Whitepaper

Why Okta for Identity

Contents

Focus on Identity

Identity has always operated as the metaphorical front door to an organization. Accessing workforce resources or consumer apps starts with a login or a sign-up. Once a user is authenticated, the role of Identity is traditionally over. However, with cloud infrastructure and SaaS application adoption, device operating system diversity, BYOD, distributed workforce, and the growing network of business partners, the role of Identity is changing. Identity is the only technology that spans an organization's IT and security stack, validating and securing access to appropriate resources for users anywhere, on any device. With that amount of integration, Identity is uniquely positioned to help organizations drive more value from their technology stack and meet their business goals.

As the first modern Identity platform, Okta has set the industry's vision for Identity and Access Management (IAM). More than 18,000 customers have chosen Okta as their Identity partner to further their business goals.

- **Organizational agility**: Cloud applications, remote work, mobile devices, and mergers and acquisitions are all driving the explosion of digital identities. Unifying decentralized users, policies, and governance helps organizations react to change more quickly.
- **Security flexibility**: Identity is foundational to Zero Trust principles and should be able to help uphold your security posture by working with security products you have already invested in.
- **Efficiency**: Digital identities impact many aspects of operations, including employee onboarding and offboarding, reporting, and compliance. Injecting automation into the Identity process and related tasks can drive efficiencies across every organization.
- **Business growth and revenue**. Identity solutions should deliver value quickly for organizations, improve customer and employee experiences, and support future growth.

Read on for more information on how Okta helps organizations meet these business goals.

Goal

Organizational Agility

With Okta, you can quickly and seamlessly unify decentralized identities and coordinate changing user populations and needs without months of complex consolidation and migrations.

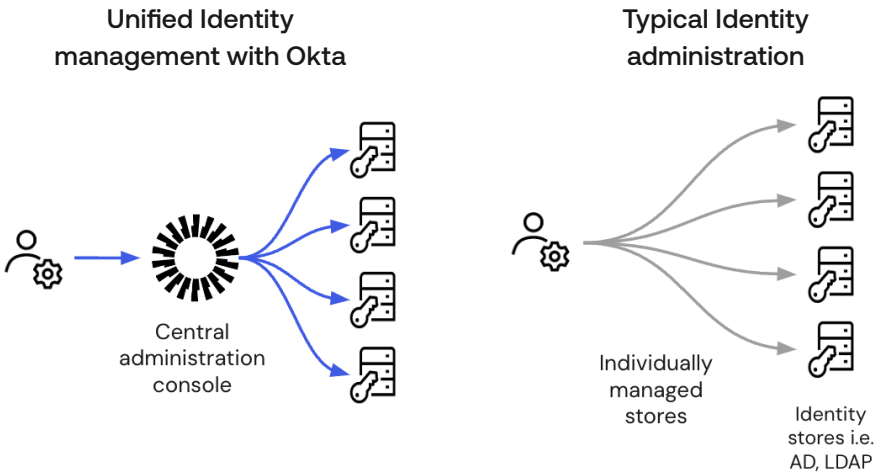
Eliminate Identity fragmentation

Many organizations have multiple Identity stores with different types of users, such as contractors, partners, customers, and employees from mergers and acquisitions. Okta provides a single view across all these groups with a single, unified directory that integrates AD and LDAP directories while:

- Supporting rapid integration of mergers and acquisitions
- Synchronizing organizations/business units
- Coordinating Identity policies across all user populations

News Corp

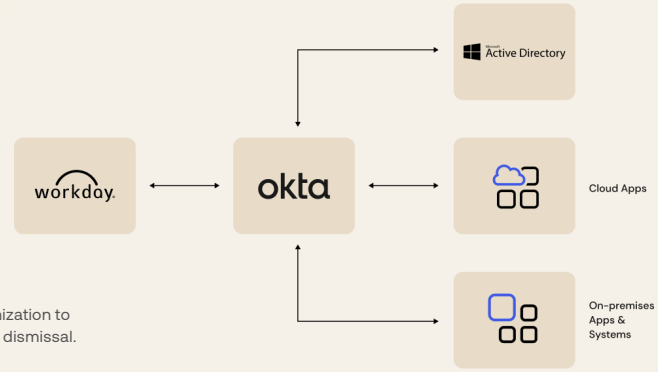
- Saves 1000 work hours annually on synchronizing and consolidating domains after mergers and acquisitions
- Automates 70% of provisioning tasks and gets new employees up and running two hours faster



