MODERN IDENTITY

Addressing Risk, Complexity & User Experience

INDEX

PREFACE

Today, we have thousands of cloud apps at our disposal that deliver a better user experience with broader accessibility, substantially lower total cost of ownership with no hardware and maintenance requirements, and more elastic licensing models- all of which are conducive to optimizing a business. In fact, many organizations founded after the year 2005 run purely in the cloud. For those invested in on-premises or hosted applications with perimeter-based security, transitioning towards a pure-cloud or a transitional hybrid operation is inevitable. And while many are embarking on the process, we've been talking about the benefits of cloud app adoption for years and it's still not as fast as it could be.

So where is the inertia, and how is an organization to successfully navigate through a changing application landscape? And for cloud-first companies, how does identity play into it all?

In Modern Identity | Addressing Risk, Complexity and User Experience, we will first contextualize Cloud Identity and Access Management (IAM) by discussing the basic questions of why it's important and what it is. We will then discuss the current cloud app adoption challenges around risk, complexity and the user experience, and how Cloud IAM addresses those challenges.

INTRODUCTION

We're living through a time where people, organizations and societies not only rely but thrive upon secure, simple and fast access to information. From small businesses, startups, enterprises and global conglomerates across all verticals; to local, state and federal governments; to educational institutions and nonprofits, we are continuously investing in our employees, devices, applications, networks and infrastructure that enable us to drive our collective missions forward.

Ten years ago, business and technology leaders catalyzed a cloud app revolution that has changed the way organizations manage IT. However, through this transformative shift, the core requirements of IT remain the same. Technology leaders are responsible for ensuring that 1) information assets remain confidential and protected, 2) information systems are available and operational, and 3) people are empowered and productive with the apps and information they need.

So what is Identity and Access Management?

> IAM is a technology and security discipline that has a history going back just about as far as networked computing. Some of the basic elements of IAM, like passwords or keys, go back thousands of years.

Identity is simply the fact of who a person is. In an organizational context, we need to be able to assert, verify, manage and propagate user identities against the services or resources provided to their employees, partners, or customers. We need to ensure that we know for certain that a person is, in fact, who they're claiming to be, and we need a single source of truth or system of record to manage and maintain identities across all of our apps and resources.

INTRODUCTION

The second piece of the IAM discussion is access. Access is a little more easily defined; it is about organizational resources and enabling the right people to create, view, use, consume, or modify those resources. Just as importantly, it is about ensuring that the wrong people do not have these permissions or privileges.

Organizations invest in resources for specific reasons and, in order for our company to function we need to maintain the security and confidentiality of these resources. For example, we should control access to our CRM app because it's where our customer information, sales details and forecasts live. Making an analogy for physical access, we might also want to control access to our inventory room to control inventory shrinkage, or our CFO's office because guarded financial information may be exposed or vulnerable.

We need to control access, but we also want to make it as easy as possible for people with the right privilege to use their resources and get the most utility out of them, thus contributing to their success as well as the organization's.

