Centrify
THE BREACH STOPS HERE™

WHITE PAPER

TOP SIX THINGS TO CONSIDER WITH AN IDENTITY-AS-A-SERVICE (IDAAS) SOLUTION

Contents

Executive Summary

The number and variety of apps that are being adopted by organizations—from on-premises apps, cloud-based apps, to mobile apps — is rapidly increasing. While IT continues to deliver new and varying apps, lines of business and even individuals are now also adopting apps independently of IT at an astonishing rate. As a result, employees typically need to authenticate with a dizzying array of systems, from a variety of PC and mobile devices, with each app representing another silo of identity for IT to manage. Identity-as-a-Service (IDaaS) is an emerging solution category for managing and simplifying access to apps, but there are a number of feature, architecture and maturity considerations when selecting an IDaaS. This paper will discuss six of the top considerations.

Introduction

Business enterprises and government organizations clearly have a painful problem: today's users are required to remember and self-manage too many passwords. The need to access apps on-premises or in the cloud, while on the go from mobile devices (where it's more difficult to enter passwords), makes the problem even worse for remote and mobile workers. In fact, employees in a study conducted by NIST (The National Institute of Standards and Technology) recorded an average of 23 authentication events per day to a variety of systems and apps. The NIST study and many others have found that the resulting frustration — dubbed "password fatigue" — causes users to circumvent sound security practices. Workers often cope by using:

- Their email address as the login across multiple sites
- The same password across as many apps as possible (61% do this)
- Simple passwords (including use of simple mnemonic devices)
- Spreadsheets (or even writing down their passwords on sticky notes)

Allowing your users to self-manage their own passwords opens the door to poor habits and burdens IT in numerous ways. The number and frequency of helpdesk calls to reset forgotten passwords burdens expensive IT resources and prevents them from investing in more important objectives. Users may also attempt to simplify their daily workflow by creating simple, easy-to-remember (and also easy to hack) passwords thus exposing the organization to a reduced security posture and increasing the risk of exploitation. Finally, when employees leave the company, there is greatly reduced likelihood of consistently de-provisioning their access to apps such as Office 365, Salesforce, WebEx, HR systems, and other apps.

To effectively address these problems, enterprises have attempted to synchronize passwords by extending or implementing Identity and Access Management (IAM) solutions. However, many of these IAM approaches have been designed and implemented without the appropriate considerations for cloud apps or mobile use cases. The result has been a range of IAM solutions that can prove awkward or frustrating to integrate with cloud apps and fail to effectively integrate mobile access. What is needed is a simple, turnkey IDaaS solution that supports all of an organization's apps, unifies access policies across apps and devices, and is integrated across all of device platforms (laptops, smartphones, tablets).

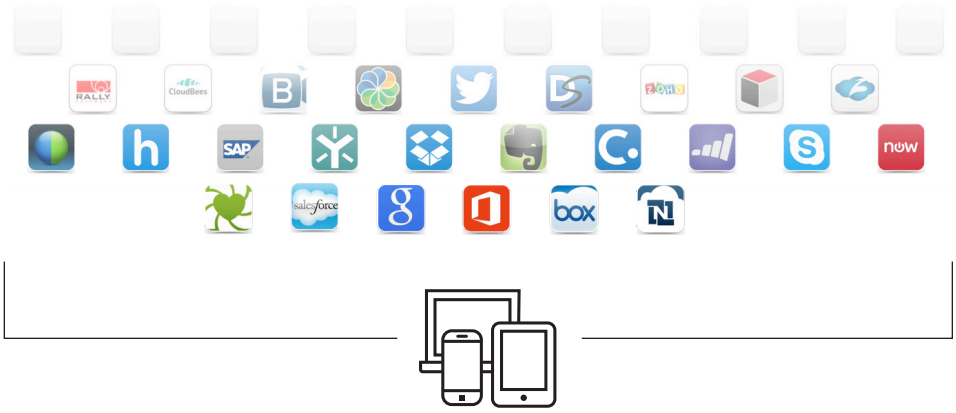
With this background in mind, here are the top 6 things to consider when selecting an Identity and Access Management as a Service (IDaaS):

1. Single Sign-On Everywhere

Single Sign-On (SSO) is the ability to log into an app (cloud-based, on premises, or mobile app) every time using a single/federated identity. For consumers this identity can be their social media identity, such as Facebook or Google, while an enterprise identity is typically the user's Active Directory ID. Without SSO, users need to remember complex passwords for each app. Or worse, they use common or easily remembered (i.e. weak) passwords. For users, the result is a frustratingly fragmented workflow, which can include signing into dozens of different apps during the workday. For IT, the problems of too many passwords, or insecure passwords, are obvious—with a costly data breach ranking at the top among concerns. A properly architected SSO increases both user productivity and corporate app security.

