Single sign-on the way it should be

Six ways Citrix delivers seamless access to all apps
while improving security and the user experience

Single sign-on (SSO) solutions were designed to make life easier for employees and IT.

SSO solutions are meant to reduce the cost of management and provide better security, all while delivering an improved user experience. However, many solutions fall short, covering only one type or a subset of application types. This forces you to implement several access solutions from different vendors to cover your entire application landscape—negating the productivity and user experience benefits you hoped for. The complexity this type of implementation creates also runs counter to the zero trust initiatives that many organizations are undertaking.

Citrix helps you unify all apps and data across your distributed IT architecture to provide single sign-on to all the applications and data your people need to be productive.

Working with your existing infrastructure, Citrix Secure Private Access consolidates multiple remote access solutions, like traditional VPNs or SSO solutions, simplifying management for IT and providing unified access for employees.

Six benefits of the Citrix SSO solution

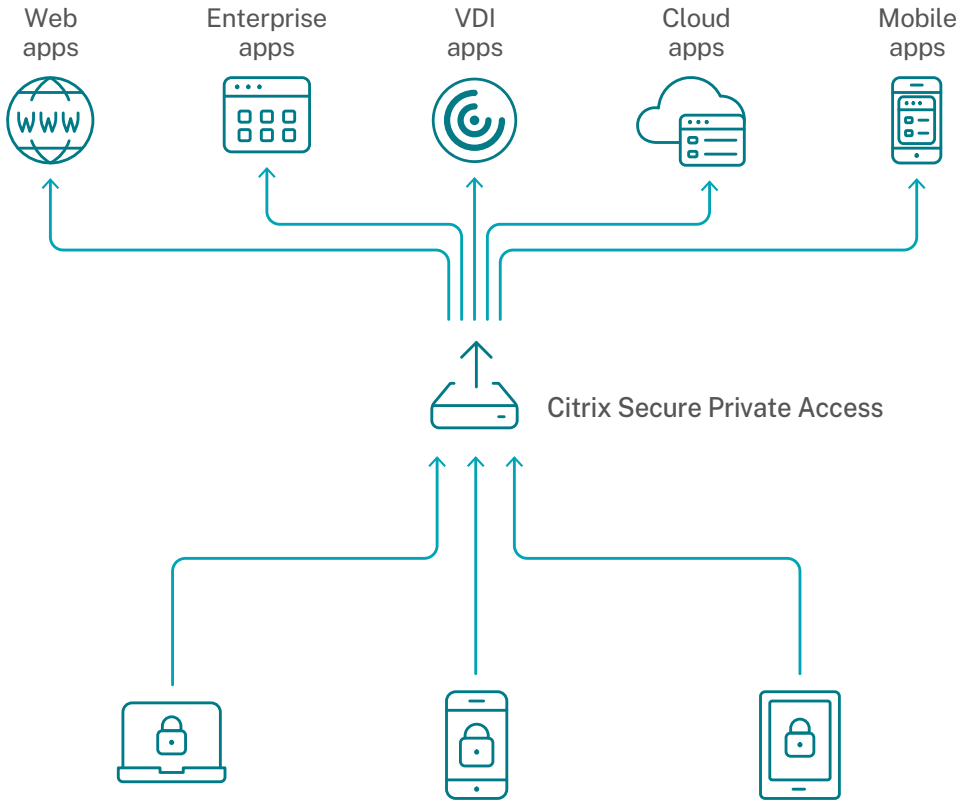
1. VPN-less and Secure Private Access to corporate resources
2. Granular controls for SaaS apps and the web
3. Control over your user identity
4. Security beyond user names and passwords
5. Seamless integration with your existing environment
6. Resolving issues faster with end-to-end visibility

Explore the details of each benefit on the following pages.

1 VPN-less and Secure Private Access to corporate resources

Many solutions are limited in the scope of the application landscape they cover. If you have a solution that covers only your virtual and enterprise apps, for example, you'd need a separate SSO solution to provide access to your web and SaaS applications.

Citrix simplifies access with SSO to virtual, SaaS, and web apps, as well as to file repositories in the cloud and in your datacenter. By reducing the complexity of multiple access solutions like VPNs and SSO, IT can achieve the outcomes to fit their zero trust strategy while enhancing the end-user experience.



