onelogin

WHITEPAPER

The Evolution of Access and the Emergence of Unified Access Management

Letter from the CEO

Over the last 25 years, I have been fortunate to have rich and varied experiences in technology, from leading the Microsoft Windows brand and consumer business, to reshaping the network software and security market at Juniper Networks, to redefining the way business is transacted at DocuSign.

As a technology leader, I share your passion, and I share your challenges. We live in an incredibly dynamic age with an unprecedented rate of innovation—and technology is the primary fuel behind this innovation. We are fortunate to witness—if not directly shape—the digital transformation that is driving change across business models and entire industries at an unbelievable pace.

Digital transformation is the application of technology to fundamentally improve all aspects of an organization. It often means providing employees, business partners, and customers with access to better data, tools, and applications.

Today we find ourselves in the driver's seat of this transformation. The Information Technology (IT) function is increasingly essential, with IT leaders at the forefront of organizational initiatives and directly impacting business strategy.

Never has it been more critical—or more complex—to get the right technology to the right people at the right time. In fact, 91% of IT decision-makers consider Access Management important or critical to their business' digital transformation strategy[1]. And the scope of managing access is widening to include a growing number of SaaS and on-premises applications as well as networks, directories, and devices.

This complexity presents challenges paired with an opportunity to simplify. Organizations must forge this transformation gap to successfully emerge as a transformed enterprise.

The future is in our hands. It is up to us—collectively—to rise to the occasion and not simply witness this revolution, but to drive it. In the following pages, we will explore the evolution of Access Management, including the good, the bad, and the ugly, as well as share our perspective on the opportunity for a new, unified approach to Access Management. We hope this document serves useful on your journey.

Brad Brooks, CEO

Content

[1] *"The Future of Access is Here: Why Organizations Need Unified Access Management," Arlington Research, February 2018*

The Evolution of Access

Access Management grew principally out of necessity. With the proliferation of web applications in the late 1990s and early 2000s, employees required access to an increasing number of systems.

Commercial information systems offered by vendors such as Oracle and IBM as well as custom-built systems and applications offered increased productivity and accelerated business growth. As these tools developed organically, they lacked the standardization of web and native services, particularly with respect to configuration, administration and authentication architectures, and were not designed to operate at massive scale.

