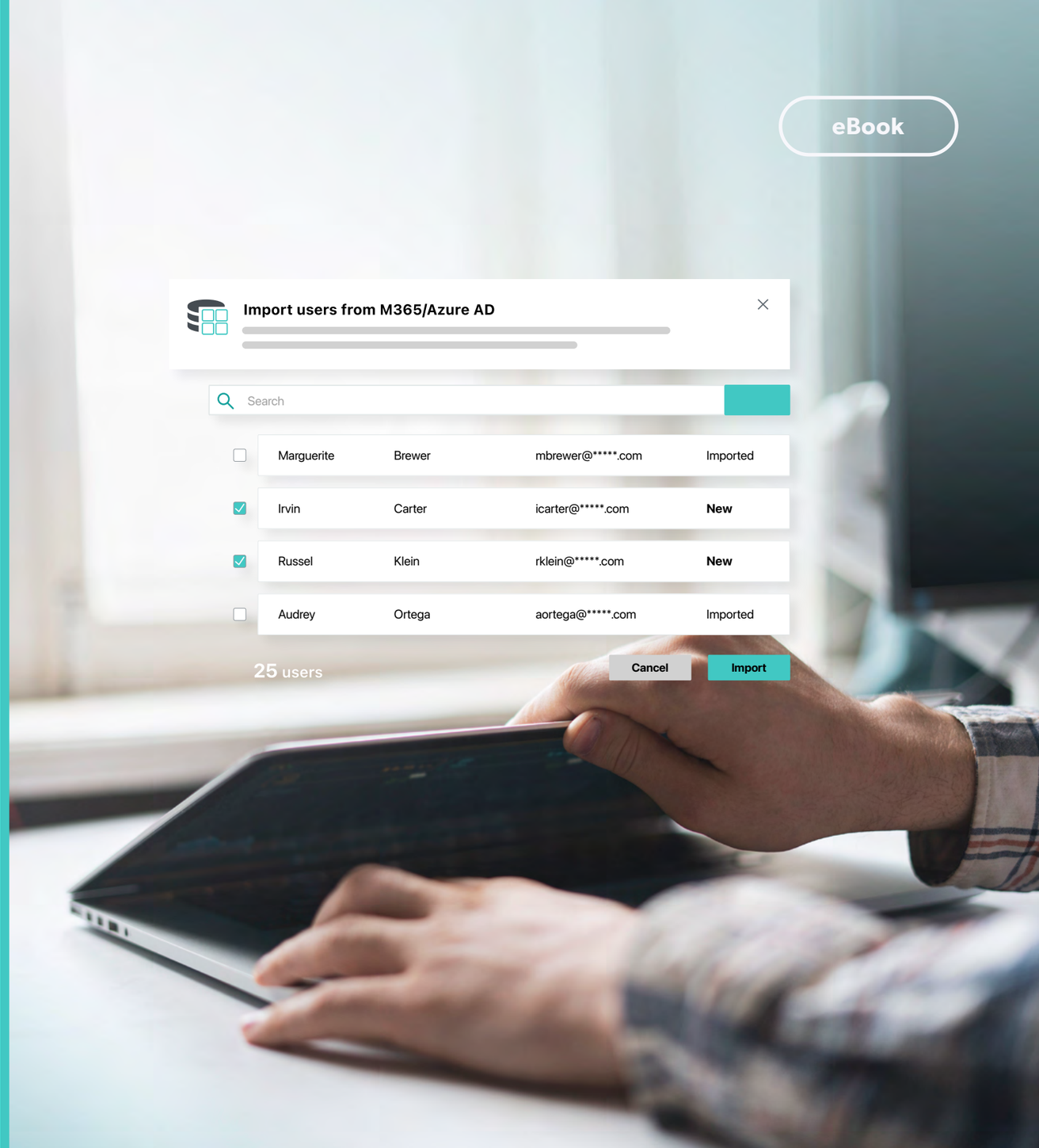
jumpcloud™

eBook

Breaking Up With Active Directory

KONTAIN



Setting the Scene

You've seen this movie before.

Sometimes, a great beginning doesn't guarantee a great ending. Reevaluating and breaking up with a long-standing product and vendor relationship can be hard, but not doing so can prevent you from growing. Breakups are never fun, but neither is getting left behind because you were afraid to make a change.