So what should you look for when deploying SSO? At the simplest, a solution should enable you to improve end-user satisfaction and streamline workflows by providing a single identity to access all business apps — whether the apps reside in the cloud, or on-premises behind your firewall. It also needs to unify and deliver access to apps from all end-user platforms—desktops, laptops and mobile devices.

In a properly architected system, once users authenticate by logging in with their enterprise ID (e.g., Active Directory) they should enjoy one-click access to cloud, on-premises or mobile apps. Enabling "Zero Sign-On" for mobile and web apps is also important, especially for rich mobile apps as silent authentication saves time. Once a user is initially authenticated, he/she never has to type in the ID again when an app is launched. Remote access to on-premises apps should be just as simple as accessing cloud apps: without requiring VPN hardware or client software. This type of SSO — using standards like SAML — will not only reduce user frustration and improve productivity but also enhance security. Federated SSO is better because it does not transmit the user name and password to the app over the network, but instead sends a time-limited and secured token verifying that the user who is attempting access is known and trusted. In addition, by eliminating the use of passwords and their transmission across networks, you can reduce the likelihood of users locking their accounts and calling the helpdesk, eliminate password risks such as non-compliant and user-managed passwords, and make it possible to instantly revoke or change a user's access to apps without an admin having to reach out to each and every app.



Centrify delivers single sign-on (SSO) to all your apps whether on-premises, in the cloud, or from your mobile device.

2. Secure Access for All Identities

Today cyber criminals are breaching systems with direct access via a compromised credential — the password. According to Verizon's latest 2017 Data Breach Incident Report (DBIR), over 80% of attacks were due to compromised credentials. The perimeter-based approach that we have historically relied on which focuses on protecting endpoints, firewalls and networks completely ignores the vulnerability of identities and passwords.

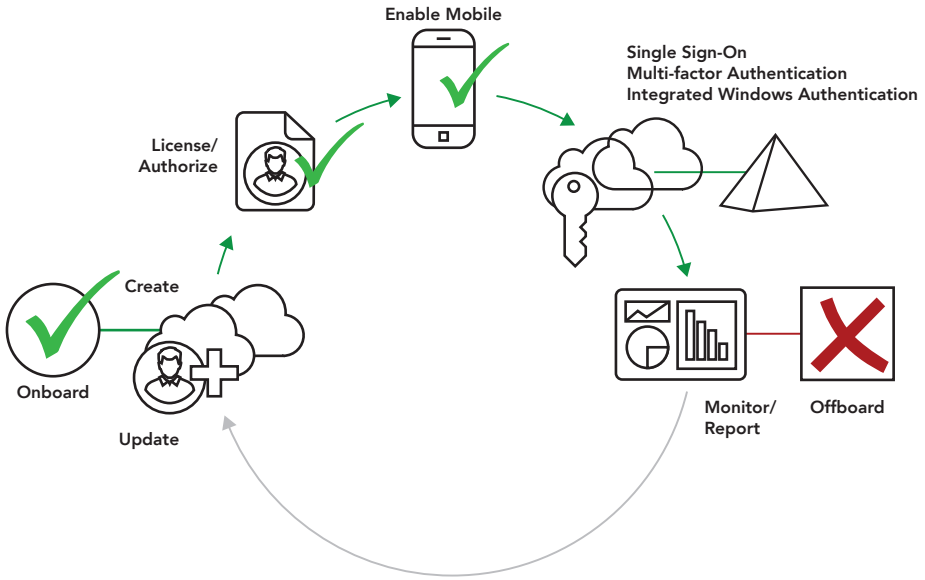
When it comes to securing access, organizations need to ensure that full identity security is provided to all types of users. Look for solutions that not only provide full identity security for employees, customers, and partners, but also for the most important type of user you would want to secure — privileged users (i.e. your IT admins) — those who have privileged access. Hacking passwords and privileged credentials can ultimately lead to a catastrophe as once attackers gain access they are able to escalate their privileges and move through the corporate network to compromise confidential data. Ensure that the solution you invest can address the entire spectrum, securing every user's access to apps, endpoints and infrastructure through single sign-on, risk-based multi-factor authentication and privileged access security.

