onelogin

WHITEPAPER

Modern Identity

Addressing Risk, Complexity & User Experience

150 Spear Street, Suite 1400 San Francisco, CA 94105 877 979 0411 onelogin onelogin.com

Preface

Today, thousands of cloud apps are available that deliver a better user experience, provide more elastic licensing models, and substantially lower total cost of ownership. Organizations are constantly adopting new cloud apps: CRMs like Salesforce.com or SugarCRM, Marketing tools like Marketo and Hubspot, HR apps like Workday and Zenefits, Collaboration tools like Box, Dropbox or Egnyte, productivity suites like Microsoft Office 365 and Google Apps, Recruitment apps like Greenhouse, messaging apps like HipChat or Slack, and the thousands of other business applications that contain business-critical and sensitive information.

In fact, nearly all organizations founded after the year 2005 run purely in the cloud. For those invested in on-premises or hosted applications, transitioning towards a transitional hybrid operation or pure-cloud set-up has become inevitable. But cloud adoption is still not as fast as it could be. So where is the inertia, and how is an organization to successfully navigate through a changing app landscape? And for cloud-first companies, how does identity play into it all?

In this whitepaper, we will first contextualize Cloud IAM, and then discuss the current cloud app adoption challenges around risk, complexity and the user experience, and how Cloud IAM addresses them.

Introduction

We're living in a time where people, organizations and societies not only rely, but thrive on simple and fast access to information. This is true for small businesses, startups, enterprises and global conglomerates across all verticals. It also applies to local, state and federal governments, as well as to educational institutions and nonprofits.

Ten years ago, the cloud app revolution started to change the way organizations manage IT. However, the core requirements of IT have stayed the same. Technology leaders are chartered to ensure that 1) information remains confidential and protected, 2) information systems are available and operational, and 3) people are empowered and productive in their roles.

So what is **Identity and Access Management (IAM)**? Simply put, IAM is a technology and security discipline that goes back just about as far as networked computing.

Identity is simply the fact of who a person is. In an organization, we need to assert, verify, manage and propagate that person's user identity. We need to ensure that a person is, in fact, who they claim to be, and we need to manage identities across apps and resources.

Access is even more easily defined; it is about organizational resources and how to enable the right people to create, view, use, consume, or modify those. Just as importantly, it is about ensuring that the wrong people do not have these permissions.

Formally, IAM is the discipline of securely enabling the right people to have convenient access to the right resources at the right time for the right reason. As a software system, it's a set of complex functions that simplify the effort involved in accomplishing that goal. This goes beyond IT Administration, Security, Operations and Governance, and has a lot to do with HR, line of business managers and, of course, end users. And the latest trend for IAM is to maintain identities in the cloud.

According to a recent Forrester Report on the State of Identity and Access Management, 43% of North American and European technology decision-makers are either already heavily investing in expansion & upgrading, or now planning to implement storing identities in the cloud.

Risk

What is Risk?

Risk, in the business context, is measured by the level of likelihood that some process or event will cause an organization to fall short of that goal. As such, risk is directly tied to the business goal of ensuring the confidentiality, integrity and availability of information.

Confidentiality is ensuring the right people have access to the right information, while the wrong people do not. What if external people were able to gain access to privileged information?

Integrity is about ensuring that information is accurate and consistent. What if an unauthorized person were to gain access and tamper with sensitive information? What if an authorized person were to delete or corrupt that information and there was no visibility into who last accessed it?

Availability is about ensuring people's ability to access information. What if the right people were unable to access the information they need? How would that impact their productivity? How would that impact the organization as a whole?

While risk has always been part of the boardroom discussion, today, with the emphasis on information, Access Control and Cloud IAM, it has become a central discussion topic, and for good reason. In a recent IBM Study, it was revealed that the average total cost of a data breach in 2015 has increased to $3.79 million, compared to $3.5 million in 2014.

The good news is that Identity and Access Management has emerged to address this increasing level of risk outfall. Let's look at the most common risk challenges associated with cloud app adoption, and how IAM can help to address them.

PASSWORD LOSS AND THEFT

In recent years, the overwhelming majority of security breaches have involved some form of credential loss or theft, resulting in unauthorized access and information disclosure. Employees, challenged with the growing number of passwords, have started to write passwords down, or use the same weak version across all apps. It's also common for collaborators to use the same account for a given app, further heightening the risk of password loss or theft.