This eBook stories the steps many small and medium-sized enterprises (SMEs) go through when they realize they need to expand beyond or move away from Microsoft Active Directory (AD). It's not easy — many have been using AD for decades. But AD is becoming more difficult to integrate into modern environments, and your future IT decisions shouldn't have to revolve around what will work with a depreciating solution. Fortunately, there are ways to either expand beyond or break away from AD to achieve the flexibility, simplicity, and modernity that will empower your organization to thrive.

The Meet-Cute

How Most Businesses Got Their Start With Active Directory

Imagine: It's some time pre-pandemic, and for most businesses, the office is still… well, a traditional office. Think stationary computers (or permanently docked laptops), wired phones, and server rooms. Every employee is an in-office worker.

Take Example Game Studio (a fictional mobile game studio we'll follow throughout this eBook) for instance.* Example Game Studio is on the cusp of something big. Business is booming, and it expects its 25 employees to double in the next year. It's set up like most businesses: a fully in-office team and a fully on-premises infrastructure.

As the game studio grows, a directory becomes the next logical step. And what better choice than the leading name: Microsoft Active Directory? It's designed to support all the Windows machines in the office, can keep employee data organized, and will be right at home in the server room. AD was made for instances like this. It's a perfect match.

This was the decision process that led many businesses to choose AD as their directory. Microsoft AD was released in 1999 and was the reigning business directory solution for quite some time. It was designed to support an on-premises office environment built on expected (though quickly seen as legacy) technology; for most businesses, this made it a no-brainer choice.

However, the way we do business has changed, and the typical business environment no longer looks like the one AD was designed to support. This has created challenges that are beginning to snowball as businesses modernize.

*Example Game Studio is a fictional company developed for the purposes of illustrating the concepts in this eBook. No identification with an actual organization is intended and should not be inferred.

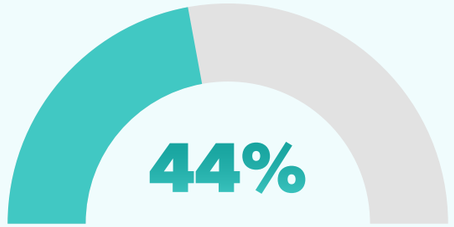
We're Growing Apart

Modern Businesses Need More From Their Directory

Things have changed over the years at Example Game Studio. For one thing, employees no longer commute to the office every day. They work in a hybrid model, with some days in the office and some days remote. The business has grown significantly, and it's added many resources to its stack. Most of them are cloud-based. It's even begun to transition some of its existing legacy applications to SaaS alternatives. The server room is looking a little worse for wear as the business has put off upkeep, opting instead to host more of its functionality in the cloud.

Active Directory was built for legacy. It was created in the early 2000s and was intended for LANs that weren't federated out to web applications. Its model is still based on that time period. As SaaS and cloud-based resources overtake legacy, Active Directory struggles to keep up.

Further, the number of resources most businesses need is rising faster than AD can accommodate: about 44% of employees require access to **six or more accounts** to do their jobs. Today's work resources tend to be diverse in type and vendor, which calls for a robust domain to support them all. The foundational compatibility that initially made AD such a perfect match is crumbling.



About 44% of employees require access to six or more accounts to do their jobs.

Key Changes Influencing How the Modern Business Works

The need to support remote and hybrid work.

The average SME now has **more remote and hybrid workers** than people fully on-site. This requires user identities, resources, devices, and security to extend beyond the physical office.

Business keeps moving to the cloud.

From how businesses source their infrastructure to the types of resources they use, the cloud is becoming the preferred method for doing business.

More variety in resource types and vendors in a typical business' stack.

Vendors are creating more products to solve the business needs that are amidst these changes. From remote team-building apps to cloud-based training platforms, these solutions tend to be specialized and diverse in both type and vendor.

This expands the average business' stack and requires a directory that's capable of connecting users to many different cloud applications using a wide variety of authentication protocols.

More heterogeneous device environments.

Windows is no longer the business go-to for devices. In fact, Windows machines now only account for **68% of the average SME's fleet**. On the other hand, Mac, Linux, and mobile devices are becoming more popular.