Simplify lifecycle management

An HR information system (HRIS) is the system of record for employees. Can you efficiently share data with IT to create user accounts, assign applications, and deactivate users? Okta integrates with all major HRIS solutions, including Workday, SuccessFactors, UltiPro, BambooHR, and Namely. In addition, support for Anything-as-a-Source (XaaS) enables Okta to leverage any data container as a source (for example, a CSV file or database). Okta's pre-built integrations with HRISs:

- Unify HR and IT under a single source of truth, using employee data and updates to inform the user lifecycle across IT systems, including directories, SaaS and on-premises applications
- Include attribute-based sourcing, which enables Okta to draw upon multiple sources to create a user profile from many existing data sources



In the diagram above, the Okta and Workday integration provides near real-time synchronization to mitigate deprovisioning security exposures that may occur, such as during an employee's dismissal.

Goal

Security Flexibility

Managing and securing digital identities is a top-three security priority for a majority of businesses. Okta enhances your existing security solutions, avoiding costly, time-consuming redeployments of platform-based security products.

Simplify multi-factor authentication adoption

Until recently, multi-factor authentication (MFA) has been the single most valuable solution for preventing phishing attacks, account compromises, and other Identity-driven threats. It is also a critical capability for Zero Trust architectures. Since 2020, enterprise global MFA adoption has risen, but some vendors are struggling to gain momentum, with MFA adoption rates for administrators at only 34%. Weak adoption is typically caused by difficulty integrating into current systems, limited MFA endpoint support, poor user experiences, and a lack of factor choices.

Okta addresses all of these limitations with support for:

- A seamless end-user experience that is as secure as it is easy to adopt
- Phishing-resistant factors that work consistently across all major platforms
- Authentication policies that tell admins which types of factors are in their environment, are easy to administer, can be tied to specific factors, and can have as many as the org needs without performance degradation
- SSO and MFA for cloud and on-premises apps (for example, Oracle EBS) and MFA for legacy access points (LDAP, RADIUS, API)
- Pre-authorization, risk, and context-based protection
- The Identity industry's broadest and deepest set of pre-integrated cloud and security apps

The result: Okta business customers adopt MFA more than the industry average. As of January 2023, **64% of Okta workforce users and 90% of administrators use MFA[2].**

> "Okta is the center of our Zero Trust universe."
>
> **Steve Williams**
> Enterprise Chief Information Security Officer NTT DATA

[1] ISDA 2023 Trends in Identity Security

[2] Okta Secure Sign-In Trends Report 2023

Adopt phishing-resistant authentication

Phishing schemes were the number one internet crime reported in the US in 2022 and caused the highest financial loss to victims[3]. While MFA has been the gold standard for preventing phishing, recent high-profile attacks have shown that MFA is no longer enough to prevent successful data breaches. Phishing-resistant authentication is now needed to combat the increasing sophistication of these attacks.

Okta supports all major phishing-resistant authenticators, including:

- FIDO2 Web Authentication (WebAuthn) that allows users to leverage security keys and biometric data to authenticate their identity (for example, Windows Hello for Business and macOS TouchID)
- Smart Card Personal Identity Verification (PIV) or Common Access Card (CAC)
- FIDO2 Passkeys for multiple devices and across multiple operating systems

In addition, Okta FastPass is a phishing-resistant, passwordless authentication service that works on most major platforms (e.g. Windows, macOS, Android, iOS, and iPadOS). It enables secure, passwordless login to any SAML, OIDC, or WS-Fed app in Okta, and can work with your device management tool of choice.

