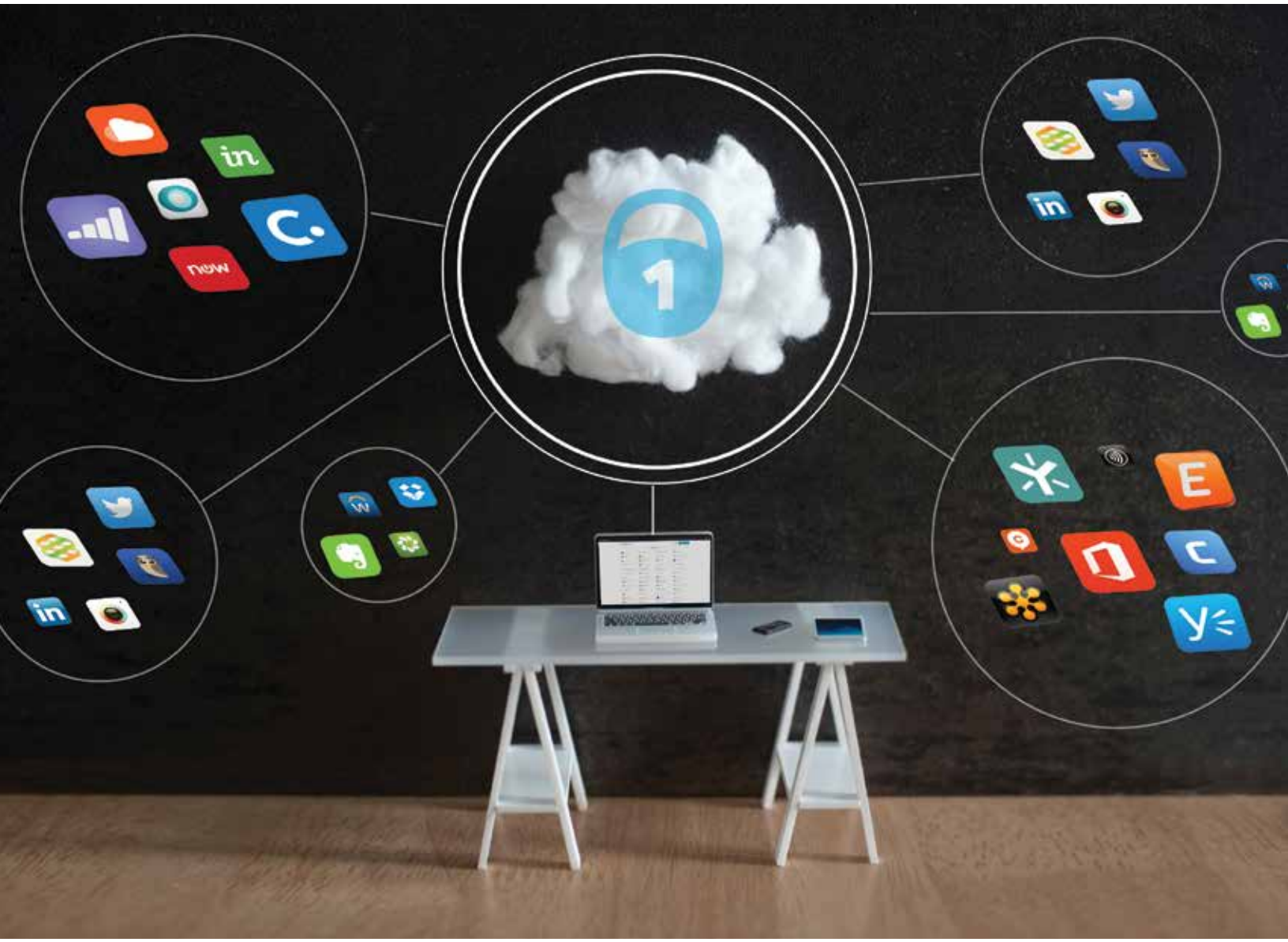
onelogin

WHITEPAPER

How to Overcome Challenges in Deploying Cloud Apps to Get the Most from your IAM Investment



www.onelogin.com • 150 Spear Street, Suite 1400, San Francisco, CA 94105 • 855.426.7272

