OneLogin Single Sign-On

Simple and secure access to all your applications

Solving the Identity Chaos Crisis

As organizations grow, the technology puzzle pieces multiply: more applications, users, and devices — all distributed across more locations. Information Technology (IT) and security teams must secure application access to protect corporate data while making that same access easy for the employees who need to stay productive.

Challenge One: Security risks

- 81% of hacking-related breaches are caused by compromised credentials, especially passwords.[1] Protecting passwords is key to protecting the enterprise.

- 50% of businesses fail to cut off access for ex-employees, meaning they can access apps and exfiltrate sensitive data post termination.[2]

Challenge Two: Costly access mgmt. operations

- 51% of IT execs say that having too many identity systems is the primary IAM challenge they face.[2]

- Legacy access systems cost precious IT budget. They're complex, decentralized, and ill-equipped to address the continued growth of cloud applications in businesses.

- IT wastes hours on inefficient operations for onboarding new employees, rolling out applications, and offboarding departing employees.

Challenge Three: Employee productivity

- Poor employee experience is one of the top three IAM challenges cited by 84% of businesses today.[3]

- Employees are forced to remember dozens of passwords and use time-consuming tools such as VPNs or physical tokens for authentication. It reduces productivity and introduces digital friction.

The OneLogin SSO portal as viewed by an end-user.

OneLogin: Connecting people with technology

OneLogin streamlines app access with a simple, secure, single login, empowering organizations to access the world. The Onelogin Unified Access Management platform is key to unlocking the apps, devices, and data that drive productivity and facilitate collaboration. OneLogin:

- Simplifies access management for IT, security staff, and end-users by providing a single destination to manage and access all apps.

- Protects apps behind a secure Single Sign-On (SSO) portal powered with strong security policies and adaptive Multi-Factor Authentication (MFA).

- Terminates access for departing employees with one click, preventing malicious actions via dormant accounts.

How OneLogin helps
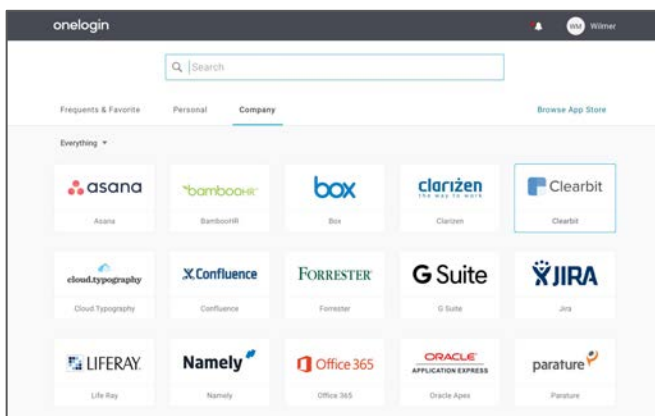
Security benefits

- Secures access by placing all applications behind an SSO portal protected by a policy-compliant password.
- Eliminates the weak link of passwords using SAML tokens to improve security for cloud apps.

IT benefits

- Accelerates strategic initiatives such as digital transformation, cloud migration, and M&A integrations.
- Streamlines IT operations by integrating all existing directories and apps and automates resource-intensive workflows like onboarding/offboarding.
- Reduces costs by cutting help desk tickets by up to 50% or more via self-service password reset for end-users.

