CYBERARK®

WHITE PAPER

TOP TEN CONSIDERATIONS WHEN CHOOSING A MODERN SINGLE SIGN-ON SOLUTION

Table of Contents

Introduction 3
1. Versatile Directory Integration Services 4
2. Self-Service Capabilities 5
    Self-Service Password reset and Self-Service Account Unlock 5
    Self-Service Access requests 6
    Self-Service Application Onboarding 6
3. VPN-less Access and SSO to On-premise Applications 6
4. Comprehensive Protocol, API and Widget Support 7
5. Application Catalog and Wizard-driven Application Onboarding 7
6. Partner Federation and Identity Proxying (Chaining) 8
7. Application Access Governance 10
8. Adaptive Single Sign-On 11
9. Mobile Experience 11
10. Availability, Scalability, and Performance 12

Introduction

The adoption of cloud and hybrid infrastructure, the increasing number and variety of apps, and the proliferation of remote workforce are forcing companies to abandon traditional, perimeter-based security approaches. Instead, companies now embrace the "Zero Trust" based security strategy with identity at its core.

The concept of Zero Trust is based on the principle of maintaining strict access controls for every person or system, regardless of whether they are within or outside of the network perimeter. The Zero Trust approach to access ensures that every user is verified, their device validated, and their access is intelligently limited using the principle of least privilege. Consequently, Single Sign-On (SSO) and Access Management are foundational to Zero Trust and identity management.

Since identity is the only true perimeter, user credentials are now one of the main targets for cybercriminals. According to the 2019 Verizon Data Breach Investigations Report[1], 80% of hacking-related breaches still involving compromised and weak credentials, with 29% of all breaches, regardless of attack type, involved the use of stolen credentials. Despite these figures and the ever-increasing cost of security breaches, companies continue to leverage passwords to secure user credentials. According to estimates from Microsoft[2], there are over 300,000,000 fraudulent daily sign-in attempts to Microsoft Services, and 53% of all users have not changed their passwords in the past 12 months[3]. Poor identity management practices and compromised passwords rapidly erode trust in the organizations' digital transformation initiatives and expose companies to unnecessary risk.

Overreliance on passwords negatively impacts end-user productivity as well. The typical employee user loses about 12.6 minutes per week[4] entering or resetting passwords. For an organization with 48 workweeks in a year, this can translate into $284 per employee lost annually on passwords, assuming an average wage of $28.44/hour in the United States[5]. In addition, the average number of helpdesk calls a typical employee makes in an organization is about 21[6]. About 30% of those calls are related to passwords[7]. At the average cost of $70 per helpdesk call, this could translate into an annual helpdesk cost of $441 per employee.

Single sign-on enables organizations to eliminate password sprawl, implement more robust credential controls, and use a single secure identity for all the organizations' applications, endpoints, and resources. This not only helps increase user productivity and improve user experience but also helps reduce helpdesk costs and IT burden.

However, not all SSO solutions are created equal, and choosing the right one can be a challenging process. This whitepaper discusses the top ten considerations that will help you to select the best SSO for your organization.

[1] 2019 Data Breach Investigations Report by Verizon.

[2] "One simple action you can take to prevent 99.9 percent of attacks on your accounts" blog by Melanie Maynes; Microsoft.

[3] Psychology of Passwords: Neglect is Helping Hackers Win. 2018 report by LastPass by LogMeIn.

[4] 2019 State of Password and Authentication Security Behaviors Report, conducted by the Ponemon Institute.

[5] US Bureau of Labor Statistics, Jan 2020.