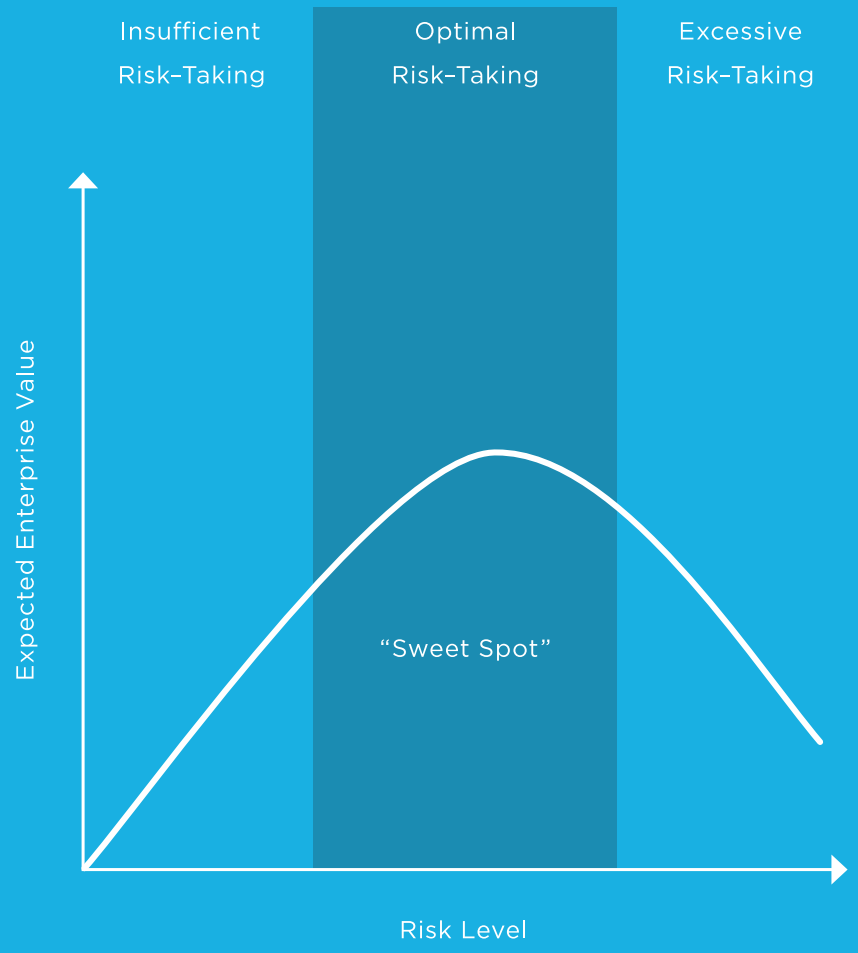
> Formally, identity management is the security discipline where the goal is to securely enable the right people to have convenient access to the right resources at the right times for the right reasons.

As a software system, it's a set of complex functions that simplify the management effort involved in accomplishing that goal. It affects every aspect of the organization, going beyond just IT Administration, Security, Operations and Governance/Audit teams. Identity has a lot to do with HR, managers within each line of business and, of course, end users.

RISK

WHAT IS RISK?

Every organization is ultimately a group of people in pursuit of some vision. Organizational risk, in its broadest sense, is the uncertainty about some future state of the organization. Risk to a finance department might be the uncertainty about an organization's future financial position and goal attainment. Risk to a product engineering department might be the uncertainty about product milestones, quality or delivery. It is a highly contextual element of the organization, so how we define and plan for risk varies depending on the stakeholders and their interests.



THE COMMITTEE OF SPONSORING ORGANIZATIONS (COSO) OF THE TREADWAY COMMISSION

RISK

INFORMATION RISK

The goal of information security is to ensure the confidentiality, integrity and availability of information. Information security risk is the likelihood that some current process or future event will cause an organization to fall short of that goal.

Confidentiality is ensuring the right people have access to the right information, and the wrong people do not. Take a moment to think about the kinds of confidential information your business handles each day. What if people external to your organization were able to gain access to that privileged information? What if someone in a different department had access to your department's information? What if the person beside you had access to your email?

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 was to delete or corrupt that information and there was no log providing 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?

These three core tenets of information security can be examined in great detail from both a technical and organizational perspective. To each one, the "people" and "access" components are arguably the most relevant. Furthermore, while risk has always been a boardroom discussion, today, with such a strong emphasis on information in our organizations, access control and, more generally, cloud IAM, are central to that discussion.

A few tangible risk challenges with cloud app adoption, and how IAM can help to address them.

RISK

Password Theft or Loss

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 are expected to maintain several personal and work accounts over the course of their day. Managing so much login information can be fatiguing or intolerably inconvenient, so employees will often write passwords down on paper, text documents or spreadsheets, or use the same weak password across all their apps. It's also common for multiple people within an organization or team to use the same user account for a given app. This also introduces the risk of password loss or theft since users in the scenario would share the password in an insecure manner. These practices put an organization's data at risk, as they make it easier for unauthorized parties to gain access to sensitive and business-critical information.