Phishing Resistant Authenticators at Okta

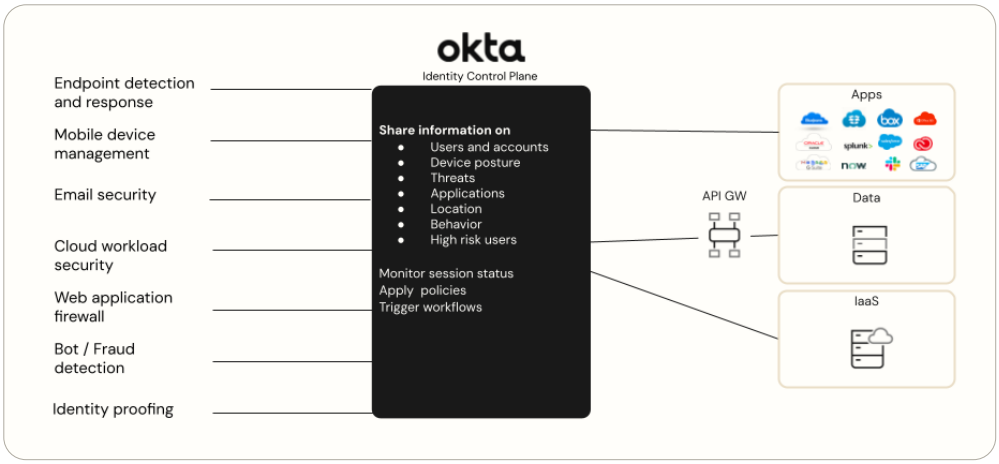
	FIDO2 WebAuthn / Passkeys			Okta FastPass	Smart Card
	Device Bound Passkeys		Synchable Passkeys		PIV/CAC, CBA
	Security Keys (e.g Yubikeys)	Windows Platform (Single-device)	Platform Authenticator (Multi-device)		
Phishing Resistant	✓	✓	✓	✓	✓
Hardware Protected (TPM/Secure Enclave)	✓	✓ System dependent	✗	✓ System dependent	✓
Authenticator Bound	✓	✓	✗	✓	✓
Browser / OS Support	✓	✓	Platform dependent	✓	Limited mobile support
Self Enroll/Recover	✓	✓	✓	✓	✗
Deployability	Additional Hardware	✓	✓	✓	Additional Hardware
Device Assurance	✗	✗	✗	✓	✗

[3] Federal Bureau of Investigation Internet Crime Report 2021

Establish defense-in-depth

Identity solutions comprise one aspect of a defense-in-depth security approach. With more than 100 verified integrations with security vendors, Okta integrates with your existing security technologies and makes it easy to adopt new ones. These unique integrations enhance the capabilities of your existing security technologies by aggregating risk signals for easier analysis and actionable insights. Based on these aggregated risk signals, organizations can take immediate action to mitigate threats beyond a user's initial authentication. Okta works with leading security vendors to detect and take action against threats, support many authentication factors, and promote a Zero Trust architecture.

In the example below, Okta manages Identity and works with the other vendors to secure valid users and their sessions and protect against threats.



NTT DATA

- Took only **two months to deploy Okta** to support a workforce of 120,000 across countries
- Gained ability to **integrate with security solutions** such as CrowdStrike, Proofpoint, and Tanium

Reduce risk exposure from legacy solutions

Legacy directory solutions have been around for 20 years. While they have been a cornerstone for many organizations, attackers have exposed many vulnerabilities over that period, including:

- Pass-the-Hash attacks
- Kerberoasting
- NTLM Relay
- Over-permissioned accounts
- Improper group nesting

By using Okta, customers can reduce reliance on legacy solutions. Together with credential best practices, you can prevent legacy vulnerabilities from exposing cloud apps and resources.

Goal

Efficiency

Organizations often struggle to grant users appropriate access to apps in a timely fashion. Complex or manual processes can limit productivity for IT and the organization as a whole. Okta simplifies Identity processes with tools and automation that free up IT and developers' time, enabling them to focus on delivering new innovations that improve business productivity. Okta simplifies compliance by integrating governance capabilities with IAM.

With Okta, Priceline

- Reduces time spent on IT application access requests by 75%
- Saves 25 minutes on every application provisioning request, per employee

Automate Identity processes

Okta workflows make it easy to automate any Identity process at scale without writing code. Pre-built connectors to the most popular SaaS applications, simple logic, and the ability to connect to any publicly available API make innovation quick and simple. Customize employee or partner user lifecycle processes (for example, joining, moving, or leaving), schedule audits and reports, take pre-programmed actions on suspicious activity to improve security posture, and much more.

Make compliance easier

Once you've linked your HRIS systems to Identity and automated onboarding and offboarding workflows, how do you demonstrate compliance with access policies? Okta unifies Identity Governance and Administration (IGA) and IAM, providing a comprehensive view of every user's access patterns, so administrators and reviewers can make informed decisions about access. Automatically approve appropriate access requests and enforce access policies with no-code workflows. Easily produce reports that demonstrate compliance to auditors. As with all Okta solutions, businesses can deploy quickly, scale as needed, and integrate with their solution stack, providing a quick time-to-value.

