ZTrust

EBOOK

ZTrust SSO: Simplifying Identity and Access Management

PRODEVANS

The Modern Access Conundrum

In the digital age, organizations face critical challenges in access management:

- Cloud adoption drives a rapid increase in the number of cloud applications.
- Anywhere, anytime access necessitates supporting users across remote devices.
- The prevalence of consumer apps raises employee expectations for simple user experiences.

According to industry reports, enterprises now utilize an average of 1,000 cloud apps across departments[1]. Moreover, 60% of IT decision-makers believe apps handling critical data must remain on-premises.[2]

> IT teams face immense pressure to securely support numerous apps in a hybrid environment while delivering an exceptional user experience.

As the app landscape expands, so do the threats. The evolving work environment boosts productivity but also creates a new security challenge—managing access.

The Password Dilemma

Historically, users accessed corporate applications and data through passwords. Two main principles govern secure password practices:

- Use long passwords with numbers and symbols.
- Never reuse the same password across multiple apps or websites.

1 https://www.kleinerperkins.com/perspectives/internet-trends-report-2017
2 https://www.enterprise-cio.com/news/2018/jan/23/why-cios-say-cloud-isnt-replacing-premises-systems/

While sound in theory, these principles are challenging to implement. 72% of people struggle to remember passwords, leading 59% of employees to reuse the same or similar passwords across multiple apps. Alarmingly, 50% use the same passwords for personal and work accounts.

> Studies reveal that 59% of employees reuse the same or similar passwords across multiple apps.

Additionally, password sharing among coworkers is prevalent, where employees share credentials to grant access to those who have forgotten passwords or lack proper permissions.

For IT teams tasked with safeguarding sensitive data, a company with 2,000 employees averaging 100 cloud apps must manage 20,000 usernames and passwords—20,000 potential entry points for hackers.

That's 20,000 too many.

Requiring separate credentials for every app is not a viable security solution, Enter single sign-on (SSO).

What is single sign-on?

The concept behind SSO is straightforward: provide users with a single set of credentials to access all their applications. One password for applications like Salesforce, Dropbox, Office 365, and even personal or social apps often accessed from work, such as Facebook, Twitter, and LinkedIn.

SSO is a user authentication process that allows employees to enter one username and password to gain access to multiple applications. After initial sign-in, SSO authenticates users for all permitted applications, eliminating the need to re-enter credentials when switching between tools.

- arubanetworks.com/pdf-viewer/?q=/assets/EIUStudy.pdf
- dropbox.com/s/57hp1hjpizzj451/app-survey-report-digital-sep2017.pdf?dl=0
- journals.plos.org/plosone/article?id=10.1371/journal.pone.0051067#s4
- symantec.com/content/en/us/enterprise/white_papers/b-mobile-apps-in-the-workplace-norton-mobile-insight-WP-21344085-en-us.pdf

Users sign in once to access multiple applications.

SSO is a robust, standards-based solution that provides a high level of user security across the enterprise. It's a foundational component within an organization's broader identity and access management (IAM) solution.

For modern organizations, simpler sign-in is just one part of a comprehensive IAM solution addressing employee onboarding/offboarding, enforcing security policies, and providing access reports. While SSO plays a central role, a complete IAM solution covering areas like multi-factor authentication (MFA) and provisioning is required to truly protect the enterprise.

Benefits of SSO

SSO offers multiple benefits.

SSO increases employee productivity.
A recent survey found 68% of employees switch between 10 different apps every hour. Reducing this to a single login per day significantly saves time

SSO provides a dashboard to consolidate apps.

After logging in, users access a single dashboard to launch applications, eliminating the need to remember or bookmark URLs.