EXECUTIVE SUMMARY

Overcoming Challenges in Deploying Cloud Applications, and Getting the Most from your IAM Investment

At the end of the day, business is about delivering value to customers. That value can be realized in various products and services that solve customer problems at a reasonable cost. Bringing solutions together that optimize delivery and maintenance of these services is paramount in the connected world. As organizations move from on-premises software to on-demand cloud-based services, a new set of identity management challenges emerge. In response to these trends the role of IT is changing and users are looking to IT as the facilitator during this transition. Subsequently, IT has prioritized those challenges associated with deploying cloud and Software as a Service (SaaS) applications in order to ensure the company is maximizing the value of these investments. Identity and access management (IAM) sits at the crossroad between employee or user challenges and those faced by IT.

EMPLOYEE-FACING CHALLENGES

1. Application Access

Automate User Provisioning and De-Provisioning

Time is money, and the longer it takes to get the right tools like Office 365, Salesforce, and Box into the hands of employees, the longer it takes for them to start being productive. For both existing employees and anxious new hires, waiting to get access to the applications they require in order to do their job has a direct impact on their sense of contribution and satisfaction.

As more organizations transition to a SaaS model, new multi-tenant applications need to be set up. Given the dozens, if not hundreds, of cloud based applications placed into service, each with their own management console and user store, IT simply can't interface with every application on behalf of every employee in a manual, one-off manner. Granting access to SaaS applications impacts both the productivity of end users and similarly that of the IT organization. And failing to update or revoke access in a timely manner has security implications. Bottom line- manual provisioning is time consuming and error prone, thus impractical at scale.

Several factors influence the actions necessary to provide application access for users, including:

- Defining workflows for on-boarding and off-boarding employees
- Connecting Human Resource systems with IT systems, bridging information about users, their roles and entitlements, with the resources and services available through IT
- Procuring licenses and managing subscriptions in the target applications
- Creating user accounts within each SaaS application, as each has its own proprietary user
- Defining entitlement mappings through each application's provisioning APIs
- Deleting users and their access to data upon leaving the organization

OneLogin supports automated provisioning and de-provisioning to hundreds of leading enterprise cloud applications as a natural extension of the existing on-boarding and off-boarding process. For example, when a user is added to the core directory service such as Active Directory (AD), the user is automatically provisioned to those applications associated with that role or group and access permissions are granted as needed. And when users leave the organization or are terminated their accounts can be quickly de-provisioned to minimize inadvertent or intentional data corruption or loss.

EMPLOYEE-FACING CHALLENGES

2. Password Fatigue and Resets

Provide Single Sign-On (SSO), Establish System of Record and Synchronize in Real-time

It wasn't long ago that business users, working inside the organization's firewall, logged into their Windows laptop and were automatically authenticated against Active Directory thereby granting them access to the applicable IT resources on the network. With the growing adoption of SaaS over traditional on-premises client-server solutions, users now have access to web-based cloud applications from anywhere, anytime, from any device.

However with each application requiring its own password, with different password requirements and expiration cycles, the complexity increases exponentially as the number of applications increase. User frustration increases in response as users spend more time trying to remember, reset and manage these constantly changing passwords and URLs across all their applications. Even more worrisome is that calls into the Help Desk regarding password resets drain IT resources and detract from other strategic focus areas.