Employee benefits

- Provides quick access of any app on any device from anywhere through the OneLogin portal.
- Lets employee ditch the dozens of passwords they had to remember.
- Enables self-service: so employees get needed apps and can reset passwords without depending on the help desk.
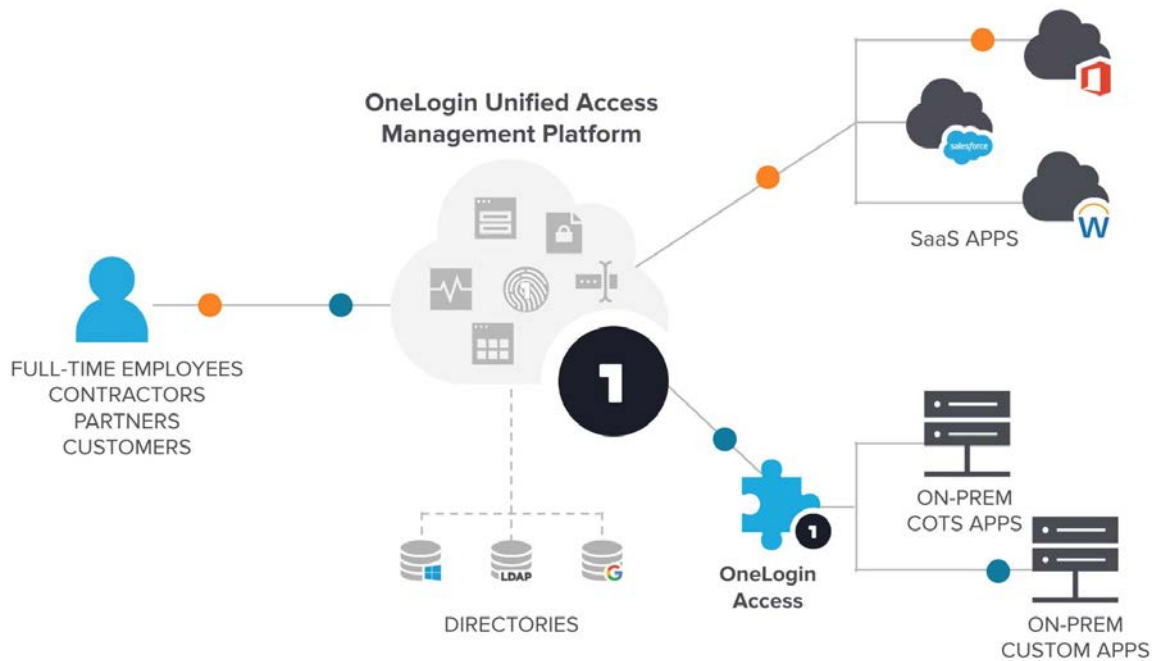
Single Sign-On with the OneLogin Unified Access Management Platform

OneLogin's **Unified Access Management (UAM) platform** is a simple, secure, and reliable solution that meets all your organization's access needs.

At the center of our UAM platform is the **OneLogin cloud directory**: a single source of truth through which you manage access. Through pre-built app integrations, OneLogin works seamlessly with existing on-prem and cloud directories, like Microsoft Active Directory, LDAP, Workday, and more.

OneLogin's **single sign-on** (SSO) gives users one-click access to all their apps, in the cloud or behind the firewall, from anywhere and anytime. With an extensive app catalog of over 5,000 apps and a secure SSO portal, it's easy for users to be productive right away.

OneLogin's **Desktop** extends SSO to operating systems (macOS or windows). Users log in to their work machine and immediately have access to everything they need, without re-entering their credentials.

OneLogin's **Access** easily extends identity management to legacy applications on-prem and to apps hosted in remote data centers, private clouds, and more.

OneLogin ensures secure authentication with **multi-factor authentication** (MFA) — which lets you implement policy-based access control for login, and password resets. And our adaptive authentication uses machine learning to identify and challenge abnormal login attempts.

OneLogin's **identity and lifecycle management** lets you provision users easily, and automate onboarding and offboarding. Connectors enable OneLogin to work with both your on-prem and your cloud directories with real-time synchronization. You can also streamline entitlements through powerful rules to enforce intelligent access policies based on user location, role, privilege level, and more.

The Company We Keep

"We had 20 apps provisioned for internal and warehouse workers, and over 45 Google admins, which was simply unsustainable. Our breadth of applications has grown significantly, yet now we're able to securely manage it all with a much smaller staff."

- Ravindra Sunku, Director of IT

"Integrating a new app with an AD security group and to have it auto provisioned is a huge time saver. If I were to describe OneLogin in a word, it would be simplicity. The end user experience is simple, with pain-free access to the apps needed, and from the admin side, we can roll out integrations quickly and neatly."

- John Hluboky, SVP Tech. Operations

"OneLogin is very easy to configure. My challenge to the IT team was to integrate these disparate systems in such a way that our users perceive them as one coherent system. OneLogin has been critical in meeting this objective."

- Brent Harris, VP of IT