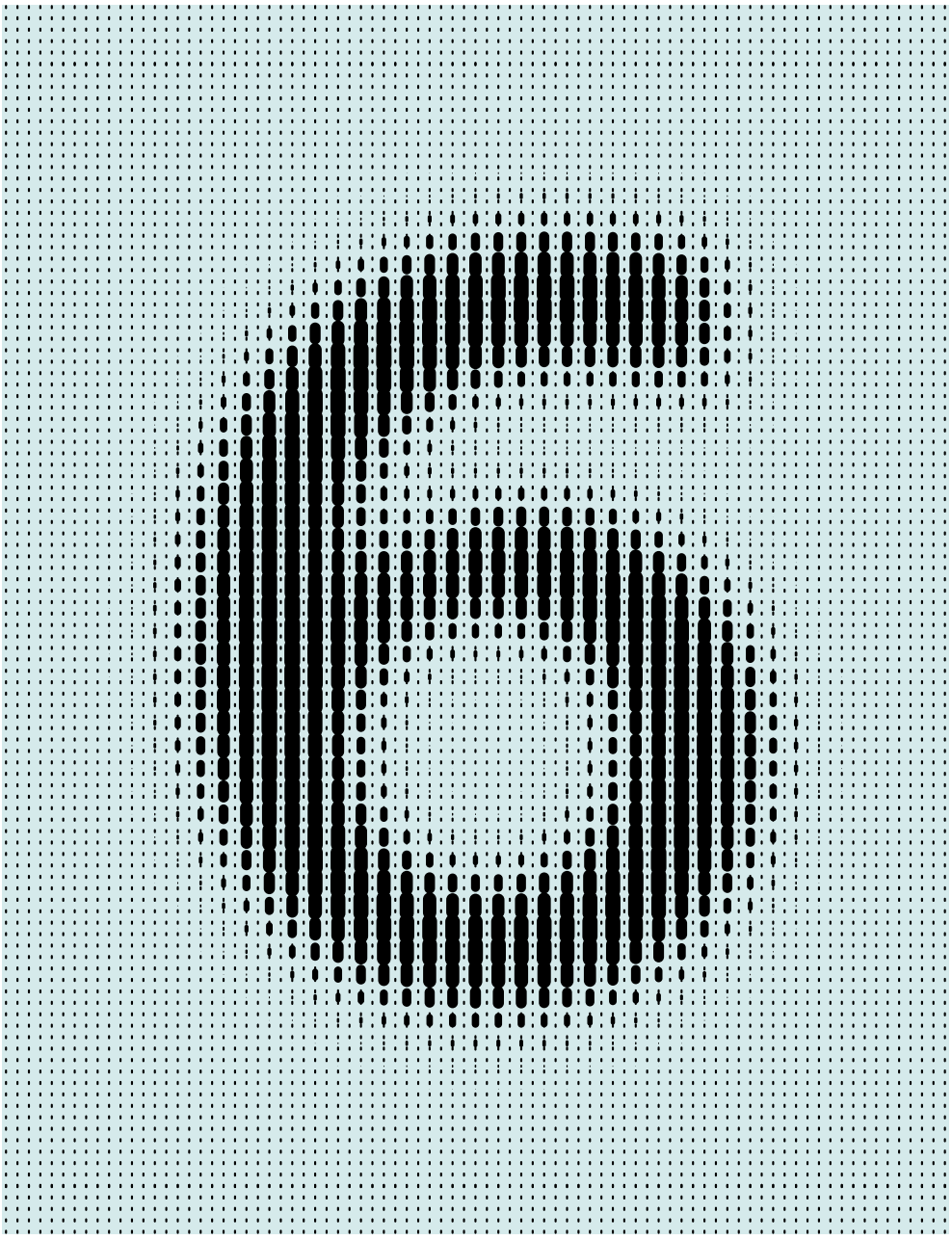
Whitepaper

November 2020

Six Reasons Microsoft Customers Choose Okta for Identity

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

Contents

Introduction

If your organization uses Microsoft, it's time to take a closer look at identity management. The right identity solution can speed adoption of cloud technologies, and help modernize legacy systems and applications for the cloud. Many Microsoft customers end up choosing Okta to manage identity for their cloud applications.

