CYBERARK®

BUYERS’ GUIDE

IDAAS BUYERS’ GUIDE

Table of Contents

Introduction

Traditional perimeter-based IT security models and conventional on-premises Identity and Access Management (IAM) solutions conceived to control access to trusted enterprise networks aren't well suited for the cloud-first, mobile-first world of IT. In today's world of SaaS solutions and mobile apps, IT infrastructure often resides outside the confines of the trusted enterprise data center. And users access business applications and services from any place, at any time, using any device.

Forward-looking organizations are implementing Zero Trust Security architectures and deploying cloud-based Identity-as-a-Service (IDaaS) solutions for the era of on-the-go employees and on-demand services. In a Zero Trust Security model all users are authenticated, authorized and secured in real-time upon session establishment, regardless of location (inside or outside the corporate network) or endpoint.

Purpose

An IDaaS solution is an IAM platform delivered in the form of a cloud-based service hosted and managed by a trusted provider. The right IDaaS solution can provide enormous benefits, such as risk reduction, cost savings and productivity gains. Researching and choosing the best solution requires careful consideration. This buyers' guide is intended to help you critically evaluate and choose the optimal IDaaS solution for your organization. It is organized by the key capabilities you should consider when evaluating an IDaaS solution, and includes important questions to ask your IT partner or vendor to determine if their offering will meet your needs.

Zero Trust Security Through IDaaS

An IDaaS offering combines all the functions and benefits of an enterprise-class IAM solution with all the economic and operational advantages of a cloud-based service, and helps your organization institute a Zero Trust Security model. An IDaaS lets you verify every user's identity, validate their devices, and intelligently limit their access — the key pillars of Zero Trust Security.

How to use this guide

There are many solution features and vendor attributes to consider when evaluating an IDaaS solution. This guide examines the various IDaaS functions and considerations categorized below. Each section includes a detailed list of key features and capabilities with corresponding questions you can ask vendors to assess their solutions and competencies.

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

Modern Single Sign-On

Single sign-on (SSO) is an authentication method that lets users access multiple applications and services using a single set of login credentials. 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? 4. Does the solution support 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 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, additional infrastructure, or changes in application code? 3. If the solution leverages connector software to communicate with on-premises applications, 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 common directories, such as Microsoft Active Directory (AD), Azure AD, Google Directory, or LDAP-based directories? 2. Does the solution force you to replicate user data from your existing directories to the centralized cloud directory? 3. Can the solution support search and role creation across multiple directories? 4. Does the solution provide a robust cloud directory for users who aren't in existing directories?

Adaptive Multi-factor Authentication

Multi-factor Authentication (MFA) is an authentication method that uses two or more distinct mechanisms to validate a user's identity, rather than relying on just a simple username and password combination. It helps prevent unauthorized access to applications and sensitive data, helping organizations defend against identity theft, cyber attacks, and data breaches. Users confirm their identity with something they know like a password, something they have like a proximity badge or mobile phone, or something biometric like a fingerprint or facial scan. Adaptive MFA leverages contextual information (location, time-of-day, IP address, device type, etc.) and business rules to determine which authentication factors to apply to a particular user in a particular situation. For example, a user accessing business application from a verified computer and a known IP address might be able to log on using only a username and password. But to access the same application from a foreign country or a new device, the user might also have to enter a one-time, short-lived code sent to their mobile phone.

Capabilities to Look For	Description	Questions to Ask Your Vendor
Authentication Methods	Strong identity assurance starts with authentication mechanisms to verify the user.	1. Does the solution support a broad range of authentication factors, such as secret questions, mobile authenticators, SMS, FIDO U2F, hardware tokens, OATH-based on-time passcodes (OTP)? 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 passwordless authentication methods such as QR codes, magic links, and on-device FIDO 2-based factors, such as fingerprint readers?
Conditional Access	Conditional access goes beyond authentication to examine the context and risk of each access attempt. For example, a solution might take into consideration contextual factors such as consecutive login failures, geo-location, user account, or device IP to grant or deny access.	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, and user 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?