> "Average total cost of a data breach increased 23percent over the past two years to $3.79 million"
>
> PONEMON INSTITUTE 2015 COST OF DATA BREACH STUDY

There are, however, ways to mitigate the risk of password theft or loss. A key feature in modern Cloud IAM solutions is Single Sign-On (SSO). SSO delivers secure authentication across all applications including SaaS and internally developed apps, cloud-hosted and on-premises, web and mobile, with one set of credentials (one username and one password). This effectively eliminates passwords through the implementation of digital certificates, and consequently, marginalizes the risk of password theft or loss entirely to the portfolio of cloud services in use. A more advanced capability provides centralized management of shared credentials enabling multiple users to access the same account for a given app.

RISK

Lingering Access

When an employee leaves an organization they may be putting company data at risk whether they know it or not. It's not uncommon for departing employees to take home a mobile device or computer that retains access to company apps and information. This threat becomes even more important considering the increasing use of personally owned devices. If access is not revoked across all of their applications, what is to stop them from simply logging in from a personal device?

Additionally, when employees move laterally or vertically within the organization, they need to forgo access to information associated with their previous role.

> "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 laterally within the organization, IT can easily, and in an automated manner, revoke access to the apps to which an employee is no longer authorized. The recurring process of recertifying access is intended to ensure organizations take action to manage risk associated with lingering access.

RISK

Insecure Authentication

The various cloud apps in use today have varying degrees of maturity in their respective authentication processes. From handling passwords in clear text, to complex hash algorithms, to biometrics that read the user fingerprint or facial topography, information security is only as strong as the weakest link. Should security controls be breached, organizations are subject to information disclosure, potentially suffering a serious loss of credibility, which further adds to the total cost of a breach.

> "Time to break an 8-digit password is 3 days...a 12-digit password is ~300 thousand years"
>
> HOWSECUREISMYPASSWORD.NET

Leading Cloud IAM solutions practically 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 enter and submit passwords for access to all their apps. Instead, once authenticated to their identity management system (i.e. Identity Provider or IdP), they are automatically and securely authenticated to their applications "behind the scenes".

Secondly, Cloud IAM solutions that support multi-factor authentication enable organizations to protect apps and information with an added level of security. This ensures that even if an unauthorized person somehow obtained a correct username and password, they would still need to provide a one-time password, for example, that demonstrates possession of an additional security factor often served from their mobile device.

RISK

Visibility, Auditing & Reporting

We mentioned data integrity as a key aspect of any information security program. When it comes to cloud applications, even authorized users could maliciously tamper, damage, delete or steal information within company apps.

Since Cloud IAM systems serve as a single point of access to apps and information, your organization has true visibility into who accessed which applications, when, and how. This log data can then be fed into a broader security information and event management system (SIEM) or security operations center (SOC) to infer more context around that activity.

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.

OPERATIONS RISK

Operations risk is the uncertainty that potential business shortcomings, such as inadequate or failed procedures, systems or policies, might translate to degraded productivity, lost or foregone revenue, and opportunity costs. For example, poor data integrity precipitated by employee errors (e.g. the result of labor intensive tasks such as data entry), systems failures, fraud or other malicious activity may have an impact on critical business decisions.

How much loss an organization is prepared to accept, combined with the cost of correcting those errors, determines the organization's risk appetite.

Downtime

We've become more reliant on our own IT to deliver services and enable our businesses. For organizations invested in on-premises or hosted apps where IT has held the responsibility of managing and maintaining their own directory and authentication services, they also bear the risk of downtime and managing to service

RISK

levels. Authentication systems are inherently complex, and their deployments meticulous to maintain and potentially error-prone. Since authentication serves as a crux to access business apps and information, the eventuality of a service degradation or outage will result in lost productivity leading to some negative business impact.

Offloading the tasks of architecting and managing diverse systems and configurations to your Cloud infrastructure and identity management servicers ensures integrity and resiliency with limited risk to availability and performance as the burden of responsibility is transferred to a dedicated expert provider. This also reduces the risk of human error since Cloud IAM solutions simplify the administration and management effort by design due to the multi tenant nature.