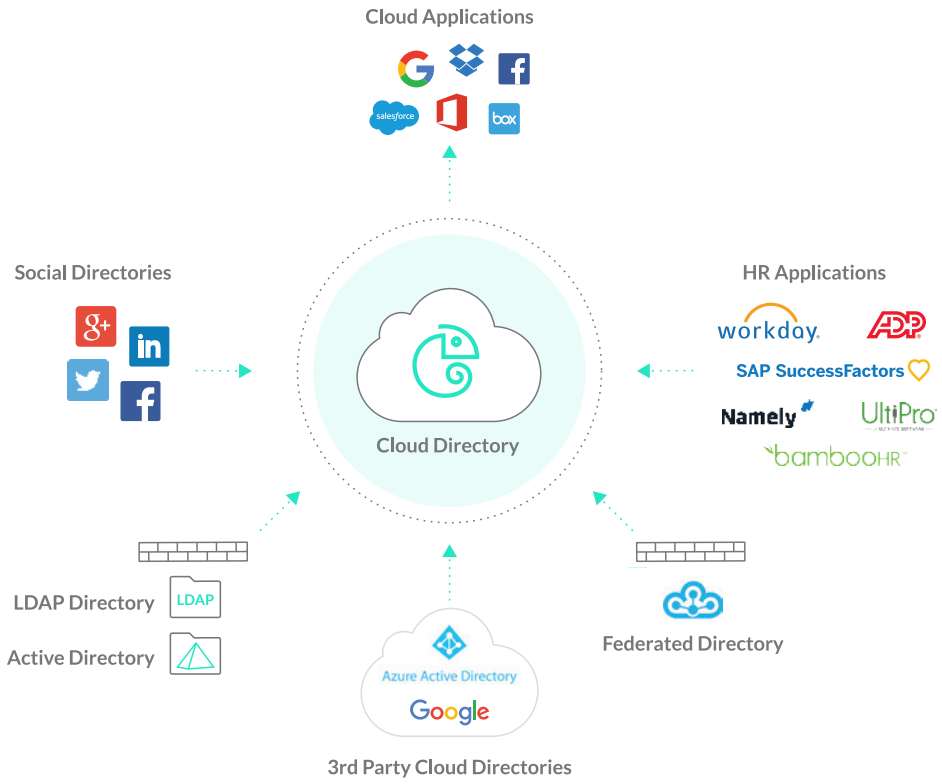
[6] META Group research conducted on behalf of PricewaterhouseCoopers

[7] META Group research conducted on behalf of PricewaterhouseCoopers

1. Versatile Directory Integration Services

One of the most important considerations for a modern single sign-on solution is its versatility in integrating with the organizations' existing directory service that serves as the authoritative source of all user identities. Many organizations, especially larger, more established enterprises, often require complex user directory structures. For organizations that use Microsoft Active Directory (AD), these can involve multiple domains and forests, with each domain having dozens of, if not more, organizational units (OU) and hundreds of groups. In some cases, these organizations have been formed through mergers and acquisitions, adding further complexity to their environment. In such cases, consolidating all the user identities across the enterprise into a new directory can be a multi-year project by itself.

Any SSO solution that recommends and necessitates this type of consolidation before its implementation not only risks the project itself but can also cause considerable hardship and overhead across the entire IT department. So, choosing an SSO solution that enables organizations to decide where they want to store and manage their authoritative source of identities is advisable. In other words, a good SSO solution will seamlessly integrate with the organization's Active Directory domains and forests, Lightweight Directory Authentication Protocol (LDAP) compliant directories, as well as other connected user directories.



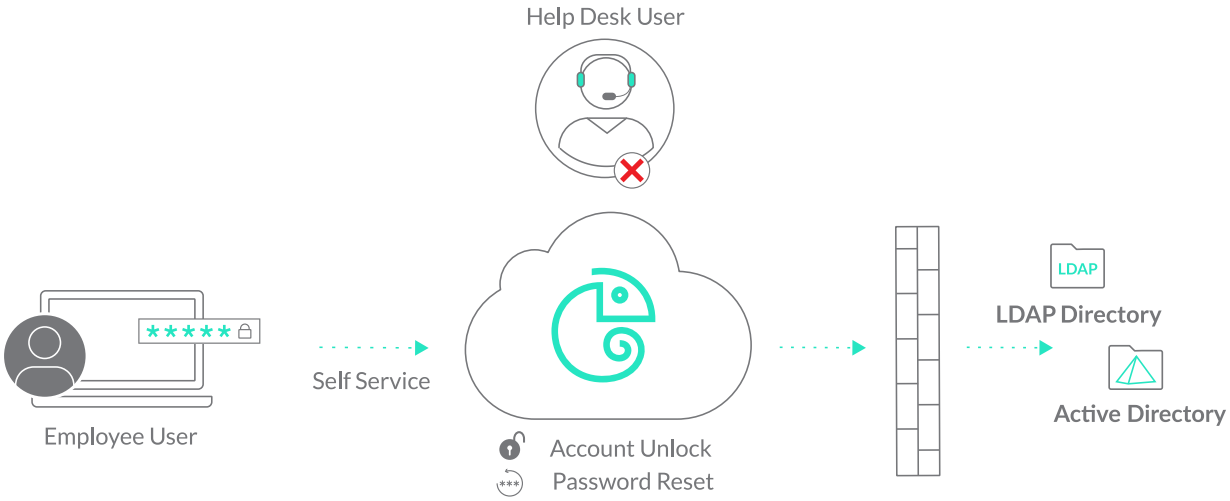
Additionally, a robust SSO solution should provide its own Directory Service that has customizable schemas for users and other types of identities, such as computers and servers. It is crucial that this service allows an organization to extend its existing AD schema with more attributes without needing to modify the schema in their AD. Stand-alone Directory Service is particularly important for organizations with diverse sets of end-users. For example, an organization may want to separate partner, contractor, and consumer identities from the employee identities and store them in a separate, highly scalable directory independent from the organization's core employee authoritative directory.