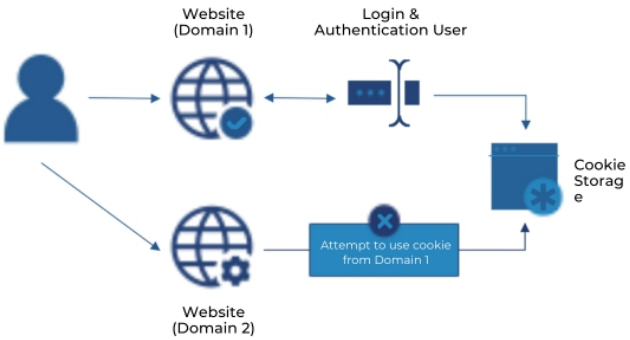
SSO reduces Help Desk tickets.

Employees have only one set of credentials to remember, and if forgotten, they can reset it without involving IT.

How does SSO work?

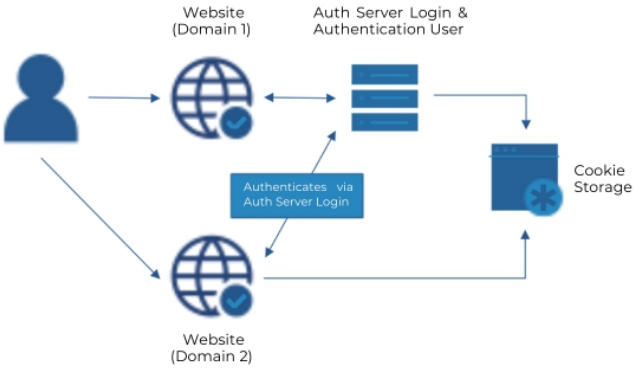
SSO establishes a user's identity and shares it with systems requiring that data.

Traditionally, when users log in to one domain, they cannot automatically log in to another due to the same origin policy enforced by browsers for security reasons. This ensures authentication data like cookies can only be accessed by their creator. For example, one domain cannot access cookies stored on another.



SSO solves this by authenticating the user at a central domain and securely sharing the session with other domains. The session sharing method varies per solution but ensures the user identification information cannot be tampered with and is passed securely.

When the user accesses a domain requiring authentication, they are redirected to the central domain where they are already logged in, and then redirected back to the requesting domain.



SSO implementation varies, with protocols like OpenID Connect, Microsoft account, and Security Assertion Markup Language (SAML), a widely used XML-based standard.

SAML

SAML is considered the gold standard for single sign-on, widely used across security platforms. According to a recent study by the Cloud Security Alliance, 67% of SaaS vendors use SAML for SSO identity management, and 19% plan to implement it within 12 months. Customer demand, improved security and compliance, and integration speed drove SAML adoption.

SAML allows secure web domains to exchange user authentication and authorization data. With SAML, an organization uses an online identity provider to authenticate users accessing secure content. Authentication is done via digital signatures, establishing trust between the identity provider and the application.

What does SAML offer?

USABILITY

Users benefit from one-click app access, eliminating the need to remember multiple passwords. SAML also automatically renews sessions to avoid timeout.

SPEED

SAML is fast, requiring only one browser redirect to securely sign a user into an application.

SECURITY

With digital signatures as the basis for authentication, SAML is a secure SSO protocol trusted by the world's largest and most security-conscious enterprises.

PHISHING PREVENTION

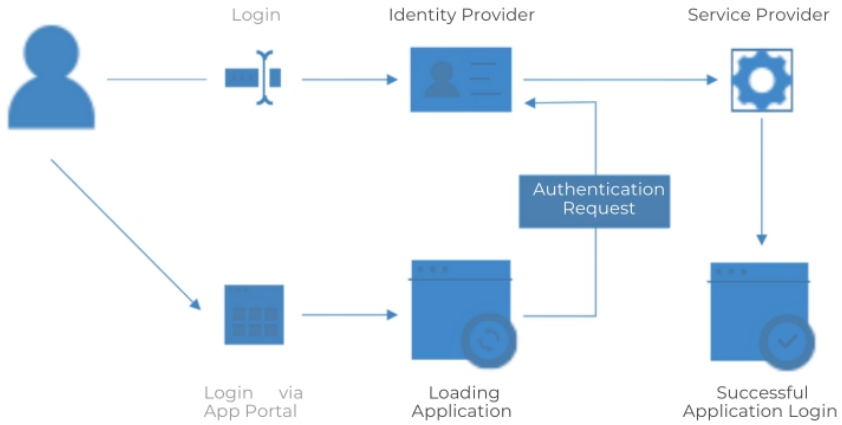
If users don't enter app passwords, they can't be tricked into entering them on fake login pages.

