jumpcloud

WHITEPAPER

SSO Redefined

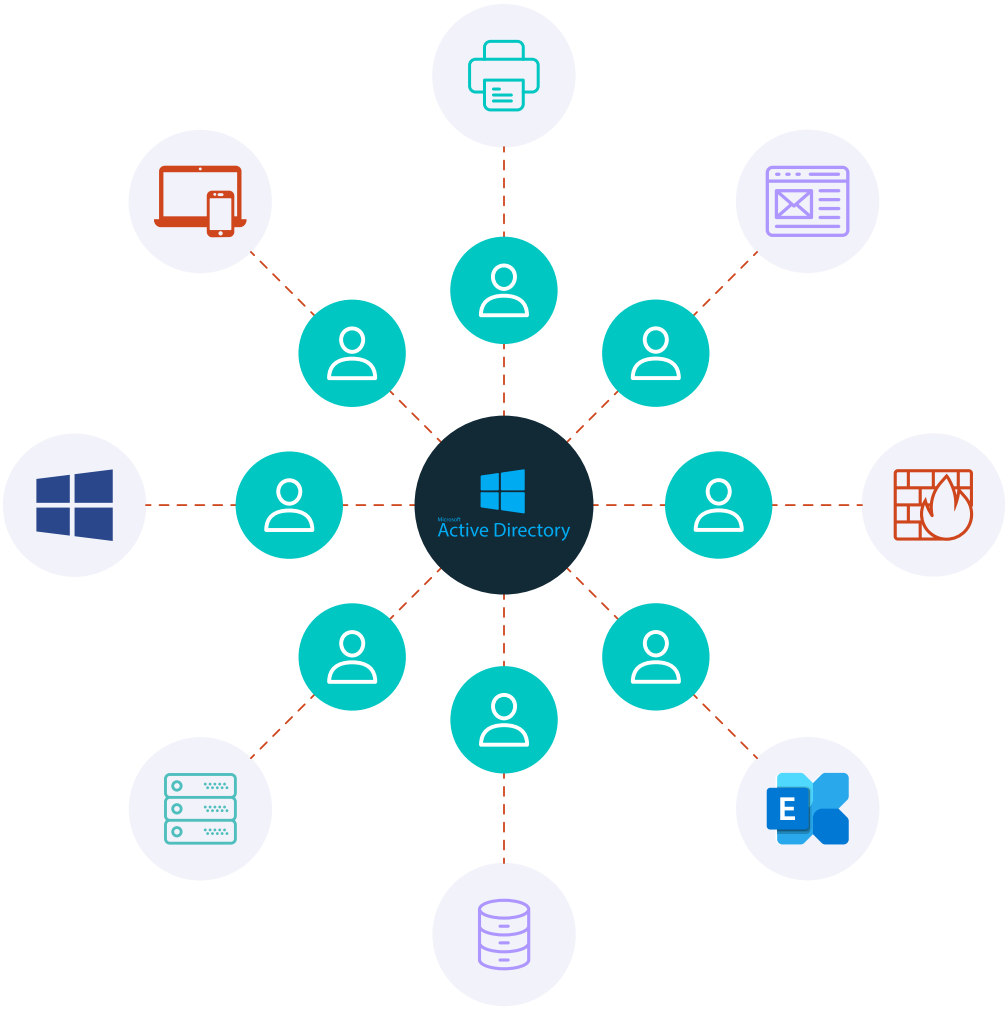
Table of Contents

Traditional single sign-on (SSO) is not enough for the access and security demands of today's workforce. SSO solutions were originally meant to connect users to web applications and were built upon Microsoft Active Directory (AD) as the central identity provider; however, the world has changed since the first versions of web app SSO (with the cloud versions also known as IDaaS) in the mid-2000s and even since these solutions garnered increased attention during the late 2010s. With accelerated cloud migration and use of third-party cloud providers, increased adoption of Mac and Linux systems across the enterprise, and a growing shift toward remote work catalyzed in response to the global pandemic, traditional SSO solutions are no longer enough to effectively connect users to modern IT systems in a secure, seamless manner.

To support the modern workforce and IT admins alike, SSO needs to be redefined and connect to more than just web applications. SSO must enable end users to access their legacy and web applications, multiple devices and types, Wi-Fi and VPN networks, physical and virtual file servers, and any additional resources necessary to perform their jobs at the highest level from anywhere in the world. With these new requirements for SSO, the on-premises directory combined with web SSO needs to be replaced by a modern cloud-based directory platform.