"Average total cost of a data breach increased 23 percent over the past two years to $3.79 million"

–PONEMON INSTITUTE 2015 COST OF DATA BREACH STUDY

In 2011, the hacker group, Lulzsec, released 62,000 random usernames and passwords to the public. The most common passwords released were "12345," "123456789," or some simple variation of "password." And even more complicated passwords may not be as secure as you think. You can visit howsecureismypassword.net to see just how long it would take for your password to be cracked. The results may surprise you.

There are, however, ways to mitigate the risk of password loss and theft. A key feature in modern Cloud IAM solutions is Single Sign-On. SSO delivers secure authentication across all applications including cloud-hosted and on-premises, web and mobile, with one set of credentials (one username and one password). This effectively eliminates passwords and, consequently, the risk of password loss or theft. Furthermore, advanced functionality supports centralized management of shared credentials.

LINGERING ACCESS

When an employee leaves an organization, it's not uncommon for them to take home a computer that retains company access. This threat grows with the increasing use of personally owned devices for work, as does the move of employees within the organization.

"55% of [insider misuse] incidents were privilege abuse- where internal actors abuse the access they have been entrusted with."

–VERIZON DATA BREACH INVESTIGATIONS REPORT 2015

Cloud IAM serves as a control point for people and apps. Under this model, organizations not only have a "kill switch" for departing users but, for those moving within the organization, IT can revoke access in an automated manner.

INSECURE AUTHENTICATION

Cloud apps in use today have varying degrees of authentication maturity. From handling passwords in clear text, to complex hash algorithms, to biometrics, information security is only as strong as the weakest link.

"Time to break an 8-digit password is 3 days…a 12-digit password is ~300 thousand years"

–HOWSECUREISMYPASSWORD.NET

Leading Cloud IAM solutions eliminate this risk in a couple of powerful ways. Firstly, Cloud IAM solutions integrate with applications and use certificate-based authentication. This eliminates the need for users to submit passwords for each individual app. Instead, once authenticated to their IAM system, they are automatically and securely authenticated to all their applications.

Secondly, Cloud IAM solutions that support multi-factor authentication enable organizations to protect apps and information with an added level of security (we discuss multi-factor authentication in greater depth below). So even if an unauthorized person obtained a correct username and password, they will still need to provide a second, separate authentication.

VISIBILITY, AUDITING AND REPORTING

Even authorized users may maliciously tamper, damage, delete or steal information, cloud-based visibility, making auditing and reporting functionality critical to protect organizations.

Since Cloud IAM systems serve as a single point of access to apps and information, organizations gain true visibility into who accessed which applications from where and when. This log data can then be fed into a broader security information and event management system (SIEM) or security operations center (SOC) for more context.

Risk is also introduced by apps that do not have adequate admin capabilities. For example, if a given user is the only person that has access to an account, organizations have no visibility and control over the information that lives in that user's account.

With the ability to "assume" user accounts, Cloud IAM centralizes access to all user accounts so that IT is not in the dark.

Complexity

What is Complexity?

The Word "Complexities" refers to issues that result in lost time, effort, or resources involved in cloud adoption. While Cloud Integration gives organizations greater agility, scalability, and resilience, technology advancements have always increased the complexities for those in the organization chartered to introduce, manage and support them.

MULTIPLE DISPARATE IDENTITY SOURCES (USER STORES)

Traditionally, organizations would use Microsoft Active Directory or some other database using LDAP (Lightweight Directory Access Protocol) as the central place to structure and store all user information.

"Getting to one version of the truth 'doesn't have anything to do with accuracy, it has everything to do with declaring it.'"

-MIT SLOAN SCHOOL

While most cloud-based SaaS products have their own user administration capabilities, it is becoming mission critical to have a single source of truth to manage users universally across their entire app set. Furthermore, in scenarios, such as mergers and acquisitions or deployment of LoB systems like HR apps serving as the system of record (HR-driven Identity Management), organizations will accumulate multiple systems of record. This increases the challenge to maintain centralized control over access to apps and information.

Cloud IAM delivers the unique capability to unify multiple disparate users directories and bridge the gap to cloud applications.