3. Complete App Access Lifecycle Management

When a user is new to the organization or takes on a different role within the company, an IDaaS solution should make it easy — and automatic — for you to provision users to cloud or on-premises apps with automated account creation, role-based license and authorization management, single sign-on, mobile app client management and automated account de-provisioning. This automation frees up your precious few IT resources and empowers the user to be productive sooner than through existing and often manual onboarding checklists.

Full app access lifecycle management offers key benefits, enabling IT organizations to save time and money by automatically creating user accounts across cloud apps for new employees. Provisioning can eliminate helpdesk calls by allowing you to deploy the right apps — with the right access — the very first time. Provisioning eliminates any follow-on tasks by IT for enabling the user, and also eliminates user confusion. Automatic identity federation provides single sign-on to those apps, without requiring multiple passwords that can be easily lost, stolen or forgotten. Role-based licensing and authorization management for key apps such as Office 365, Salesforce, Box, and more further reduces your IT burden and allows you to quickly get users productive. The same capabilities make it possible to offboard users automatically (disabling or removing users from a group triggers user account de-provisioning) ensuring security and compliance by removing access immediately, removing mobile client apps and their data, instantly deactivating app accounts, and freeing up app licenses.

Centrify manages the complete lifecycle for app access including account provisioning, federation for SSO, mobile app management, centralized visibility and complete de-provisioning when the users changes roles



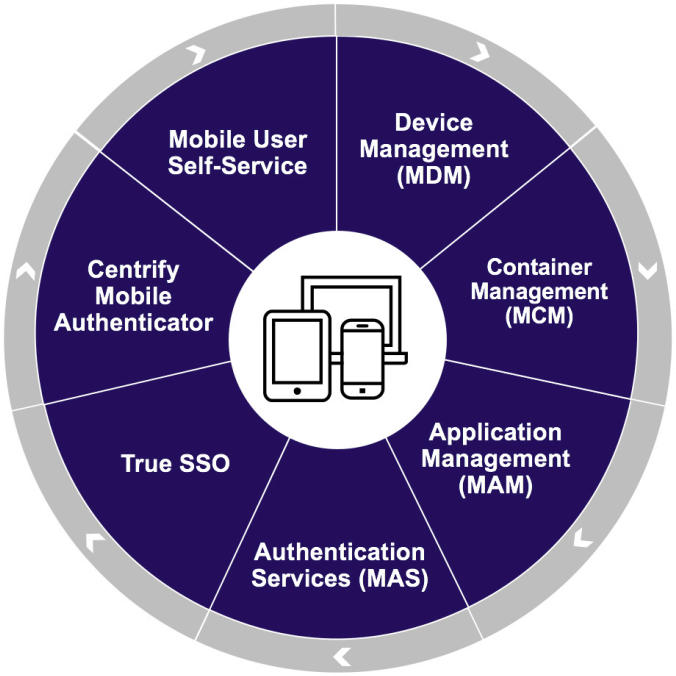
4. Mobile Access Management

Mobile has become the de facto way to access cloud apps requiring you to ensure security and enable functionality of users devices. This includes deploying appropriate client apps to the right device and ensuring an appropriately streamlined mobile experience. Unfortunately, most existing Identity and Access Management as a Service (IDaaS) solutions fall short when it comes to mobile support because they were built and architected before it became clear that mobile devices (smart phones and tablets) were going to become the preeminent means to access apps. Instead, they are very web browser centric—i.e. their mobile IDaaS experience just supports web-based apps vs. also supporting rich mobile apps and device security. They also provide no means to ensure that the user's mobile device is trusted and secure, and while they may provision a user in the cloud service, they ignore giving the end user the corresponding app on their device.

Consequently, you should look for an IDaaS solution that allows your users to enroll their mobile devices and deliver strong authentication mechanisms (using PKI certificates). The solution should let you apply mobile device-specific group policies to ensure the underlying device is secure (e.g., ensure that a PIN is required to unlock the phone, etc.), detect jailbroken or rooted devices, and allow you to remotely lock, unenroll or wipe a lost or stolen device.

Once you associate the device with a user and can trust the device you can leverage the device as an identifying factor for the user in cases where additional factors are required for multi-factor and step-up authentication.

The solution should also provide unified app management for both web-based and mobile client apps. This ensures that users are not left with partial access or access defined and managed in separate silos of access management such as separate mobile device management solutions (MDM). Both app and mobile management should share the same roles, identities, management tools, reports and event logs. This unification of mobile and app access management reduces redundant tools, processes and skillsets.



Mobile has quickly become the de facto way to access apps. Centrify uniquely unifies app and mobile access management.