To better understand the how and why SSO must change, it is helpful to take a step back and analyze its origins.

Origins of Single Sign-On



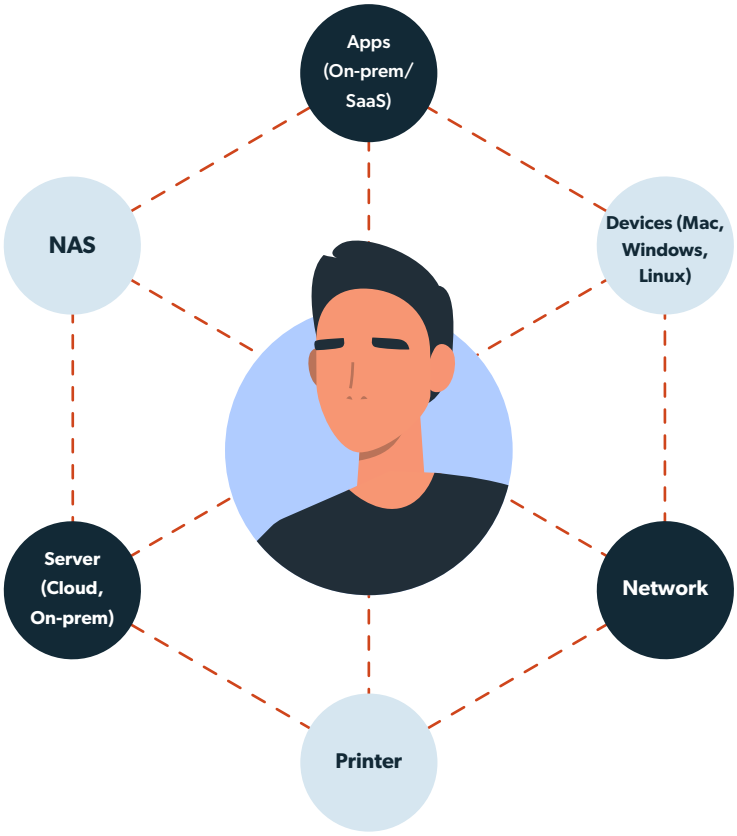
IT networks looked a lot different around the turn of the century than they do today. There were no mainstream web applications, no cloud computing solutions in the current format, and even Wi-Fi was still in its infancy as a business resource. Instead, IT networks were largely built, hosted, and used on-prem, and predominantly built from Microsoft®-based IT solutions. Data centers were either built in-house or organizations leveraged co-location facilities where they needed to manage their own racks, servers, and networking gear.

The Windows-centric environment from the 1990s led to the rise of Microsoft Active Directory (AD or MAD). AD, introduced in late 1999, provided IT with centralized user and system management over the Microsoft resources in their on-prem environment. At the time, infrastructure effectively only existed on-prem, and virtually every workstation, application, file server, and other IT resource that dominated the office was from Microsoft: Windows®, Office, and Exchange. As long as IT environments stuck to the Microsoft ecosystem, IT admins only had to leverage one solution to manage their company's identities and access to IT resources, which were virtually all, of course, Windows-based applications. Further, because Microsoft wanted to give IT admins more control over their environment, they also enabled Windows system management from AD through a construct known as Group Policy Objects or GPOs for short.

When web applications emerged in the early 2000s, the user access landscape changed. The challenge was that authentication to web applications didn't work in the same way that users (and IT admins) had become accustomed to with legacy applications. AD, which was designed to manage Microsoft IT resources on-prem, began to lose its place as the single source of truth when it came to employee accounts.

End users would simply create user accounts on web application services and have to remember those passwords. They would navigate directly to that application and enter those credentials. In the off case that IT managed those applications, IT was required to manually provision each account and then send the end user a temporary password to login (which they would subsequently change) and then the user would start to use their account. If an end user lost their password, needed help with their account, or left the organization, IT was in the middle of all of these access changes. For a long time, there was no integration with AD, and even after Microsoft products emerged to help manage access to web applications such as AD FS (Active Directory Federation Services), the solutions didn't really solve the core problem for IT organizations due to the exploding cloud computing landscape and shift to non-Windows systems and resources.

