and enhance token security • Accelerate service accounts in SaaS and hyperscalers as a protected resource in Okta Privileged Access • Restrict enrollment of FastPass to managed devices • Expand in-product best practice guides • And more...

Recently announced/delivered

Recent product and feature launches that strengthen customer security include:

- **Okta Privileged Access** that helps customers implement zero standing privileges and reduce risk
- **Entitlement Management**, to reduce potential threats from misconfigurations by automatically detecting and right-sizing entitlements
- **Passkeys**, to provide secure, passwordless access for consumer apps
- **Highly Regulated Identity**, which provides Financial-Grade Security in identity workflows
- **Okta Expert Assist** to help customers boost security and configuration with Okta security expertise
- **Spera acquisition** to advance Identity-powered security and helps organizations reduce risk and drive down fragmented enterprise IT and costs
- **Identity Threat Protection with Okta AI** *coming soon to Early Access*, which includes powerful actions like Universal Logout (e.g., in response to threats across customer ecosystem)

Okta Expert Assist

Customers can partner with Okta to take additional steps to boost their security and overall configurations.

Here's how the Okta Expert Assist service works:

1. **Discover: Get matched with an Identity security expert**. Your Okta Architect will perform a comprehensive security review of your Okta tenants (via workshops) over the course of 2 weeks.
2. **Analyze: Actionable steps identified by your security expert**. Your Okta Architect will examine your settings holistically — against best practices that consider the latest Okta product features and the ongoing evolution of the threat landscape.
3. **Plan: Boost your security posture for today and tomorrow**. Your Okta Architect will provide prioritized, practical, and prescriptive guidance to improve your security posture and stay ahead of growing security threats.

→ **Learn more at**: https://www.okta.com/expert-assist/

Additional updates that have recently launched include:

- **Change in case access on the Okta Help Center:** Okta support cases can only be accessed on the Okta Help Center by the admin user who opens the support case.
- **Admin session authentication:** The Admin Console default timeouts will be set to a default of 12-hour session lifetime and a 15-minute idle time. Customers have the option to edit these settings.
- **Management APIs - Admin session required for Okta API calls:** Okta's best practices are for customers to use API tokens when making API calls with automation or Terraform. The product change will enforce this and improve customer administrator security.

Features planned for Early Access in February 2024:

- **Require MFA to access the Okta Admin Console:** Okta will improve secure access to the Okta Admin Console by requiring MFA for all Okta admin roles. Enforcing MFA to the admin console provides an additional security layer that can help lower the likelihood of a breach. We are taking a phased approach, with the initial phase preventing new admin app authentication policies from being created without MFA.
- **MFA required 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 any anonymizer:** Okta will provide administrators the ability to allow or deny access based on an evaluation of whether an IP address is associated with anonymizers, which will strengthen an organization's control against unauthorized access through such sources.
- **Apply IP binding to Okta admin console and IP or ASN binding to Admin Console:** To prevent potential session takeovers, 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. Customer administrators will be able to automatically revoke an administrative session if the IP address observed 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.
- ***Deliver Zero Standing Privileges for Okta admin roles:** Manage Okta admin roles with Okta Identity Governance (OIG). By requiring access requests and certifications for admin permissions, Okta can help customers mitigate insider threats and unauthorized access and enable least privilege access.

*Coming Soon to Early Access (EA) for OIG Customers in February 2024 and EA to more customers beginning in March

Features planned for General Availability in February 2024:

- **Enforce token binding for M2M application service integrations:** Okta will enhance 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.
- **Preventing account lockout for Okta users**: Okta will provide 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.
- **Apply IP binding to Privileged Access Management (PAM):** Customer administrators will be able to automatically revoke an administrative Privileged Access Management session if the IP address observed during an API or web request differs from the IP address recorded when the session was established. A support ticket is required to disable this functionality.

Features planned for July 2024:

- **Device-bound session cookies for Okta applications:** Device-bound session cookies will further prevent the replay of Okta sessions by requiring proof of possession of a private key stored on a user device. This challenge creates a strong bond between the session and device to reduce risk of token theft or replay attacks.
- **Enhance Bot Detection:** Introduce an added layer of bot detection and protection using third-party scores and edge-based component signals.
- **Strengthen the default CAPTCHA:** By default, events that trigger a CAPTCHA in the Okta Customer Identity Cloud will result in challenges with complexity proportional to the observed risk.
- **Extend session management control and enhance token security:** Provide full programmatic control of sessions to empower customers to build their own session control dashboards and tailor their users' experience.
- **Accelerate service accounts in SaaS and hyperscalers** as a protected resource in Okta Privileged Access.
- **Restrict enrollment of FastPass to managed devices:** Okta will provide administrators greater control by allowing pre-enrolment of users in Okta Verify and FastPass using a mobile device management (MDM) solution. This empowers customers to restrict authenticator enrolments to managed devices.
- **Expand in-product best practice guides:** Okta will provide additional in-product guides to help customers implement best practices to protect their Okta tenants.

