BUYERS' GUIDE

IDaaS BUYERS' GUIDE

idaptive

IDAPTIVE.COM

Introduction

The rapid rise in SaaS adoption and an increasingly mobile workforce has made old security models based on a strong perimeter defense obsolete. By extension, on-premises Identity and Access Management (IAM) solutions have followed suit. "Trust but verify," a security model that relied on well-defined network boundaries, has sunsetted—replaced by an "always verify" approach for everything — users, endpoints, networks, servers and applications. Modern organizations have adopted a Zero Trust Security model to protect their SaaS, mobile and on-premises applications from cyberattacks. This approach eliminates trust in users who reside in a protected network. Instead, the identity of every user is always verified before access is granted to an application, regardless if the user originates within or outside of a network.

How to use this guide

The right Identity-as-a-Service (IDaaS) solution can reap enormous benefits, such as risk reduction, cost savings and productivity gains. Researching and choosing the best solution requires careful consideration. This buyers' guide is designed to help you critically evaluate and choose the optimal IDaaS solution for your organization. It's organized by the key capabilities you should consider when evaluating an IDaaS solution with important questions to ask your IT partner or vendor to determine if their offering will meet your needs. We've also added a time-saving chart to help you create a shortlist of suitable vendors. Finally, we have included an overview of additional resources to shed some more light on your selection process.

Zero Trust Security Through IDaaS

Far beyond just single sign-on (SSO), a modern Identity-as-a-Service (IDaaS) solution can help your organization achieve a Zero Trust Security model. Using advanced access control mechanisms across cloud, mobile and on-premises applications, IDaaS solutions enable organizations to verify every user's identity, validate their devices, and intelligently limit their access — the key pillars of Zero Trust Security.

Key capabilities for a strong IDaaS solution

There are several key areas to consider when evaluating an IDaaS solution. We'll explore the specific capabilities you need within these areas and provide some questions you should ask vendors to be sure their solutions provide them:

Modern Single Sign-On | Adaptive Multi-Factor Authentication | Endpoint and Mobile Context
Dashboards and Reporting | Workflow and Lifecycle Management | Critical Non-Technical Considerations

Modern Single Sign-On

Single sign-on (SSO) secures access to apps by minimizing password entry and transmission while enabling users to access cloud, mobile and on-premises apps from any device. With a single identity, users verify their identity once to get secure SSO access to authorized applications and devices. A Modern SSO solution should provide support for both internal users (employees and contractors) and external users (partners and customers).

Capabilities to Look For	Description	Questions to Ask Your Vendor
Application Federation	Federation enables SSO without passwords. The IDaaS solution knows the user and presents the application or target system with a temporary token that securely identifies the user. Because of a trust relationship between the two systems, the target application accepts this token from the IDaaS solution and authenticates the user.	1. Does the solution have a robust catalog with thousands of pre-integrated apps? 2. Does the solution support custom apps through protocols, such as SAML, WS-Federation, OpenID Connect and OAuth 2.0? 3. Does the solution support federation to other IDaaS providers? 4. Can the solution easily customize SAML assertions, supporting custom integration scenarios?
Password Vaulting	Not all applications support Federation. However, IDaaS solutions can still deliver SSO by securely vaulting the user's passwords for each application, retrieving it and presenting it to the application at login time.	1. Can the solution quickly discover, capture and add forms-based username/password applications, without special skills or vendor support? 2. Does the solution allow the end user to add their own personal apps and manage their app passwords? 3. Does the administrative interface allow the admin to prevent the user from adding their own apps if required? 4. Does the solution allow for central management of a shared account without revealing the password to the user?
Desktop SSO	Desktop SSO simplifies the user authentication experience. Once a user has authenticated to their PC or Mac, IDaaS solutions can automatically log the user in to an application without prompting them to re-authenticate to the IDaaS system.	1. Does the solution support desktop SSO via Integrated Windows Authentication without additional infrastructure, such as Internet Information Services (IIS)? 2. Can the solution provide desktop SSO for both PCs and Mac workstations? 3. Can the solution provide desktop SSO to workstations that are not joined to the domain? 4. Can the solution also provide a desktop SSO-like experience on mobile devices?

