CYBERARK®

BUYER'S GUIDE

Identity and Access Management Solutions for a Zero Trust Era

A guide for choosing modern solutions for SSO, MFA, lifecycle management, and app session security

Table of Contents

Introduction

As identity-related attacks become more sophisticated and costly, security and IT leaders are seeking new ways to combat constant breaches and threats. Cyber attackers regularly discover new access points into your network by studying and exploiting risky behaviors that are common among the workforce and by stealing credentials such as passwords. And with 61% of breaches involving credentials and 85% involving the human element, it's clear that Identity and Access Management (IAM) solutions are essential.[1]

But are your IAM solutions doing enough to protect your organization?

Enterprises with IAM solutions in place may be lured into a false sense of security, believing their solution is equipped to outpace the innovation of bad actors. In many cases, security decision makers are well aware of gaps in their solutions capabilities. But the idea of starting over with a new vendor is daunting. As organizations shift en masse to work-from-anywhere models — amid unprecedented levels of workforce turnover — IT and security leaders need a framework for vetting IAM vendors' solutions to meet their needs.

For example, a vendor may say their solution is "AI-powered." But what does that mean? Armed with the right information, you can determine whether a vendor has baseline AI or contextually aware solutions that convert data on user behavior, risks and threats into automated decisions. As an IAM solution buyer or an influential part of the buying process, asking the right questions will help you keep up with rapidly evolving threats such as sophisticated social engineering attacks.

Are your IAM solutions doing enough?

61%

of breaches involve credentials

85%

involve the human element[1]

While single sign-on (SSO) and multifactor authentication (MFA) are foundational, must-have tools in the battle against cyber crime, today's Identity Security challenges call for next-generation approaches to these mainstays. And in some cases, the relentless innovation of today's attackers calls for solutions that employ not only the principals of IAM but also Privileged Access Management (PAM).

This guide will help you vet advanced, intelligent IAM solutions — including the essential features, functions and additional data protection tools — that will empower your team to keep your systems secure, while running your daily operations at peak efficiency.

[1] Verizon. "2021 Data Breach Investigations Report."

Overview: Evaluating SSO and MFA solutions for Zero Trust security

A distributed workforce composed of on-the-go employees and on-demand service requires a refreshed perspective on Identity Security. That's why forward-looking organizations are turning to Zero Trust security architectures and cloud-based Identity-as-a-Service (IDaaS) solutions to meet their evolving cybersecurity challenges.

Trusted internal networks and untrusted external networks are things of the past. In a Zero Trust security model, users across any location or endpoint are instantly authenticated, authorized and secured the moment they establish a session. This real-time authentication architecture is a boon for disparate teams, but the Zero-Trust approach still poses problems for provisioning and deprovisioning access in practice. As users adopt new roles within the organization, managing their access becomes an ongoing headache when access control is heavily enforced.

AI and machine learning offer new ways to manage access without demanding manual processes or irritating your end-users. By developing awareness of user-specific context and risk, these capabilities help organizations mitigate prospective threats and trigger access policies based on individual use patterns assessed by integrated behavioral analytics tools. Intelligently assigning risk to each access event based on historical patterns allows organizations to streamline the way their employees access their essential systems without compromising a Zero Trust environment.

88% of businesses say adopting more of a Zero Trust approach is a top priority in 2021.[2]

[2] CyberArk. "The CISO View 2021 Survey: Zero Trust and Privileged Access." 2021

1 SSO

The must-have features

Defining and customizing access for every user across the organization demands substantial time and resources, but it often seems like a necessary evil in most security environments. That's why one of the most essential aspects of a modern SSO solution is contextual access management.

Your team can benefit from deeper insight into when, why and how users request access to an app or system. While security tools like virtual private networks (VPNs) strive to give blanket access to authorized users, VPNs offer limited insight into who is accessing your information and why. Contextual access management — combined with real-time access intelligence and behavioral analytics — allows your team dynamic control over who accesses what, without needing to manually monitor individual access patterns.

