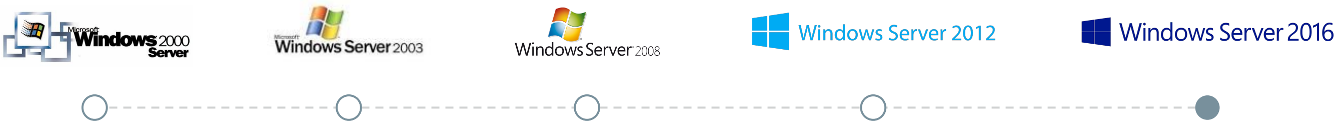
Rethink AD

A Paradigm Shift for Identity Management.
Free IT from the Constraints of Active Directory.

Index

How did Active Directory establish its foothold?



For decades, Microsoft's Active Directory (AD) has been included "free" with Windows Server and Microsoft Exchange, creating legacy lock-in. Over the years, AD's tentacles grew as it became deeply embedded in most companies' IT infrastructures. Because it was easy to integrate with, join to, and build applications and processes around, that's what companies did — until AD became the default platform in ~95% of organizations. However, it's become a legacy utility that creates more headaches than benefits for IT managers.

Microsoft originally built AD to compete with the previous directory services leader, Novell, and offer IT departments a central way to manage their organization's users and devices. Back then, IT was typically supporting a single Windows PC for each person in their organization. This device directory connected users with on-premises applications like Microsoft Exchange and Office on their individual computers, as well as with other types of machines like printers and servers. IT departments eventually built logic in AD to enforce device-specific security policies such as password reset requirements.

Along with these capabilities, AD brought several frustrations for IT. Administrators struggled to maintain brittle integrations as their IT ecosystems evolved, and didn't appreciate the extra hardware, software and people resources AD required. What's more, since it was never intended to function outside a corporate network, or with non-Microsoft apps and devices, AD has done a poor job adapting to modern challenges. AD is still useful for on-premises challenges, but its inherent limitations are holding IT back from focusing on innovation. Meanwhile, Microsoft is economically incentivized to keep customers on AD as long as possible or risk taking a hit to their operating system and application revenue.

Although AD may never disappear from the landscape completely, IT departments now have alternatives. Today there are paths toward retiring AD, or at least reducing its role in the infrastructure. The benefits of minimizing IT's reliance on AD far outweigh any effort this will take.

Today’s evolving IT ecosystem

Most of AD’s initial reasons for being back in 1999 have since been supplanted by the capabilities of modern solutions, such as single sign-on (SSO) tools and human resource management systems (HRMS). Yet IT still spends inordinate amounts of time maintaining AD because its tentacles reach across the ecosystem. That said, broad industry trends are chipping away at AD’s effectiveness.

The rise of cloud computing

Integration with Microsoft Exchange is no longer a top priority for IT, since many companies are rapidly moving to Office 365 and other cloud-based applications. The cloud has not only upended the delivery model for software, it’s disrupted access for end users, management for devices and security as well. More applications are now accessed through browsers, and the average enterprise uses a whopping 329 different business apps from a variety of vendors and platforms.

A heterogeneous mobile landscape

If they want to retain top talent, companies have no choice but to support flexible bring-your-own-device (BYOD) policies. Windows holds a shrinking share of the desktop and mobile OS markets — declining from 57% to just 35% from 2016-2018[1]— as people and companies flock to Apple and Android. This means that IT must be able to manage all types of devices, including iPhones, Android tablets and Apple Watches—none of which can be joined to AD natively.

Flexible workforces

More businesses employ virtual, remote and contract workers than ever before. According to UpWork, 69% of younger managers support remote employees.[2] Fluid organizational boundaries require efficient, dynamic collaboration and shared access to key business systems. Remote workers, as well as external contributors like partners and customers, must be able to securely access these applications from any public network.

Today’s workers demand freedom to use any device, application or network they prefer, and simply won’t tolerate Microsoft lock-in anymore. In this new status quo, simple and secure user access is more important than ever, yet the key factors that AD was built around (like operating system and device-centric identities housed on a private corporate network) are no longer relevant.