Lastly, another key consideration of an SSO solution is the ability to present a Virtual Directory Interface to any application. Virtual Directories can dynamically link together disparate identities across several authoritative directories and perform User Disambiguation to resolve into a single master identity. **User Disambiguation** refers to the ability to search through multiple user directories that may have an identical user identifier (e.g., username) and choose the identity from the right directory that matches the credentials supplied by the end-user.

2. Self-Service Capabilities

Self-Service Password reset and Self-Service Account Unlock

Helpdesk requests for password resets and account unlocks not only negatively impact end-user productivity but also increase the overall helpdesk costs substantially. Consequently, a leading SSO solution must include capabilities that enable end-users to reset their passwords and unlock their accounts without the need to make helpdesk calls.



The critical thing to be on a lookout for when evaluating self-service capabilities is the ability for end- users to reset passwords or unlock accounts without the need to first login to a computer to get access to the self-service tools. In other words, it is not reasonable to expect your users to log in to their work computer with their forgotten AD password or into a locked AD account to use self-service tools. Instead, the self-service tools need to be available at the login screen or through a cloud interface that can be accessed from anywhere. When selecting an SSO solution, choose one that acts as a credential provider for Windows (or includes a pluggable authentication module for Mac) and enables end-users to perform self-service actions on desktops as well as mobile devices.

The other key aspect of self-service password reset and account unlock, is related to adding an appropriate level of authentication assurance. Meaning, the SSO solution should have the ability to verify the user identity using authentication factors other than the user's password prior to allowing self-service action. To that end, choose an SSO solution that has built-in Multi-Factor Authentication (MFA) capabilities for self-service password reset and account unlock, or one that seamlessly integrates with your existing MFA vendor for the same.

Self-Service Access requests

Employees within an organization are often on the move, changing departments, expanding on their roles and responsibilities, and getting promoted. Events like these often result in employees needing access to new applications and resources. Traditionally, this meant that employees had to submit helpdesk requests to get access. The helpdesk would then provision access to new applications upon the IT administrator or the employee manager's approval.

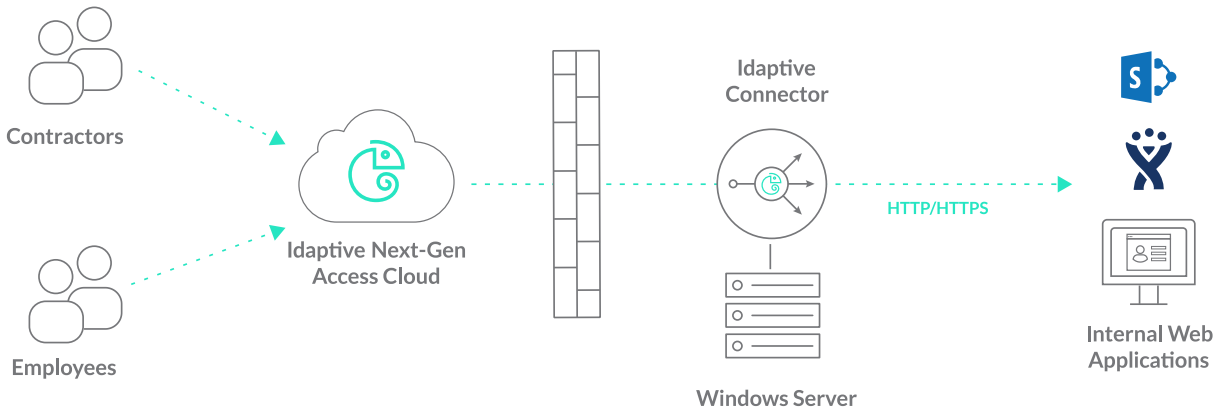
Leading SSO solutions should incorporate this access request workflow and enable end-users to gain access to apps without helpdesk support. Therefore when selecting your SSO solution, spend some time evaluating the application access request capability. The solution should include a searchable application catalog, the ability for end-users to easily request access, and a flexible back-end approval workflow. This workflow may, for instance, notify the employee's management chain, an application administrator, or a group of users to review the request and, if legitimate, approve it directly in the SSO portal or a mobile app.