Key Limitations of Active Directory in a Modern Business

AD no longer meets the needs of modern businesses as it once did. Some of AD's key limitations in the modern market include:

Legacy ties.

AD relies on on-premises infrastructure and isn't designed to support the cloud. This hinders a business's ability to support the cloud-based resources and the remote and hybrid work that have become a business norm.

Over time, this can prevent businesses from choosing the best IT solutions for them, instead forcing them to pick from a limited range of solutions that can work with their AD instance.

Inability to support Zero Trust security.

AD's on-premises domain conflicts with Zero Trust principles, which reject the concept of security at the physical perimeter and instead advocate for identity-based security at every access transaction.

Increasing complexity.

The wider the gap between AD's services and a business's needs, the more hoops they'll have to jump through to get AD to work. These hoops usually involve complex expansions and integrations that require deep expertise and manual management.

These additions tend to make Microsoft's already complex pricing structure even more confusing. It becomes hard to know what services you need, and many businesses end up overbuying.

The "Microsoft Monoculture."

Microsoft products are designed for a Microsoft-exclusive environment. But as businesses incorporate more solutions from different sources into their stacks, they need flexibility and vendor-agnosticism.

Catered to enterprise.

Microsoft solutions tend to cater to enterprise-level organizations. This often leaves SMEs without the internal expertise and resources to manage AD effectively.

Making Concessions

At this stage, businesses often start making some alterations to keep AD serving its purpose. Some of those key changes include:

Incorporating third-party add-ons from multiple vendors.

Establishing SaaS solutions in an on-premises AD environment often requires third-party add-ons. These add-ons usually mean complex integrations, which can be difficult to manage and secure — especially when they pile up, which they tend to do as businesses grow and modernize.

Extending proprietary integrations across the Microsoft domain.

For AD to support a cloud-based environment, it needs to undergo some changes. For example, a traditional, on-premises AD environment can't support remote workers without the use of a VPN. In another example, applying multi-factor authentication (MFA) across the infrastructure becomes more difficult when it's riddled with third-party add-ons.

These extensions tend to be fragile and cumbersome: they're difficult to configure, resistant to change, and highly vulnerable to domino-effect breakage when something else in the domain changes. And because they're proprietary, they create vendor lock-in, which can significantly stunt growth.

Overspending on infrastructure.

The increased use of cloud-based tools has shed light on how much (more) time and labor go into managing an on-premises AD environment. In addition to the routine manual labor premised environments pose, businesses may also face the need for expensive bulk infrastructure purchases and upgrades as their business grows and adopts more cloud-based technology. These investments can seem particularly expensive when compared with the low costs and flexibility of using cloud-based infrastructure.

In addition, Microsoft's complex licensing structure can be difficult to navigate, and every layer of add-ons and changes makes it more confusing. Compared to the trend toward straightforward SaaS pricing tiers, navigating AD's costs can feel particularly frustrating. Many businesses end up paying for services they don't need.

Infrastructure TCO

Usually, the costs of hosting infrastructure far outstrip the costs of migrating to the cloud. Calculate the total cost of ownership (TCO) of your infrastructure and compare it with the TCO of alternatives you're considering with the **free TCO Calculator**.

But Wait… I Can Change!

Microsoft Introduces Azure AD. Can It Bridge the Gap?

Essentially, you need both AD *and* Azure AD unless your infrastructure is 100% in the cloud or 100% on premises — and you'll have to manage each independently.

Growing apart hurts. As companies began turning to cloud-based solutions, Microsoft released Azure (its cloud environment) and Azure AD to manage Azure identities. However, while Azure AD sounds like the cloud-based version of AD, it's far from it. Azure AD is not a cloud version of AD, nor does it replace AD.

Like many companies, Example Game Studio adopted Azure AD as they started using Microsoft's cloud-based solutions, like Microsoft 365. However, it soon became clear that Azure AD couldn't effectively replace its on-premises instance of AD.

Azure AD's Limitations

Azure AD is not simply a cloud copy of, nor a replacement for, AD. It's an entirely different tool: AD and Azure AD's architecture, security policies, and functionality are different, and they function independently from one another. They can sync with one another, but even then, some data — like group configurations — are fundamentally different and don't carry over smoothly from AD to Azure AD.

