Fragmented Access Management Compounds Risk & Inefficiency

Today, the vast majority of organizations struggle to manage complex application environments consisting of a growing portfolio of Software-as-a-Service (SaaS) applications as well as commercial off-the-shelf and custom web apps hosted on-premises, at remote data centers, and in private clouds.

Organizations are challenged by the disparate management of access to applications in different environments, most notably on-premises applications and SaaS applications. While SaaS applications enjoy frequent updates and modern standards, such as SAML and SCIM for secure sign-in integrations and user synchronization, on-premises applications often have an outdated tech stack, with custom or outdated authentication and authorization mechanisms, and no automated controls for access policy updates.

Furthermore, these legacy applications are often managed using aging Web Access Management (WAM) solutions. In other cases, homegrown applications are modern and well designed, but are managed separately from the growing portfolio of commercial SaaS applications, and are not fully connected to the same security controls such as access policies, authentication factors, or monitoring.

OneLogin Access

OneLogin Access solves that problem by extending the reach of the OneLogin Unified Access Management Platform to applications hosted on-premises, at remote data centers, or in private clouds to simplify access administration, reduce IT costs, improve security, and optimize the user experience.

Administrative staff manage solution configuration and application access policies using the OneLogin administration user interface and APIs for cloud applications, eliminating dependencies on aging Access Management tools that are complex to operate, expensive to maintain, and are incapable of addressing the access needs for both cloud and on-premises environments.

Access to commercial, open source, and custom customer managed applications, regardless of their worldwide locations, is provided to users from a unified cloud portal.

End-users, including employees, partners, and even customers, experience a simplified access experience through a Single Sign-On portal to access both SaaS and web apps from any device and any location. OneLogin strengthens security and protects accounts through adaptive authentication to automatically respond to anomalous activity with Multi-Factor Authentication.

Access for IT Practitioners

- Eliminate complex Access Management tools that are complex and incapable of supporting SaaS apps
- Manage access for all of your apps from a centralized platform with a single user interface
- Modernize Access Management for legacy apps with features including Federation, Single Sign-On (SSO), and Adaptive Authentication

Access for IT Executives

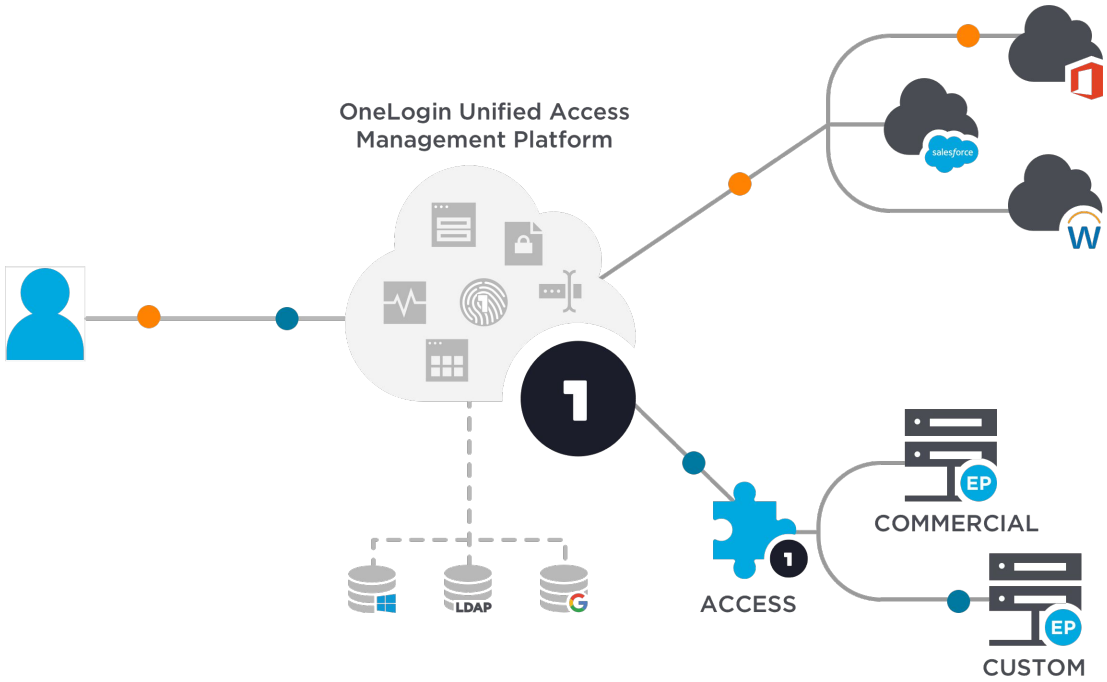
- Migrate off of expensive and labor-intensive legacy Access Management tools
- Increase security with a single portal for employees, partners, and even customers to access their apps
- Consolidate Access Management vendors and gain operational efficiency

Access for Everyone

- Access all apps through a single secure portal from anywhere on any device
- Eliminate the need to recall dozens of passwords
- Make security easy with Adaptive Authentication for dynamic, risk-appropriate Multi-Factor Authentication

"The unification of OneLogin for SaaS apps and for our on-premises applications simplifies and secures access for our employees, scales our growth globally, and streamlines our ability to support business critical operations for our global customers."

Mustafa Ebadi, SENIOR VICE PRESIDENT OF CUSTOMER EXPERIENCE AND IT AT SOTI



High-level architecture of OneLogin Access, which provides user session information and access control services to applications hosted on premises, at data centers, and in private clouds.

How OneLogin Access Works

OneLogin's cloud-based Unified Access Management Platform is the central point of management for all directories, users, and policies for authentication and authorization across the organization.

As such, the Unified Access Management Platform serves as the configuration, policy management, and policy distribution point for applications managed and secured with OneLogin Access. Configuration and policy are distributed from the cloud-based OneLogin platform to Enforcement Points, which are local gatekeepers (e.g. deployed on servers on-premises) to customer managed applications.

Enforcement Points are lightweight OneLogin Access software components, which are available for download and deployment as modern packages such as Docker containers. They are downloaded from OneLogin and install on the local network where applications reside. Enforcement Points can be of type Gateway, which include a HTTP reverse proxy, or type of Agent, which integrates with customer web servers such as Apache, IIS, and Java EE.

Using the combination of Enforcement Points and a cloud-based administration point, OneLogin Access connects your web applications with the Unified Access Management Platform in two critical ways.

First, OneLogin Access automatically provisions application-custom access policies to otherwise manually or disparately managed applications where the policies need to be enforced locally.

Second, it standardizes and modernizes the user's authentication and authorization flow, such that it is the exact same single sign-on experience for all corporate applications whether on-premises or in the cloud, and it leverages the same role-based access control policies as well as advanced controls such as multi-factor authentication and security events.

Each instance of an Enforcement Point is uniquely identified at OneLogin. The Enforcement Points self-register at startup, and automatically retrieve configuration, policy, and software updates from OneLogin using secure, firewall friendly connections.

Enforcement Points control and manage access based on cloud-managed policies. They essentially redirect users to OneLogin for a secure sign-in using SAML. The Enforcement Point handles the secure authentication response (i.e. SAML response) from OneLogin, creates application sessions with fixed and inactivity timeouts, and sets secure HTTP headers that enable signing-in to legacy applications such as Oracle E-Business Suite.

This also enables organizations to replace legacy solutions like CA SiteMinder®, and Oracle Access Manager by mimicking and automating the underlying mechanism, such as setting the user identity HTTP header to SiteMinder's SM_USER. OneLogin offers professional servicesconsultative engagements and materials to support integrationmanagementwith of popular legacy applications as well as migration from common aging Web Access Management solutions.