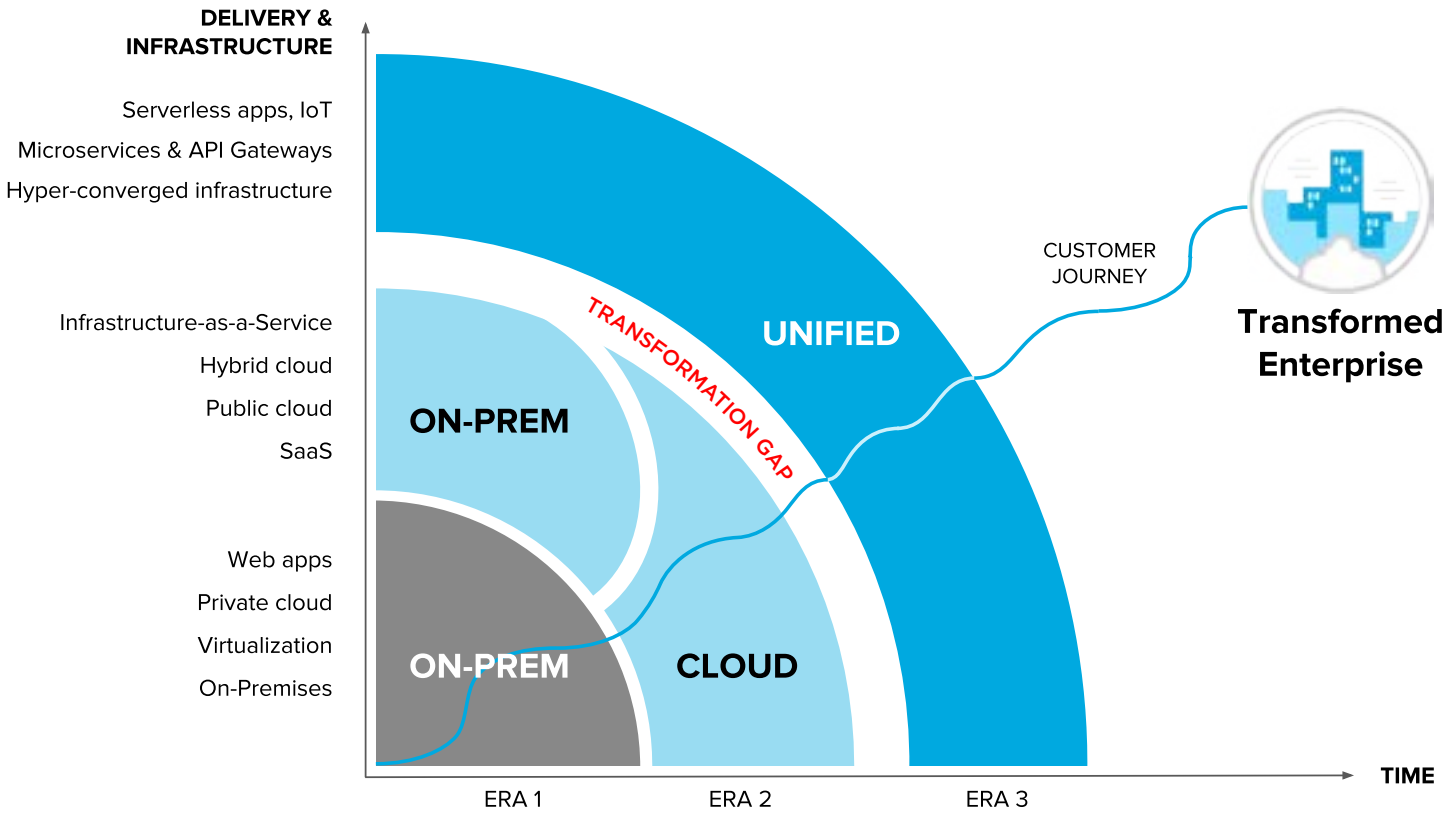
The IT staff took charge of Access Management, granting and revoking application access, ensuring proper privilege levels within apps, supporting access-related end-user needs, and protecting accounts and their associated credentials.

To reduce the Access Management workload, savvy IT professionals began writing their own tools in-house to automate as much of the redundant and laborious tasks as possible. Meanwhile, large software vendors identified the growing need for Access Management products and began developing solutions to bring to market.

"By 2020, a typical small enterprise's IAM program will span 1 million people, 10 million things, and billions of relationships."

—Gartner Research[2]

The Three Era of Access Management



[2] *"Gartner Events Presentation, Tutorial: IAM 101, David Anthony Mahdi, Gartner Identity & Access Management Summit, 28—30 November 2017, Las Vegas, NV*

Compliance regulations and governing bodies grew increasingly concerned with Access Management (and the associated security implications) in response to a number of large scale accounting fraud incidents in the private sector in the early 2000s. Meanwhile, the threat landscape evolved quickly in response to the interconnectivity of computing resources and valuable payloads within them.

New regulations required companies to control, audit, and document application access within their organization. Most notably, the Sarbanes-Oxley Act (SOX)—alternately known as the "Corporate Auditing Accountability, Responsibility, and Transparency Act" was signed into law in July of 2002 and catalyzed a sea change within IT organizations, specifically with regard to managing—and documenting—access.

These two primary drivers—the inefficiencies associated with managing access manually as well as the need for increased access control for both compliance and security purposes—established themselves as the principal motivations for organizations to adopt Access Management solutions.

