CYBERARK®
The Identity Security Company

EBOOK

2023 Buyers Guide: How to Vet Identity and Access Management Solutions

Table of Contents

Introduction

The pressure is on.

Ninety-seven percent of CISOs have gotten the call to present to their boards in the next 12 months.[1] Chances are, many of these discussions will cover issues around rising threats and the need for new cybersecurity tools and resources.

Decision-makers across IT and security are facing increased scrutiny from their boards and senior leaders over cybersecurity preparedness. But do these stakeholders — who often play a key role in influencing or approving cybersecurity investment — see how challenging your job has become?

Teams like yours are relied upon to protect the enterprise at a time when everything seems to be surging in concert and complexity:

- The size, hybrid model and churn of your organization
- The number of applications, and in turn credentials, your users need
- The scope of sensitive resources your users can access
- The frequency of attacks beginning with compromised identities

You might be a CIO or CISO preparing to make the case for investing in new solutions. You might be an IT or security team member who's researching vendors. Either way, you could use some unbiased advice on how to vet solutions that can strengthen your organization's security posture.

That's exactly what this eBook covers.

[1] "CISO: Communications Redefined - Navigating the Journey from Control Room to Board Room," FTI Consulting, 2022

We're providing you with vendor-agnostic recommendations and checklists for several types of solutions across two key categories: Identity Management and Access Management. You'll also find viewpoints on why these two categories of solutions can be most effective when integrated into a unified platform.

Why is this guide worth your time?

The advice you'll get is rooted in specific day-to-day challenges our own customers share with us.

For example, we know you're under pressure to prevent breaches in a time of rising stress, longer hours and resource gaps. We also know your team can perform better if it's not bogged down in manual tasks — like combing through data logs for a security event's cause or building workflows from scratch with code.

Read on for insights on how to find solutions designed to solve for these challenges, as well as the bigger picture: ensuring measurable risk reduction and enabling your increasingly digital, cloud-based business.

How to Vet Identity Management Solutions

Identity Management solutions can weave every aspect of your security coverage together. In this category, it's important to look for products with a security-first design that can automate and simplify often-cumbersome processes associated with:

- Onboarding and offboarding users
- Assigning and managing access rights
- Monitoring and tracking access activity

Your team is on point to ensure only the right people have the right access to the exact corporate resources they need to do their jobs — and only for the time needed. This is true for your workforce, as well as for your partners, clients and vendors. But a variety of factors, from heightened regulation to economic trends, are making identity management more complex.

On any given day, IT and security teams may be:

- Provisioning, adjusting and removing access amid record levels of workforce churn
- Building identity workflows from scratch amid a shortage of workers with coding skills
- Manually managing processes for provisioning access as hours, stress and threats rise
- Providing dependable reporting for audits, as global regulations increase

When it comes to administration and governance of the identity lifecycle, many enterprises have reached a point of unwieldiness. Automated controls and processes can help, especially within an orchestrated framework that covers all types of identities. This approach can make the job of identity management sustainable and help your organization be resilient against risks.

In this section, we'll discuss three types of Identity Management solutions and how to vet them:

1. **Identity lifecycle management**
2. **Identity workflow automation**
3. **Identity compliance capabilities**

1 Identity Lifecycle Management

Managing the people entering and exiting your enterprise, let alone securing the data accessible through their credentials, requires substantial resources from already stretched IT and security teams. Syncing identity data to and from the applications your organization uses is key to enabling timely provisioning and deprovisioning of permissions. Automation can make the job viable.

Lifecycle management solutions can make it easier to define and enforce each user's unique role, responsibilities and access privileges — whether they are joining or leaving your organization. With the ability to federate identities across cloud and on-premises applications and systems, your team can quickly provide access when users need it — or revoke that access when they leave.

Security-first lifecycle management tools should offer insight into app usage, failed login attempts and unused accounts, making managing accounts and entitlements more secure. With the right technology, your organization can quickly identify breach attempts and eliminate old accounts to create a more powerful security posture.