VPN-less access to legacy apps is safe and possible by replacing hard-to-manage access lists with robust, secure directory services. With perspective on how your workforce uses your technology, your team can use dynamically controlled access to optimize the employee experience and reduce the need for the end-user to constantly re-verify their identity with multiple sets of weak credentials.

Naturally, simple access with a single set of strong credentials, protected by integrated MFA, is the bare minimum for any modern SSO solution. But alongside these essential features, there are some key capabilities that set exceptional SSO solutions apart.

613.6 million passwords have been exposed by data breaches.[3]

[3] Have I Been Pwned service, 2021.

About Zero Trust

Zero Trust works on the assumption that no identity can be trusted until verified. Traditional approaches centered on establishing a strong perimeter to keep the "bad guys" out no longer work. Resources (data, applications, infrastructure and devices) are increasingly hybrid or located outside of this perimeter entirely. Zero Trust is a holistic, strategic approach to security that ensures that everyone and every device granted access is who and what they say they are.

Single Sign-on (SSO) Checklist

KEY CAPABILITIES TO LOOK FOR	ASK YOUR VENDOR
✓ Secure Gateway replaces VPNs and allows users to use single credentials for all applications.	Can your solution provide easy sign on across cloud, mobile and legacy apps?
✓ A secure and frictionless sign-in experience for both internal and external users that adjusts based on risk.	How does your solution improve worker productivity?
✓ AI-equipped adaptive access allows users to sign in quickly based on behavioral data.	How does your tool leverage and present AI insights and behavioral pattern analytics?
✓ Contextual access management helps IT teams easily assign and revoke permissions.	How easily is access assigned or revoked based on policies?
✓ Real-time access intelligence allows teams to track security threats automatically.	Does your tool offer automation to assist in managing access and identifying security threats?

Key capabilities of an advanced SSO solution

Truly effective SSO solutions make it easier for your organization's employees to access the resources they need without presenting new security risks.

One-click access to enterprise applications through a centralized identity directory is a peak capability for high-quality SSO technology. In addition, leveraging an app gateway instead of a VPN can allow users to access traditional web applications with the same process and credentials as cloud or mobile-based apps.

By learning user habits through behavioral analytics, AI-equipped adaptive access allows employees to sign in faster to cloud, mobile and legacy apps, based on the SSO solution's knowledge of their historical data and perceived risk. When combined, capabilities like these offer an exceptional user experience, while strengthening security and reducing risk.

The ability to store federated identities across any combination of on-premises and cloud-based directories is a must, as well. Through user behavior analytics, organizations can strengthen federated identities to provide quick, reliable access for both internal and external users, no matter where they are and what devices they're using. Solutions that apply insights on human behavior toward automated decision-making can enable organizations to easily manage access requests and block suspicious activity, too.

Read on, to learn how integrating a multifactor authentication solution with SSO capabilities can enable a more powerful, adaptive form of Identity Security.

2 MFA

The must-have features

Compromised credentials are not only a common — but also costly — security risk: the average cost of a data breach reached $4.24 million per incident in 2021, the highest in 17 years.[4] For an SSO solution to be viable in 2022 and beyond, it should be integrated with a multifactor authentication (MFA) solution that can adapt how it authenticates based on real-time insights about users and risks, while offering a wide range of authentication methods to verify a user's identity.