[1] Source: NetMarketShare
[2] Source: UpWork new Workforce Report 2019

AD’s tenuous balance of benefits and drawbacks

While AD made it easy for IT admins to manage devices and security policies (and for employees to use Office applications), prevailing industry trends are intensifying the pain points of an infrastructure built around AD. For example, despite the potential risk of exposing too much corporate data, many companies are adding external contributors to AD even though they only required access to one or two internal applications. This is because IT departments are stuck in a catch-22. They have a litany of complaints about AD, including:

- ⓘ Poor management of non-Windows machines
- ⓘ Poor experience for web-based software
- ⓘ Poor security for external users, devices and applications
- ⓘ Expensive to install and maintain
- ⓘ Reduced flexibility for change, due to AD’s static, proprietary directory
- ⓘ Declining talent pool of AD administrators
- ⓘ Extra hardware, software and people requirements

However, IT can’t simply decommission AD, because it’s responsible for triggering important workflows, supporting government risk compliance, connecting printers and more. This business logic has proliferated to the point where current admins worry they don’t even know all of AD’s interdependencies across their infrastructure. These issues greatly hinder IT’s agility and innovation, because providing simple and secure access for every user isn’t a nice-to-have — it’s table stakes for any business.

Best-of-breed solutions make a world without AD feasible

The good news is that cloud platforms, which don't require AD, are rapidly gaining traction in the market. In our most recent Businesses @ Work report, we found that large companies are deploying 163 apps on average, and that number is growing. This even applies to businesses that already run Microsoft's Office 365 — below you can see the growing foothold of best-of-breed apps such as Salesforce, Slack, Box, AWS, Zoom and even G Suite.

G	box	slack	salesforce	aws	zoom
28%	**32%**	**28%**	**45%**	**36%**	**24%**
26%	34%	25%	45%	34%	15%
22%	37%	19%	44%	30%	8%
20%	37%	11%	44%	26%	4%

% of Office 365 customers running different best-of-breed apps, 2016 to 2019

Each new application a company adopts presents an opportunity to start minimizing its reliance on AD. In addition to the best-of-breed categories mentioned above and below, there's now a whole range of popular IT systems that are perfectly suited for a world without AD, including IT Service Management (ITSM), Security Information and Event Management (SIEM) and more.

Human Resource Management Systems (HRMS)

Cloud HR applications like Workday, Namely, BambooHR, SAP SuccessFactors and UltiPro have made rapid strides in recent years, and can now manage the user onboarding and offboarding that AD formerly handled. As companies move away from on-prem HR systems like PeopleSoft and Oracle, it's easier to make HRMS the source of truth for employees. By adopting a modern identity solution with pre-built HRMS integration, IT can avoid wasting time on re-building the rigid connections or manual processes that previously kept the HRMS synced with AD.

workday. SAP SuccessFactors bambooHR™ UltiPro® by ULTIMATE SOFTWARE

Single Sign-On (SSO) & Identity-as-a-Service (IDaaS) technologies

Comprehensive, 100% cloud-based identity and access management services maintain security beyond the firewall, and work seamlessly across the entire app ecosystem. Agnostic SSO systems like Okta can manage all identity types and broker secure access to any third-party software-as-a-service (SaaS) tool. This gives users easy access to all of their web applications without having to authenticate to each application individually, while reducing IT support and training needs.

Enterprise Mobility Management (EMM) platforms

Also known as unified endpoint management (UEM) systems, mobile management tools like VMware's AirWatch, MobileIron and Intune can control access for any device in use across the enterprise. By adopting one of these solutions, companies gain a single source of truth for all connected devices, and avoid the challenges of trying to connect non-Windows machines to AD.

airwatch by vmware MobileIron Intune

Emerging cloud-hosted printer services

New tools like Google Cloud Print, PrinterOn and PrinterLogic can fill the gap left by AD's connection to a company's local printers. They enable cloud printing to any printer across the enterprise, without compromising security policies or making changes to the network, applications or devices.