The total global public cloud market will be $178B in 2018, up from $146B in 2017 and will continue to grow at a 22% Compound Annual Growth Rate (CAGR). … By the end of 2017, Forrester Research expects that half of all global enterprises will rely on public cloud platforms.[3]

An On-Premises Solution to an On-Premises Need: The First Era of Access

Initially, Access Management solutions were designed for customer-managed applications, including web apps hosted on-premises, at data centers, and, later, in private clouds. Access Management offerings born in this era such as Netegrity, Oblix, and Wavest—which later became CA Siteminder, Oracle Access Manager, and Sun Identity Manager, gained rapid traction in the marketplace.

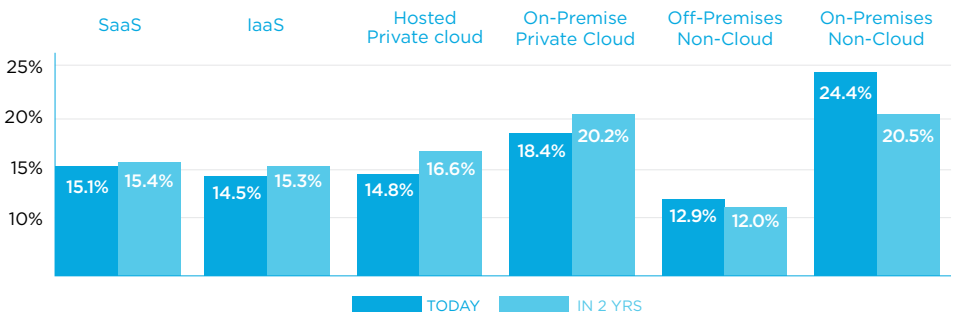
These were highly complex on-premises software solutions that used plug-ins and database integrations to create the Single Sign-On (SSO) experience. Federation did not exist and SSO was limited to allowing employees to use the same password for every application, though they were still required to sign in manually. These products were designed to deal with the complex software packages from PeopleSoft, Oracle, and SAP as well as countless of in-house applications that enterprises built over the years.

The concept was simple: on-premises Access Management software was used to manage access to exclusively on-premises applications; a one-to-one ratio of environments to Access Management solutions. However, operational deficiencies and challenges related to these solutions began to arise.

The Access Management tools born in this era are extraordinarily complex and extremely specialized software solutions, with daunting volumes of documentation and a small pool of sufficiently capable IT staff to administer the tools. They require multiple employees dedicated on a full-time basis to operate them and require a high volume of customization to meet the needs of most production environments.

[3] "Predictions 2018: Cloud Computing Accelerates Enterprise Transformation", Forrester Research, November 2017

Application Distribution—Current and In Two Years[4]



Though they were well-suited for their original purpose of managing access for on-premises applications, the Access Management solutions of this era were not designed to address the growing adoption of Software-as-a-Service (SaaS) apps in the late 2000s and 2010s.

The SaaS Tsunami, Hybrid Environments, and Fragmented Management: The Second Era of Access

SaaS applications gained traction in the workplace as they delivered on their promise of accelerated time-to-value, elasticity and scalability, dramatically reduced total cost of ownership (TCO), improved collaboration, and reduced demands on IT organizations as compared to their on-premises counterparts.

New standards, including SAML, OAuth, and SCIM emerged. SAML introduced a standard way for business applications to replace password-based authentication with secure Single Sign-On, while OAuth introduced a standard for business and consumer applications to pull consumer identity information and authentication. A later standard, SCIM, helped SaaS providers synchronize business identity stores from corporate directories in a standard and scalable way.

While the speed, convenience, and power of cloud applications were a welcome addition to the IT landscape on the whole, the rapid adoption of these technologies led to a fragmentation of application environments.

The majority of organizations were now tasked with managing access to not one, but multiple application environments: 1) an on-premises portfolio of apps, and 2) a separate portfolio of public cloud applications.