5. Robust Access Policies and Risk-based Multi-factor Authentication (MFA) Everywhere

Today you live with the risks of users accessing many more services outside the corporate network perimeter as well as users carrying many more devices to access these services. Users have too many passwords and the passwords are inherently weak. In fact passwords have become more of an impediment to users than they are protection from hackers and other malevolent individuals and organizations. In short, in many cases, passwords alone cannot be trusted to properly and securely identify users.

Consequently, you need a better solution that incorporates strong authentication and one that delivers a common multi-factor experience across all your apps — SaaS, cloud, mobile, and on-premises. The solution also needs to have access policies that take into account the complete context of the access request and helps to overcome these new security risks. In addition, you need the capability to establish flexible access policies for each app for more granular and adaptive control. For example, if a user is accessing a common app from a trusted device on the corporate network from his home country during business hours ,then simply allow him silent SSO access to the apps. But if that same user is accessing an app outside the corporate network from a device that is not trusted, outside of business hours, and from a foreign country then deny them access — or at least require additional factors of authentication.

Specifically, you need an IDaaS solution that ensures security authentication by combining multi-factor authentication (MFA) and rich, flexible per-app authentication policies. You also need a solution where you can simplify a legitimate user's access with a policy that is based on user behavior profiles.

Multi-factor authentication methods should include at least:

- Soft token with one-button authentication to simplify the experience
- One Time Passcode (OTP) over SMS text or email
- Interactive Phone Call to the user's mobile device and requirement for a confirmation before authentication can proceed
- User configurable security question to act as a second password

Per-app authentication policies should allow, deny or step up authentication based a rich understanding the context of the request based on any combination of:

- Time of day, work hours
- Inside/Outside corporate network
- User role or attributes
- Device attributes (type, management status)
- Location of request or location of user's other devices
- App client attributes
- Custom logic based on specific organizational needs

Risk-based Multi-factor Authentication

Look for MFA solutions that leverage integrated machine learning and are based on user behavior. Pending on the level of risk, a user can be allowed, prompted for further authentication, or blocked entirely. Not only does risk-based access provide real-time security, but it also flags high-

risk events, and elevates them to IT's attention – speeding analysis and greatly minimizing the effort required to assess risk across today's hybrid IT environment.

Leverage integrations with analytics and machine learning to define and enforce access policy, based on user behavior and to also improve user experience without compromising security with flexible authentication policies. Identify solutions with adaptive MFA based on risk creates automated policies that only challenge for authentication when user behavior is outside typical norms.

6. Identity Where You Want It

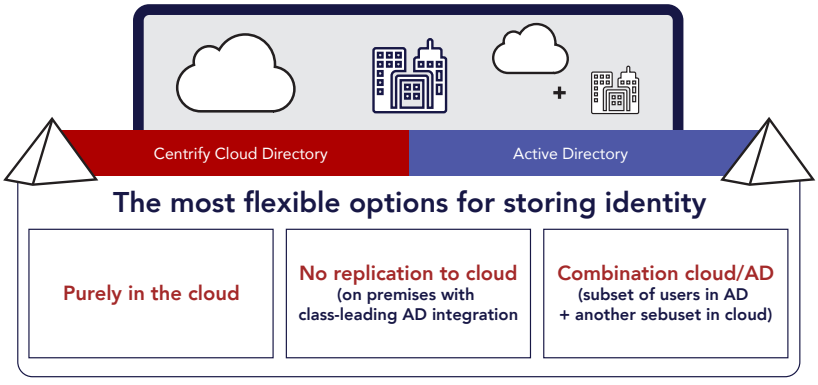
An IDaaS solution also needs to be flexible, providing robust access to corporate identities managed on-premises (e.g., Active Directory or LDAP), a directory service in the cloud for non-AD users such as partners or customers, and when appropriate, a hybrid of the on-premises and cloud directories. This is in stark contrast to other startup IDaaS vendors who only allow you to store identity data in their cloud directory. In order to leverage user data stored and managed in Active Directory, they first require that a portion of this data be replicated to their cloud and out of your control.

This cloud-only approach may not appeal to some organizations that — rightly or wrongly — have concerns about losing control of the proverbial keys to the kingdom. Organizations may also have reservations of creating another silo of identity to manage, unique security or privacy concerns, or legitimate concerns about the long-term viability of the vendor.

To enable this "identity where you want it," a well-engineered IDaaS solution should deliver robust integration with on-premises Active Directory or LDAP, should support cloud-only deployments consisting of non-Active Directory or LDAP -based user identities, as well as a hybrid of Active Directory, LDAP, and/or cloud deployment.