Capabilities to Look For	Description	Questions to Ask Your Vendor
On-Premises Application Access	IDaaS solutions should support a wide variety of both SaaS and on-premises applications through standards support and native integrations.	1. Can the solution provide external users with direct access to on-premises web apps without requiring a VPN? 2. Does the solution natively integrate with on-premises apps without requiring third-party software or additional infrastructure? 3. Is the connector highly available, and does it automatically load balance external connections to on-premises apps? 4. Does the solution provide integrated support for external URLs for app access on or off the corporate network?
Directory Integration	For most organizations, IDaaS is not their primary source of identity data. IDaaS integrates with existing identity repositories for authentication, user attributes and security group data.	1. Does the solution seamlessly integrate with Active Directory, LDAP and G-Suite? 2. Does the solution avoid the security mistake of replicating on-premises user directories to their cloud? 3. Can the solution support search and role creation across multiple directories? 4. Does the solution provide a full native cloud directory for users who aren't in existing directories?

Adaptive Multi-factor Authentication

Multi-factor authentication (MFA) adds a layer of security that allows companies to protect against the leading cause of data breaches — compromised credentials. Users confirm their identity with something they know, something they have or something they are before access is granted to endpoints, networks, servers and applications. Adaptive MFA adds an additional layer of context-aware conditional access based on the individual user's risk and historical behavior.

Capabilities to Look For	Description	Questions to Ask Your Vendor
Authentication Methods	Strong Identity Assurance starts with authentication mechanisms to verify the identity of every user.	1. Does the solution support a broad range of authentication factors, such as email, SMS, telephone call, user-defined security question, OATH OTP, RADIUS, FIDO U2F and Smart Cards? 2. Can the solution enforce strong authentication across not only applications, but also endpoints, mobile devices, and VPNs? 3. Does the vendor offer a mobile authenticator app that supports both OTP and PUSH for strong authentication? 4. Does the solution support derived credentials for Smart Card login to mobile apps without requiring a Smart Card reader?
Conditional Access	Conditional access goes beyond authentication to examine the context and risk of each access attempt. Conditional access evaluates the most current information about the user, their device, location, time, behavior and risk for every access attempt.	1. Is the solution configurable to either allow SSO access, challenge the user with MFA or block access based on pre-defined conditions? 2. Does the solution offer a broad range of conditions, such as by IP range, day of week, time of day, time range, device O/S, browser type, country, device and risk level? 3. Are context-based access policies enforceable across users, applications, workstations, mobile devices, servers, network devices and VPNs? 4. Can the solution make risk-based access decisions using a behavior profile calculated for each user?
Identity Analytics	Identity Analytics uses machine learning to define individual user behavior profiles and enforce risk-aware access policies in real-time. Analytics also enhance visibility through rich activity dashboards with drilldown investigations to monitor IT risk and user experience across applications, endpoints and infrastructure.	1. Does the solution use machine learning to profile each user across factors such as device, time, date, geo-velocity and location? 2. Does the solution use analytics and machine learning to identify anomalous authentication activity? 3. Does the solution offer drillable dashboards and audit trails of authentication activity? 4. Does the solution integrate with third-party SIEM tools for real-time alerting and reporting?

Endpoint and Mobile Context

Endpoint and Mobile Context provides critical controls for access to corporate resources from only validated devices with a secure posture. Next-Gen Access delivers device security, identity and configuration for corporate-owned and BYOD devices.

Capabilities to Look For	Description	Questions to Ask Your Vendor
Mobile Identity and Access Management	This capability provides context for smarter access decisions. It leverages device attributes such as location, network and device certificates to ensure application data is protected from unauthorized access.	1. Can the solution enroll PC, Mac, iOS and Android devices to enforce mobile security policies? 2. Can the solution provide end users with a desktop SSO experience to mobile apps via a certificate deployed onto the device? 3. Can the solution leverage the device posture (managed vs. unmanaged) for access control decisions to apps? 4. Does the solution support biometric login to apps for strong authentication?
Mobile Application Management	The ability to push, manage and wipe mobile applications across mobile devices is critical for efficiency. Ensure corporate data stays separate from personal data and provide app single sign-on seamlessly — all with a unified policy.	1. Can the solution silently push and remove managed mobile apps to enrolled Mac, iOS and Android devices? 2. Does the solution support the creation of an approved enterprise app-catalog that end users can install or remove as needed? 3. Does the solution support deployment of custom Mac, iOS and Android apps? 4. Does the solution support Per-App VPN?
Device Security Management	Control device security posture with policy and configuration management, ensuring consistent preventative security.	1. Does the solution offer hundreds of tested configuration and security policies for Mac, PC, iOS and Android devices? 2. Does the solution support Apple Configurator, Device Enrollment Program (DEP) and Volume Purchase Program (VPP)? 3. Can the solution push pre-defined Wi-Fi profiles, mail, contacts and calendars to enrolled devices for Day One productivity? 4. Can the solution provide information on enrolled devices, such as inventory, serial number, installed apps, O/S version, jailbroken or rooted and more?