Several factors influence the actions necessary to reduce password fatigue and password resets, including:

- Defining an SSO strategy including password requirements and access controls
- Leveraging the IT system of record and single authoritative store for user passwords, such as the on-premises AD
- Taking advantage of Desktop SSO capabilities and existing Integrated Windows Authentication (IWA) services to extend successful Windows logins to other applications
- Providing self-service password reset services including security questions
- Updating credentials in all cloud applications from a centralized service

OneLogin provides a single point for managing passwords to all subscribed cloud applications delivered to the organization. And with Desktop SSO and integration to Active Directory, OneLogin users extend their AD credentials to access their SaaS applications. By alleviating password requirements to each application, access to the right resources through automated provisioning is accelerated, and employees are more satisfied and productive.

EMPLOYEE-FACING CHALLENGES

3. Mobile Experience

Address Mobile Form-factor and Native Applications

Nearly 50% of cloud application requests originate from mobile devices, thus mobile applications themselves are an increasingly important tool for driving business outcomes. It's imperative that mobile applications support a positive user experience otherwise mobile users will move onto other applications to get the job done. For example, it is cumbersome for users to constantly re-enter their credentials, particularly in email and strong password format, from tiny keyboards. This inconvenience will wear on mobile users who may seek alternatives likely to be less secure.

Several factors influence the actions necessary to improve the mobile experience, including:

- Inventorying available mobile applications supporting your cloud applications
- Evaluating mobile security options beyond just mobile device management
- Understanding emerging mobile trends including initiatives like OpenID's Native Applications (NAPPS) working group
- Planning for the next-generation of user authentication, and ensuring application developers are prepared to support

OneLogin provides a mobile portal that introduces an SSO experience without requiring multiple passwords to access cloud applications. OneLogin is also an early proponent of NAPPS and offers open source toolkits to assist mobile application developers introduce mobile SSO and authentication capabilities within native mobile applications.

IT-FACING CHALLENGES

4. Shadow IT

Manage a Standard Application Catalog Sanctioned by the Enterprise

Users have gotten more savvy, and are quick to explore new applications that deliver the right services and information for them to accomplish a task. This consumerization of IT accelerated the introduction of cloud applications within lines of business without the necessary controls in place to support enterprise requirements, hence the origins of Shadow IT. With upwards of 80% of cloud applications used within the enterprise outside IT's control, having visibility into who is accessing what and where potentially sensitive data resides is crucial. By demonstrating that IT can be responsive to an agile business by, quickly bringing new applications online and provisioning users, shadow IT is marginalized. And once under IT supervision, governance policies which might include step up authentication services can easily be provided to ensure additional layers of protection are enforced to further protect data.

Several factors influence the actions necessary to eliminate shadow IT, including:

- Connecting to approved cloud applications quickly
- Keeping application integrations up to date and working with each service update
- Provisioning and de-provisioning users to all cloud applications automatically
- Reporting on user access and cloud application use

OneLogin provides a catalog of over 4,000 web applications which support SSO and automated user provisioning. With pre-built connectors, many based on standards like SAML (Security Assertion Markup Language), and automated provisioning integrations that promote on-boarding users with the services they need quickly, OneLogin helps IT be part of the overall value chain.

5. Federation and Single Sign On (& Sign Off)

Enable Cross Domain Authentication

Digital business has become more distributed, sharing cloud infrastructures and applications through numerous multi-tenant service providers. For organizations to successfully manage their user accounts across all these applications, they need to begin by federating numerous user directories and cloud app user stores, and reconciling them against a chosen directory of record or single source of truth. As the federation of identities and centralization of authentication become more common to support Single Sign-On (SSO), risk is aggregated to a singular point serving multiple services. It becomes critical that additional credentialing or multi-factor authentication (MFA) technologies be implemented alongside federation services to support the levels of assurance (LOA) required to meet trust requirements. A cloud identity-as-a-service or IDaaS provider is tasked with federating identity and access policies, and applying rules to resolve conflicts. From this, organizations have complete visibility into their users, roles, applications, and behaviors.