ADMINISTRATION

Every organization today has a user directory- a database that contains all user identities. For now let's just say these are employees, although they might include people external to the organization like partners or customers. This is often the "system of record" or "single source of truth" for the people that work at your organization. For each employee, there is a record of who they are, and a set of "attributes" including their username, password, and contact information etc.. These records, or "digital identities", might also contain any set of custom attributes which are used by other systems that rely on such information.

DECENTRALIZED ADMINISTRATION AND MANUAL USER PROVISIONING/DEPROVISIONING

Before Cloud IAM solutions, the only way to effectively manage user accounts in cloud apps was through the admin console of each respective app. For example, in order for IT to control who gets access to Salesforce.com or to reset a user's password, IT admins would need to log in and manually add or remove users. With 20 employees and three applications, this is fairly manageable.

But what if you have 500 employees and 20 cloud apps, or 10,000 employees and 200 apps? According to Forrester, "Organizations… realize that decentralized ownership of AD and LDAP -- either geographic- or line of business-based -- is no longer sustainable." Going through the manual process of adding, removing and modifying users within each of our apps doesn't scale to large and growing organizations, and so organizations need to centralize control and automate user management across the app set.

This takes us to how Cloud IAM acts as a hub for accessing all our apps. Leading Cloud IAM solutions partner with ISVs (independent software vendors) and SPs (service providers) using open standards, i.e. software protocols designed for user authentication and automating the exchange of user attributes, to centralize the administration and access security efforts.

COMPLEX ENTITLEMENTS

Administration of users deals with defining, creating, updating and deleting information specific to user identities. Based on specific policies, organizations can control the apps that users are allowed to access, and the actions they can take within each app. We might create a policy that entitles anyone in a sales role to access our CRM system and modify sales opportunity records, but anyone in a marketing role to only view sales opportunity records. As you can imagine, these rules can get really complex at large organizations.

"Having a suitable organizational structure in place…is a prerequisite for long-term success."

-INC.COM

To make the process of entitlements management less complicated, mature Cloud IAM services enable organizations to preserve the directory's organizational hierarchy when synchronizing users between systems.

INTEGRATION COSTS

Integrating cloud apps into an existing directory system takes specialized knowledge and significant development effort. Cloud app vendors and internal application developers alike are focused on building the best solution for the business need and less on secure authentication or integrating their apps into other services. While implementing authentication and federation functionality is key to delivering the service to end-users, it can be a major burden.

"The TCO to federate Active Directory to Azure AD in order to secure your cloud apps will cost you between $132k and $940k over 3 years."

–ONELOGIN TCO OVERVIEW OF ADFS VS ONELOGIN

Cloud IAM enables organizations to eliminate these time costs in a couple of ways. Firstly, for third party apps, Cloud IAM delivers a catalogue of pre-integrated apps. This enables IT to simply connect their instance of the vendor solution to their instance of their Cloud IAM solution with a few clicks. In some cases, as with Google Apps or Microsoft Office 365, it can be accomplished with just one click. Secondly, for internally developed apps, leading Cloud IAM vendors deliver developer toolkits which detail the integration for each authentication and federation standard i.e. SAML, WS-Federation, OAuth, NAPPS and others.

Experience

What Defines User Experience?

Cloud adoption is empowering users like never before. Employees can be easily enabled with an unprecedented amount of applications residing in cyberspace, each with very specific functions for just about everything. But cloud infrastructures are not providing the best user experience. Issues like onboarding delays and app access friction still frustrate users, and inhibit them from optimizing their productivity.

ONBOARDING DELAYS

Without a centralized Cloud IAM service, an organization lacks the engine that can automate the entire onboarding process. When a new person joins the organization, she can be left idle for days or even weeks waiting for access to the resources she needs to become productive in her new role. This doesn't have to be the case, especially with cloud applications, as she could be equipped with the tools and information she needs right away to hit the ground running. Making this happen is not only a reflection on the organization, but it sets the precedent for her inclusion in the organization as a productive member.

Cloud IAM makes onboarding simple through role-based app provisioning. When a new user is created, she can be provisioned to her entire app set based on her role. This ensures that new users gain access to all the tools they need right out of the gate.

