onelogin

WHITEPAPER

3 Easy Steps to Implement Cloud-Based Identity and Access Management (IAM)

Like many others, your organization is moving applications and resources to the cloud as part of a broader digital transformation. But it's not enough to move to the cloud; you need to secure the cloud as well.

But how do you do this when your company subscribes to dozens of cloud applications like Office 365, G Suite, Salesforce, and Box? How do you ensure that access to these apps is optimized for user productivity, and also falls in line with your organization's security and compliance requirements?

This may all sound overwhelming, but you can address these concerns in 3 simple steps:

Step 1: Assess your current IAM situation

- **Take inventory of your current cloud versus on-premises adoption and deployment.**
- **Review what apps are currently in use, and what kind of sensitive data reside within them.**
- **Assess your current security posture with respect to application access and access control.**
- **Take inventory of your end-user needs & preferences.**

Your first step is to review the gaps within your current IAM (Identity and Access Management) environment and use that information to define your future requirements. Take inventory of your current policies and infrastructure so you can better understand the costs and benefits of a new IAM solution.

Ask Yourself The Following Questions:

What applications are your users utilizing today? Which users and groups need to authenticate with which resources? How many of them are external to your organization (think partners and vendors)? What is your current process for managing employee entitlements and provisioning new user access?

What is the relationship between your cloud resources and your on-premises network? Do you use an on-premises directory? What on-premises applications are in use? How are users accessing them?

Are users accessing applications securely? Are they securely accessing company data from remote locations or devices?

Content

What “Shadow IT” apps have been implemented outside of IT’s control? Who is using them?

What is your current process for off-boarding former users? How confident do you feel that you are offboarding all users from all apps?

What are the current support and administrative costs related to managing user identities and access? Are those costs growing?

Step 2: Evaluate what IAM approach is right for you

- **Think about your identity and access management needs.**
- **Review the infrastructure, maintenance, and personnel costs associated with each vendor.**
- **Consider security, productivity, compliance concerns.**
- **Think about future cloud versus on-premises deployments.**
- **Consider out-of-the-box ready versus custom deployment options.**
- **Review vendor practices around security, compliance, redundancy, and accountability.**
- **Consider open standards versus proprietary interfaces, e.g. SAML, OpenID Connect, SCIM.**

The idea of outsourcing this foundational element of your application strategy can cause some understandable anxiety, which makes it all the more important that you and your vendor have a trusting relationship. You can separate this trust into a few areas: security, compliance, accountability, and redundancy.

Once you’ve answered the questions from step one, you’ll have most of what you need to start researching solutions. Here are some key factors to consider while you evaluate vendors:

Directory Integration

Perhaps your enterprise relies on Active Directory and LDAP directory running on-premises. You may even have an on-premises legacy IAM solution. Administration of your users’ access to cloud applications through these is possible, but probably very difficult.

So your cloud IAM solution needs to have a strong integration with on-prem Active Directory and LDAP. It needs to operate smoothly with AD and LDAP, providing real-time, bi-directional synchronization of users, their attributes, and their groups from your on-prem directories to your cloud IAM directory. And it needs to smoothly merge multiple directories into a single, unified cloud directory.

Vendor Practices

Identity management is a critical part of your IT infrastructure, and plays an even more important role as these services move to the cloud.

The idea of outsourcing this foundational element of your application strategy can cause some understandable anxiety, which makes it all the more important that you and your vendor have a trusting relationship.

You can separate this trust into a few areas: security, compliance, accountability, and redundancy. Here’s how to evaluate each.

To evaluate your IAM vendor's **security** practices, consider this list of questions:

1. Can the vendor provide protected access across your entire app deployment, including both on-premises applications and cloud applications?
2. Does the vendor offer single sign-on to reduce the likelihood of users writing down or reusing passwords?
3. Does the vendor offer the option to set custom password requirements based on length, character types, and reset frequency?
4. What multi-factor authentication (MFA) options are supported by the platform?
5. Can the vendor detect suspicious login activity based on factors like unusual devices, locations, browsers, or timing?
6. Can the vendor remotely revoke access from stolen company laptops?
7. How confident is the vendor that they can maintain the correct level of access privileges for all apps throughout the entire employee lifecycle?
8. How confident is the vendor that they can completely revoke app access from former employees?
9. Can the vendor protect access across the corporate network, for example, by protecting access to Wifi?

Can the vendor provide protected access across your entire app deployment, including both on-premises applications and cloud applications?