Self-Service Application Onboarding

In times when the IT teams are overwhelmed, finding resources to enable SSO for new applications can be challenging, so apps with smaller userbase get de-prioritized. To save time, power users of these apps often reuse other application credentials, thereby exposing companies to additional risk. The more applications are not implemented with SSO, the higher the risk. Modern SSO solutions should, therefore, provide the capability to auto-capture the passwords entered into applications and auto-fill them at a later time. In this way, end-users can create a complex and unique password for each of the non-integrated apps and leverage the SSO solution for the seamless login experience.

3. VPN-less Access and SSO to On-premise Applications

As organizations migrate their workloads to the cloud, some of the key applications remain hosted in local, on-premises data centers. Concerns over security, application availability, and compliance are some of the main reasons why CIOs choose to keep applications in-house. Employees need to access these on- premises applications in the same way they access cloud-based apps – seamlessly, from any device, and at any time – to stay productive. Traditionally, IT leveraged Virtual Private Networks (VPNs) to provide employees the remote access to resources hosted on-premises. However, providing users access to the VPN, when all the user needs is to access an application running within the on-premise data center amounts to giving the user keys to the kingdom. Once users are authenticated and connected to a VPN, they can theoretically access any resource on the entire network, limited only by policies already in place at the authentication and authorization step. In other words, VPN enables "all-or-nothing" access. A better way to control access to on-prem apps is through an application or a reverse proxy capability. With reverse proxies, you can provide users app-specific access based on their roles and further secure on-prem resources with multi-factor authentication.



The other aspect of this requirement is related to the ability to proxy the user's identity to the application, which allows you to integrate the on-premises apps with SSO solutions. Many on-prem and legacy applications do not support modern SSO protocols like SAML, OpenID Connect, WS-Trust, and others. Instead, they support basic authentication methods, such as form-based authentication, HTTP header- based authentication (e.g., remote_user, X-Forwarded-For headers), username and password replay, and the likes. Consequently, leading SSO solutions should be able to support a variety of authentication methods mentioned above to ensure that you can set up SSO with your on-prem applications.

4. Comprehensive Protocol, API and Widget Support

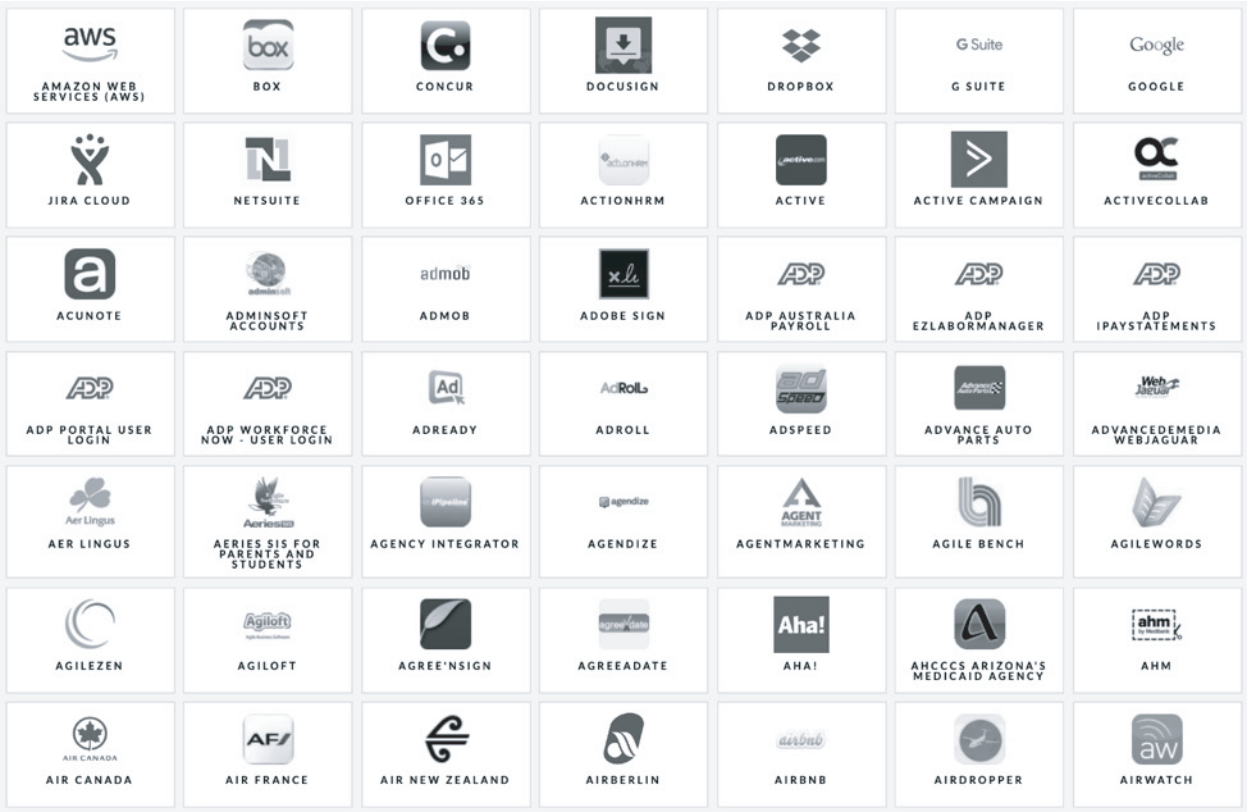
Most enterprises today have a mix of cloud and on-premises applications. These applications often leverage a range of protocols related to authentication and SSO. For example, modern cloud and on-premises applications can support standards such as Security Assertion Markup language (SAML v1.0, 1.1, 2.0), OpenID Connect (OIDC), OAuth v2.0, and WS-Federation. Legacy applications, on the other hand, may only support basic or form-based authentication, which allows an identity provider to supply the username and (protected) passwords to the app via a form. Header-based authentication is yet another way for applications to receive information about a user from trusted identity providers and enable SSO. A leading SSO solution, therefore, needs to support all the protocols and methods mentioned above.