Capabilities to Look For	Description	Questions to Ask Your Vendor
User Behavior Analytics	User Behavior Analytics (UBA) uses machine learning to define individual user behavior profiles and enforce risk-aware access policies in real-time. UBA also enhances 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. Can the solution identify anomalous user behavior or authentication activity? 3. Does the solution offer customizable dashboards and audit trail of all 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 ensures only validated and approved devices can gain access to critical corporate resources.

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 grant mobile devices access to corporate resources.	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?
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

IDaaS solutions provide unified, automated tools for managing user identities and access privileges throughout an employee's tenure — from day one through separation. Workflow and lifecycle management functionality lets you 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' positions and responsibilities 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 licenses and entitlements 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 window into your organization's security posture. They provide insights into authentication activity and help you identify and investigate anomalous activity. Reporting tools address make it easy to monitor compliance and support audits.

Capabilities to Look For	Description	Questions to Ask Your Vendor
Analytics and Dashboards	Dashboards provide an at-a-glance view of real-time access security metrics and suspicious behavior across your IT environment.	1. Does the solution provide rich graphical dashboards to monitor user activity in real-time? 2. Does the solution allow you to create custom filters and drill down to the source data? 3. Can you easily export dashboard data?
Event Logging	Gather historical data and audit trails 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 drill-down dashboards for investigating end-user activity and forensics? 3. Can the solution provide a summary of policy settings and applications assigned to a user? 4. Are logs exportable to third-party SIEM tools for alerting and reporting?
Reporting	IDaaS systems should provide a collection of canned and customizable compliance and management reports.	1. Does the solution offer a large library of built-in reports? 2. Are the built-in 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	The IDaaS provider should be transparent about service availability, reliability, scalability, security and privacy to instill confidence and trust.	1. Has the vendor ever suffered a significant breach? 2. Does the vendor offer a centralized knowledge base with information on system performance and security.
Global Availability and Support	The IDaaS provider offers worldwide service and support.	1. Is the solution globally available with support for multiple languages? 2. Does the vendor offer 24X7 support in multiple languages?
Admin and Developer Resources	IDaaS providers often become an integral component of many IT processes. Be sure your IDaaS vendor offers the APIs, documentation and support resources necessary to tie your IDaaS solution into the rest of your IT ecosystem and process.	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 vendor offer developer resources and documented APIs to simplify integration with existing IT infrastructure and tools? 3. Are logs exportable to third-party SIEM tools for alerting and reporting?
Analyst and Peer Recognition	Look for an IDaaS vendor recommended by industry experts and peers.	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 Privileged Access Management. 3. Is the vendor rated highly on peer review sites like Gartner Peer Insights?

Summary

The Right IDaaS Solution

Choosing the right IDaaS solution with the right capabilities is a first step toward achieving Zero Trust Security and dramatically improving your organization's security posture. Some key capabilities to consider when evaluating IDaaS vendors are listed below.

IDaaS Solution Must-Haves

- Provide a consistent and non-intrusive user experience for all users, across devices
- Offer self-service capabilities, including resetting passwords, unlocking accounts, and self-provisioning of apps
- Provide a unified administrative console for securing all applications and endpoints, whether on-premises, or mobile, or in the cloud.
- Be intuitive and flexible to help administrators address organization-specific requirements
- Delivered on highly available, redundant and fault-tolerant systems to ensure continuous service availability
- Support privileged access management to provide end-to-end identity security across your organization.

The CyberArk Identity Security Platform enforces least privilege and enables access across any device, anywhere, at just the right time. Architected for the Modern Enterprise, CyberArk is built on a foundation of Privileged Access Management and powered by Artificial Intelligence-based behavior and risk analytics. CyberArk is an Identity Security innovator with proven expertise in securing all types of identities while delivering continuous protection for any identity – human or machine. With CyberArk as a trusted partner, organizations secure access to critical business applications and infrastructure, support a distributed workforce, accelerate business in the cloud, and drive trusted customer experiences.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S., 03.21 Doc. 145608

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CYBERARK®

Connection
we solve IT

1.800.800.0014
www.connection.com/CyberArk