Lifecycle Management Checklist

Look for these capabilities:	Ask your vendor:
✓ Provides seamless integration with HR applications and other repositories	✓ Does your solution provide both inbound and outbound provisioning to and from any publicly accessible HR system?
✓ Automates onboarding and offboarding capabilities to simplify provisioning and deprovisioning of user access	✓ What automation capabilities does your tool offer for user and access management?
✓ Includes out-of-the-box reporting with insights into app usage, failed login attempts, unused accounts and more	✓ How does your solution leverage user behavior analytics to simplify access while enhancing security?
✓ Leverages customizable no-code provisioning workflows to automate manual processes and help security, IT and HR teams collaborate	

Two-thirds (68%) of security decision-makers say the accelerated rate of employee turnover has led to a spike in security issues over the past 12 months.[2] A key example: failure to deprovision users' access rights.

[2] "Identity Security Threat Landscape Report," CyberArk, 2022

2 Identity Workflow Automation

IT and security teams are increasingly bogged down, manually connecting the dots between variables such as applications, data, events, provisioning and services. As a result, many organizations are dealing with:

- Hindered IT service agility
- Squandered resources
- Heightened risk and vulnerability to attacks

Consider the bandwidth lost to inefficiencies when it's time to track or reassign user privileges across disparate apps and systems. And think about the consequences of missed action steps — such as shutting off a departing employee's access — due to delays, human error or manually coded workflows. Bad actors exploit mis-provisioned, overprivileged or orphaned accounts to launch attacks or steal data.

In concert with a lifecycle management solution, it's important to have automated capabilities for:

- Designing configurable provisioning workflows
- Adjusting access to resources based on events such as role changes or security incidents

This approach can help ensure users have access to the resources they need, even if their status or position changes – while keeping attackers out.

Identity Workflow Management Checklist

Look for these capabilities:	Ask your vendor:
✓ Enables integration with any publicly available applications	✓ What type of provisioning workflows can I design using your tool, and can these be created by anyone in the company, without requiring heavy scripting or specialized skills?
✓ Centers on an easy-to-use, no-code interface so that citizen integrators and other non-developer personas can build and execute workflows	✓ Does your solution have prebuilt connectors to applications that are searchable?
✓ Includes workflow steps for notifying users about newly granted access and permissions	✓ Can I use this solution to limit access within applications for certain users?
✓ Allows security teams to build and customize workflows for identifying risky actions, notifying admins and taking automated actions (e.g., removing access)	✓ How can I ensure that threat data informs my workflows in case of risky events or suspicious behavior?
✓ Makes it possible to gather and transform data, both structured and non-structured	

Workflow automation can help organizations orchestrate responses to security incidents, by automatically adjusting access privileges or changing roles for a given user — based on factors such as risky activity or external threat intelligence data.

3 Identity Compliance Capabilities

In addition to protecting the organization and ensuring users have secure access to the resources they need, there's a decent chance your team is also relied upon to:

- Ensure transparency for internal security reviews
- Meet complex and continuously multiplying industry and government regulations
- Satisfy audit and compliance needs

And yet ensuring and demonstrating compliance with data and cybersecurity regulations is a struggle for many IT and security teams. It seems like rules, reporting requirements and penalties are proliferating as fast as the identities you need to protect.

With reputation and trust on the line, it's important to look for Identity Management solutions that include strong compliance capabilities. This includes a simple, unified view of who has access to what information — and functionalities for discovering, reviewing, adjusting and certifying access privileges.

Here's how to vet Identity Management solutions for these essential, security-first capabilities.

Identity Compliance Checklist

Look for these capabilities:	Ask your vendor:
✓ Integration with the rest of your security stack, including PAM solutions	✓ Do you offer audit reports and dashboards to help identify potential compliance issues?
✓ Ability to audit and certify access rights to not only applications but roles and privileged access	✓ How can I use your tool to set up reminders to certifiers to review access for their users?
✓ Strong analytics and reporting capabilities for auditors	✓ What kind of contextual data is provided to certifiers to help inform their decisions?
✓ Enables certifiers with risk data, as well as dual controls for added checks and balances	✓ Can I use your tool to certify access for a set of users in bulk?
✓ Automation of access review and certification cycles	✓ Can I use your tool to certify cloud entitlements?
✓ Detailed audit trails and reporting for demonstrating compliance and streamlining audits	