Project Failure

As IT leaders we're asked to respond to new business challenges by innovating, yet our adoption of new technologies challenges our budgets and skills. Opportunity costs often outweigh these challenges however, and we're faced with evaluating options. Historically, the deployment timeline of new enterprise applications has been in the order of months or years. The risk of deploying or extending identity solutions arises with possibility of projects stalling or failing completely due to shortcomings in the rollout. The business impact would be, in many cases, lost opportunity and lost revenue potential.

Today, organizations can "light up" a cloud application at the "flip of a switch." And as organizations leverage more point-solutions on a project basis, service providers are delivering greater agility through automation in the deployment and user provisioning process. Leading Cloud IAM solutions that embrace open authentication and authorization standards can

deliver pre-integrated catalogs of applications that support authentication and provisioning in minutes.

And from this mindset, they often offer development resources needed to substantially expedite and ensure successful configuration for internally developed apps. This ultimately results in faster concept-to-production turnarounds and unprecedented levels of operational excellence.

SUMMARY

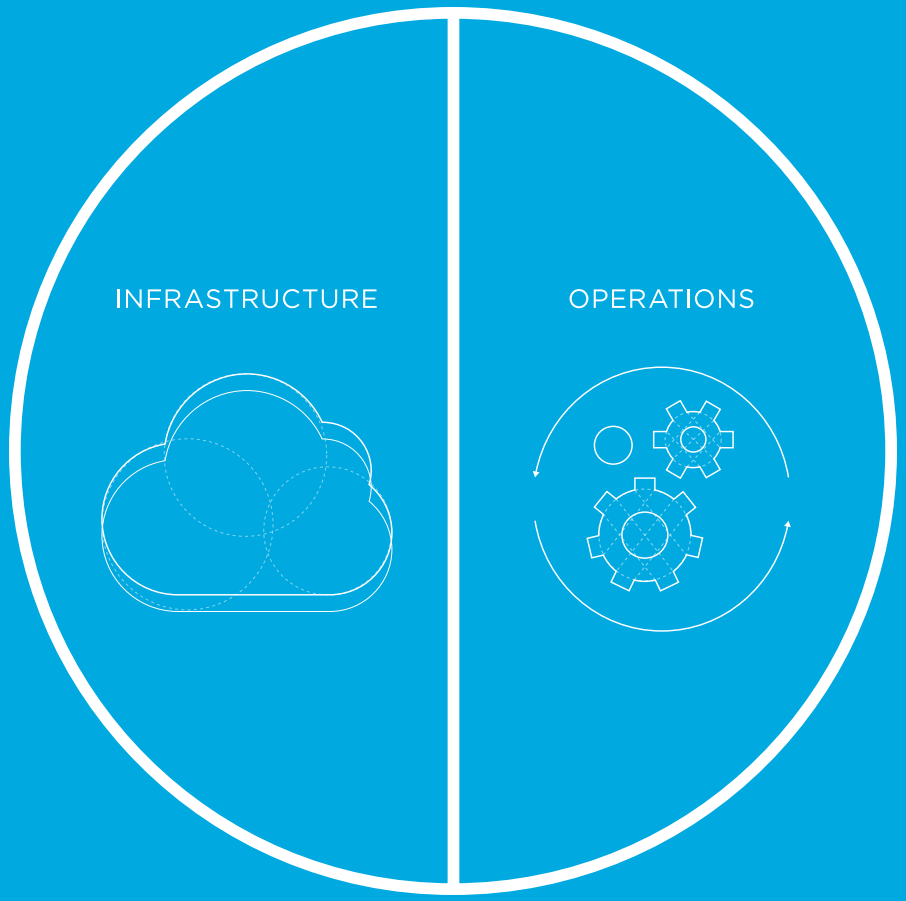
As organizations embark on new cloud initiatives, the risks they face come in various forms, with varying implications. In order to maintain information assurance and operational excellence, organizations need to consider the risks and how they can be minimized or eliminated with a fully integrated Cloud IAM solution.

COMPLEXITY

What is Complexity?