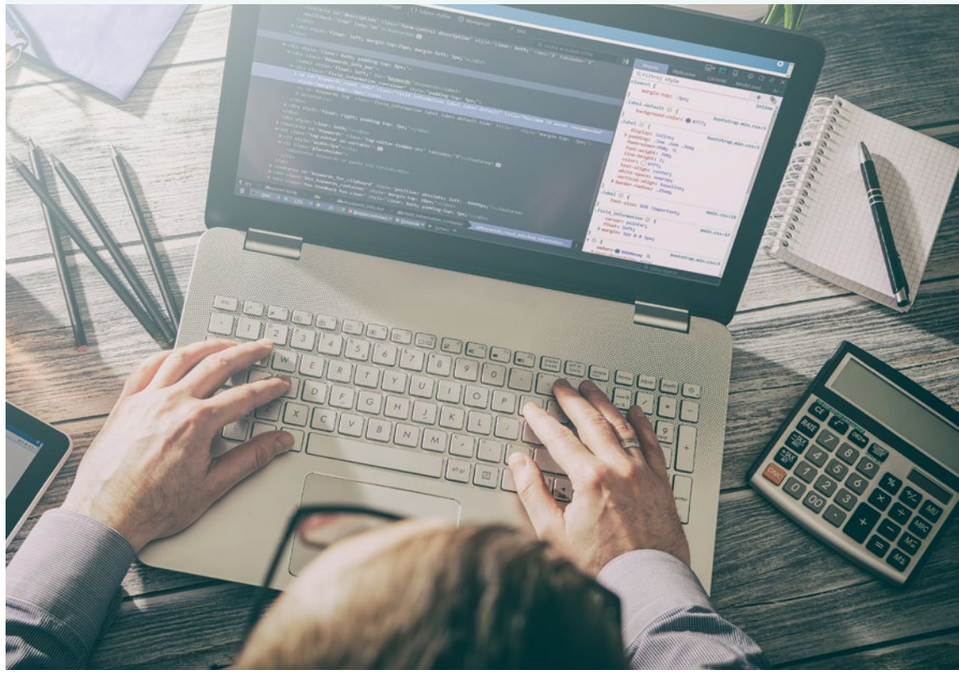
A modern MFA solution must be able to analyze and apply contextual information to adjust how it protects against credential theft and misuse, without creating barriers to user workflows. Therefore, any MFA worth considering should offer the ability to combine customizable risk-based policies with intelligent capabilities that "know" whether a user is seeking access within a context that is typical or anomalous to their identity. MFA solutions should also give users a range of options for verifying their identities through multiple authentication methods. This empowers the seamless nature of SSO with the added security necessary in a Zero Trust environment, giving IT and security teams the ability to prevent attackers from exploiting compromised credentials — and limit the impact following a breach.

MFA solutions with adaptive, modern capabilities can help organizations increase the likelihood that users will adopt and comply with security policies. Therefore, the most effective MFA solutions for today's challenges should be vetted against the following capabilities to empower users with a streamlined and secure user experience (UX).

97%

of security leaders say credential theft attempts are on the rise.

Source: CyberArk's CISO View 2021 Survey



[4] IBM, Ponemon Institute. "Cost of a Data Breach Report." 2021

Multifactor Authentication (MFA) Checklist

KEY CAPABILITIES TO LOOK FOR	ASK YOUR VENDOR
✓ Leverages user behavior analytics to identify irregular user activity and automatically trigger access policies the organization can predefine.	Does your solution use behavioral analytics to assess whether individual users across your organization are attempting access in contexts that are typical or unusual?
✓ Adjusts authentication methods dynamically based on insights gained from user context.	Does your solution dynamically change authentication type, based on factors such as device, IP address, location, time and more?
✓ Offers a UX that provides a wide range of authentication methods, based on the shifting needs of today's distributed workforce.	What authentication options do you offer, beyond the standard set? For example, do you offer QR code? And what if a user doesn't have access to a required authentication type?
✓ Able to secure everything from business applications and VPNs to workstations such as Mac, Windows and virtual desktops.	What does your MFA solution protect at the endpoint level, and how can it secure the wide range of locations and devices today's workforce entails

Key capabilities of an advanced MFA solution

For the best MFA solutions, context — and the ability to use it — is key. Strong MFA solutions use behavioral analytics to gain insights from tracked user activity and then generate user-specific context and risk assessments. By creating a baseline for typical user behavior, AI-enabled MFA solutions readily identify irregular behavior and trigger access policies to combat threats. Assessing risk levels through easy tracking and visualization on a user-level significantly improves forensics and responses, facilitating stronger overall protection with virtually zero IT intervention.