Several factors influence the actions necessary to federate user stores and provide strong authentication, including:

- Connecting to the organization's directory service (e.g. Active Directory) as well as each cloud application's user store
- Supporting real-time synchronization and data exchange between applications and the system of record
- Mapping data elements of each user store to OneLogin's user directory and providing flexibility to respond to custom fields
- Providing additional authentication factors and defining step up requirements based on policy

OneLogin provides facilities to easily federate various directory stores, and supports cross domain authentication.

6. Strong Authentication

Centralize Authentication Services via an Identity Provider (IdP)

At the crossroads between users and their cloud applications sits Identity and Access Management. As more cloud applications are placed into service and systems become more distributed, organizations must provide trusted authentication across domains. There are three types of authentication factors:

- Something you know: a password or a PIN
- Something you have: a mobile phone or a key fob
- Something you are: fingerprint, voice pattern or iris scan

The password is something users know is most often compromised, so a second authentication factor should be applied. Mobile phone apps or key fobs that generate a unique PIN every 30 seconds are the most practical ones, thereby reinforcing passwords with additional authentications mechanisms..

Several factors influence the actions necessary to provide SSO and single sign-off, including:

- Connecting all cloud applications to a cloud-based Identity Provider (IdP) like OneLogin
- Providing cross domain authentication through API interfaces or open standards
- Ensuring compatible browsers and devices reside in the custody of the user
- Leveraging users' mobile devices as a secondary factor for authentication to deliver time-based one-time passwords (OTP)

OneLogin alleviates the challenges of disparate user stores and different authentication mechanisms across all the cloud applications. This is accomplished by supporting SSO services which internally translate and store credentials for the different mechanisms so that the user experience is simplified, yet more secure..

7. Audit Reporting and Compliance

Monitor and Attest Application Access

Responding to auditors is a task everyone recognizes as a periodic cost, yet it ensures the organization fulfills its compliance obligations by providing operational checkpoints that verify proper controls are in place. Ensuring that processes and systems support tasks like defining employee entitlements to applications, tracking management approvals, and responding to changes ensures the organization's attestation process proceeds smoothly. Comprehensive audit reporting easily summarizes information pertaining to who has access to what, and who has accessed what. Doing this in an automated manner across hundreds of cloud applications and countless organizational roles and policies, versus manually, can save time and money, and alleviate lots of frustrations.

Several factors influence the actions necessary to report on user access for audit and compliance concerns, including:

- Inventorying enterprise applications available to the organization
- Identifying employee entitlements to these applications, and associated roles, as well as the information accessible
- Enforcing access control policies unique to each cloud application
- Automating reporting across all cloud applications

OneLogin plays a critical role in meeting contemporary audit requirements as more organizations move to the cloud. Both standardized, out of box reporting and custom reporting capabilities help IT admins monitor application use and quickly respond to changes in access policy.

SUMMARY

OneLogin provides an Identity-as-a-Service (IDaaS) solution that helps organizations overcome these challenges, and delivers the features, scalability, and availability required to meet the needs of leading enterprises.

For more information regarding Why OneLogin, visit: www.onelogin.com

The only Challenger in Gartner's IDaaS MQ, considered a "Major Player" in IAM by IDC, and Ranked #1 in Network World Magazine's review of SSO tools, OneLogin's cloud identity management platform provides secure single sign-on, multi-factor authentication, integration with common directory infrastructures such as Active Directory and LDAP, user provisioning and more. OneLogin is SAML-enabled and pre-integrated with thousands of applications commonly used by today's enterprises, including Microsoft Office 365, Asure Software, BMC Remedyforce, Coupa, Box, Clarizen, DocuSign, Dropbox, Egnyte, EMC Syncplicity, EchoSign, Google Apps, Jive, Innotas, LotusLive, NetSuite, Oracle CRM On-Demand, Parature, Salesforce.com, SuccessFactors, WebEx, Workday, Yammer, ServiceNow, Zscaler and Zendesk. OneLogin, Inc. is backed by CRV and The Social+Capital Partnership.