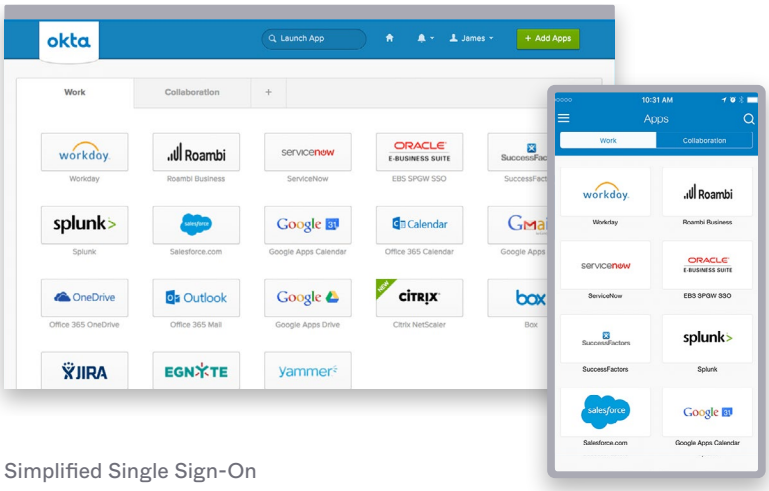
Here are six reasons why.

1. Simplified Single Sign-On from Active Directory

Organizations with investments in a directory service such as Active Directory want to use it to enable Single Sign-On (SSO) to both on-premises and cloud applications. When architected properly, Single Sign-On eliminates the frustration of having to create and remember unique passwords for each application, and it improves the security of corporate data.

Microsoft provides a set of tools to enable SSO via their Azure AD cloud service: Active Directory Federation Services (AD FS), Azure AD Connect (previously known as DirSync), Password Sync, Passthrough authentication, and Microsoft Identity Manager (previously Forefront Identity Manager). These tools have gradually improved over time, but require deploying, configuring, and managing significant server resources. Each service requires individual configuration and integration with the Azure AD cloud service.

Customers turn to Okta when they realize they can deploy SSO from Active Directory in much less time. Okta is a vendor-neutral cloud based identity and access solution that requires no tradeoffs between ease of use and full functionality.



Simplified Single Sign-On

2. Automated User Lifecycle Management

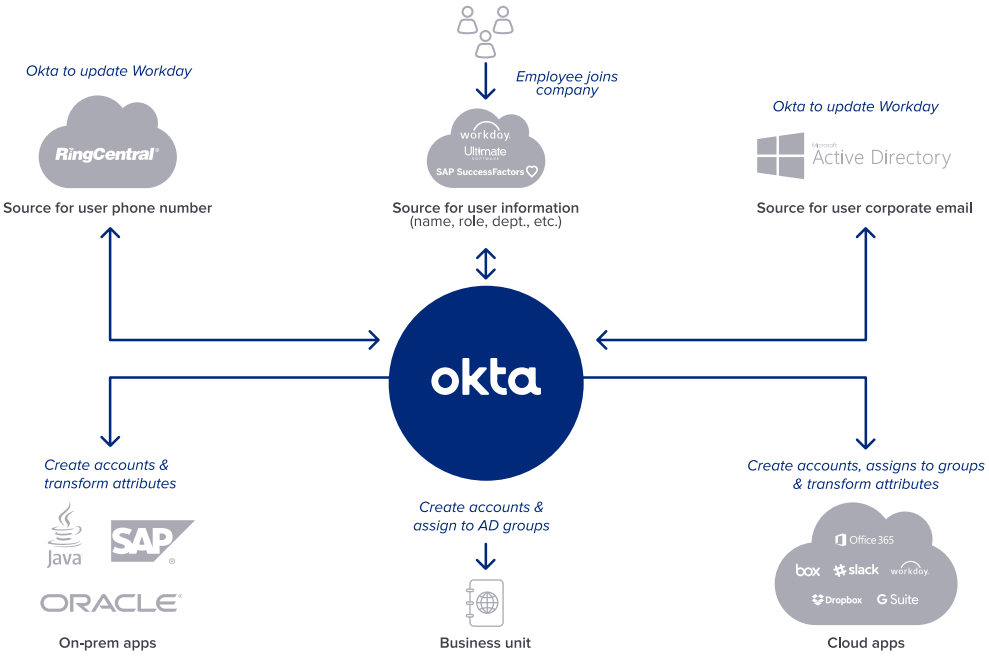
There will always be a flux of users that join and leave your organization. When IT says they can no longer manage user onboarding and offboarding using a checklist, it's time for lifecycle management. As users join, they require day one access to the applications they need. When they leave, IT must remove their access to everything, immediately.