Identity is the fundamental enabler of digital business. And as we face greater demands to accelerate the pace of IT service delivery including the adoption of software as a service (SaaS), bimodal IAM capabilities strike a balance between innovation and core, i.e. cloud and legacy on-premises, as we renovate our underlying architectures and systems. Cloud integration promises organizations greater business agility, operational scalability, and service resilience.

The word “complexity” refers to issues that result in lost time, effort, or resources, much of which can be associated with transitioning to bimodal IT and honoring legacy IAM while embracing and enabling the future. For example, every organization today has a user directory- a database that contains all user identities. 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, first name, last name, email



COMPLEXITY

address, phone number, department, role, job title and office location. These records, or “digital identities”, might also contain any set of custom attributes that the business sees as relevant to the user identity. More specifically, these custom attributes are used by other systems that rely on such information. Now transition to cloud where every SaaS application retains its own user store and entitlement structure, thus IT should be prepared to cope with a number of complexities that come with utilizing the cloud.

These challenges can be divided into two categories: **Infrastructure and Operational**. Infrastructure Complexity refers to challenges that arise from the cloud framework itself, while Operational Complexity involves challenges that arise from IT operations within the cloud. Issues in both of these categories can have a significant impact on business, and should be addressed in the most efficient way possible.

Infrastructure Complexity

Multiple Disparate Identity Sources

To provide some additional context, organizations often use Microsoft Active Directory or some other database using LDAP (Lightweight Directory Access Protocol) as the central place to store all user information. This database serves as the source of truth to control access to computers, networks, apps and other information resources. For example, when we create a new user in Microsoft Active Directory, the user would then be able to log into their computer and access the information on the corporate network based on the rules associated with that role.

Today, organizations are adopting new cloud apps, each with their own user store: CRM apps like Salesforce.com or SugarCRM, Marketing tools like Marketo and Hubspot, file synchronization and collaboration tools like Box, Dropbox or Egnyte, email and business productivity suites like Microsoft Office 365 and Google Apps for Work, recruitment apps like

COMPLEXITY

Greenhouse, messaging apps like HipChat or Slack, and the thousands of other business applications that contain business-critical and sensitive 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

Also, in scenarios such as mergers and acquisitions or deployment of specific line of business (LoB) systems like HR apps serving as the system of record (i.e. HR-driven Identity Management), organizations will accumulate multiple systems of record. This makes it challenging to maintain centralized control over access to apps and information.

While most cloud-based SaaS products have their own user administration capabilities, organizations need a single source of truth to manage users universally across their entire app set. Cloud IAM delivers the unique capability to unify multiple disparate users directories and bridge the gap to cloud applications.

OPERATIONAL COMPLEXITY

Decentralized Administration

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, or whomever is responsible for managing access to Salesforce, would need to log in as an admin user and manually add or remove users accordingly. With 20 employees and three applications, this way of doing things has been fairly manageable. Your HR person

COMPLEXITY

would notify IT when an employee joins, leaves or changes their role within the company, and then IT would make those changes as necessary.

But what if you have 500 employees and 20 cloud apps, or 10,000 employees and 200 apps? The process of managing user access quickly becomes unmanageable. 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.

> "Organizations... realize that decentralized ownership of AD and LDAP -- either geographic- or line of business-based -- is no longer sustainable."
>
> FORRESTER RESEARCH

This takes us to how Cloud IAM acts as a hub for both. Firstly, automating administrative tasks such as onboarding and off boarding employees across all your cloud apps, (i.e. provisioning and de-provisioning activities). Secondly, enabling single sign on to simplify user access to all their apps. Leading Cloud IAM solutions partner with ISVs (independent software vendors) and SPs (service providers) to implement open standards, i.e. software protocols designed for user authentication and automating the exchange of user attributes, to effectively communicate cross domains and centralize the administration and access security efforts.

Complex Organization Structure & Entitlements

Administering user accounts deals with defining, creating, updating, and deleting information specific to their identities. Based on policies set around the information within users' digital identities, including their role and place in the organization, IT can control the apps that users are allowed or not allowed to

COMPLEXITY

access and the actions they can or cannot take against information 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 depending on the scope of their hierarchal structure.