IT FRIENDLY

By providing centralized authentication, SAML offers greater visibility and easier directory integration.

https://www.businesswire.com/news/home/20140225005753/en/97-of-SaaS-Vendors-Backing-SAML-based-Single-Sign-on

Here's how SAML works as part of single sign-on:



1. The user logs in to a system acting as an identity provider.

2. Later, the user wants to log in to a remote application, such as an accounting app. The user clicks a link to that application (for instance, through the SSO solution's app portal).

3. The accounting app loads.

4. The app identifies the user origin (e.g., by application subdomain or user IP address) and redirects the user back to the identity provider, asking for authentication. This is called the authentication request.

5. The identity provider uses digital signature technology and builds the authentication response as an XML document containing the user's username or email address, signs it using an X.509 certificate, and posts this information to the service provider.

6. The service provider (which already knows the identity provider and has a certificate fingerprint) retrieves the authentication response and validates it using the certificate fingerprint.

7. The user's identity is established, and the user is authenticated with the accounting application and can use it.

SSO and your directories

The best SSO solutions integrate with your enterprise's directory infrastructure, such as Microsoft Active Directory (AD), Google Apps, Workday, or a combination. Since organizations often maintain multiple directories (e.g., different cloud and on-premises directories), the solution must integrate with all of them.

After integrating SSO with the directory infrastructure, users gain access to specific applications based on their roles and responsibilities within the company. They log in once and can then access any permitted application.

Cloud SSO versus on-premises SSO

SSO can be implemented as a cloud solution or an on-premises one. The most common on-prem SSO solution for enterprises is Active Directory. However, enterprises are moving to the cloud for reasons that also apply to SSO—scalability, flexibility, and freeing up IT resources.

If you're moving to the cloud, a cloud-based SSO solution makes sense:

YOU LEVERAGE TECHNOLOGY LEARNING.

An on-premises implementation must be installed and provisioned uniquely, adding to overall costs. Yet many companies use the same popular applications—likely even the same combination as your organization. It doesn't make sense to reinvent the wheel when a strong alternative already exists in the cloud.

SOMEONE ELSE HANDLES UPGRADES

Like every other technology, SSO technology changes and improves over time. An on-premises SSO solution locks you in and forces you to own the maintenance and upgrade cycle. With cloud-based solutions, the provider takes care of upgrades, ensuring you always have access to the latest technologies.

IT'S EASIER TO SCALE.

Your needs will change over time. Your company may shrink —or grow considerably. An on-premises solution makes it harder to quickly provision new applications. It's less flexible. Cloud-based SSO solutions allow you to get up and running quickly and expand as needed.

IT SAVES IT TIME.

With on-premises SSO solutions, the onus is on IT. Your already-taxed IT staff will be even busier monitoring the installation and managing vendor integrations. Cloud-based SSO provides a near plug-and-play solution that is secure, can be provisioned quickly, and provides a lower cost of ownership.

SSO and Identity Access Management

Enterprises may start with SSO to solve a specific problem for IT managers looking to strengthen user security. But today, SSO solutions are often offered as part of a larger IAM system. IAM defines what users can do (on and off the network) with specific devices and under what circumstances.

A complete identity management strategy usually includes:

DIRECTORY INTEGRATION

Using Active Directory, LDAP, and other systems, enterprises can create a rules-based hierarchy that uses the corporate directories as authoritative sources for providing access to applications and resources.