Hardening our corporate infrastructure

We are accelerating our investments to further harden our ancillary (production-adjacent) and corporate systems.

Recently Delivered	Updates planned for April 2024	Updates planned for July 2024
• Removing all personal access to Google Chrome accounts • Increasing the level of monitoring and detection for all service accounts • Sanitizing HAR files within the Okta Help Center to detect sensitive data • Hardening source code management and database monitoring	• Extend phishing resistance across the complete employee lifecycle • Automate discovery and reporting of M2M service accounts in SaaS applications • Conduct an internal security assessment • Conduct a SaaS application security assessment	• Enhanced detection and response capabilities • Standardized and centralized vulnerability management, asset management, and CSPM • Standardized and centralized reporting for security risk management • Enhanced laptop protections • Enhanced mobile device protections

Recently delivered:

Recent changes, upgrades, and enhancements to Okta's corporate infrastructure include:

- Removing all personal access to Google Chrome accounts
- Increasing the level of monitoring and detection for all service accounts
- Sanitizing HAR (HTTP Archive Format) files within the Okta Help Center to detect sensitive data (e.g., session tokens)
- Hardening source code management and database monitoring

Updates planned for April 2024:

- **Extend phishing resistance across the complete employee lifecycle:** We've long deployed Okta FastPass for phishing-resistant MFA — we will implement phishing resistance across the complete employee lifecycle, from enrollment/onboarding through to recovery.
- **Automate discovery and reporting of M2M service accounts in SaaS applications:** We will implement a tool that provides visibility into local service accounts created within SaaS applications, improving ability to manage and rotate the secrets used for authentication.
- **Conduct an internal security assessment:** Okta is partnering with a leading global advisory firm to conduct a comprehensive security review of our products, infrastructure, and corporate systems.
- **Conduct a SaaS application security assessment**: Okta is partnering with third-party security experts to conduct security assessments of our critical SaaS applications, including the Okta Help Center.

Updates planned for July 2024:

- **Enhanced detection and response capabilities:** We will deploy solutions to enhance our detection and response capabilities, including a new security incident case management tool, a new threat intelligence platform, and additional dark web monitoring capabilities.
- **Standardized and centralized reporting for vulnerability management, asset management, and cloud security posture management (CSPM):** We will deploy a single-vendor solution to centralize all vulnerability-related information across our production and corporate environments.
- **Standardized and centralized reporting for security risk management:** We will deploy a single vendor solution to centralize risk and issue management related to our governance, risk and compliance program, including third-party risk management.
- **Enhanced laptop protections:** We will further limit and restrict how Okta laptops can be used by employees — while we have removed local admin access from all corporate employees, we plan to remove local admin access from exempted developers and engineers.
- **Enhanced mobile device protections:** We will be taking a hard line with mobile device security. While the Okta Verify product already provides assurance around device security posture — such as PIN, encryption, and operating system version checks — we will require MDM software for access to our corporate applications.

Champion customer best practices to help ensure they are best protected

We are focused on optimizing best practices for our industry to stay in lockstep with the threat landscape.

- **Phishing-resistant factors:** 100% of Okta Employees use Okta FastPass and AMFA for phishing-resistant factors. We encourage customers to consider how they can embed phishing-resistant factors into their Identity stack as well.
- **MFA enrollments and self-serve:** We are reinforcing the importance of MFA, and are focused on providing visibility for customers into all MFA enrollments (admins + users) and the ability to self-serve enroll.
- **Tailored expert assistance:** We launched Okta Expert Assist to help customers boost security and configuration with Okta security expertise. We encourage customers to leverage this for tailored recommendations.
- **Awareness and training:** We are reinforcing phishing awareness training, and deploying phishing-resistant authentication methods.
- **Expand in-product best practice guides:** We will provide additional in-product guides to help customers with best practices for protecting their Okta tenants.

Elevate our industry to be more protected from Identity attacks

Recent Okta for Good initiatives to advance the cybersecurity industry include:

- **NetHope's Global Humanitarian Information Sharing & Analysis Center** (ISAC) launched as a public-private partnership between NetHope, USAID and Okta to help global humanitarian NGOs respond to growing cyber threats
- **Cybersecurity Futures 2030**, Okta funded this global research in partnership with the UC Berkeley Center for Long-term Cybersecurity and the World Economic Forum's Centre for Cybersecurity. The goal is to identify emerging cybersecurity trends and risks for government, industry and civil society and enable better collaboration in approaching these future challenges
- **Cybersecurity Workforce Development Initiative** offers new philanthropic and educational grants to advance inclusive pathways into tech and cyber industries, and help close skills gaps in the industry
- **Nonprofit Cybersecurity Grant Portfolio**, deployed $1M+ over 2 years to support better cybersecurity practices for nonprofits

Conclusion

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

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

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