Citrix Secure Private Access gives you access to all your apps and data.

2 Granular controls for SaaS apps and the web

Your SSO solution should go beyond basic access and provide you with granular, contextual controls over SaaS and web apps.

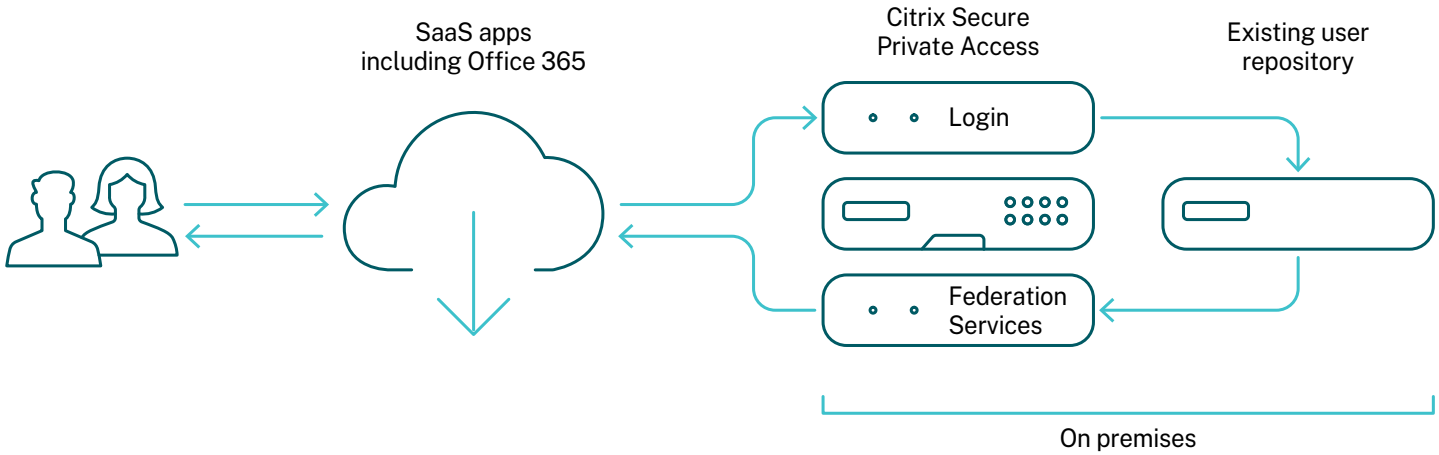
Additionally, unmonitored internet browsing opens up your organization to risk. Some organizations restrict internet browsing, but this can hamper productivity.

Data protection is a top zero trust outcome most organizations are looking to achieve. Secure Private Access helps protect data through enhanced security policies for SaaS and web apps. Controls include restricting copy/paste, printing, and downloading content, as well as enabling watermarking.

Admins can blacklist and whitelist URLs to allow or deny access to websites. You can also disable URLs launched from SaaS apps, or use remote browser isolation to present unknown SaaS apps or web links in a secure browser to isolate them from corporate network or resources. This protects the organization, as malware distributed through malicious sites never touches the corporate infrastructure.

Secure Private Access supports the most popular SaaS apps—including Salesforce, G Suite, Office 365, Zoom, Workday, and Expensify—in its out-of-the-box catalog. You can use preconfigured application templates to easily publish apps and configure single sign-on policies.

3 Control over your user identity



SaaS applications like Microsoft Office 365, Salesforce, Workday, and ADP are becoming essential to how we work today. In fact, the average enterprise uses 1,427 distinct cloud services.[1]

To provide SSO to these apps—which are delivered from the cloud and are outside of the datacenter network—most solutions require you to move your user directory to the cloud, forcing you to rip and replace your existing identity infrastructure.

Secure Private Access enables choice, empowering you to bring your own identity. Our rich ecosystem of supported identity platforms include Microsoft, Google, and Okta. This is accomplished through identity federation, using internal SAML or ADFS federation services to provide the cloud service with a secure trusted token containing a series of claims about the authenticated user, including their identity. These claims are in turn validated by the cloud services' own federation services.

By providing this choice, Citrix empowers you to leverage your existing investments in identity providers while providing Secure Private Access to your corporate resources.