To asses **compliance** here is a checklist of items to look for in a cloud IAM vendor:

1. Has the vendor been audited by third parties as part of a SOC 1, SOC 2, or other compliance frameworks?
2. Do they adhere to globally recognized standards such as ISO 27001, 27017, and 27018?
3. Does the vendor take steps to safeguard personal information by participating in Privacy Shield, complying with GDPR or other privacy standards?
4. Does the vendor have a vulnerability management program that includes penetration tests, network scans, and/or bug bounty programs?

Accountability is a key part of establishing trust. To that end, ask your vendor the following:

1. Does the vendor contractually commit to an SLA for both overall service availability, and for support responsiveness? Are these SLAs acceptable to you given your business needs? Remember: an SLA

of 99.9% uptime might sound great, but lets a vendor get away with over eight of hours of downtime a year. What happens if those eight hours happen to fall on your busiest day of the year?

2. Does the vendor display their overall uptime and provide historical tracking of not just full-service outages, but also performance degradation, feature disruptions, and planned downtime? This demonstrates that they are committed to transparency in their SLA reporting.
3. Does the vendor report on the root cause analysis of their outages? This shows that their operations team has a culture of accountability and continuous improvement.

Redundancy is key for a cloud identity vendor. If your cloud IAM vendor is down, you can't access their single sign-on portal, and thus you're shut out of your applications. Ask the following to evaluate your vendors' levels of redundancy:

1. Does the vendor run their service in multiple, geographically separate regions? Running in multiple geographies means that if there's a service disruption in one area, the service should continue running smoothly in other geographic regions.
2. Does the vendor use multiple DNS providers? This is crucial, since distributed denial of service attacks (DDoS) on DNS providers are the Achilles' heel of Internet infrastructure and have brought down large portions of the web.
3. Does the vendor support redundant instances of connectors to on-prem directories? This ensures that your cloud directory is always syncing with your on-prem directories.

Open Standards

Do your cloud application providers support standards like SAML, OpenID Connect, SCIM, and OAuth? Are these standards supported by your IAM provider's connectors? Does your IAM provider support TOTP?

You should expect both your IAM and cloud application providers to support these open standards. They provide you with greater vendor choice when moving to cloud IAM, and greater flexibility to move to a different IAM vendor if you're not happy with your initial decision. A quick overview of each of these standards and why they matter to an IAM buyer:

1. SAML and OpenID Connect are application sign-in standards that can be used to securely log into an application from a single sign-on portal.
2. SCIM is an application user provisioning standard. It provides an easy way for IAM providers to create new user accounts in an application based on identities in your directory.

You should expect both your IAM and cloud application providers to support these open standards. They provide you with greater vendor choice when moving to cloud IAM, and greater flexibility to move to a different IAM vendor if you're not happy with your initial decision.

3. OAuth is an open standard API for access delegation, meaning it is often used to grant users temporary access to company data or resources. Identity solutions provide OAuth integrations that can be used for anything from managing logins to automation.
4. OTP is a standard for multi-factor authentication (MFA) that lets you use a range of MFA applications as an additional authentication factor to access a single sign-on portal.

While custom connectors may be required to connect “must have” apps to your cloud IAM, these should ideally be the exception to the rule.

Cost Factors

Subscription-based pricing associated with SaaS models like Cloud IAM differ from traditional perpetual licensing and maintenance models. Many organizations view subscription models as an advantage because they move the cost from capital to the operations budgets, and include the ongoing maintenance of the system.

A robust IAM solution should significantly reduce IT costs. For example, IAM solutions equipped with single sign-on reduce the frequency with which users submit password reset tickets, which means that IT can spend more time on more strategic projects. According to Forrester, one OneLogin customer saved roughly $112,500 by eliminating roughly 4,500 password resets each year.

Your IAM solution should also make user provisioning and deprovisioning much more efficient. Instead of manually provisioning and deprovisioning individual users, make sure that your IAM vendor offers ways to automate these processes, further saving time for your IT team.

Your IAM provider should also be willing to provide an ROI calculator, explaining how their solution can provide measurable, quantified value to your organization.

Step 3: Define a strategy for implementing your IAM plan

- **Engage the right stakeholders early.**
  - **Representatives from your line of business**
  - **Security, network, and compliance teams**
  - **Human resource teams**
- **Drive toward achievable milestones supporting early successes.**
- **Expand the reach and scope of your solution.**

Figure 1: Examples of achievable step-by-step milestones

Rollout Step	Example
Integrate to Existing Directory	Active Directory
Establish App Catalog	Connectors to 1000’s of Cloud Apps
Rollout Key Productivity Apps	Office 365 G Suite
Implement SSO & MFA	Desktop SSO and Adaptive Authentication
Implement User Provisioning	Onboard Offboard SCIM
Integrate Laptops	OneLogin Desktop
Implement CASB	CloudLock or SkyHigh
Implement SIEM	Sumo Logic or Splunk
Expand App Rollout	Salesforce Social Apps Travel Expenses
Analyze and Provide Feedback	User Experience Platform Access Usage

All IT projects are better off for having cooperation and buy-in from other parts of the company. This is especially true for IAM, as it affects nearly everyone. Approach it step-by-step, carefully ensuring that things are working correctly, and others will see the value to them.