While some institutions resisted the cloud—sanctioning solely on-premises solutions—other organizations went all-in on cloud technologies as quickly as possible. Most institutions found themselves somewhere between these two extremes, with a heterogeneous mix of both on-premises applications and cloud apps and no clear solution to centrally manage access across these disparate environments.

Do you currently have an Identity and Access Management solution deployed within your organization?[5]

17.0%
Yes: On-premises only

16.0%
Yes: Cloud applications only

57.8%
Yes: Both on-premises and cloud applications in multiple solutions

6.8%
Yes: Both on-premises and cloud applications in one solution

2.4%
No

[4] *"Success Factors for Managing Hybrid IT," 451 Research, March 2017*

[5] *"The Future of Access is Here: Why Organizations Need Unified Access Management," Arlington Research, February 2018*

Inadequate Approaches to Access Management in the Hybrid Era

In response to the surging portfolio of cloud applications, multi-tenant Identity-as-a-Service (IDaaS) offerings aimed at managing access for SaaS applications began to emerge, including Centrify, Microsoft Azure AD Premium, Okta, and OneLogin. Generally, these services offered their own cloud directory and/or synchronized with existing user stores and identity infrastructure such as Microsoft Active Directory and LDAP to perform fundamental Access Management tasks.

IT organizations faced a considerable challenge: how to manage access for two completely distinct environments, each with their own set of vendors focused on addressing one half of the equation. This led to a series of less-than-ideal approaches to managing access:

1. For some organizations, the cloud application environment went unmanaged entirely, becoming a digital wild west. For other organizations, the fear of such a wild west or splintered scenario led to outright resistance to the adoption of cloud applications—an unrealistic approach that encouraged subversion in the form of Shadow IT and exposed the organization to increased security risk.
2. Other companies accepted the only comprehensive (albeit splintered) option based on products available in the marketplace: a fragmented approach, where they invested in a dedicated Identity-as-a-Service solution aimed at managing access to their growing portfolio of cloud applications while continuing to manage access to their on-premises apps with the existing vendor deployed in the first era of Access Management. This approach proved extremely time-consuming, inefficient, and expensive as organizations were forced to work with multiple vendors and systems.
3. An additional set of businesses attempted to migrate to the cloud at full speed, hoping to put their labor-intensive and expensive on-premises footprint in the rear-view mirror, but were stymied by dependencies on customer-managed on-premises systems ingrained in processes throughout the organization.

The Pain of Fragmented Access Management

The challenges of managing access in this hybrid era—particularly at the scale of contemporary global enterprises—were hauntingly familiar to the initial drivers for Access Management solutions: 1) to reduce the inefficiencies associated with Access Management, and 2) to increase access control capabilities for both compliance and security purposes.

Fragmented Access Management at Scale

Consider the case of an enterprise that needs to manage and secure access to hundreds of SaaS applications such as Salesforce.com or Box in addition to a collection of commercial and homegrown apps that they host, such as Oracle eBusiness Suite or SAP.

Naturally, the enterprise wants the ability to enable users (ranging from employees to partners and, in select cases, customers) to access these applications from anywhere with a single set of credentials. Additionally, the organization wants to protect each and every app with Multi-Factor Authentication and to manage this access efficiently, minimizing manual work and scalability challenges.

Unfortunately, some of these apps do not support modern authentication standards. Further, some of the apps live in environments disconnected from corporate directories, or have access policy files that require manual updating.

But access can, in fact, be governed, administered, and audited from a single source that provisions and asserts the same identity information to any environment and any app through a unified approach to Access Management.

While IDaaS solutions delivered on their promise of intuitive simplicity, reduced total cost of ownership, and the benefits of standards such as SAML, OAuth, and SCIM, they lacked the ability to manage access for on-premises applications, which, for many organizations, represented a sizable portion of their overall application portfolio.

