Reduce IT Friction

Automate the Identity Lifecycle to Streamline IT Operations

okta

Executive Summary

Whether it is a large enterprise or a company growing at a fast pace, when it comes to managing the identity lifecycle, IT teams become a bottleneck for providing access and a security risk when it's time to remove it.

Manual processes and automation through scripts that require ongoing maintenance is how many companies choose to manage onboarding, transitions and offboarding often to realize that with the pace of change in the business and increased adoption of cloud applications these approaches cannot scale. A modern identity lifecycle management to streamline operations, provide day one access, and prevent former users retaining business accounts is required.

Such an identity strategy helps businesses increase agility by deploying a single identity architecture, and facilitating change through automating many IT lifecycles. Businesses that embrace this change are able to decrease costs, increase efficiency and their security posture at the same time.

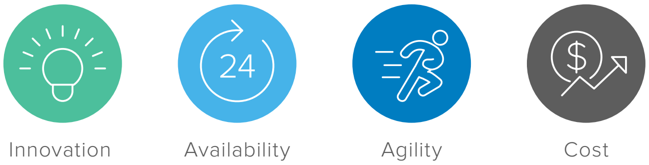
The Challenge: Increasing Pace of Change

If there is any constant in modern business and IT, it's change.

- Companies who used to have a handful of applications to manage for just their core employee base, now adopt cloud services in the tens or hundreds, adding new ones every month.
- IT is now managing an increasing amount of identities that are considered non-employee.
- Compounding reality is the fact that IT organizations are constantly being asked to do more with less. To provide value to shareholders, IT organizations push for efficiency, which often means making tough prioritization choices.

There's a desire to focus on innovation so the business can keep growing, but agility, availability and cost, often become the focus.

Integration periods stifle innovation, along with on-prem system failures, slow onboarding process that impacts the entire company, as well as an overwhelming amounts of service requests directed at IT. Security is also applying pressure, with risk of breach from error prone manual process and lack of visibility into who has access to what.



Business areas impacted from manual identity lifecycle management

Left unchecked these impacts become a massive burden:

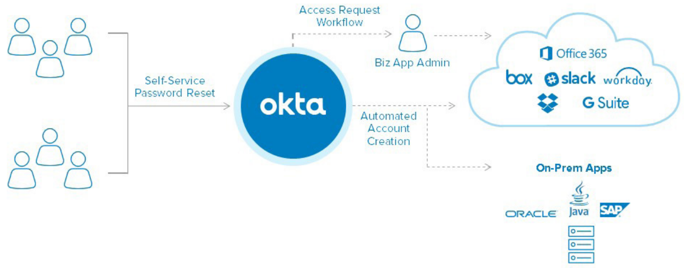
- **40%** of the workforce is going to be flexible (non-employee) by 2020 from 20% today[1]
- **81%** of employees admitted to using unauthorized SaaS applications[2]
- **73%** of IT leaders agreed that keeping track of identity and permissions across environments is a primary challenge[3]

Providing Day One Access

A survey[4], held by Okta's partner ServiceNow, found that 8 in 10 companies both large and small, still use unstructured manual tools such as email, spreadsheets and even personal visits to drive routine work processes, and fewer than 1 in 10 have automated applications assignment for employee onboarding. The result is frustrated and unproductive employees, and an overwhelmed IT department.

Modern organizations provide self-service tools like password reset or access requests, through a single identity management system. Account management is downstream applications are automated using provisioning connectors and access decisions are delegated to right people automatically without generating IT tickets.

[1] Intuit 2020 Report–Freelancer Study
[2] Shadow IT: Data protection and cloud security by Gigaom Research
[3] IDG Survey, 2017
[4] Today's state of work: the productivity drain, ServiceNow 2015



Okta streamlines day one access

The result is faster integration of acquired products and services, IT focus shifting to money generating initiatives and reduced likelihood of assignment error or unauthorized access.

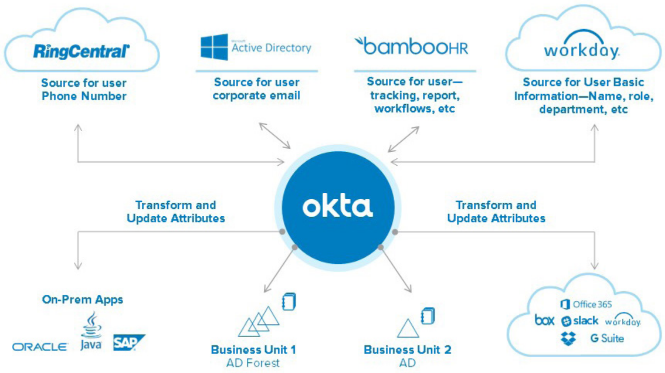
Creating a Single Source of Truth

Every company needs a directory to manage information on employees joining, moving and leaving the organization. HR owns that directory, but IT needs its own directory for managing access and permissions. In some cases, IT will have more than one directory to manage—one for contractors and partners, and one that they inherited from an acquisition or a merger, etc. IT is typically tasked with keeping information across all systems up to date, and that includes all downstream applications profiles, which turns into a tedious ongoing task.