It could be the case that applications in your environment support none of the modern or traditional authentication methods. Your SSO solution would then need to have a secure, encrypted password vault and a browser extension to support SSO for these types of apps. The browser extension, an add-on that you install in your web browser, captures user credentials, stores them in the vault, and injects them into the username and password fields or forms to log users into applications automatically.

Lastly, custom-built applications can be designed to authenticate against an identity provider by receiving an authenticated user token. These tokens frequently adhere to specifications mentioned in the SAML, OIDC, OAuth, or WS-Trust standards. The SSO solution must provide easily consumable APIs to integrate these custom-built applications. In addition, well-documented APIs greatly simplify and accelerate app development. Therefore, the availability of a dedicated developer portal with published code snippets and widgets that can be easily embedded into applications by developers should be one of the considerations in your vendor selection process. For example, a vendor could provide code for a login widget, which can be embedded in the application and reduce the time developers need to spend working on app authentication. The SSO solution must also provide development toolkits (SDKs) for app development platforms like React, Swift, Python, PHP, Java, and C# to help developers to incorporate security controls to their web and mobile apps.

5. Application Catalog and Wizard-driven Application Onboarding

Today, enterprises leverage hundreds of applications to support a variety of user populations and use cases. The value derived from the SSO solution is, therefore, directly proportional to the number of applications that can be integrated with the solution, and the ease with which new apps can be added. The process of onboarding applications into an SSO solution can be a challenging task that may take substantial effort, time, and knowledge of the SSO protocols and standards that applications support.



A leading SSO solution addresses this challenge by providing a catalog of pre-built application templates and integrations. These templates remove the need to understand SSO protocols and simplify the configuration down to a few key settings. As part of your evaluation process, ensure that applications that are currently used in your organization or that you plan on deploying are present in the catalog.

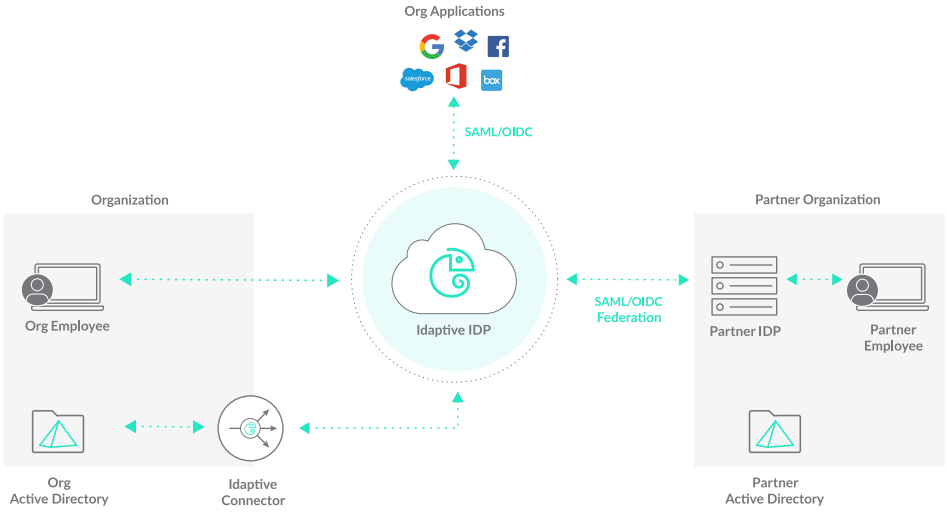
It is important to note that no catalog will contain all of the possible enterprise applications. For applications that do not have templates in the app catalog, the SSO solution must provide an intuitive, easy to use onboarding wizard to guide administrators through the onboarding process. These wizards should have clear documentation or embedded how-to videos that further help administrators to learn how to onboard the applications rapidly and reduce the time required to derive value from the SSO solution.