Consider these strategies for charting the path of your rollout:

Directory Integration

You must plan on the prerequisite exercise of mapping your legacy directory groups and attributes into your new cloud directory and defining new roles and application entitlements. Engage your stakeholders in resolving what data is important. For example, do you plan to include employee's mobile number field to take advantage of any SMS forgotten password features?

SSO (Single Sign-On)

A profound benefit of a good IAM implementation to both users and IT is enterprise single sign-on. Implement this feature to reduce the amount of time needed for users to sign into their apps, as well as to reduce the amount of time that IT wastes resolving password reset tickets for forgotten passwords.

MFA (Multi-Factor Authentication)

As SSO gains acceptance and the federation of cloud apps begins, the need to better secure the authentication process emerges. IAM greatly eases the work involved in implementing multi-factor authentication, yet it increases demands on the end user to implement additional authentication factors.

You may need to implement some of this at the same time you implement enterprise SSO, but a good second step would be to expand the use of multi-factor authentication after the SSO capabilities are rolled out successfully. You want to choose an MFA solution that provides you with a number of reliable MFA options, such that you can choose the right combination of MFA options that fits your needs.

As SSO gains acceptance and the federation of cloud apps begins, the need to better secure the authentication process emerges. IAM greatly eases the work involved in implementing multi-factor authentication, yet it increases demands on the end user to implement additional authentication factors.

Provisioning

As employee roles shift and change within the organization, it's helpful to automate the processes of adjusting user app access and permissions. Automated provisioning means faster onboarding and faster time to productivity. And faster offboarding means mitigated security risks for departed employees.

In addition, consider the value of HR-driven identity for your organization. If you use Workday, UltiPro or Namely as a Human Capital Management (HCM) solution, consider an integration that imports identities from the HCM application into your Cloud Directory. You can import any user attribute to power your security and access policies based on HR metadata, such as department or job function.

Risk-based authentication

Consider implementing a risk-based authentication strategy. That is, implement a system wherein login factors like geography, device, network reputation, and time of day are all automatically evaluated, and an appropriate MFA response is generated if the login attempt seems suspicious.

Consider implementing a risk-based authentication strategy. That is, implement a system wherein login factors like geography, device, network reputation, and time of day are all automatically evaluated, and an appropriate MFA response is generated if the login attempt seems suspicious.

CASB solutions such as CloudLock or SkyHigh also protect against account compromises through cross-platform User and Entity Behavior Analytics. That is, they use advanced machine learning to flag unusual app use, and improve security.

If, for example, a user logs into an app in San Francisco, and 30 minutes later tries to log into the app in Boston, the CASB solution will flag the second attempt, and prompt your IAM solution to apply more authentication factors.

SIEM (Security Information and Event Management) Integration

A SIEM integration is also highly recommended. When a security breach happens, an infosec team often uses their SIEM to scour terabytes of data, and determine the cause and extent of the breach. SIEM's pull in log data from a broad range of security software and cloud resources, and make them instantly searchable; think "Google for machine data."

To enable your security team to connect the dots, it is essential for IAM data to be part of this data set. For these reasons, consider when to integrate your IAM vendor with your SIEM, such as Splunk, Elastic, or Sumo Logic.

On-Premise Applications and Network Appliances

Don't neglect your on-premises resources when implementing IAM. Ensure that your implementation offers unified user access control so that your IT can efficiently grant employees access to both cloud and on-premises web apps. Your users should be able to **access both SaaS and custom web apps** on any device from a single consolidated portal.

One Step at a Time

You may also want to consider taking the above steps with just one part of the organization initially—perhaps a single Active Directory Organizational Unit—before moving on. You can pay extra attention to that test project and move other groups over when you have the system running smoothly.

Closing Thoughts

Extending your IAM practices to support the growing cloud application environment within your organization does not need to be a large rip-and-replace exercise. The adage, evolution over revolution, can be applied. We hope this simple framework will serve you in advancing your cloud identity services in a thoughtful manner.

Please contact us with questions around any of these steps.

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, or connect with us on our blog, Facebook, Twitter, or LinkedIn.