However, with Microsoft struggling to provide solutions and once IT admins started to need access control and user management for their users' web applications, a whole market of third-party web application SSO providers quickly emerged. This type of solution was initially delivered on-prem as an enterprise-class solution, just like AD. IT organizations needed to purchase hardware, software, professional services, and work through a complicated integration process. In short, it was the traditional enterprise buying and implementation process. Over time, cloud-as-a-service versions of the on-prem web application SSO products emerged and were promptly called Identity-as-a-Service (IDaaS).



But the name was slightly misleading; the first generation of IDaaS acted more as a proxy than an identity platform. IT organizations still managed their on-prem directory service (generally AD), and would simply federate those credentials to the web application SSO platform. The identity was actually stored within the on-prem directory service, and the IDaaS platform extended it to web applications. It wasn't a central platform to manage the user's identity, but the name IDaaS stuck.

In fact, the term Identity-as-a-Service would eventually come to describe a future technology platform built to address these shortcomings: the cloud directory that would be the authoritative source of the identity, yet also include single sign-on services to not only web applications, but to workstations, servers, on-prem applications, cloud and physical file storage systems, and networking infrastructure among others.

AD and Web SSO Struggle with the Growing Cloud

As described above, at this point in time, the best-in-class identity management approach was increasingly AD and SSO (with a handful of prominent vendors rising to the top). This worked well for a while, especially given the (relatively) small number of web applications in use by businesses at the time and the homogenous Windows infrastructure. But as is commonplace in technology, another seismic change took hold in the IT world: a massive shift of on-prem IT resources to the cloud.

Data center operations transitioned to providers like AWS and Google Cloud and the market for cloud-based solutions took off. According to **MarketsandMarkets**, the global cloud computing market size is expected to grow from USD $371.4 billion in 2020 to USD $832.1 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 17.5% during the forecast period.

This coincided with another shift; workers became more mobile, had the capability to work from anywhere in the world, and demanded access to the devices and applications they wanted no matter where they were. They could accomplish so much of their work directly via their smartphones (or tablets) that the user experience and design of B2B applications went "consumer." More cloud-based applications were developed, touching all aspects of an enterprise well beyond IT. And, now in the era of a global pandemic, a remote workforce that must be productive is more critical than ever.

All of this inadvertently drove another interesting trend: workers started to veer away from Windows platforms to leverage Mac and Linux devices more frequently. At one time this shift had become so common for workers that only one in five devices in an enterprise were Windows **(Forbes)**. A massive difference compared to the early 2000s.

+350%

macOS market share has increased by over 350% since 2009.

-20%

Windows market share has decreased by nearly 20% in that same time period.

These trends created three main issues for IT admins. First, AD was becoming less and less valuable to IT organizations. SSO uncovered a critical flaw in AD, as more applications and services began moving to the cloud an identity management provider locked on-prem was not designed for this change. AD was built for Windows-based devices and served as a point solution, at best, for Mac and Linux. This worked while companies were operating from the corporate office. IT organizations also realized that SSO couldn't just mean web applications. Even the words "single sign-on" had come to evoke a different meaning and with each successive piece of technology being introduced, users moved further away from the single login experience, even with traditional SSO providers.

Second, the abrupt shift in 2020 to remote work exposed AD's Achilles' heel. It struggles to securely allow remote workers to access their company's IT resources. End users need VPN access back to the on-prem network to authenticate with AD and then subsequently access their IT resources. The global pandemic has also further introduced more types of IT resources creating more challenges for IT admins and end users alike for secure, frictionless access.

Third, as IT organizations struggle with cloud transformation, a remote workforce, new technologies, and security risks, the antiquated concept of AD and web app SSO is getting a hard look. Is that architecture going to prepare their organization to compete in the now global marketplace, create greater efficiency and productivity for their team, and comply with security regulations? Most modern organizations are realizing that there is a better approach to creating and managing secure, frictionless access to IT resources for their end users.

The Future of SSO: A Single Identity to Access Virtually All IT Resources Through a Cloud Directory

With the dramatic shift to remote work and accelerated pace of cloud transformation, admins are now managing users' access to a wide range of applications, devices, files, and networks. As we have seen, AD and traditional SSO were not designed to support this new modern era of IT.