Below are examples and descriptions of capabilities across the five key areas that help an organization achieve the Basic Level of Maturity.

6. Partner Federation and Identity Proxying (Chaining)

Mergers and acquisitions are one of the most common ways companies grow. As organizations combine systems and employee populations, the management of user identities becomes challenging. For example, each of the merging organizations may leverage different user directories and SSO solutions (Identity Providers) for their employees and contractors. Along similar lines, companies often work closely with partner organizations who, in turn, have their own SSO systems. Regardless of the

circumstances, employees of one organization frequently need to access applications of another organization. It may not be feasible or desirable for one organization to duplicate the other organizations' identities across systems to enable access. This is where the concept of federations comes in. Federation enables an organization to seamlessly allow another organization's users to access its applications without the need to authenticate, duplicate, and manage the lifecycle of the other organization's users or setting up a separate VPN infrastructure for partner access. In essence, federation enables the one identity provider to trust another organization's identity provider to authenticate and manage users.

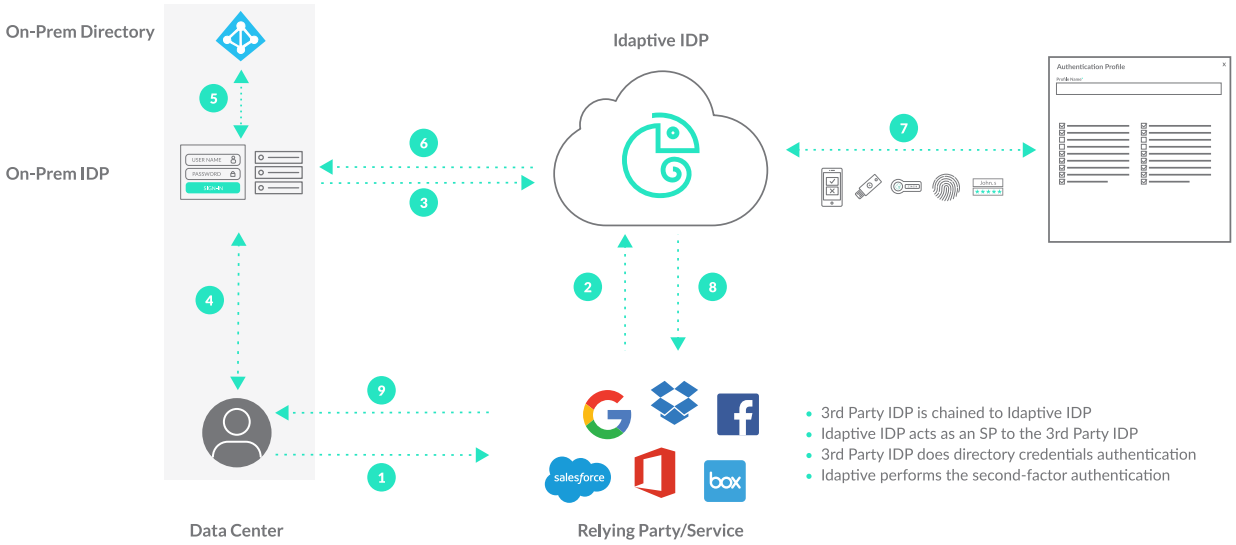


A leading SSO solution should support partner federations using both SAML and OIDC standards and have the ability to receive trusted authentication tokens. The trusted tokens should be encrypted (Federated Assurance Level 3[8]) and prove that the user has indeed authenticated with the other identity provider. The SSO solution should also be able to leverage any additional user-related information (SAML attributes, for instance) provided in the token to further authenticate and authorize the user for access to applications and data.

In other cases, organizations may have an existing legacy SSO solution, with hundreds of applications already integrated with it. The legacy solution may come with many challenges and limitations. For example, legacy SSO systems may have a poor end-user experience, require complex scripting or development for application integration, or demand dedicated headcount to manage the infrastructure that the SSO solution runs on. For such organizations, transitioning to a modern, cloud-based SSO solution can be made seamless through the concept of the Identity Provider (IdP) proxying or chaining.