Active Directory support should offer built-in integrated windows authentication (IWA) without separate infrastructure and should automatically load balance and failover without any additional infrastructure or configuration. Most importantly, it should not replicate Active Directory data to the cloud where it is out of the organization's control — even if you choose to manage some of your users via a cloud model.

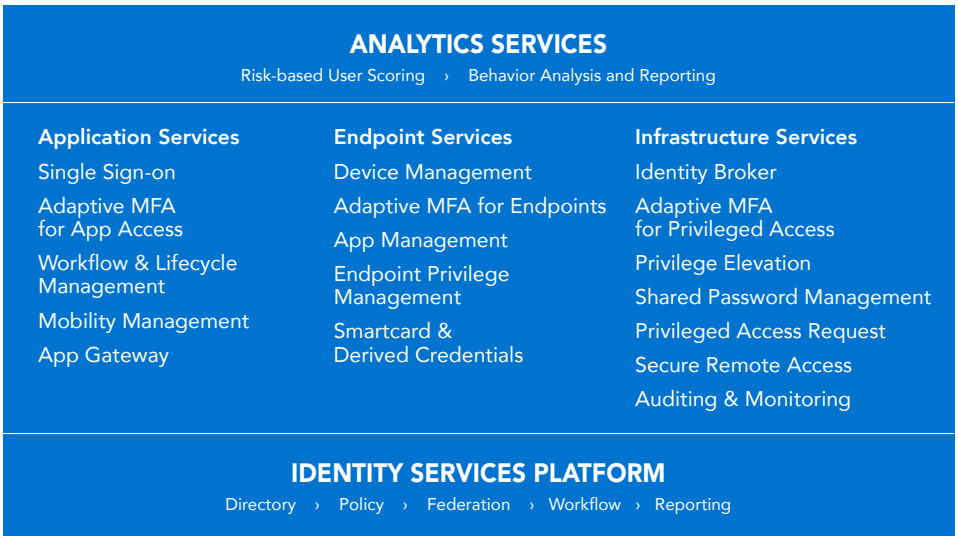
The diagram below shows the deployment options an IDaaS solution should support. As you can see, this hybrid approach gives you the best of both worlds in terms of flexibility.



Centrify delivers class-leading integration with both on-premises directories, the Centrify Cloud Directory, or any combination.

Conclusion

An IDaaS solution can prove to be a tremendous time saver, improve user satisfaction and IT productivity and addresses many of the shortcomings associated with password sprawl. When considering an IDaaS solution, partner with a vendor that can deliver on all of the top IDaaS considerations discussed in this paper and select an IDaaS solution that can centrally authenticate users with their Active Directory identity without replicating to the cloud, that unifies mobile and app access management, is ready for your enterprise globally and one which gives IT valuable insight into which applications and how devices are used and when —restoring lost visibility and control. In doing so you will reap many important benefits including:



Centrify uniquely unifies cloud app and mobile management.

Improved user productivity and satisfaction: Make users productive day one without extensive manual checklists and time consuming helpdesk calls. Reduce the number of times a user has to remember and self-manage passwords, and make it easier to self-service access to all of their apps, devices and identity.

Reduced helpdesk costs: Return value in improved productivity and as much as a 95% reduction in app account and password reset calls.

Lower app lifecycle costs: Through turnkey provisioning for apps and by tightly integrating with Active Directory the delivery of app single sign-on and mobile security is more cost efficient because IT uses existing technology, skillsets and processes that are already in place.

Improved security: IT can remove users' access to all business-owned cloud and on-premises applications by simply disabling their Active Directory account, which is already a common practice at the time an employee leaves the company. And unlike other solutions, it does not duplicate your existing identity data into the cloud and out of your control — it remains secure inside your corporation.

Reduced compliance costs: Free up expensive IT resources with easy and thorough reporting on who in the organization has access to which cloud and on-premises applications, and what they did with their access. Quickly demonstrate compliance with regulations and industry best practices.

Only Centrify uniquely unifies mobile security and app access management while delivering on all of the important considerations discussed in this paper. Reach out to us for a demo, questions and more information or simply register for a trial subscription today.

Next Steps

Register for a trial subscription of Centrify Application Service and Centrify Endpoint Service today to see how it can benefit your organization: www.centrify.com/saas/trial.asp

SANTA CLARA, CALIFORNIA	+1 (669) 444 5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11 3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	sales@centrify.com
WEB	www.centrify.com

WHP001583EN-07012017