Streamline remote work and BYOD

Remote work and bring-your-own-device (BYOD) have many benefits but introduce extra security risks. To combat this risk, organizations often introduce extra authentication steps, introducing friction for users and impacting productivity. With Okta, organizations can offer secure, consistent, and frictionless access for employees, partners, and contractors, on managed or unmanaged devices. Okta delivers:

- A consistent user experience across major consumer devices and platforms
- Integrations with mobile device management (MDM) apps for managed devices
- Secure access for unmanaged devices without requiring MDM
- Many supported native and third-party factors
- The option to go passwordless and reduce friction while maintaining strong security

Goal

Business Growth and Revenue

Identity has the potential to increase customer sign-ups, improve employee productivity, and get apps to market faster. Managing your customer or workforce identities with Okta improves the bottom line and can also improve the top line. Develop secure digital relationships with frictionless sign-ups that turn consumers into loyal customers. Streamline worker onboarding and offboarding with intuitive Identity interfaces, automated access management workflows, and self-serve access requests so they can contribute to revenue faster.

> "Okta's Customer Identity Cloud has been critical to our success as we continue to scale and grow globally. It enables an easy, frictionless, and secure experience that's vital to our customers."
>
> **Kim Huffman**
> CIO, Navan

Tailor customer experiences

For digital-first organizations or those wrestling with digital transformation, Customer Identity and Access Management (CIAM) is fundamental. CIAM solutions optimize customer experiences while keeping their data secure. Engaged customers who trust a brand buy more and spend more. Okta's CIAM solution provides out-of-the-box building blocks and customizability. Your business units can deliver the next great mobile app or breakaway portal initiative with tools like:

- Authentication to custom apps with frictionless login via social, SAML, or OIDC
- IdP discovery with adaptive context
- Robust password enforcement and management
- Passwordless user/email magic link
- Risk-based auth and pre-auth sign-on policy
- Out-of-the-box but customizable sign-in experience with software development kits (SDKs), REST API, and event hooks
- Pre-built workflows and customizable templates
- Per-app branding

Enjoy faster time to value

Okta customers deploy in weeks, not months, and transform their organizations in months, not years, gaining competitive advantage while freeing up developers' time for other projects. Developers can take advantage of private and public cloud deployment, built-in attack protection, and no-code integrations. Teams can use drag-and-drop actions to build custom Identity flows that address your unique requirements. Instantly add new capabilities as you need them.

Future-proof technology choices

Okta helps bridge the gap between what you have and what you need and never forces customers to rip out existing technologies or replace them with Okta's infrastructure or cloud stack. Okta does not save the best capabilities or performance for its own productivity or security tools. Rather, Okta:

- Supports all apps and services equally as a pure-play Identity platform
- Works with best-of-breed technologies as a neutral vendor
- Empowers customers to choose the best IT for their needs and requirements

Okta customers have the freedom to choose whichever technology solves their problems most effectively today and into the future. Customers modernize their environments while leveraging their existing architecture and established, successful IT implementations.

Ensure availability and scalability

Okta's commitment to freeing anyone to safely use any technology has resulted in one of the most robust, modern cloud architectures on the market, delivering real-time performance, scalability, availability, and burstability. Okta's operational track record demonstrates ongoing consistency and reliability.