Capabilities to Look For	Description	Questions to Ask Your Vendor
Enterprise Workspace Management	Leverage Apple, Google and Samsung built-in capabilities to separate work from personal data and secure app distribution.	1. Can end users access enterprise apps through a secure Enterprise Workspace? 2. Can end users or administrators selectively wipe the Enterprise Workspace, managed apps and policies? 3. Can end users remotely reset passcode to workspace apps without IT involvement? 4. Can end users remotely lock access to the Enterprise Workspace for lost or stolen devices? 5. Does the solution support Samsung Knox Workspace?
Self-Service	Reduces helpdesk burden by supporting self-service capabilities, such as enrollment of BYOD devices and device management features, such as locate, lock and wipe.	1. Can end users easily enroll/un-enroll their iOS, Android, OSX and Windows devices without IT involvement? 2. Can end users and administrators manage devices with capabilities, such as remote locate, lock, factory reset and un-enroll? 3. Can end users remotely reset their device passcode without IT involvement? 4. Can administrators send notifications to enrolled devices?

Workflow and Lifecycle Management

Provision users across apps all from a central control point. Automatically route application requests for review, create user accounts upon approval, manage entitlements for each user, deploy client applications across devices, revoke access when necessary and remove client applications across devices.

Capabilities to Look For	Description	Questions to Ask Your Vendor
Workflow	End users can request app access directly from the app owners or approvers who receive email notifications. Approved apps are provisioned immediately without manual IT intervention.	1. Can end users easily request access to an app while providing justification for access natively within the solution? 2. Does the solution notify authorized owners when application requests are made for their review? 3. Can the solution automatically provision application clients to end user devices upon approval, eliminating IT involvement? 4. Does the solution provide certified integrations with IT Service Management applications, such as ServiceNow?
Application Provisioning	User accounts are created with the appropriate access based on role, which can change as employees' roles change. When access is revoked, accounts and their data are kept, suspended or deleted as appropriate.	1. Does the vendor have a catalog of pre-built applications that support provisioning? 2. Does the vendor support SCIM (System for Cross-Domain Identity Management) for provisioning to any custom application that supports the protocol? 3. Can the solution provision and de-provision not only user accounts, but also license management and entitlement assignment automatically? 4. Does the solution allow for flexible provisioning schedules that include manual, automatic or pre-defined syncs?
Inbound (HR and HCM) Provisioning	HR and Human Capital Management (HCM) systems are often the master for user data and company roles. Inbound provisioning supports the mastering of data within the HR or HCM application and keeps it in sync with enterprise directories, such as Active Directory.	1. Does the solution support identity mastering and provisioning from HR and HCM applications, such as Workday? 2. Does the solution support bi-directional provisioning between the HR or HCM application and Active Directory? 3. Does the solution enable flexible customization of user attributes between the HR or HCM application and Active Directory? 4. Can the solution automatically generate and distribute a random Active Directory password for each new hire to streamline the on-boarding process?

Dashboards and Reporting

Dashboards provide a pulse check of your organization's security in a moment's notice. They provide insights into authentication activity and details of anomalous activity detected. Reporting tools address ongoing audit requirements and ever-changing compliance mandates.

Capabilities to Look For	Description	Questions to Ask Your Vendor
Analytics and Dashboards	Dashboards provide an at-a-glance review of real-time metrics of access security and risky behavior across your IDaaS landscape.	1. Does the solution provide rich graphical dashboards to monitor user activity in real-time? 2. Does the solution allow custom filtering and drilldown of dashboard widgets? 3. Does the solution support drag-and-drop customization of all dashboard widgets? 4. Does the solution easily support the exporting of any dashboard widget data?
Event Logging	The ability to access events from your selected IDaaS solution is critical for monitoring, analysis and integration with external systems, such as SIEM.	1. Does the solution log user activity, such as login time, MFA challenge failures, password resets or location of login and device? 2. Does the solution offer drillable dashboards for insights into end user activity? 3. Can the solution provide a summary of policies settings and applications assigned to a user? 4. Are logs exportable to third-party SIEM tools for alerting and reporting?
Reporting	From compliance to management reporting, IDaaS systems should provide a large library of pre-built but customizable reports.	1. Does the solution offer a large library of pre-built reports? 2. Are the pre-built reports parameterized for easy customization? 3. Can any of the dashboard widgets be converted to data that can be externalized? 4. Are reports exportable via email, txt and CSV file formats?