Further, while Azure AD makes Microsoft's cloud resources more accessible, it doesn't provide any support for on-premises functionality, like LDAP or RADIUS. For companies with a hybrid infrastructure or plans to adopt the cloud gradually, this means they need both AD *and* Azure AD. Managing two independent directories is a headache for even the best-equipped admins, let alone lean IT teams working at a resource-strapped SME.

Some of Azure AD's key limitations include:

Azure AD can't do everything AD can do. The following capabilities are either unavailable or cost extra under Azure AD:

- Patching (unavailable).
- Asset management (unavailable).
- Remote support (additional cost).
- Conditional access (additional cost).

It is not an endpoint manager. Azure AD is an identity provider for Azure resources, but it does not manage devices. Managing devices requires a separate tool, like Microsoft Endpoint Manager. These additions create complexity in the environment, which makes it harder to secure and manage. And it favors Windows devices over others, which can make multi-OS environments more difficult to manage.

It lacks workflow automation. Azure AD requires manual, in-depth management. This can be a significant source of strain for an SME with a lean IT team. And because Microsoft generally caters to enterprises rather than SMEs, it often fails to provide the level of support SMEs need to configure and manage Azure AD.

It does not support rich identity lifecycle management. Lifecycle management is highly manual with few tools to speed up tedious processes like group onboarding and provisioning. Azure AD does not offer group policy (which is one of the management strengths of on-premises AD). This creates problems when trying to duplicate proven and powerful management paradigms from AD to Azure AD — it's virtually impossible.

It locks you in. Azure AD creates the same monoculture that AD does — it supports Microsoft products well and makes it difficult to use alternatives. MFA, for example, can only be natively integrated for Microsoft products. And the more layers you add to Azure AD, the harder it is to pry them apart if you want to expand or move away from it.

It doesn't support legacy resources. Azure AD doesn't support legacy resources. It can't support LDAP, for example, and it can't natively connect to RADIUS.

It lacks flexibility. Azure AD prescribes the way you work, not the other way around. It defines which solutions it can connect with and how those connections must be made. This makes it hard to choose the solutions that are best for your organization, forcing you to instead choose the solutions that are best for Azure AD.

Pricing and subscriptions are unclear. It's hard to tell what you need and what you don't, and businesses frequently overbuy services without realizing it.

Are We Even Compatible?

Fundamental Issues Make AD a Poor Fit for Many Organizations

Neither AD nor Azure AD can meet the needs of the modern business. At the end of the day, AD is no longer compatible with modern, cloud-friendly business models, and Azure AD isn't a viable fix. Example Game Studio has big plans for expansion and a possible merger in its future, and it's realizing AD might be hurting its potential to grow. It begins to face the reality that it may need to move on from AD.

Let's Talk About the Future

If things are bumpy now, what will that mean in the future?

Because Microsoft tends to lock its customers in with complex layers of proprietary configurations and products, businesses often feel stuck with AD. And many of those feeling stuck with AD *now* are likely to see things worsen as their business moves forward and AD… doesn't.

But sticking with AD is like trying to save a bad joke: the harder you try to fix it, the worse it becomes. Only too late do you realize you should have accepted the loss and moved on.

Businesses end up twisting themselves in knots to get AD to support the solutions and processes they need. This involves complex integrations and increasing third-party add-ons, both of which require intensive manual management. As SaaS and cloud-based technology continue to overtake legacy, these knots will only worsen, and ties will tighten. These tethers will box you in when it comes to future decisions: they'll have to align with your existing AD environment.

That's not to mention the backbends you and your IT team will go through to configure and maintain these increasingly complex and manual processes. While the world moves forward with automation and user-friendly solutions (for end-users *and* IT), your team will be increasingly bogged down with complexity.

The last few years saw significant changes to the average workplace, and the next few years are likely to see more as businesses adapt. AD, a platform designed for legacy technology, isn't a platform that will grow with you as you modernize. Sticking with AD will force you to make future decisions through a Microsoft AD lens, which can hold you back from choosing the best processes and solutions for your organization.

The best way to Make Work Happen™ anywhere as your business evolves is with an Open Directory Platform.