ADAPTIVE MULTI-FACTOR AUTHENTICATION

MFA is an effective way of increasing security because it requires an extra authentication factor during login. Adaptive MFA is powered by machine learning that analyzes user behavior during login and adjusts authentication requirements based on risk.

PASSWORD INJECTION

Not every application supports a password-free SSO protocol like SAML. IAM systems handle form-based authentication, usually by storing passwords securely on the server side and injecting them into an application's login page during sign-on.

USER PROVISIONING AND DEPROVISIONING

The process of manually creating, updating, and deleting users in cloud apps burns up valuable IT resources. Deprovisioning former employees quickly is important, to reduce the risk posed by potentially disgruntled ex-employees. A solid IAM solution lets you quickly provision and deprovision users from a single central location, rather than having to do this directly in individual apps.

MOBILE IDENTITY MANAGEMENT

These tools allow users access to their web applications, regardless of device, in the cloud and behind the firewall.

REPORTING

Identity management includes user behavior analysis. Strong reporting tools give instant insight into inactive users, application utilization, login activity, and weak passwords. They provide information for potential SOX, GDPR or other regulatory audits.

What about unified access management?

As enterprises move to the cloud, they are increasingly dealing with a mix of on-premises and hybrid apps; multiple directories, like on-premises Active Directory and cloud Azure AD; plus different types of users, including employees, customers, partners, and others. All of these users are accessing the cloud and on-premises apps and are accessing enterprise data through a wide variety of devices.

> Fragmented IAM solutions add cost, reduce security and complicate reporting.

This has left many organizations managing identity through several different systems. For example, they provision users with on-premises apps through one system and cloud apps through another. Or they add some users to Active Directory and others to Azure AD. The complexity of managing user identities in multiple systems adds to cost, increases the chance of error, complicates reporting, and raises security risk.

That's why organizations are moving to unified access management (UAM) solutions. A superset of IAM, UAM solutions provide one tool that can be used to manage identity across all the organization's different users, directories, devices, and apps—on-premises and in the cloud. UAM solutions include a single way to:

- Provide SSO for the wide variety of cloud and on-premises apps used in the enterprise.
- Enable MFA with risk-based authentication.
- Manage access through a centralized cloud directory that acts as the intermediary between on-premises and cloud directories.
- Support users throughout the life cycle, including user provisioning and the ability to implement role-based access control (RBAC) and granular security policies.
- Be extensible and provide support for in-house custom apps through an API/SDK, OIDC, webhooks, and other tools and methods designed for developers.

Increasingly, enterprises are looking to eliminate the problem of fragmentation by moving to unified access management solutions.

Conclusion

Today, cloud-based single sign-on is a key tool in enterprise identity access management. SSO increases employee productivity, fills security gaps, and saves IT time and money. However, it's only part of the identity and access management solution that enterprises need to protect their intellectual property and corporate data.

NEXT STEPS:

Find out what to look for in your SSO solution.

Learn more about Prodevans Technologies' ZTrust SSO unified access management solution.

About Prodevans Technologies Pvt. Ltd.

Prodevans Technologies is a provider of Unified Access Management solutions, Enabling Organizations to Access the World. Businesses of all sizes can use Prodevans Technologies' **ZTrust SSO** to secure company data while increasing IT administrator and end-user efficiencies.

Implementation of our identity management solutions can be achieved in hours rather than days, delivering a fully featured administrative and self-service portal. Our ability to handle on-premises and cloud/SaaS applications makes us the identity as a service vendor of choice for the hybrid enterprise.

contact@ztrust.in to learn more about OneLogin.

OUR ADDRESS:
403, 4th Floor, SAKET CALLIPOLIS
Rainbow Drive, Doddakannelli
Bengaluru, Karnataka 560035

OUR CONTACTS:
contact@prodevans.com
+91 97044 56015