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

We need to automate these kinds of controls and processes, and make them simple enough for anyone to manage. 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 and act as the single source of truth to all served cloud applications

Integration Costs

Integrating cloud apps into an existing directory system takes specialized knowledge and significant development effort. Hence IAM projects are often managed separately. So while cloud app vendors and internal application developers alike are focused on building the best solutions for the business, less investment is made to facilitate secure authentication or integrating these apps into other services. Authentication and federation functionality is key to delivering services to end-users, and 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

COMPLEXITY

Cloud IAM enables organizations to eliminate these integration and 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 provide developer toolkits that detail the integration for each authentication and federation standard i.e. SAML, WS-Federation, OAuth, NAPPS and others.

SUMMARY

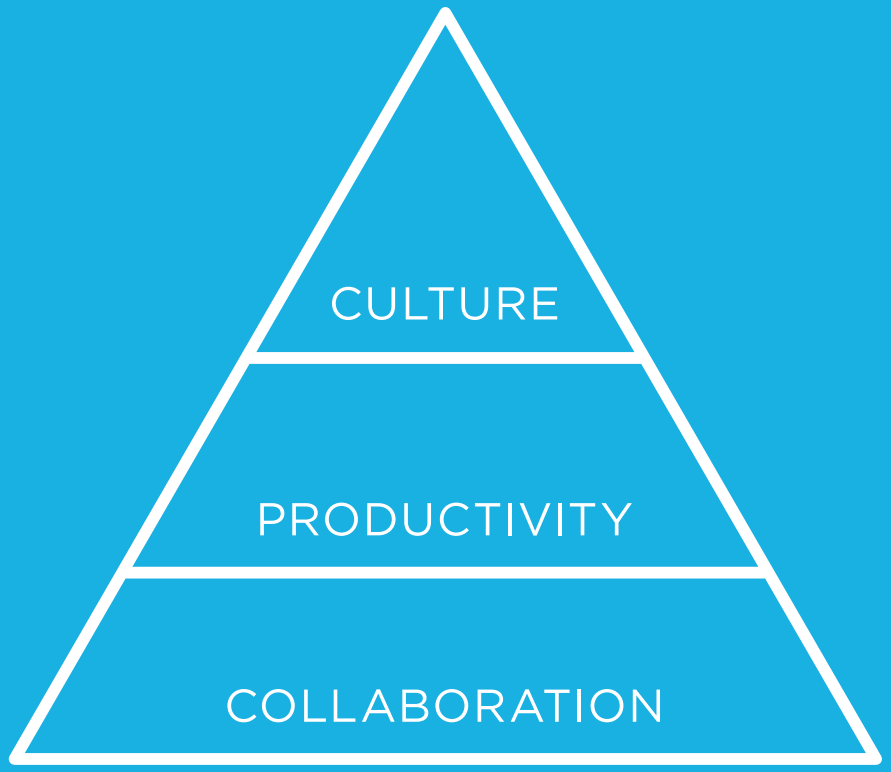
With any great shift in technology, new challenges are inevitable. And cloud integration is no exception. Cloud adoption is enabling businesses like never before, but complexities like multiple, potentially conflicting sources of truth, manual provisioning and entitlement complications are all common issues that IT needs to address. By leveraging a Cloud IAM solution, IT can eliminate these issues with new levels of efficiency and convenience. Through embracing simplification, businesses can reap the rewards of cloud adoption without getting bogged down by IT set-backs.

USER EXPERIENCE

WHAT DEFINES USER EXPERIENCE?

Cloud adoption is empowering users like never before. Employees have an unprecedented number of specialized applications at their fingertips, each with very specific functions for just about everything. But cloud infrastructures are still not providing the best user experience that they could be. Issues like onboarding delays and app access friction still frustrate users, and inhibit them from optimizing their productivity. And often perceptions about lack of contribution impact their professional sense of achievement and hence their overall job satisfaction. And in today's tight labor market, we want to retain good employees. This practices starts the day they begin seeking employment with us.

The cloud user experience can be divided into three primary categories: Collaboration, Productivity, and Corporate Culture. Each of these segments has its own challenges that users must face when an IAM solution is not in place.