Okta has collected data from customers and found that an organization can spend up to 6,250 hours a year on tasks like change requests[5]. This includes updating downstream accounts in applications, informing HR and other tasks required by the business.

The friction created by directories sprawl also includes expensive cross domain infrastructure, error-prone processes that create security holes and lack of visibility into compliance.

Leveraging a modern cloud directory and connecting it to all the sources of truth in the organization, like HR, active directory, and results in information being automatically synced, no need for investing time and effort in how to scale infrastructure, and out-of-the-box real-time security and audit reporting.



Creating a single source of truth with Okta

Staying Secure with Comprehensive Offboarding

Even a single account of one employee that was left active for any reason, might create a security loophole. According to a security survey[6] "More than 13% of respondents can still access a previous employer's' systems using their old credentials." Additionally, in a recent survey done by IDG, IT professionals attested it takes 47 hours on average to manually offboard and deactivate a user who has left the organization.

While HR is tasked with offboarding users and maybe deactivating accounts in payroll or travel systems, it's too often a few days before anyone tells IT that the employee has been terminated. This is exactly the time, where an employee who was involuntarily terminated may be most motivated to inflict damage however possible. When that happens, the average cost of a data breach in the US is estimated at a staggering $7M[7]. While some organizations can recover or bare the cost, the trust with their customers likely is permanently damaged.

With a modern identity and management solution offboarding can be seamless and real-time. With HR connected to the identity system a termination in the HR system results in immediate deactivation of accounts for the terminated user. This can be customized to only take effect on situations like involuntary termination and allow grace periods in specific situations to some of the systems a user still needs access after they leave. An easy to generate report is available to show when user got deprovisioned from what systems and at what time.

[5] Okta Business Value customer research data
[6] Information Security Survey, 2014 liebsoft

[7] Ponemon Institute cost of data breach study, 2017

With such system in place both security and IT teams can feel confident that access is only granted to right people at the right time, from any device. To comply with audits—reports can easily be generated, and providing all this information through a SIEM integration can further improve security and management of security related events.

Why Okta?

Okta's modern approach to identity management is uniquely positioned to help businesses take control of identity and automate all lifecycles with any business process.

Decreased costs and enhanced efficiency

- Eliminate password reset tickets
- Reduce manual work for account management
- Delegate access decisions to the right people

Accelerate Business Growth

- Reduce disruptions to employee access to resources
- Allow IT to innovate instead of dealing with manual tasks around offboarding and onboarding

Enhance Security

- Automated deactivation of company accounts
- Automated blocked access from all devices
- Audit reporting and rogue account detection

Roadmap to Success

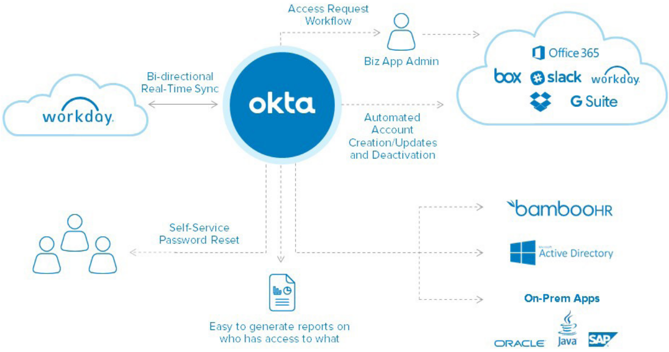
To recap, a modern, automated approach to identity lifecycle management helps improve productivity and enhance security. Where should organizations start?

We recommend you focus on these key milestones:

1. Deploying a cloud-based identity platform with high availability and user store.
2. Achieving simple integration as new access requirements are introduced.
3. Automating account management through provisioning connectors.
4. Integrating your HR system with the identity system to achieve full automation of onboarding and offboarding.

We are Here to Help

Okta provides an end-to-end suite for modern identity management. We connect with complex service infrastructures, integrate with all of the top cloud services and HR systems to automate lifecycle management. We do all of that by working with your existing infrastructure to provide value.


Access Request Workflow
Biz App Admin
Office 365
box
slack
workday.
G Suite
Bi-directional Real-Time Sync
workday.
okta
Automated Account Creation/Updates and Deactivation
bambooHR
Active Directory
On-Prem Apps
ORACLE
Java
SAP
Self-Service Password Reset
Easy to generate reports on who has access to what

Automate onboarding and offboarding with Okta

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device.

Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

For more information, go to https://okta.com