Conventional Access Management solutions failed to address the rapidly growing volume of cloud applications and exacerbated other pain points. According to a 2018 Arlington Research study, the top pain points[6] of on-premises Access Management tools are:

1. **Cost**
2. **Maintenance**
3. **Complexity**
4. **Overhead (labor)**
5. **Redundancy**
6. **Reliability**
7. **Compliance**

According to a January 2018 McKinsey article, sixty percent of respondents reported they employ on-premises access solutions today, but *only half as many expect to be using on-premises access solutions in three years.*[7]

By that time, 60 percent of interviewees anticipate that their enterprises will rely on a third-party access service that supports multiple public-cloud environments and *unifies access controls across on-premises and public-cloud resources*. But what would such a technology look like?

If we were to design an ideal solution to address the Access Management needs of modern enterprises, what would it look like? What capabilities and functionalities would it include? How would it be delivered and managed?

[6] *"The Future of Access is Here: Why Organizations Need Unified Access Management," Arlington Research, February 2018*
[7] *"Making a Secure Transition to the Public Cloud," McKinsey & Company, January 2018*

A New Approach to Access Management for a New Era

The technology landscape has shifted dramatically from the early days of web apps and basic Web Access Management. We are rapidly approaching an era where complete networks can be managed remotely from the cloud and applications can be migrated to and from any environment (private, public, or hosted).

The objective of this fluidity is to increase efficiency for both IT staff as well as the broader employee base and ultimately gain meaningful and measurable business value from technology. But in order to thrive in this new era, we must eliminate barriers in the form of unnecessarily complex, inefficient, and costly technologies in favor of simple, scalable, and flexible solutions.

Today, the vast majority of organizations struggle to manage complex application environments consisting of a growing portfolio of SaaS applications as well as Commercial Off-The-Shelf (COTS) and custom web apps hosted on-premises, at remote data centers, and in private clouds. Organizations are further challenged to manage access to applications, networks, and devices for users stored in disparate directories.

Conventional Identity and Access Management tools force organizations to manage access to these distinct environments, networks, and devices separately, leading to a fragmented approach that is plagued with complexity, inefficiency, and high cost.

A Unified Approach to Access Management

Unified Access Management enables a unified approach to managing access for both SaaS and on-premises application environments, as well as extending Access Management to networks and devices, using SaaS infrastructure which unifies all corporate users and user directories. In doing so, Unified Access Management greatly simplifies the overall administration experience, reduces costs and operational complexity considerably, improves the end-user experience, and improves organizational security.

In 2018, ninety-eight percent of IT decision makers polled expressed interest in a cloud-delivered Access Management solution for both on-premises and SaaS apps that offers functionality such as a centralized directory, automated provisioning, one SSO portal for access to all apps, and Multi-Factor Authentication (MFA), with 39% expressing an extreme level of interest and 46% responding as “very interested”.[8]

If we were to design an ideal solution to address the Access Management needs of modern enterprises, what would it look like? What capabilities and functionalities would it include? How would it be delivered and managed?

[8] *“The Future of Access is Here: Why Organizations Need Unified Access Management,” Arlington Research, February 2018*

Ideally, a Unified Access Management solution would fuse the most desirable components of both conventional on-premises tools and Identity-as-a-Service offerings, marrying the speed, scalability, and elegance of the cloud with the functional capabilities of on-premises solutions.