156

countries (80% of the world) have enacted cybercrime legislation.[3]

130+

global jurisdictions have enacted data privacy laws.[4]

Only 9%

of executives are highly confident they can effectively meet all disclosure requirements.[5]

[3] "Cybercrime Legislation Worldwide," United Nations Conference on Trade and Development, 2022
[4] "A Look Ahead at New Data Privacy Regulations: How Do They Compare to ISO/IEC 27701?" ISACA, 2022
[5] "Global Digital Trust Insights Survey," PWC, 2022

How to Vet Access Management Solutions

From third-party vendors and hybrid workforces to DevOps teams and their automated workflows, the universe of identities accessing your organizations' sensitive resources keeps expanding. Layer by layer, the entry points and internal pathways used by these identities contain a range of vulnerabilities. What's worse, they're often guarded by poorly secured credentials that bad actors can easily compromise.

Some of the four solution types we'll cover in this section are mainstays in the Access field; others you might associate with a different security category: Privileged Access Management. We're including PAM-inspired capabilities in our vetting criteria for a reason. In an era when any user can become privileged, depending on what resources they've gained access to, it's essential to apply privilege controls across the board.

Four types of Access Management solutions can help you secure the digital identities that are driving your organization's most important initiatives:

1. **Intelligent SSO**
2. **An adaptive form of MFA**
3. **Enterprise-grade password management**
4. **Secure web application sessions**

Here are recommendations on the capabilities a solution should offer, so you can protect all types of identities with the same degree of fierceness.

1 Intelligent Single Sign-On (SSO)

Covering the dual priorities of network security and user experience, SSO is table stakes. Rather than requiring users to remember myriad login credentials for every application they need, SSO solutions can allow users to access what they need quickly, reliably and securely.

But despite the table stakes status, not all SSO tools are the same.

A key example: many legacy SSO tools can streamline access to applications but lack the ability to escalate controls if log-in behavior shows signs of foul play. In contrast, modern SSO can employ behavioral analytics to assess risk and then streamline access for legitimate users — or keep would-be attackers out.

Here's what to keep in mind as you vet SSO solutions:

.

Single Sign-on (SSO) Checklist

Look for these capabilities:	Ask your vendor:
✓ Provide secure access to all applications and IT services via a single set of user credentials	✓ Can your solution provide easy sign on across cloud, mobile and legacy apps?
✓ Federate identities across on-premises and cloud-based directories using any combination of directories	✓ How does your solution help create a balance of securing identities across your workforce and enabling worker productivity?
✓ Use AI, machine learning and user behavior analytics to identify and assess risk and take action	✓ How does your tool leverage and present AI insights and behavioral pattern analytics?
✓ VPN-less access to legacy apps via secure gateway functionality with uniform control policies	✓ How easily is access assigned or revoked based on policies?

2 Adaptive Multifactor Authentication (MFA)

Working in coordination with SSO, MFA solutions can strengthen an organization's security posture through additional checks to validate identities in multiple layers. But there's a big difference between legacy approaches to MFA and what's needed to protect the enterprise.

You may be accustomed to an MFA experience entailing a simple SMS and/or email verification when using consumer apps. This approach isn't workable for large, complex enterprises that need to protect employees, vendors, partners and clients.

The next wave of MFA solutions offers users a range of options for verifying identities depending on levels of access, privilege and risk.

An adaptive MFA solution can learn from a user's history of access habits — and be able to discern typical behavior from risky activity. This allows the solution ramp up or streamline authentication challenges based on real-time insights.

The flexibility of this adaptive form of MFA provides a balance that takes care of job #1: protection. But it also prevents your enhanced security measures from having a detrimental impact on user experience.

Here are vetting criteria to help you confirm which vendors offer modern MFA approaches.