Things to Plan for

Directories must be able to accommodate future growth and change. Consider the following likelihoods and how well your directory will be able to adapt to them:

Your business will evolve. The resources you use today may not be those you need to depend upon tomorrow.

You need to Make Work Happen™. Secure, Frictionless Access™ to *all* resources for *all* employees is non-negotiable; nothing can stand in its way.

The way your employees work should not matter. From home. From a beach. From an office full time or part time. It should never matter. The new office is your employee and their device.

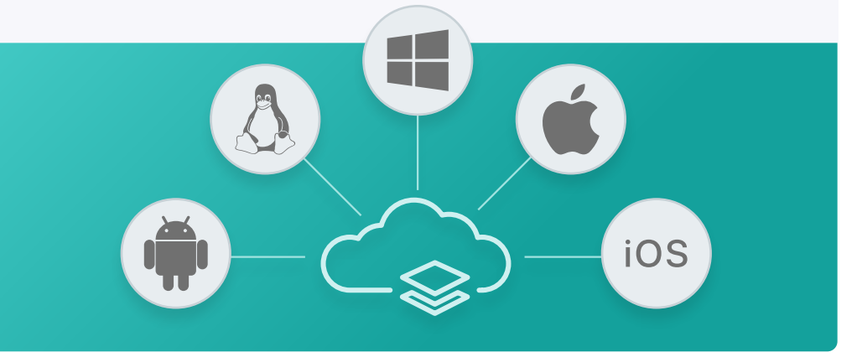
The Problem With IT Sprawl

A cluttered, disorganized environment can create problems with security, compliance, IT management, and rising expenses. Learn more in the eBook, **The Problem With IT Sprawl**.

Find Someone Who Lets You Be You

Work the Way *You* Want with an Open Directory Platform

Example Game Studio finally cut ties with AD to go with a platform that lets the studio and its employees decide how, where, and with which resources they work. It went with an Open Directory Platform, which delivers flexibility, security, and the freedom of choice — all from the cloud. Now, the studio's employees can access all their resources seamlessly, from anywhere and with any trusted device (including mobile, Mac, and Linux), with just one set of login credentials. IT can devote more of their time to working on the product and business with the help of simple processes, automation, and Zero Trust alignment. The studio's opportunities for growth and expansion never looked so achievable.



You should get to decide how you work — not your provider. When it comes to the directory, businesses need a solution that allows them to work how they want, where they want, and with the solutions that best suit their needs (not their provider's). AD's on-premises infrastructure and Microsoft-exclusive ecosystem prevent you from doing that. The best way to achieve this freedom of flexibility and choice is with an Open Directory Platform.

What Is an Open Directory Platform?

An Open Directory Platform fixes the problems AD poses by providing a flexible, cloud-first directory. It connects users *from* anywhere *to* anywhere. That means secure, frictionless access to all resources (including those locked into AD) from any location and any trusted device. Every user is managed with *one* secure identity and always granted precisely the right amount of access to each resource.

An Open Directory Platform offers multi-OS support, which allows companies to expand beyond just Windows: employees can use the trusted device(s) and OS they prefer. This lifts the burden of complex manual processes, point solutions like Okta, JAMF or Duo, and the Microsoft monoculture, which limits options and only caters to its own ecosystem.

This alternative approach to a directory grants businesses flexibility, the freedom of choice, and the potential for unhindered growth.

Further, this shift away from a domain with a traditional perimeter and toward identity-based security supports Zero Trust security. Companies switching from AD to an Open Directory Platform immediately improve their security posture by supporting these Zero Trust principles.