Okta makes it easy to create new user accounts for cloud apps, and deploy the apps with the correct access level. Okta syncs in real-time to Active Directory, LDAP, or other directories. As people change job roles or leave, Okta automatically changes or removes their access to applications and services based on these identity changes.

Many companies today are using cloud-based human capital management (HCM) systems like Workday to simplify the way their Human Resources department gets work done. Even with a powerful HCM tool, the onboarding process for new hires can be painful, often requiring IT to respond to tickets manually, and create accounts in apps and systems for each new user.

With Okta's Workday Integration, the HR department can drive the entire employee lifecycle from onboarding to job changes to offboarding, and provide access to the apps and directories users need.

Microsoft currently supports integration with Workday, while other HCM systems require custom integration using Microsoft Identity Manager and SQL servers. Okta supports HR-driven onboarding and offboarding from Workday and all other popular HCM systems including UltiPro, BambooHR, SuccessFactors, G Suite and Netsuite.

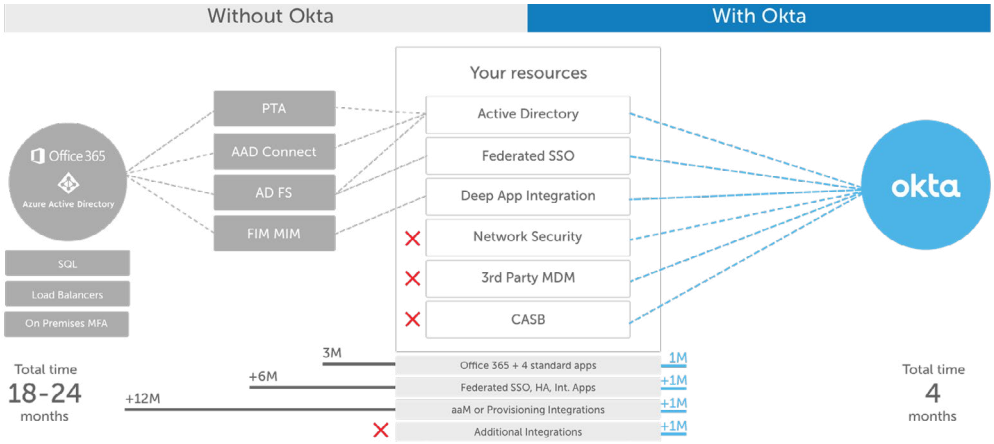


Automated used lifecycle management

3. Faster Office 365 Deployments

Office 365 is by far the most complex cloud application suite you may ever have to manage, and many Microsoft-centric organizations choose Okta specifically for Office 365. That's because Okta shortens Office 365 deployment time, supports both web and native Office 365 apps, and offers unique automation and user experience improvements that save on long-term operational costs.

Many medium- to large-sized organizations using Office 365 require high availability, automated onboarding and offboarding, and license management. For better security, they need federated Single Sign-On instead of synced passwords. They may also need to support third-party mobile device management, network security, and integration with a cloud application security broker. To achieve all this, Microsoft recommends deploying Office 365 with AD FS, Azure AD Connect, and Microsoft Identity Manager (MIM)—a process that can take about 18-24 months. Okta supports all of these requirements out-of-box, and gets it all done six times faster.



