OneLogin for Managed Service Providers
Deliver secure managed identity services to your customers

Solving the Identity Chaos Crisis

As your business grows, so do security challenges around supporting new users, applications, and devices—all distributed across locations you don't control. Organizations are looking to consolidate digital identities and protect user data to keep account compromise at bay, while also provide easy application access for those who need to stay productive.

Challenge One: Rise of data breaches

- 80% 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, allowing them to access apps and do damage post-termination.[2]

Challenge Two: Costly access management 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, which reduces productivity and introduces digital friction.

The OneLogin SSO portal as viewed by an end-user

OneLogin: Securely connect people with technology

The OneLogin Trusted Experience™ platform is the foundation for building simple and secure identity and access management (IAM) experiences between people and technology. It allows you to:

- **Simplify** access management for IT, security staff, and end-users by providing a single destination to manage and access all corporate applications

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

- **Terminate** access for departing employees with one click, preventing malicious attacks from dormant accounts

How OneLogin helps
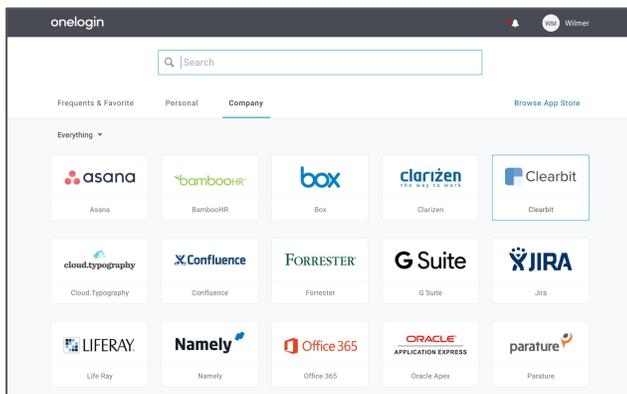
Security benefits

- Secure access by placing all applications behind an SSO portal using SAML or OIDC protected by a policy-compliant password, which is infinitely more secure than your typical Password Vault solution

IT benefits

- Accelerate strategic initiatives such as digital transformation, cloud migration, and M&A integrations

- Streamline IT operations by integrating all existing directories using our directory integration with Active Directory or an alternative LDAP directory

- Automate resource-intensive workflows like onboarding/offboarding

- Reduce costs by cutting help desk tickets by up to 50% or more via self-service password reset

Employee benefits

- Provide quick access of any app on any device from anywhere through the OneLogin portal.

- Let employees access the resources they need without having to memorize all their passwords

- Enable self-service so employees can reset passwords without depending on the IT help desk.

1 Verizon Data Breach Investigations Report, May 2019, Verizon
2 New Research Finds Over 50% of Ex-Employees Still Have Access to Corporate Applications, July 13 2017, OneLogin
3 State of Identity and Access Management, April 2019, Pulse Q&A

We are made for MSPs

Secure and protect your internal systems and your customers' systems with one, multi-tenant administration interface. Streamline user management to enhance collaboration between customers and internal employees. Improve automation, strengthen customer retention, and prevent breaches, while increasing revenue and boosting productivity.
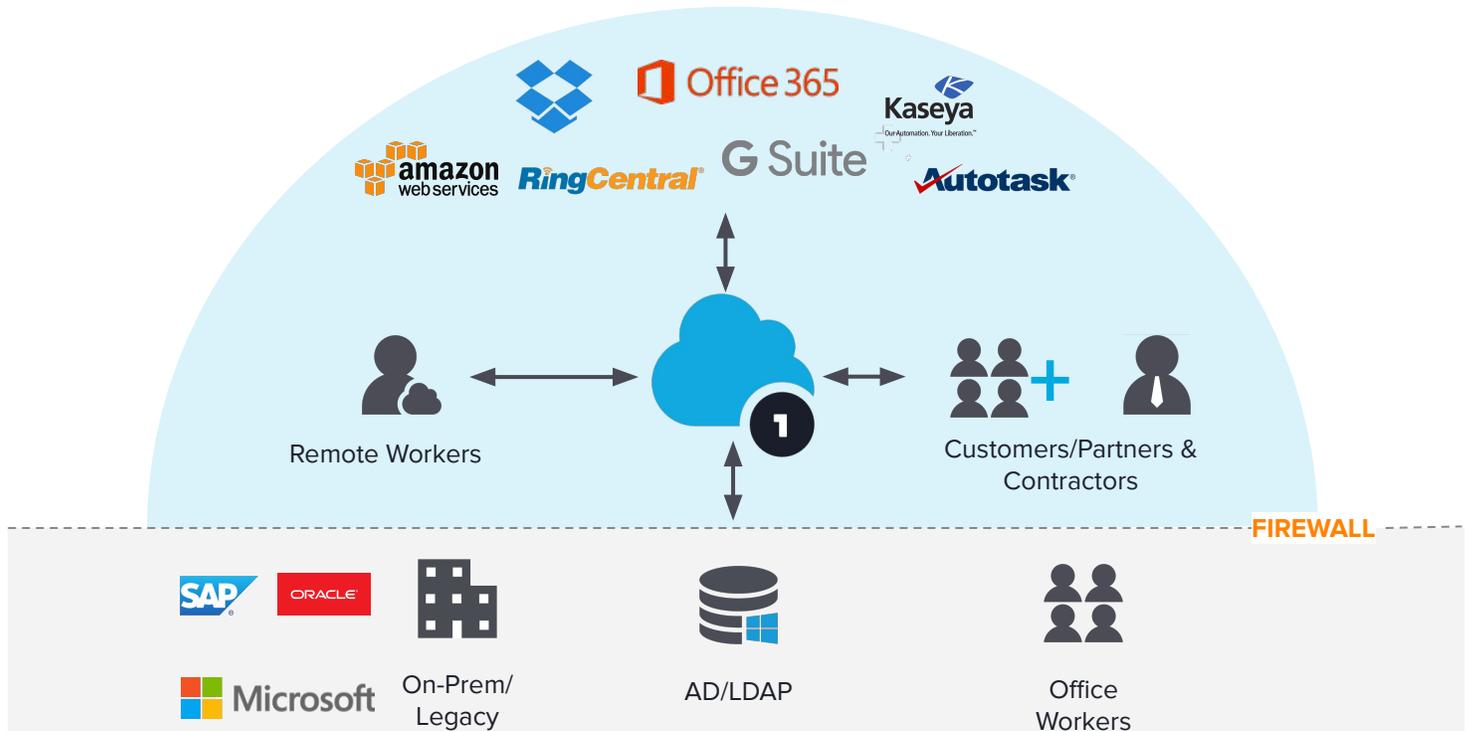
Figure 1: *OneLogin's unified cloud directory allows all your employees, customers, partners and contractors to access business-critical applications–whether on-premises or in the cloud (SaaS)–no matter where they are located. Robust MFA, including risk-based authentication, adds a second layer of security over WiFi and VPN. Move off of AD altogether using OneLogin's VLDAP service or leverage your existing Active Directory (AD) or LDAP username and password credentials.*

Want to learn more?

Visit https://www.onelogin.com/partners/msp to learn more about our MSP program and sign up for a free OneLogin account to get started.

Email partners@onelogin.com to connect with a OneLogin representative for a free assessment of your identity management strategy.

Dozens of MSPs from the MSP 501 partner with OneLogin to protect 1,000,000+ users, 10,000s of apps, and eliminate 1,000,000+ Passwords