Google Cloud Print PRINTERON print simply anywhere PrinterLogic

Microsoft's response

Microsoft also recognizes the problems with its legacy approach, but the company's new extensions for AD each come with their own limitations.

Active Directory Federation Services

This on-premises service offers better access to cloud apps, but lacks flexibility because it necessitates multiple network/hardware components and additional software. It requires complex configuration and maintenance for each new application. So, while the license for ADFS is "free," there are several hidden costs associated with its setup, ongoing support and hardware. It's also built on top of Active Directory, which hardly liberates companies from that dependency.

Azure Active Directory

Many consider this cloud-based solution to be the default alternative for on-prem AD, but Azure AD still has a long way to go before it will manage external users or non-Microsoft apps or devices effectively. Moving to Azure AD is not as easy as it may sound, because it mostly works with cloud apps, and doesn't easily support the on-prem systems that currently rely on AD. Plus, it's even more optimized for Microsoft software, with just a handful of connectors to other apps.

Harness identity management to fuel growth

While there's big opportunity ahead, let's be clear — the move away from on-prem AD will be gradual, similar to other paradigm shifts that have taken place in the technology industry. Think about the evolution from mainframes to client servers, from data centers to hybrid or public clouds, and from on-prem to SaaS applications. During each of these progressions, some companies embraced the new technology sooner than others. Ultimately, even the holdouts who feared loss of control found that by leveraging the latest advances, they greatly improved agility and reduced cost while maintaining oversight of their environments.

It's time to accelerate this transition for identity management and identify the ideal approach for today's realities. The market is poised for this change, and since cloud identity solutions meet secure access needs with or without AD in place, there's no need for you to rip it out in one fell swoop.

The Identity Management Maturity Curve

The rethink of AD and the journey towards full identity and access management in the cloud will look different for each IT organization. Your particular company might fit into any of these typical stages:

Level 4

Secure modern infrastructure

The ultimate goal is to keep AD to a minimum and move to a predominantly cloud-based identity infrastructure for 90-100% of needs. IdaaS controls access to servers, network resources like WiFi and VPN, enabling passwordless factors and adaptive controls to secure access to all. Management of file servers and print servers shift to cloud-based equivalents

Level 3

Establishing an IdaaS Identity Hub

Customers that are streamlining their onboarding can source employees and users from their HR system, and provision, update, and revoke resources automatically. Non-employees, contractors, partners, and customers are also managed natively in IdaaS. A device management solution (e.g. UEM or EMM) controls end user devices

Level 2

Extending AD with SSO and MFA

Forward-thinking IT departments use modern IdaaS to augment their legacy AD investment, securing it with SSO integration to accommodate on-premises apps, web apps, and resources with MFA

Level 1

Initial State

This is a baseline state, where customers still rely on on-prem AD despite strong reservations, and often have to build brittle, ad hoc workarounds to fill its gaps

Consider your company's unique identity management requirements

Depending on your organization's characteristics, you'll have various things to keep in mind as you move through this identity maturity curve.

New cloud and mobile-forward startups or spin-offs

- Newer businesses, with younger workforces and more technical savviness
- Less on-prem infrastructure, less technical debt
- Moving 100% into the cloud requires less work and budget

Large organizations with multiple domains and a big on-prem footprint

- Older businesses that have typically acquired other companies or evolved into a distributed model
- Likely to rely on legacy technologies that may not be compatible with IDaaS
- More on-prem inertia, having put years or decades of IT budgets into products that depend on AD
- IT is not managed centrally, requiring more coordination for change management

Companies in highly-regulated industries with extensive data centers

- Organizations of any size, with extra layer of security and compliance requirements
- More on-prem infrastructure, with reporting and compliance tooling embedded in their stack
- Likely to have extensive data centers and larger management staffs
- Requirements are harder for cloud services to match in terms of security, compliance, performance and availability
- Migration path to IDaaS is likely to be slower

Start minimizing your dependence on AD

When it comes to escaping the constraints of AD, several best practices can help expedite the process — both today and throughout your longer-term evolution. The best place to start is by shrinking the footprint of AD in your infrastructure and gradually shifting more identity and access management tasks over to an IDaaS solution. Below are some specific steps you can take.