In a chained IdP model, the modern SSO solution trusts the SSO token provided by the legacy IdP authenticating the user to an existing app. Both the legacy and the modern IdPs are interconnected and integrated with a single authoritative user directory. All the existing applications remain integrated with the legacy SSO, while all of the new applications are integrated directly with the modern SSO. In other words, if the modern SSO solution supports IdP chaining, an organization does not need to adopt a big bang approach and modify all of the existing application integrations to work with the new SSO. This allows for a gradual migration to the modern SSO solution and makes the transition seamless and easy, especially for the application owners and IT administrators.

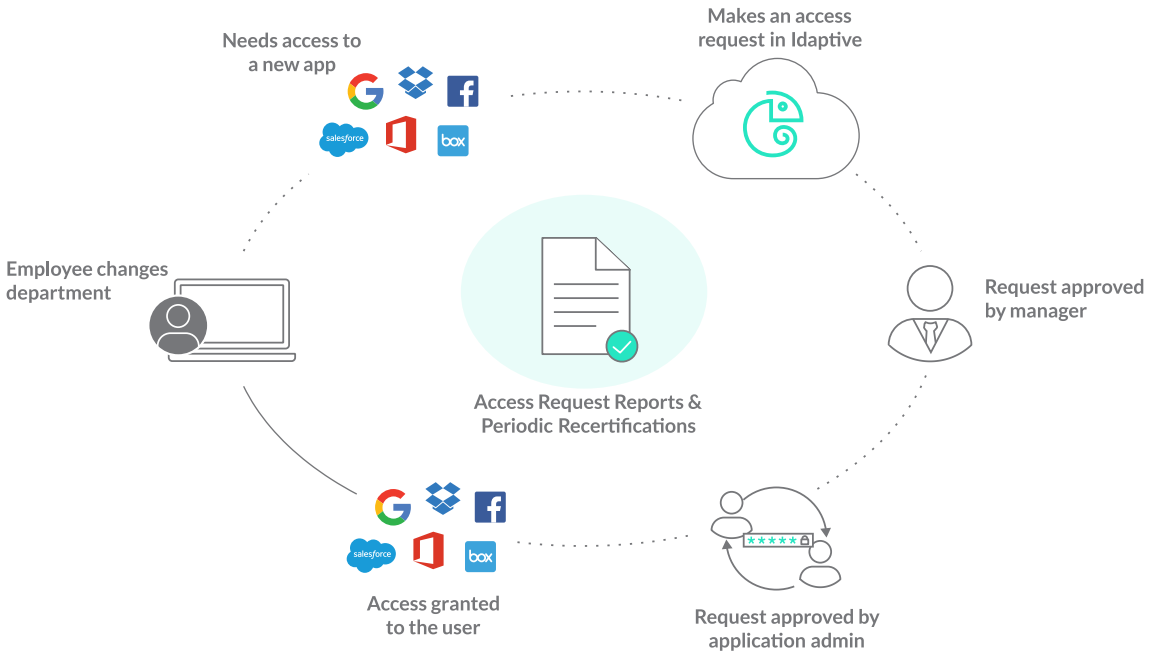
[8] NIST standard 800-63c



With chained IdPs, organizations can also dramatically improve the user experience. In the chained IdP model, employees only interact with the modern SSO solution, which provides a more streamlined login experience regardless of the application users need to access.

7. Application Access Governance

Access Governance is one of the key capabilities needed by individuals responsible for application security and compliance. The goal of access governance is to reduce the cost and effort involved in overseeing and enforcing access policies and demonstrating compliance. To this effect, leading SSO solutions should be able to provide reports that track user access, identify non-compliance with role-based access controls. For example, these reports should identify specific users that have access to sensitive applications, what roles have permissions to which applications, and what changes have occurred in the access permissions of a particular user. These reports are essential to continually ensure that users only have access to applications they need to perform their duties.



Another capability related to Access Governance is the ability to orchestrate an approval workflow for self-service application access requests. Self-service application access requests, as we mentioned earlier, enable employees to request access to applications without submitting helpdesk support tickets. These workflows can be configured to include multi-level approvals from the employee's management chain, the security team, the application administrator, or even the IT administration team. The approval workflow is instrumental in ensuring that there is a governance model in place for end-users being granted access to applications, and the organization remains compliant with their regulatory and security obligations.

Lastly, many leading SSO solutions are now starting to implement Access Certification capabilities. Access Certifications allow organizations to operationalize continuous or periodic access reviews to ensure that the users have access to only what they need. During these reviews, management, application owners, or IT administrators have to certify that only approved users have access to the applications. If automated Access Certifications capabilities are not available, ensure that the SSO solution is capable of interfacing with the enterprise's HR system to automatically provision access according to the user's identity and roles. When a user is terminated or changes positions, the HR system should notify the SSO system to perform the deprovisioning for all the systems in the user's role that are no longer needed. This will ensure that manual access certifications produce relatively clean results, and organizations remain in compliance with their access policies or government regulations.