Simplify and accelerate Office 365 deployments—all from a single platform

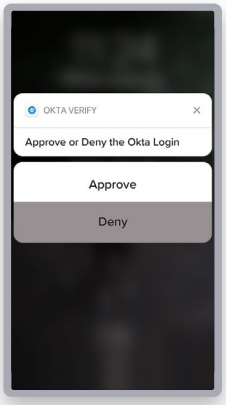
How are you managing Office 365 licenses? Can you provision licenses automatically based on user roles and group membership? Ideally you should be able to specify which Office 365 services get enabled during user onboarding. For example, you could assign Microsoft E3 licenses with only Exchange and Lync enabled for your Sales team, while your Support team gets an E3 license with SharePoint Online enabled. Okta takes care of license management. IT just needs to create a user in Active Directory and assign them to a group, and Okta will automate everything else. The new employee can easily gain access to Office 365 within a matter of seconds of IT initiating the process. Enhanced offboarding capabilities will allow IT to remove licenses for deactivated users.

4. Adaptive Security

Microsoft-centric organizations have the same concerns as any organization adopting cloud technologies. 73% of passwords are duplicates[1], so it's no wonder that 81% of data breaches involve stolen or weak credentials[2], and 91% of phishing attacks target user credentials[3]. Multi-Factor Authentication (MFA) is a way to reduce the risk of stolen passwords by requiring a second, or even a third way to verify a user's identity before they are allowed access to any applications and systems.

Security needs to adapt to changing circumstances and unusual events, so identities and assets are still secured without overburdening users. Okta's adaptive MFA allows for dynamic policy changes and step-up authentication that responds to changes in user and device behavior, location, or other contexts. Okta's MFA is built for rapid expansion into the cloud, and supports on-premises authentication for VPN, RDP, and SSH. Hybrid environments and mobile users are also covered, so access to apps and data is always secured.

While Microsoft offers a cloud-based solution for MFA, you would need to deploy their on-premises MFA server along with AD FS to get the same level of features that Okta provides out-of-box. Okta's adaptive MFA provides strong authentication across all applications, and supports more third-party MFA factors like U2F, YubiKey, Smart Cards, Google Authenticator and more. Okta requires no on-premises MFA servers, and is easy to use for both administrators and end users.



Adaptive security

[1] Source: TeleSign 2016 Consumer Account Security Report
[2] Source: 2017 Verizon Data Breach Investigations Report
[3] Source: 2016 Verizon Data Breach Investigations Report

5. Smoother Mergers and Acquisitions

Organizations undergoing mergers & acquisitions need to consolidate multiple user domains to provide access to business-critical applications.

After a merger, there are multiple directories or domains for different user populations. Consolidating these domains is costly, takes a long time and has security implications. IT becomes a bottleneck and end users spend weeks to months waiting for access to parent company resources. Multiple, inconsistent security policies can create a security risk for the business. Meanwhile IT has limited visibility into who has access to what resources.

Identity management is the key control point to integrate users in different organizations to shared applications. Okta helps organizations connect different populations and geographies without the need to set up Active Directory Trusts, modify firewall policies, or invest in more infrastructure to connect them all together. Okta integrates identities from any number of Active Directory domains and reduces the directory cleanup and reconciliation process. Users in newly acquired organizations get day one access to parent company resources, while IT gets a single pane view of security for the entire organization.

Centralize identities across any number of directories or domains

6. Works Great with Microsoft and Other Technologies

Microsoft customers also choose Okta for identity because of its strong partnership and broad integration with Microsoft products including Office 365, Windows 10, Azure Active Directory, SharePoint, and Intune. Okta's cloud-based identity solution works great with Microsoft and other technology vendors. Our vendor-neutral identity architecture makes it easy to roll out Microsoft products and thousands of other cloud applications and services.

Broad integration for Microsoft products

For more information, visit **https://www.okta.com/microsoft-integrations/** or contact us at **https://www.okta.com/contact-sales/** to talk to a sales representative.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 application integrations, Okta customers can easily and securely use the best technologies for their business. To learn more, visit **okta.com**.