USER EXPERIENCE

COLLABORATION

Onboarding Delays

Without a centralized Cloud IAM service, an organization lacks the engine that automates the entire onboarding process. When a new person joins the organization, she can be left idle for weeks waiting for access to the resources she needs to engage with her co-workers and become productive in her new role. On the other hand, she can be equipped with the tools and information she needs right away to hit the ground running. This is not only a reflection on the organization, but it sets the precedent for her inclusion in the organization.

Cloud IAM makes onboarding simple through role-based app provisioning. When a new user is created, she is automatically 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 tools for the same business purpose. 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.

USER EXPERIENCE

PRODUCTIVITY

Access Friction

People are constantly seeking the fastest path to accomplish their tasks and, collectively, we have never had such a great wealth of tools, apps and services at our disposal. However, the overhead of managing our own apps, the pain of logging into each one separately, and delays in closing simple service requests, has grown into an intolerable experience. Password fatigue is a common term to describe the end user experience. Compounding the situation are periodic password resets, complex password policies, incidental lockouts and multi-factor authentication for each app, accessing apps goes from intolerable to unusable.

Cloud IAM delivers to users a single sign-on (SSO) experience that makes the process of authenticating and accessing apps and information effortless for users. Firstly, Web SSO 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.

> "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

The user is 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 SSO 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.

USER EXPERIENCE

Device Limitation

Since the emergence of smartphones and tablets, there has been a recurring theme in organizations concerning the use of personal devices serving as a secondary factor of authentication as well as accessing work information outside the office from these devices, particularly in Bring Your Own Device (BYOD) scenarios. The discussion has evolved and taken many forms but the problem remains - people are still demanding access to company apps and information from any device, from anywhere outside the firewall, with the same user experience and security as if they were in the office.

> "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

Cloud integration has made it possible for employees to access their work information anywhere from any device. Smartphones, tablets and home computers are all fair game when it comes to working outside the office, and the facts show that this is boosting productivity. By utilizing Cloud IAM, organizations can rest assured that their employees can remain productive outside of the office, with the same level of SSO simplicity, and can do so securely.

USER EXPERIENCE

CORPORATE CULTURE

Brand Nurture

Matters of corporate culture can spawn extensive discussion about brand, values and collective identity. How an organization develops and perpetuates its culture is often an exercise in nurture. Among the ways organizations build internal culture is largely about consistency across all aspects of the employee and customer experience, and part of this can be achieved through brand reinforcement.

Cloud IAM services, like many cloud applications, enable organizations to customize the login screen and color scheme to represent that of their brand. Whenever users go to access their apps, they experience a degree of familiarity with their organization's brand identity.

> "The 'culture' of a company consists of the values and practices shared by those that work there."
>
> STAFFING SOLUTIONS

SUMMARY

Employees may have every app in the world at their disposal, but it doesn't matter unless they are able to utilize them easily and efficiently. The end user experience that a business provides will influence collaboration, productivity, and the overall culture of the corporation. 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 contribute to the business.

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 now common across all fields of business. What's more, it's highly likely that the cloud is only going to alter business practices to a greater extent in the coming years.

All of that said, the cloud landscape is still developing, and moving to create a seamless experience for businesses. Organizations, regardless of size, still face risks, complex IT structures, and frustrations with user experiences while utilizing cloud apps. If these businesses don't want to be left behind, they must find some way to mitigate these challenges, while still taking advantage of the agility and power that cloud apps have to offer.

By leveraging a Cloud Identity and Access Management solution, businesses can gain a new level of control and insight over their cloud app activity. This type of approach minimizes the primary risks involved in utilizing cloud apps, like password theft of loss and lingering user access. What's more, Cloud IAM can also simplify IT complexities like conflicting identity sources and complex entitlements. And finally, Cloud IAM solutions provide users with a simple, easily integrated experience that enables them to bring efficiency and productivity to an all-time high.

To learn more about how OneLogin's Cloud IAM solution can help your business manage challenges within the cloud, visit OneLogin.com.