Critical Non-Technical

The following capabilities may not be top of mind but are just as critical to your IDaaS evaluation.

Capabilities to Look For	Description	Questions to Ask Your Vendor
Security and Trust	IDaaS provider transparency regarding their approach to availability, reliability, scalability, security and privacy ensures that you can depend on them as a trusted partner and provider.	1. Is the solution globally available with support for over 15 languages? 2. Has the vendor ever suffered a significant breach? More than once? 3. Does the vendor offer developer resources with documented code samples, APIs and access to a developer? 4. Does the vendor offer a customer success team to ensure the success of every deployment?
Admin and Developer Resources	IDaaS providers often become an integral component for many IT processes. Questions should be raised about their commitment and support to not only successfully deploy their solution but also to integrate across your IT ecosystem and processes.	1. Does the solution log user activity, such as login time, MFA challenge failures, password resets or location of login and device? 2. Does the solution offer drillable dashboards for insights into end user activity? 3. Can the solution provide a summary of policies settings and applications assigned to a user? 4. Are logs exportable to third-party SIEM tools for alerting and reporting?
Analyst Recognition	An important barometer of a vendor's standing and suitability can be found in analyst evaluations and comparative guides.	1. Is the vendor recognized in industry-leading analysts' reviews, such as Gartner, Forrester, Frost & Sullivan and KuppingerCole? 2. Is the vendor a recognized leader across multiple identity and access management categories, such as IDaaS, Multi-factor Authentication, and Enterprise Mobility 3. Management and Privileged Access Management?

Vendor Capability Comparison

IDaaS Solution Must-Haves

- Provide a consistent and non-invasive user experience for all users and across devices
- Offer self-service capabilities, including resetting passwords, unlocking accounts, device management and self-provision apps
- Provide administrators with one management console to secure applications and endpoints, whether on-premises, or mobile, or in the cloud.
- Be intuitive and flexible to help administrators address organization-specific requirements
- Reside on highly available, redundant and fault-tolerant systems to avoid potential disruption
- On-premises components should also be reliable and flexible enough to adapt to any environment

Vendor Capability Comparison Chart

	Idaptive	OKTA	Microsoft (Azure AD Premium)	OneLogin
Single Sign-On				
Application Federation	●	●	◕	◕
Password Vaulting	●	◑	◔	◑
Desktop SSO	●	◔	◔	◔
On-premises Application Access	●	◑	◑	○
Directory Integration	●	◔	◔	◔
Multi-factor Authenication (MFA)				
Authentication Methods	●	◑	◑	◑
Conditional Access	●	◑	◑	◕
Identity Analytics	●	◔	◑	◑
Enterprise Mobility Management				
Mobile Identity and Access Management	●	◔	◑	◑
Mobile Application Management	●	○	◑	◔
Device Security Management	●	○	○	○
Enterprise Workspace Management	●	○	○	○
Self-Service	●	○	○	○

Most Capabilites ● ◕ ◑ ◔ ○ No Capabilites

Vendor Capability Comparison Chart

	Idaptive	OKTA	Microsoft (Azure AD Premium)	OneLogin
Workflow and Lifecycle Management				
Workflow	●	◑	◔	◔
Application Provisioning	●	●	●	◕
Inbound (HR and HCM) Provisioning	●	●	●	◕
Dashboards and Reporting				
Analytics and Dashboards	●	◑	◑	◑
Event Logging	●	◑	◑	◑
Reporting	●	◑	◑	◑
Critical Non-Technical				
Security and Trust	●	●	●	◑
Admin and Developer Resources	●	●	●	●
Analyst Recognition	●	●	●	◑

Most Capabilites ● ◕ ◑ ◔ ○ No Capabilites

Summary

The Right IDaaS Solution

Choosing the right IDaaS solution with the right capabilities is a first step toward achieving Zero Trust — dramatically reducing your organization's chances of a breach. We hope you've found this Buyers' Guide useful as you start the process of choosing the right IDaaS solution for your company.

To explore further if Idaptive Next-Gen Access is the right IDaaS solution for you

Start a free, full-featured 30-day trial of Idaptive today.

idaptive

3300 Tannery Way
Santa Clara, CA 95054

hello@idaptive.com