A high-quality MFA solution should also be able to apply behavioral insights toward determining which authentication factors are relevant and necessary for a given situation. This is where context comes into play: MFA solutions must be able to continuously monitor, learn and apply contextual data such as location, time-of-day, IP address and device type.

With a deep understanding of how and when users access your organizations' systems, applications and information, intelligent MFA solutions can automatically present the right authentication methods for a particular user in a specific situation. With multiple methods to choose from — such as mobile push notifications, SMS messages, biometric data, and QR codes — teams can provide employees ways to verify their identity that aren't cumbersome or inconvenient.

These robust MFA and SSO capabilities can form the foundation of an IAM solution that will take your security to the next level. However, to realize the true value of a Zero Trust architecture, organizations must complement SSO and MFA with two critical components:

- Capabilities for managing identities across the entire employee lifecycle
- Capabilities for ensuring employees' web application sessions are secure

Above and beyond: Managing identity lifecycles and securing users' web sessions

Delivering on the intention of Zero Trust security involves covering all your organizations' Identity Security vulnerabilities, including managing personnel changes and reducing user error. Adding lifecycle management (LCM) and web application session monitoring to your security posture can provide another (and more granular) layer or protection your enterprise needs to cover your bases.

3 Lifecycle management

Managing the people entering and exiting your enterprise requires substantial IT and HR resources, often leading to delays in getting users the access they need to effectively do their work. Employing a lifecycle management solution makes it easier to define and enforce each user's unique role, responsibilities and access privileges.

Seamless importing from your HR applications to a central location is key to enable timely provisioning and deprovisioning of permissions. With the ability to federate identities across cloud and on-premises applications and systems, your team could avoid needing days or weeks to provide users access when they need it — or revoke that access when users leave.

1 in 4

workers resigned from a job in 2021.[5]

[5] Visier. "Visier Insights Report: Stop the Exit." 2021.

$4.61 million

Average total cost of a malicious insider attack, when an initial attack vector.[6]

87%

Security leaders who say reducing standing privileges is an “important” or “very important” aspect of Zero Trust[7]

Ensuring employees have the right permissions is essential to keep your business secure, especially as employee turnover reaches record highs. Strained onboarding and offboarding processes call for automation-driven support to maintain appropriate access for the right users. Otherwise, new employees without access to the right tools may resort to risky behavior such as password workarounds to complete their work, while dissatisfied former employees with unchecked, lingering access can pose a form of insider threat to your organization.

Lifecycle management allows you to design configurable provisioning workflows and automatically adjust access to corporate resources based on role changes. This makes sure your employees, contractors, customers and partners always have access to the information they need, even if their status or position changes.

In addition, lifecycle management tools can offer insight into app usage, failed login attempts and unused accounts, making managing accounts and entitlements easier than ever. With this technology, your organization can quickly identify breach attempts and eliminate old accounts to create a more powerful security posture. Out-of-the-box reporting with lifecycle management is just one way to reduce Identity Security blind spots. Reviewing these insights in tandem with a continuous record of users’ protected web sessions can offer the transparency and your organization needs.

[6] IBM, Ponemon Institute. “Cost of a Data Breach Report.” 2021
[7] CyberArk. “The CISO View 2021 Survey: Zero Trust and Privileged Access.” 2021.

Lifecycle Management Checklist

KEY CAPABILITIES TO LOOK FOR	ASK YOUR VENDOR
✓ Seamless importing from your HR applications to a central location.	Does your solution integrate with common HR solutions?
✓ Automated onboarding and offboarding capabilities simplify provisioning and deprovisioning of user access.	What automation capabilities does your tool offer for user and access management?
✓ Out-of-the-box reporting gives insights into app usage, failed login attempts and unused accounts.	How does your solution leverage behavior analytics to simplify access management?
✓ Customizable configurable provisioning workflows help security, IT, and HR teams collaborate.	What type of provisioning workflows can I design using your tool?