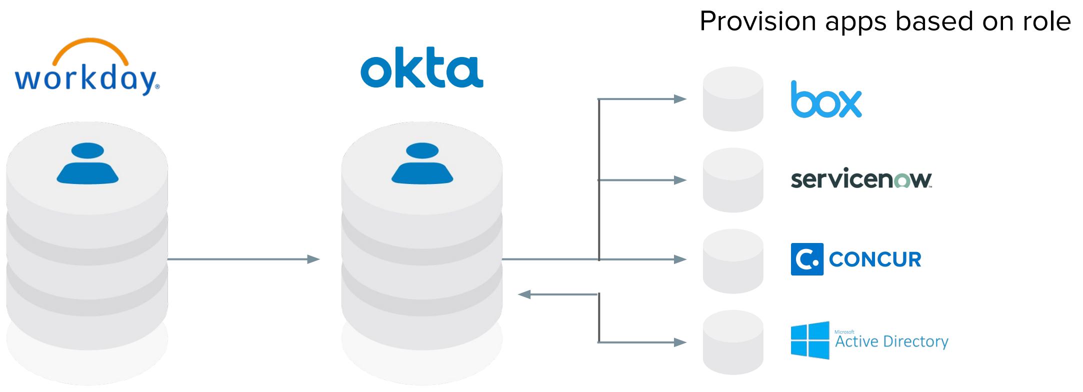
Move select user groups and applications out of AD

Most company directories now house a growing subset of external users who don't actually need profiles in AD. You might be paying Microsoft extortionary Client Access prices for thousands of contractors or temp workers, and their devices. And these users are probably getting too many network or application access privileges and could even move laterally around your network to access to sensitive resources.

Moving these identities into the cloud is much easier than moving employee identities with complicated access dependencies. Instead of keeping external contributors in AD, you can manage their identities in a secure, dynamic cloud directory with zero default access. IDaaS solutions make it easy to add or remove people, and set appropriate restrictions for each user group, e.g. automatically suspending their access on specified dates.

Next, consider moving any web-based applications or on-prem systems that already have modern authentication protocols (e.g. SAML, OIDC) over to your IDaaS for access management. Also look for key IT workflows and processes you can easily move to the cloud for more efficient updates and maintenance.

Make HRMS your master people record



Provision apps based on role

Import users & groups into Okta

(Start date or X days before)

Create accounts in AD
Write back email & phone

Rather than provisioning new users first in AD and pushing their profiles to your HRMS, try moving AD downstream in that process. This will marginalize AD's role in your infrastructure, while speeding up onboarding for new users connecting to your enterprise. Once your HRMS is the single source of truth for your entire workforce, you can connect their records effortlessly to a unified directory in the cloud.

Your identity solution should integrate automatically and act as a translator, managing groups, roles and access rights as they change. At the same time, it will ensure proper authentication to all apps that support current protocols. All this, while synching with AD and provisioning access to older apps when needed.

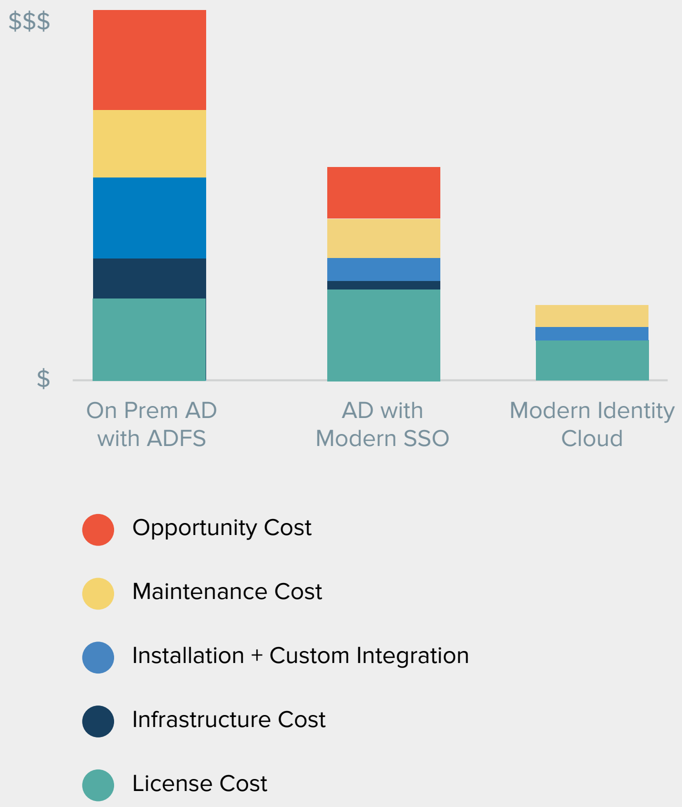
Adopt EMM to manage heterogeneous devices