A new approach to True Single Sign-On™ has emerged through a cloud directory platform. Traditionally, the on-prem, legacy directory service was essentially used to authenticate and authorize access to Window-based resources. Now, though, a cloud directory platform is a unified point for user and system management across a wide range of on-prem and cloud-based IT resources. Cloud directory solutions are integrating categories such as web applications single sign-on with user management over Mac, Windows, and Linux systems, on-prem LDAP-based applications, on-prem file servers via Samba Wi-Fi, and VPN networks through RADIUS, and more. A modern cloud directory is really "One Identity to Rule Them All™."

The key advantage of a cloud directory is that IT admins can build, manage, and maintain a single, secure account for every employee that connects them to virtually any IT resource, regardless of location, platform, protocol, and provider. There are a number of benefits to a cloud directory that enhance both the end users' and the IT admins' lives. Though varied, they tend to center around a few key themes: better control of over a user's identity, reduced complexity, and more secure access to critical resources. Both IT admins and end users can save significant time and rest assured that they are more safe and secure.

Better Control of User Identity

Employees gain simplicity and efficiency by having one identity to access their business IT resources. Administrators improve management and security by centralizing control over the employee's access to their assigned resources. With employees working remotely, managing employee devices and applications poses a security risk. A **2020 Wrike study** found that 41% of remote workers are accessing confidential work information using unsecured personal applications. With a cloud directory, admins have complete control over the applications, devices, files, and networks their employees can access.

A cloud directory streamlines the user onboarding and offboarding process. An admin can easily provision and deprovision a wide range of IT assets. From a single console, an admin can use group-based access control to instantly grant new users access to the resources their role/department requires. When a user leaves the organization, an admin can simply suspend / terminate their account and their resource access goes with it — keeping confidential data and processes secure.

IT organizations can further leverage step-up authentication and conditional access control methods to enhance security. These capabilities can include multi-factor authentication (MFA), passwordless/biometric access options, geofencing, and device or network trust mechanisms.

Reduced Complexity

From an IT admin's perspective, a comprehensive cloud directory leverages one platform that manages users' identities and securely connects them to IT resources regardless of platform, protocol, provider, and location. To accomplish this, a cloud directory supports authentication standards such as LDAP that connects users to their on-premise applications and file servers; RADIUS that provisions and deprovisions user access to VPN and Wi-Fi networks, and SAML 2.0 that connects users to the business-critical web applications they need. A modern cloud directory also controls user access to Mac, Windows, and Linux systems through native APIs as well as SSH keys. While a user can leverage one identity to access virtually all of their resources, an IT organization needs to be able to manage their user's identity in one platform. Both of those increase security, save time, and ultimately reduce costs.

More Secure Access

The concept of single sign-on was born out of usability and increased security. By having one secure identity that can be federated through secure mechanisms, IT organizations have more control over user accounts. User accounts can be auto provisioned and, perhaps more critically, deprovisioned upon exit. Authentication can be supported through a wide range of techniques including passwords, SSH keys, certificates, and through attestations. Further, in the modern era, a cloud directory can secure step-up authentication through multi-factor authentication capabilities including time-based, one-time password (TOTP), push notification MFA, or universal second factor (U2F) keys like in-device biometrics to meet your organization's needs.

An even higher level of security can be added to single sign-on services through conditional access capabilities — often, also referred to as Zero Trust principles. Zero Trust works on the approach of identity, device, and network trust in addition to least privilege access through authorization rights. Leading cloud directory platforms offer these additional levels of security in an easy to implement manner.

Conclusion

As more companies migrate to the cloud, leverage a wide range of new technology, and continue to support a growing remote workforce, the concept of having a single secure identity to access virtually all of a user's IT resources is critical. For end users, a True Single Sign-On approach saves them time and makes them more productive. For IT organizations, the level of control over user accounts and the resulting security is game changing. Traditionally, IT organizations have had to stitch together a broad solution set to achieve some semblance of SSO, but a modern cloud directory platform is changing that approach. With one integrated identity management platform, organizations can connect and manage one user identity to virtually all of a user's IT resources including their workstations, on-prem and cloud servers, legacy and web applications, physical and virtual file servers, and Wi-Fi and VPN networks.

Evaluate JumpCloud Free Today

If you're new to JumpCloud and interested in learning more about the platform and how to achieve stronger security practices, evaluate JumpCloud today! JumpCloud Free grants admins 10 devices and 10 users free to help evaluate or use the entirety of the product. Once you've created your JumpCloud account, you're also given 10 days of Premium 24x7 in-app chat support to help you with any questions or issues if they arise.