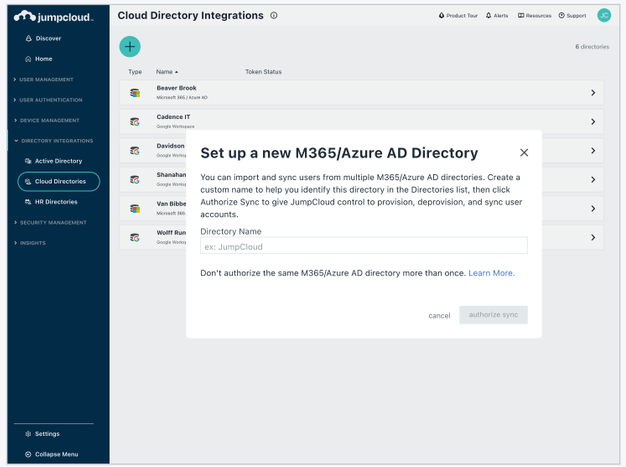
By moving from AD to an Open Directory Platform, you can:

- **Do more with the people and products that you have.** Empower your employees by lifting burdensome processes and make the most of your products with a directory that supports them natively.
- **Empower employees.** Allow your workers to use the device(s) they prefer and all the applications they need to do their work.
- **Improve the end-user and admin experience.** Equip users with the tools they need and frictionless processes to access them by the means they choose. IT admins enjoy similar flexibility with fewer manual processes and more straightforward management.
- **Adopt a Zero Trust posture.** Protect your resources with identity-based security.
- **Ditch the Microsoft monoculture.** The Open Directory Platform supports *any* resources, not just those that fit within the Microsoft ecosystem.
- **Grow and evolve without restraint from your IT solutions.** The Open Directory Platform is cloud-based, allowing it to adapt to organizational and structural changes easily. It can support any and all resources — even the ones you don't know you'll need yet.

You should get to decide how you work — not your provider.

JumpCloud's Open Directory Platform

JumpCloud offers a cloud-based, Open Directory Platform that's designed to respond to the problems businesses face when working with AD in a modern environment. To combat AD's complexity, stubbornly legacy base, and lock-in policies, JumpCloud is intentionally simple to configure and manage, cloud-based, and compatible with just about everything. It's OS-agnostic and supports a wide variety of resources and identity providers.



Why JumpCloud?

JumpCloud delivers an Open Directory Platform for IT admins who want to Make Work Happen™ for their employees by provisioning them the best resources from any vendor they need to do their job.

- JumpCloud was made for SMEs and their unique needs. The console is catered to IT admins and what they need to get done.
- It is OS-agnostic and supports a wide variety of protocols for authentication.
- Its identity and access management (IAM) includes extensive and automated user lifecycle management, from onboarding to offboarding.
- It enables MFA everywhere and native SAML and OpenID Connect single sign-on (SSO). SSO extends to virtually all your resources without the need to integrate with a third-party SSO solution.
- Its roadmap is driven by customer requests.
- It allows you to bring your own identity or use its directory as your IdP. You maintain the freedom to choose who manages your identities.
- It keeps licensing simple with clear and straightforward pricing.
- It offers professional services to make your integrations clear, approachable, and step-by-step.

Learn more about why businesses choose JumpCloud.

JumpCloud Offers Secure, Frictionless Access™:

To Any Resource

With the password authority of your choice (JumpCloud, AD, AAD, Okta, or another identity provider).

- **Apps:** Cloud, legacy, web-based, etc.
- **Network:** RADIUS, LDAP, etc.
- **Infrastructure:** Cloud, on-premises, or hybrid.

From Any Location

On-premises | Home offices | Remote locations | On the go

From a Trusted Device

Windows | Apple | Linux | iOS | Android (coming soon)

With One Secure Identity

From JumpCloud | HRIS: From HR information systems | IdP: From other identity providers

JumpCloud® helps IT teams **Make Work Happen**® by centralizing management of user identities and devices, enabling small and medium-sized enterprises to adopt Zero Trust security models. JumpCloud has a global user base of more than 200,000 organizations, with more than 5,000 paying customers including Cars.com, GoFundMe, Grab, ClassPass, Uplight, Beyond Finance, and Foursquare. JumpCloud has raised over $400M from world-class investors including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.

For more information on JumpCloud and how organizations everywhere are providing Secure, Frictionless Access™ to all their IT resources, visit **jumpcloud.com/why**.

Try JumpCloud Free

Learn More About JumpCloud

Blog

Daily insights on directory services, IAM, LDAP, identity security, SSO, system management (Mac, Windows, Linux), networking, and the cloud.

Learn More

Resources

JumpCloud's hub for videos, documentation, case studies, partner enablement tools, and more.

Learn More

In the Press

Read what people are saying about JumpCloud.

Learn More