By connecting an EMM platform to your universal directory as well, you'll gain a powerful layer of access management across all kinds of devices. In addition, you'll be able to up your security game by supplementing each user's identity with their device information during the authentication process. By using an IDaaS as the gatekeeper for both people and devices, you'll ensure dynamic device access and pervasive security.

Identify and roadmap application modernization

Many companies are moving key functions onto popular cloud apps like Workday or Salesforce. Each system migration is a great opportunity to link a new app into your IDaaS platform and further reduce reliance on AD.

Understand cost implications



Source: Okta Business Value Team

For on-premises systems that won't be moving to the cloud any time soon, you can still update their authentication layers and password lists using modern protocols. This is more secure than using AD through a firewall for authentication, which can actually expose users to more data on your network. By pointing non-cloud apps to an identity solution in the cloud rather than to AD or a homegrown LDAP infrastructure, you can leverage multi-factor authentication and other security best practices. Additionally, you can store master passwords securely in the cloud, and push them downstream to AD when needed.

The Okta Identity Cloud: A modern identity platform

No matter where your company is in its identity roadmap, Okta delivers benefits today and continuous innovation for your long-term needs. Currently, the Okta Identity Cloud offers key capabilities such as:

- **Single Sign-On**

  Okta's SSO provides a great experience for end users accessing applications.

- **Universal Directory**

  Purpose-built for both internal and external users, Okta's directory aggregates and manages users of all types with an intuitive admin interface.

- **Lifecycle Management**

  Okta's solution ensures user accounts are automatically created and removed where and when they're needed.