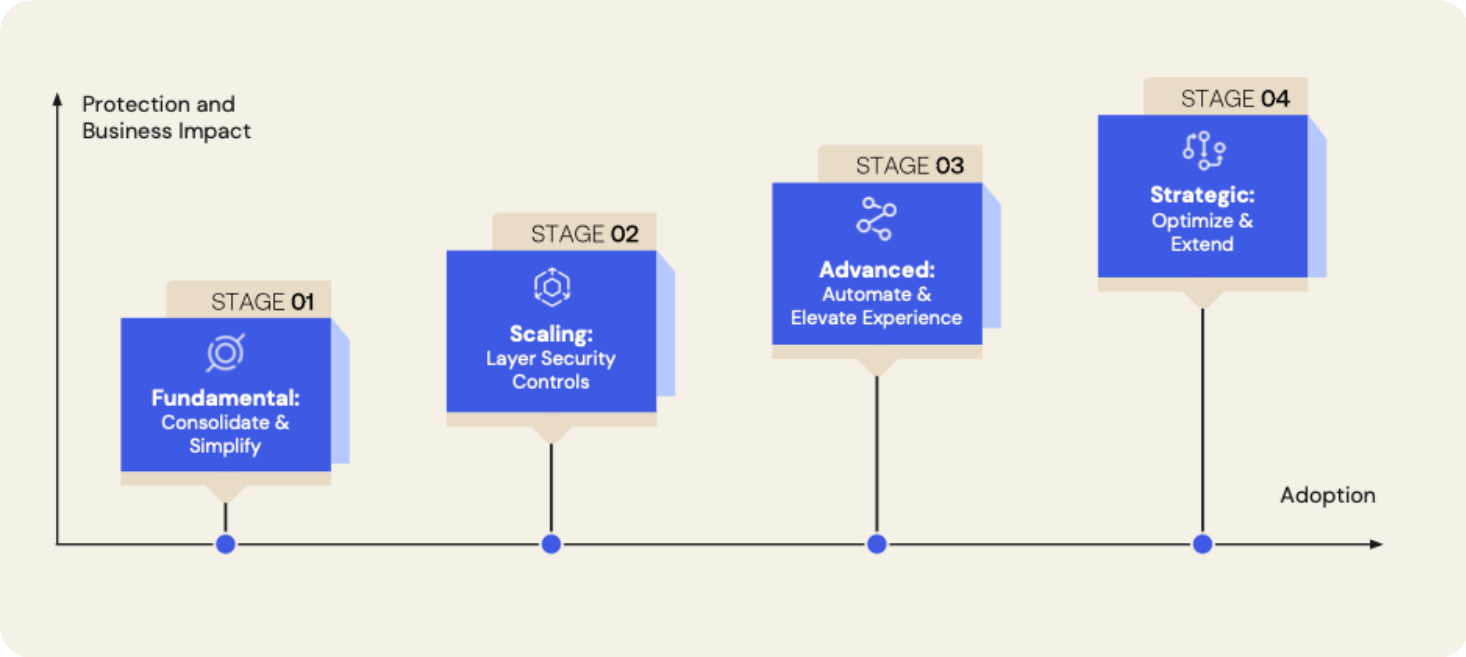
- 99.996% operational uptime from 2018–2023
- 100 minutes of outage from 2018–June 2023
- 60K continuous annual tests
- Zero planned downtime service
- 50+ annual releases

Identity Use Cases and Maturity Model

Based upon lessons learned from the most successful practices of thousands of Okta customers, Okta's Workforce Identity Maturity Model[4] aims to empower organizations to:

- Assess the state of their Identity posture
- Identify and implement Identity capabilities
- Measure the impact and outcomes of Identity initiatives

The Identity Maturity Model



Fundamental: Consolidate and simplify

Disconnected Identity solutions contribute to directory sprawl. Often, Identity solutions have limited or cumbersome integrations with each other or other systems, requiring considerable manual effort from administrators. The time-consuming undertaking of managing applications and users across multiple business units, or after mergers and acquisitions, is often what motivates organizations to take meaningful action on the Identity maturation journey. Consolidating the Identity stack provides a single view across all user groups, making organizations more agile and IT more efficient.

[4] A Comprehensive Guide for your Workforce Identity Maturity Journey, Okta, 2022

Okta in industry analyst research*

- Okta Named a Leader in the Gartner® Magic Quadrant™ for Access Management for Six Consecutive Years
- Okta placed highest in Ability to Execute for two years in a row
- Okta Recognized as a Gartner® Peer Insights™ Customers' Choice for Access Management 5X in a Row

Scaling: Layer security controls

With fundamental Identity functions in place, focus shifts to further reducing the administrative burden on IT and application owners, and increasing productivity for end users. Many of the same capabilities that enable productivity and efficiency also reduce risk, such as retiring legacy systems that cannot support Identity federation, extending MFA adoption, and consolidating access controls across cloud and on-premises applications.

Advanced: Automate and elevate experience

At this stage, organizations have integrated Identity systems with the broader IT and security stacks. The focus on increasing efficiency shifts to automating tasks and entire processes. For example, customizable workflows help manage application access requests by employees or tailor marketing experiences to registered customers.

Strategic: Optimize and extend Identity

At this stage, Identity is a business enabler and an important aspect of governance, risk management, and compliance. Identity has board-level visibility alongside other strategic programs, and KPIs track progress on how it contributes to business goals.

Okta's entire organization focused on helping customers meet their Identity needs and solve their Identity challenges. No matter where you are in your Identity journey, Okta is your go-to partner, helping you navigate the most complex use cases with the fastest time to value.

*Gartner, Magic Quadrant for Access Management, Henrique Teixeira, Abhyuday Data, Michael Kelley, James Hoover, Brian Guthrie 1 November 2022. Gartner, Voice of the Customer for Access Management, Peer Contributors, 26 April 2023. GARTNER is a registered trademark and service mark, and PEER INSIGHTS and Magic Quadrant are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Okta."

About Okta

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