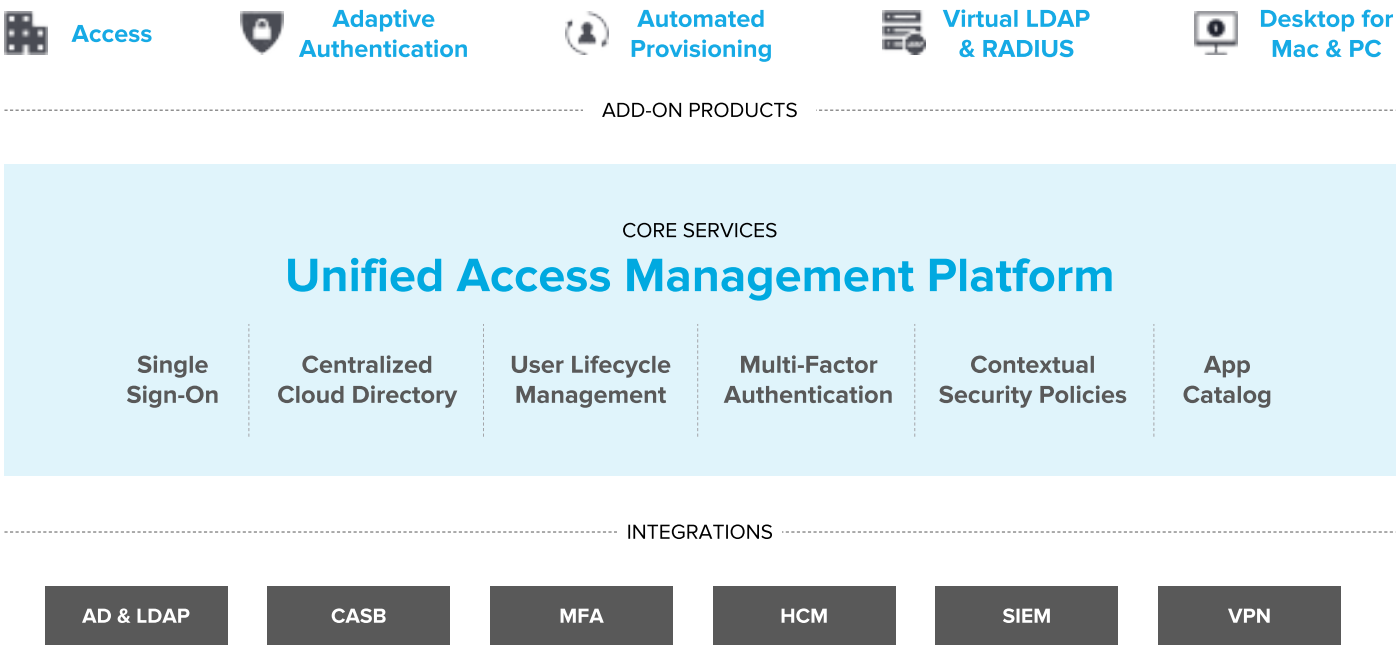
Specifically, this solution would bridge the gap between directory infrastructure and on-premises applications by translating user info from the cloud into customized HTTP headers that on-premises applications natively understand. It would connect to a range of web app servers, such as Apache, IIS, Tomcat, Weblogic, WebSphere, and JBoss.

The solution would be easy to configure and lightweight in nature but scalable for the enterprise, without requiring dependence on installation wizards or complex configuration, and offer the full of set of cloud identity features, such as Single Sign-On with adaptive Multi-Factor Authentication and the ability to automate provisioning to SaaS apps.

The OneLogin Unified Access Management Platform

The cloud-based OneLogin Unified Access Management Platform unifies access to both SaaS and on-premises applications, as well as a wide range of networks and devices. OneLogin makes it simpler and safer for everyone to access the apps and data they need, anytime and everywhere.

The OneLogin Unified Access Management Platform is comprised of multiple layers and building blocks, all purpose-built to unify directories and users, as well as access to applications, networks and devices.



The OneLogin Unified Access Management Platform serves as the configuration, policy management, and policy distribution point for OneLogin Access.

The core of the Unified Access Management Platform is the OneLogin Cloud Directory. The OneLogin Cloud Directory is a full-featured, standalone corporate directory, which can also sync users from multiple existing corporate directories such as several Active Directory domains and LDAP directories, and even Human Resources Information Systems, including Workday, Namely, UltiPro, and BambooHR. Its power is in unifying users from all corporate directories, in a single view with a flexible schema.

On top of OneLogin's Cloud Directory are components which help construct context and security policies. A key component is OneLogin Roles, which is a Role-Based Access Control engine which provides a simple way to assign any user multiple labels for Role-Based Access Control (RBAC) based on any existing user metadata. OneLogin also offers Mappings, which is a powerful product for flexible and automated mapping of attributes and roles to users.