OUT-OF-SYNC USER BASE

While organizations have a wealth of apps for various business needs, successful collaboration requires that team members are using the same tool for a specific use case. For example, if one team within a given department uses Box for file sync and collaboration while another team uses Google Apps, sharing and collaborating on documents will be a cumbersome experience. Similarly, if one department uses HipChat for messaging while another uses Slack, this will make for inefficient communication.

Cloud IAM provides the benefit of centralized app administration such that there is no confusion as to which apps are company-endorsed and which apps are being used out of compliance. This ensures that people within the organization can work effectively together using the best tool for each use-purpose. If consensus is made to switch over to a new service, IT can then acquire the new app and provision users in a matter of minutes.

ACCESS FRICTION

People are constantly seeking the fastest path to accomplish their tasks and, collectively, we never had a greater wealth of tools, apps and services at our disposal. However, the overhead of managing our own apps and the process of logging into each one has grown into a painful experience in many organizations. Softwareadvice.com reports that "31% of Employees admit to re-using work passwords" as a way to cope with access friction. Periodic password resets and minimum complexity policies, as well as incidental lockouts and multi–factor authentication for each app compound the challenges, and shift the user experience from painful to unusable.

"Typical measures of service response and resolution time for a Moderate/Limited Impact incident with Critical urgency, would have a 2 hour response time target and a 6 hour resolution time target."

–STANFORD UNIVERSITY IT

Cloud IAM on the other hand delivers to users a single sign-on experience that makes the process of authenticating and accessing apps and information effortless for users. Firstly, Web Single Sign-on gives users one central place to access all apps. Upon logging in via their organization's dedicated OneLogin subdomain, the user is authenticated to all of their apps automatically. Users are presented with their entire app set, which they can then simply click through to any given application. Secondly, organizations can leverage Cloud IAM to set up Desktop single sign-on, whereby users are authenticated using their desktop login credentials. In this case, users simply log in to their computer which then in turn authenticates the user against their Active Directory, LDAP or OneLogin directory service.

DEVICE LIMITATION

Since the emergence of smartphones and tablets, there has been a recurring theme in organizations concerning the use of personal devices for accessing work information, namely, Bring Your Own Device (BYOD). The discussion has evolved and taken many forms, but the underlying problem remains the same. People are still demanding access to company apps and information from any device, and the user experience continues to be less than optimal.

While Cloud Integration has made it possible for employees to access their work information anywhere from any device, it has also introduced unprecedented challenges. Smartphones, tablets and home computers have all become fair game when it comes to using them to still perform work outside the office, and the facts

show that this is boosting productivity. By utilizing an Identity Management Solution, organizations can rest assured that their employees are maintaining productivity outside of the office, and are doing so securely.

"42 percent of users are more productive when using their own devices."

–FORBES

"U.S. workers save an average of 81 minutes per week by using their own machines."

–CISCO

By integrating a Cloud IAM Solution, organizations can ensure that their employees are equipped with the right tools from the get-go, and that they can easily access them in the best way for them to be productive. The end user experience that a business provides will influence collaboration, productivity, and the overall culture of the corporation.

Conclusion

Businesses are engaged in an exciting era of technological advancement. As cloud technology continues to evolve, more and more apps are becoming available for businesses to utilize. These new tools have dramatically altered the way corporations create value, and are becoming common across all fields of business.

Yet, with all the advancements the cloud has introduced, tremendous security risks, complex IT structures, and frustrations with user experiences abound. Businesses must find a reliable way to mitigate the challenges, while taking advantage of the agility and power cloud apps offer.

By leveraging an Identity and Access Management solution, businesses can gain a new level of insight and control over their cloud app activity. To learn more about how OneLogin's IAM solution can help your business manage challenges within the cloud, visit OneLogin.com.

ABOUT ONELOGIN

OneLogin is the innovator in enterprise identity management and provides the industry's fastest, easiest and most secure solution for managing internal and external users across all devices and applications.

Considered a "Major Player" in IAM by IDC, and Ranked #1 in Network World Magazine's review of SSO tools, OneLogin's cloud identity managment 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 more than 4,000 applications commonly used by today's enterprises.

onelogin

150 Spear Street, Suite 1400 San Francisco, CA 94105 877 979 0411 onelogin onelogin.com