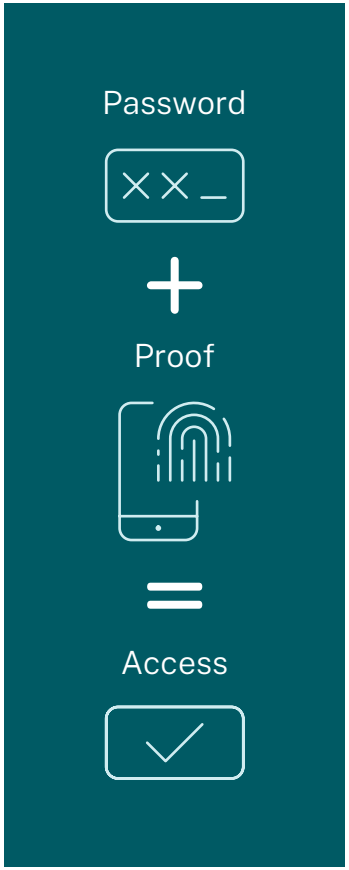
4 Security beyond user names and passwords

User authentication is becoming increasingly important, especially as organizations implement business continuity plans and have large segments of their workforce accessing corporate resources remotely. These workers, along with partners or contractors who may not be part of the corporate directory, are working off the corporate network and on personal devices. This makes it crucial to quickly and correctly identify the user and authorize their access to corporate resources.

That's why Secure Private Access doesn't rely on just user names and passwords. It supports multifactor authentication, which allows IT to have granular control over who's accessing the corporate network, what's being accessed, when it's accessed, and the device used to access it.

Secure Private Access integrates with and supports all authentication mechanisms and protocols, including LDAP, RADIUS, SAML, OAuth, and OpenID. It also supports Azure Active Directory for multifactor authentication and password-less logins, as well as on-premises Active Directory for two-factor authentication using native OTP.

Secure Private Access provides capabilities to scan end-user devices before and after a user session is established. Based on the results of user role, user location, and the device posture assessment, an administrator can define how they want to authenticate and authorize access to their applications.



5 Seamless integration within your existing environment

A single sign-on solution has a lot of touch points within your environment, from the user directory to authentication mechanisms to applications and even end-user devices.

Secure Private Access easily integrates with your existing infrastructure so that you can ensure a great user experience while simplifying IT management.

Customize your front-end application portal with your organization's own branding

Support front-end authentication, including Active Directory, AAD, Citrix Gateway, Okta, Google Identity, SAML, and Adaptive Authentication

Support all end-user devices, including Windows, Mac, Linux, iOS, and Android platforms

Support authentication for SSO, including Basic, Kerberos, form-based, and SAML

Ease of integration with existing systems was the most important factor when considering enterprise authentication solutions.[2]

6 Resolving issues faster with end-to-end visibility

Because Secure Private Access provides access across your entire application landscape, it's also able to provide the visibility you need to monitor and troubleshoot application delivery and user experience issues.

Citrix Analytics brings you complete end-to-end visibility into all TCP and HTTP user sessions. Its insight captures authentication errors from events like an expired password, locked-out account, endpoint scan failure, and any SSO or application launch failures—so that you can troubleshoot issues faster.

Citrix Analytics also provides continuous authentication and authorization, a top zero trust outcome for many organizations. Awareness of contextual factors like change in location or device can trigger added security controls, such as a second factor of authentication, before granting access to a corporate resource.

With risk indicators and criteria to help detect user anomalies, you can configure the policy controls to quickly identify and get alerted about bad or risky user behavior, such as users accessing or uploading / downloading information from malicious and risky websites. Automation with Citrix Analytics can take action on your behalf, performing tasks like recording sessions, expiring shared document links, or locking the user out of their account.

Give people the freedom to get work done their way. With Citrix, you can provide true single sign-on across all applications by replacing traditional VPNs or SSO access solutions. Deliver simpler IT management, better security, and an improved user experience.

To learn more, visit citrix.com/products/citrix-secure-private-access.

citrix®

Sources:
1. 12 Must-Know Statistics on Cloud Usage in the Enterprise, Skyhigh Networks.
2. 2017 State of Authentication Report, Javelin