OneLogin Roles, in addition to any other user metadata such as department name, job title, and existing Active Directory group memberships, can be provisioned to various parts of your broad IT environment, from on-premises applications to office wifi appliances, in order to enable authentication and authorization for all users. On top of the unified directory and the access policies are many services and

security functionality, including authentication factors, security events, and employee lifecycle management.

For example, an organization may have the following Access Management implementation and policies:

1. Users from acme.com (an Active Directory forest) and ExampleCorp.com (an LDAP directory), a subsidiary acquired by Acme, are all managed and provisioned in the same, single, unified corporate directory view. Business partners, who are not stored in any of the corporate directories but are managed in a cloud directory, are managed in the same unified view.
2. All full-time employees, but not contractors, can access the secure corporate wifi with their corporate credentials.
3. All engineering employees are able to use a cloud VPN in order to connect to the company's production environment on AWS, using their corporate credentials and a second authentication factor (2FA).
4. All sales employees have access to Salesforce, but only sales managers have managerial privileges such as approving quotes.
5. Operations managers and business partners are able to access shipping and tracking information in a custom web application hosted on-premises.
6. Remote employees and contractors can use their corporate credentials to single sign-in to their Mac computers, and access can be immediately revoked in case of a lost or stolen laptop.

To summarize, the cloud-based OneLogin Unified Access Management Platform unifies access to both SaaS and on-premises applications, as well as a wide range of networks and devices. OneLogin makes it simpler and safer for everyone to access the apps and data they need, anytime and everywhere.

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.

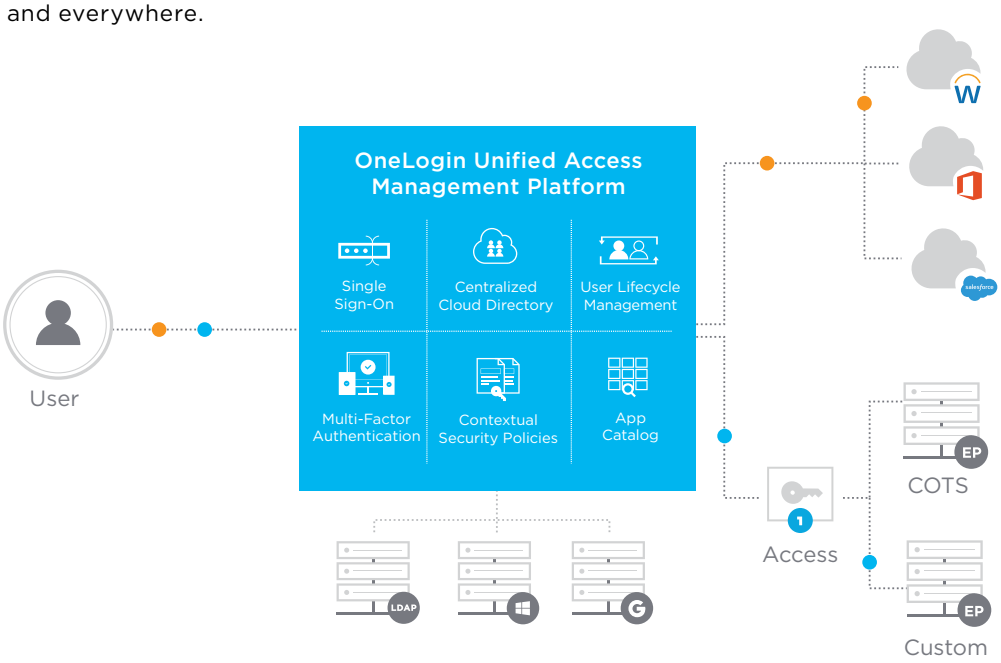


Figure 1—High-level architecture of OneLogin Access, which provides user session information and access control services to applications hosted on premises, at data centers, and in private clouds.