4 Secure web application sessions

Without insight into how your users actually use a particular app or system, you could expose your enterprise to risks ranging from unforeseen malicious activity to honest mistakes with grave consequences. Securing your users' web application sessions is a vital addition to your Identity Security toolkit. These capabilities can help you eliminate unseen vulnerabilities and provide valuable insight into how employees use systems containing your most sensitive data, like financial reports, customer information and intellectual property.

Here are some examples of why securing web application activity is so critical:

- Continuous monitoring and auditing capabilities can allow security professionals to retrace and analyze every click from users' access to business applications. By eliminating the need to manually comb through data logs, organizations can quickly recognize and address potential security issues.
- Employee mistakes, like stepping away from a computer in the middle of a high-risk session without locking it, can provide an easy target for attackers. Organizations can reduce human error when their protected web application sessions require reauthentication anytime the user walks away.
- App sessions involving sensitive data can result in risky behaviors, such as exporting information considered secret or confidential. A secured session can reduce risk at the endpoint by refusing file transfers and restricting users from copying information.

The traditional perimeter has dissolved and is now embedded into every identity — human and machine — across the organization. So, if an everyday employee has access to a business application that essentially provides a gateway to sensitive resources, that employee's identity becomes high value and/or high risk.

By empowering your team to capture, search and audit all activity, your enterprise can prevent endpoint-originated threats that could lead to unauthorized data disclosure and system downtime. Keeping web sessions secure protects against user error and ensures users access systems in protected environments, preventing malicious actions and threats across your endpoints and applications.

By the numbers: The critical need for securing web sessions

>10

number of business applications to which **the average end user** has access

>80%

of organizations report employee **abuse or misuse** of business app access in the past 12 months

Yet Nearly ½

lack visibility into user logs and activity, making it difficult to pinpoint risky behavior

Greater visibility into web app user activiy would help

41%

of organizations identify the **source of security incidents faster**

54%

of organizations investigate user activity stemming from security incidents or compliance **at least weekly**

Censuswide survey of 900 security decision makers and leaders at medium to enterprise-sized organizations in the United States, United Kingdom, France, Germany, Australia and Singapore (commissioned by CyberArk)

Securing Users' Web Sessions Checklist

KEY CAPABILITIES TO LOOK FOR	ASK YOUR VENDOR
✓ Monitoring features helps reduce human error by tracking user behavior.	What information will I receive on my user's web or application sessions?
✓ Full audits of every click give IT teams full visibility into security practices during web and application sessions.	How can I leverage your tool to audit employee usage and reduce potential risky behavior?
✓ Vulnerability coverage to reduce data disclosure and system downtime.	How do you address unforeseen vulnerabilities or visibility gaps from my existing cybersecurity tools?
✓ File transfer refusal and restricted access to copyright information.	What applications and resources can you protect?

Final thoughts: Designing the strongest possible IAM solution for your organization

Identity and Access Management solutions are critical to protect your company against breaches and attacks. As attackers become more sophisticated and leverage human behavior to gain unauthorized access, it's more important than ever that your business has an edge over potential threats.

Features such as AI, machine learning and automation are no longer nice-to-have — but just because they've become more prevalent across vendors doesn't mean all IAM capabilities are equally intelligent. Organizations need to ask more of their solutions' data-informed features. It's what the IAM solution does with the data that determines whether it can protect their systems, resources and employees from attacks. Similarly, in a Zero Trust era, IT and security leaders can go above and beyond authenticating, authorizing and securing identities the moment they establish a session. By asking more of an IAM solution, you can discover capabilities that enable you to see, understand and protect what's taking place within a session.

Even if you already have an IAM solution in place, now is the time to ask more and vet the full range of solutions to strengthen your organization's security posture.

We hope you've found this buyer's guide useful as you evaluate Identity and Access Management vendors and solutions to meet your organization's unique needs.

Learn more about Identity and Access Management solutions from CyberArk.

LEARN MORE

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

U.S., 02.22 Doc: WRQ-176

CYBERARK®