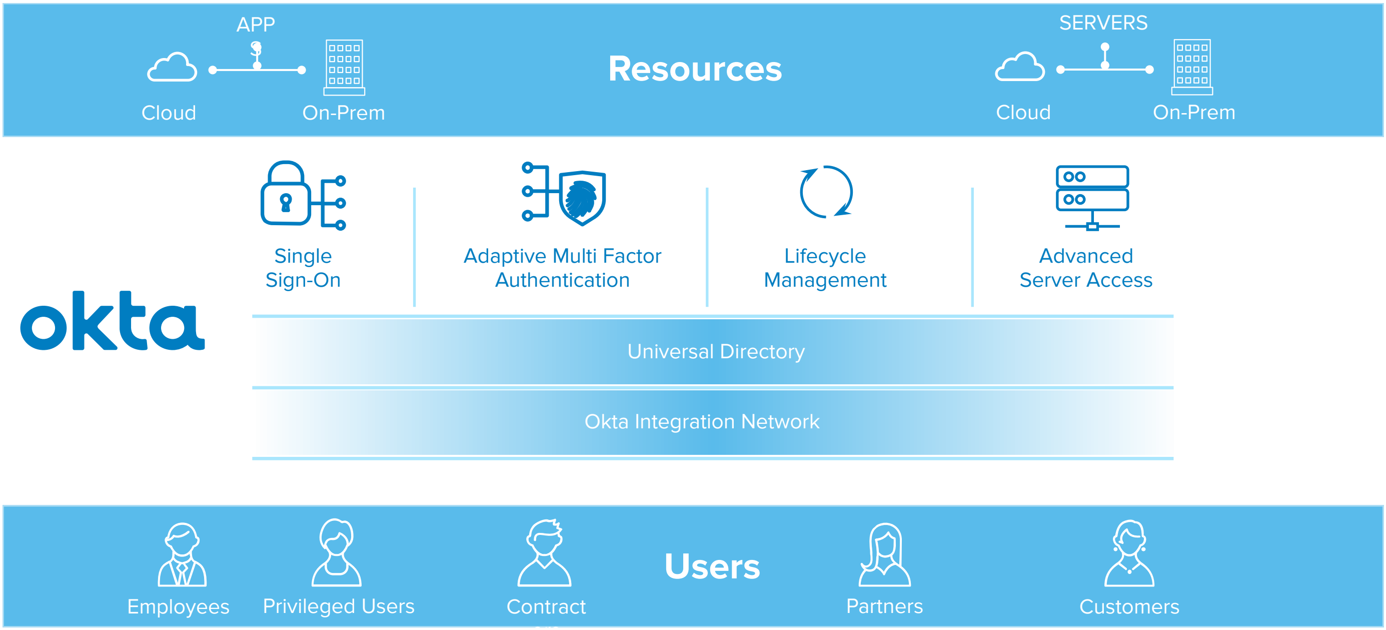
- **Multi-Factor Authentication**

  Okta's adaptive, secure authentication techniques add a layer of security to SSO to maintain security as you move IP off-network.

As the standards bearer for identity management, we'll extend these capabilities and our partnerships and to accommodate new types of identities, groups, devices and permissions over time. Just a few of the advantages you'll enjoy with Okta include:

Simplicity and support for constantly evolving identities

Identities are in motion, which is why Okta was designed to support flows of identity data, rather than a static storage directory. You can store data in Okta's Universal Directory, or simply use it as a staging area to facilitate identity changes. Either way, IT will maintain full, self-service control and visibility over all identity processes, group rules and configurations. Your team will be more productive and reduce its TCO, thanks to modern interfaces into your directory that automate tedious integration tasks.



More bi-directional integrations than any other system

Over 5k connectors enable Okta to serve as a hub and trigger user additions or changes in any system. Our connectors are equipped by default with inbound and outbound data flow templates, and can transform data in flight. Okta also provides an extensible schema to support attributes of different formats and types, from different sources, and offer flexible ways to build your own connectors. We support industry standards for SSO federation and maintain a broad set of APIs. Since Okta is agnostic and invests equally in building hooks for any app that matters to our customers, you'll gain more flexibility to extend and integrate your directory.

High availability and security

Okta's cloud platform is built for 99.99% availability and zero planned downtime. Our architecture is 100% multi-tenant, stateless and extremely redundant across multiple availability zones and regions. In addition, you never have to worry about changes to underlying applications because Okta continuously manages and monitors all web application integrations — so your employees, partners and customers have uninterrupted access to business critical applications.

Comprehensive device support

Heterogeneous device environments are inevitable, so you might as well plan for that as the rule. Our EMM partners integrate seamlessly with Okta's access platform to manage devices of all types and give you a mechanism to apply controls to those devices. Thanks to this complementary approach, Okta customers can use device context to ensure appropriate access decisions.

Rethinking Active Directory

Imagine a world where you can choose any technology your business wants, integrate it into your ecosystem rapidly, and deliver a pristine end user experience. While the path to rethinking Microsoft's Active Directory may be long, you can start chipping away at the hold it has on your organization today. The demands of your flexible, mobile workforce aren't going away. And while your business may always have some need for on-prem applications, your ratio of on-prem to cloud apps is probably declining. Soon, web-based tools will meet the vast majority of business requirements, leaving just the long tail of niche on-prem systems to worry about.

Furthermore, the risks of chugging along as a slow-moving cost center don't outweigh the opportunities that will emerge from future-proofing your business with better IT security and flexibility. Eliminating AD will significantly improve your technology infrastructure and your business as a whole — increasing agility, productivity and scalability, while reducing costs and freeing IT resources for strategic initiatives and innovation.

Given all of this, adopting IDaaS and marginalizing the role of AD in your IT ecosystem is a no brainer. This paradigm shift will help transform IT from a back-office service organization into a powerful center of true business enablement.