Unifying Fragmented Access Management with OneLogin Access

A particularly difficult problem is 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 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.

Gateways

A gateway is an enforcement point that includes an NGINX web server used as a reverse proxy. A Docker script installs the gateway on a customer's Linux system. Any number of gateways can be deployed and configured at a customer site with protected applications partitioned to gateways based on location and load balancing requirements. Multiple gateways are required for redundancy and failover.

Agents

Agents are enforcement points without a reverse proxy that plugin into customer web servers.

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

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:

1. First, OneLogin Access automatically provisions application-custom access policies to otherwise manually or disparately managed applications where the policies need to be enforced locally.
2. 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 services and materials to support integrations with popular legacy applications as well as migration from common aging Web Access Management solutions.

The Case For Unified Access Management

Today, the vast majority of organizations struggle to manage complex application environments consisting of a growing portfolio of SaaS applications as well as commercial off-the-shelf and custom web apps

> "The Unification of OneLogin's cloud directory for SaaS apps and OneLogin for our on-premises applications makes secure access easier for our employees, enabling us to have a more efficient and effective IT department."
>
> **MUSTHAFA EBAD**
>
> *Vice President of Customer Experience and IT, SOTI*

hosted on-premises, at remote data centers, and in private clouds. Organizations are further challenged to manage access to applications, networks, and devices for users stored in disparate directories.

Conventional Identity and Access Management tools force organizations to manage access to these distinct environments, networks, and devices separately, leading to a fragmented approach that is plagued with complexity, inefficiency, and high cost.

OneLogin offers a Unified Access Management which can address these pain points with the following benefits:

- **OneLogin features one integrated interface, one audit trail, and one support experience to optimize the customer experience.**
- **OneLogin integrates with Active Directory in real time versus batch-uploading to avoid delays in user onboarding and offboarding and protect customer and employee data from breaches or unauthorized access.**
- **OneLogin's Unified Access Management Platform leverages adaptive authentication technologies to benchmark typical user behavior and detect anomalies, mitigate risk, and improve security without sacrificing usability.**
- **The maturity and breadth of OneLogin's solution (including cloud-based LDAP and RADIUS support) extends Access Management control for improved security and an improved administrative and end-user access experience.**

Taking Action To Understand Your Challenges and Plan Ahead

The next step on your journey to Unified Access Management is an assessment to better understand the particular Access Management challenges you face at your organization.

For qualified parties, OneLogin is offering a complimentary Access Management maturity assessment. By answering a brief series of questions, you will enable us to provide you with an in-depth analysis of where your organization falls on an Access Management maturity continuum formulated with the collective wisdom gathered from working with thousands of innovative organizations.

We are offering you the opportunity to share your IT pains and needs, and in turn we will provide you with a prescriptive analysis of potential Access Management solutions, including a quantitative, ROI-driven case for making strategic investments in select technologies. We will also provide additional resources tailored to your organization

and share case studies detailing how relevant organizations (similar challenges, size, geography, industry, technologies) advanced their digital transformation posture with OneLogin.

To learn more about the benefits of Unified Access Management and begin your journey as a transformed enterprise, contact a OneLogin Account Executive for a complimentary Unified Access Management maturity assessment at sales@onelogin.com or by calling toll-free (855) 426-7227 or +44 (808) 109-3898, or simply visit http://www.onelogin.com/get-unified.

About OneLogin, Inc.

OneLogin is the leader in Unified Access Management, Enabling Organizations to Access the World™. OneLogin makes it simpler and safer for organizations to access the apps and data they need anytime, everywhere. The OneLogin Unified Access Management Platform secures millions of identities for thousands of companies around the globe, spans both cloud and on-prem environments, and unifies all users, devices, and applications to transform enterprises. We are headquartered in San Francisco, California. For more information, visit www.onelogin.com, Blog, Facebook, Twitter, or LinkedIn.