8. Adaptive Single Sign-On

One of the principles of the Zero Trust Access Security architecture is to leverage as much contextual information about the user as possible while making access decisions. Most traditional SSO solutions require a user to authenticate once. After that, the SSO solution grants the user access to all the authorized applications for a pre-defined period of time, typically the length of the user session. In other words, once the user has been authenticated to the SSO solution, all of the applications explicitly trust the user and let the user access them as long as the SSO session is valid. This explicit trust violates the concept of Zero Trust.

A modern SSO solution should employ a combination of rules and machine learning to determine whether a user should be granted access to an application, even after the user has successfully authenticated to the SSO solution. These rules incorporate contextual information related to the user, such as the device used for access, the network from which the user is requesting access, the time of access request, and finally, the user location. Additionally, a leading SSO solution should be able to leverage this contextual information to learn typical user behavior using machine learning. Based on the historical behavior trends, the systems should then be able to identify atypical user behavior and assign each user a risk score during the process of accessing applications. If the risk score of the user exceeds a certain threshold, the user should be prevented from getting SSO into an application, regardless of whether he or she possesses the authentication factors required to access it.

When looking for a modern SSO solution, ensure that the solution you're considering supports both a rules- based SSO as well as machine learning-driven risk-based adaptive SSO.

9. Mobile Experience

Today, employees expect anytime, anywhere access to their corporate applications from all types of devices. These devices include not only Windows laptops and Macbooks but also mobile devices such as smartphones and tablets. Accessing web-based applications with SOO from laptops and desktops is simple and only requires a web browser. SSO access to corporate apps on mobile web browsers, however, is a bit more cumbersome.

A modern SSO solution should provide a dedicated mobile app to make accessing applications from mobile devices as seamless as possible. The app should be available for both iOS and Android platforms and include a landing portal page that displays all the applications authorized to users. The app should also enable the user to enroll their mobile device with the SSO solution. The device enrollment process allows SSO solutions to verify that the device meets the minimum security requirements and enables

organizations to push specific device management policies and certificates. The ability to deploy certificates on mobile devices is necessary for certificate-based authentication (CBA), which allows end-user to access native apps, such as Salesforce, OneDrive, or Outlook, without additional authentication steps.

10. Availability, Scalability, and Performance

Since SSO solutions gate access to all applications unified under the SSO, they must be highly available and reliable. Without functional SSO, employees have no means of accessing even the most basic applications such as email, HR systems, or productivity apps. Software-as-a-Service delivered (SaaS- delivered) SSO solutions often run on highly reliable cloud-based platforms and tend to perform far better than an on-prem, privately hosted SSO systems. For example, cloud-based SSOs should be able to dynamically scale with demand and automatically failover across geographic regions in the event of a disaster. Replicating these capabilities in an on-premises data center can be a very challenging and expensive proposition for most enterprises.

When considering a cloud-based SSO solution, pay close attention to the service level agreement (SLA) commitments, especially in terms of Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is the maximum amount of time taken by the SSO solution to recover after there has been a disaster that brings the service down. RPO is the maximum amount of time prior to the disaster for which the user data may be lost permanently. A leading SSO solution will provide RPO and RTO of at most 24 hours each, and since both RTO and RPO are SLA commitments, you can hold the SSO solution vendor accountable for not meeting them.

Along similar lines, make sure that you also consider SSO solution's uptime history and commitments. Typically, you want to find a solution with an uptime commitment of at least 99.9% (three nines), meaning the service can be down for a maximum of 8.77 hours per year.

Lastly, ensure that the solution can scale up in an efficient and cost-optimal manner to your growing organization needs, whether the scaling up involves more employees, more use cases (extending the service to your partners and consumers), or adding more applications.

Idaptive delivers Next-Gen Access, protecting organizations from data breaches through a Zero Trust approach. Idaptive secures access to applications and endpoints by verifying every user, validating their devices, and intelligently limiting their access. Idaptive Next-Gen Access is the only industry-recognized solution that uniquely converges Single Sign-On (SSO), adaptive Multi-Factor Authentication (MFA), Enterprise Mobility Management (EMM) and User Behavior Analytics (UBA). With Idaptive, organizations experience increased security, reduced complexity and have newfound confidence to drive new business models and deliver awesome customer experiences. Over 2,000 organizations worldwide trust Idaptive to proactively secure their businesses.