Multifactor Authentication (MFA) Checklist

Look for these capabilities:	Ask your vendor:
✓ Offers a wide range of authentication methods to meet users' needs and security standards, such as National Institute of Standards and Technology (NIST) authenticator assurance levels	✓ Does your solution use behavioral analytics to assess whether individual users across your organization are attempting access in contexts that are typical or unusual?
✓ Leverages user behavior analytics to identify irregular user activity and automatically trigger policies the organization can predefine	✓ Does your solution dynamically change authentication type, based on factors that indicate low-risk and high-risk logins such as device, IP address, location, time, log-in errors and more?
✓ Adjusts authentication methods dynamically based on real-time insights on a wide range of attributes, such as location, time of day and IP address	✓ 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 applications, workstations, virtual desktops, VPNs and more	

More than two-thirds (67%) of security leaders use MFAs only offering a basic two-factor approach.[6]

The risk? The authentication factors required may have nothing to do with a given user's risk profile or log-in scenario. This can slow down users when added security is not needed, leading to risky workarounds.

[6] CyberArk/Gatepoint Research (survey of 100 security leaders), 2022

3 Password Management Solutions

Eighty-two percent of breaches involve the “human element.” And what’s more human than how users store, access and share passwords? To reduce users’ reliance on passwords, many organizations turn to SSO. As we’ve discussed, SSO provides a foundational layer of protection for your workforce’s credentials. The problem is, many applications don’t support SSO or use modern identity protocols.

As a result, users turn to browser-based password managers and consumer-grade password manager tools. These options may be viable for start-ups and small businesses with low headcounts. But they aren’t designed to secure enterprises with large hybrid workforces and an ever-growing number of identities.

In contrast, an enterprise-focused password manager can provide visibility and control for security teams, while keeping your employees safe and productive. The key step is, once again, taking controls usually reserved for privileged users and applying them to the workforce at large.

For example, employing secure vault storage, where password-based credentials are encrypted end to end. Or password-sharing features that let managers limit how long a team member can use credentials.

Password protection for the enterprise should include the following:

Enterprise-Grade Password Management Checklist

Look for these capabilities:	Ask your vendor:
✓ Captures, stores and autofills passwords for virtually any publicly available application	✓ Where exactly do you store users’ passwords, and how do you ensure privacy?
✓ Retrieves passwords via just-in-time principles, never storing them locally on endpoints	✓ Can your solution secure and store other text-based items, such as license keys?
✓ Autogenerates strong, secure, unique passwords that are readily available for future logins	✓ To what extent can you protect the sharing of passwords among users? For example, can you control whether the recipient can view a password if you want it hidden?
✓ Dashboard-based reporting on user activity for internal analysis and for auditing	✓ Do you offer controls for preventing use of browsers’ built-in password managers?
✓ Integration with an adaptive form of MFA for added credential security	

4 Web Session Security Solutions

Security controls must continue past the point of authentication and build upon password security. Enterprises require an extra layer of protection that allows them to monitor and record all actions taking place once a user is logged in — backed up by a full audit trail.

And yet, nearly half (48%) of organizations have a limited ability to view data logs and audit user activity.[7] This keeps them in the dark about potentially risky actions taken in web application sessions. Security teams need to know what's happening within applications from end to end and whether any of those behaviors raise red flags (such as changing, copying or downloading data).

As with the enterprise-grade approach to password management, this type of solution applies the same controls used for privileged users' sessions to the web app sessions of everyday employees.

Securing Users' Web Sessions Checklist

Look for these capabilities:	Ask your vendor:
✓ Provide continuous monitoring of user sessions in web-based applications without interfering with user experience	✓ How can I leverage your tool to audit employee usage and reduce potential risky behavior?
✓ Offer full step-by-step recordings and audits of every click to give IT teams full visibility into user activity in high-risk apps	✓ How do you address unforeseen vulnerabilities or visibility gaps from my existing tools?
✓ Enable file transfer refusal and restricted access to copyright information	✓ What information will I receive on my user's web or application sessions?
✓ Integrate with MFA to reverify after periods of inactivity in a given session (e.g., if a user walks away from their workstation)	✓ What applications and resources can you protect?

[7] CyberArk, The Hidden Gap in Web Application Security: User Sessions

How to Approach the Bigger Picture: An Integrated Platform

Whether you're overhauling your solutions or looking to add or replace a few tools, it's essential to look at the big picture: how each solution you vet will integrate with everything in your cybersecurity solution stack.

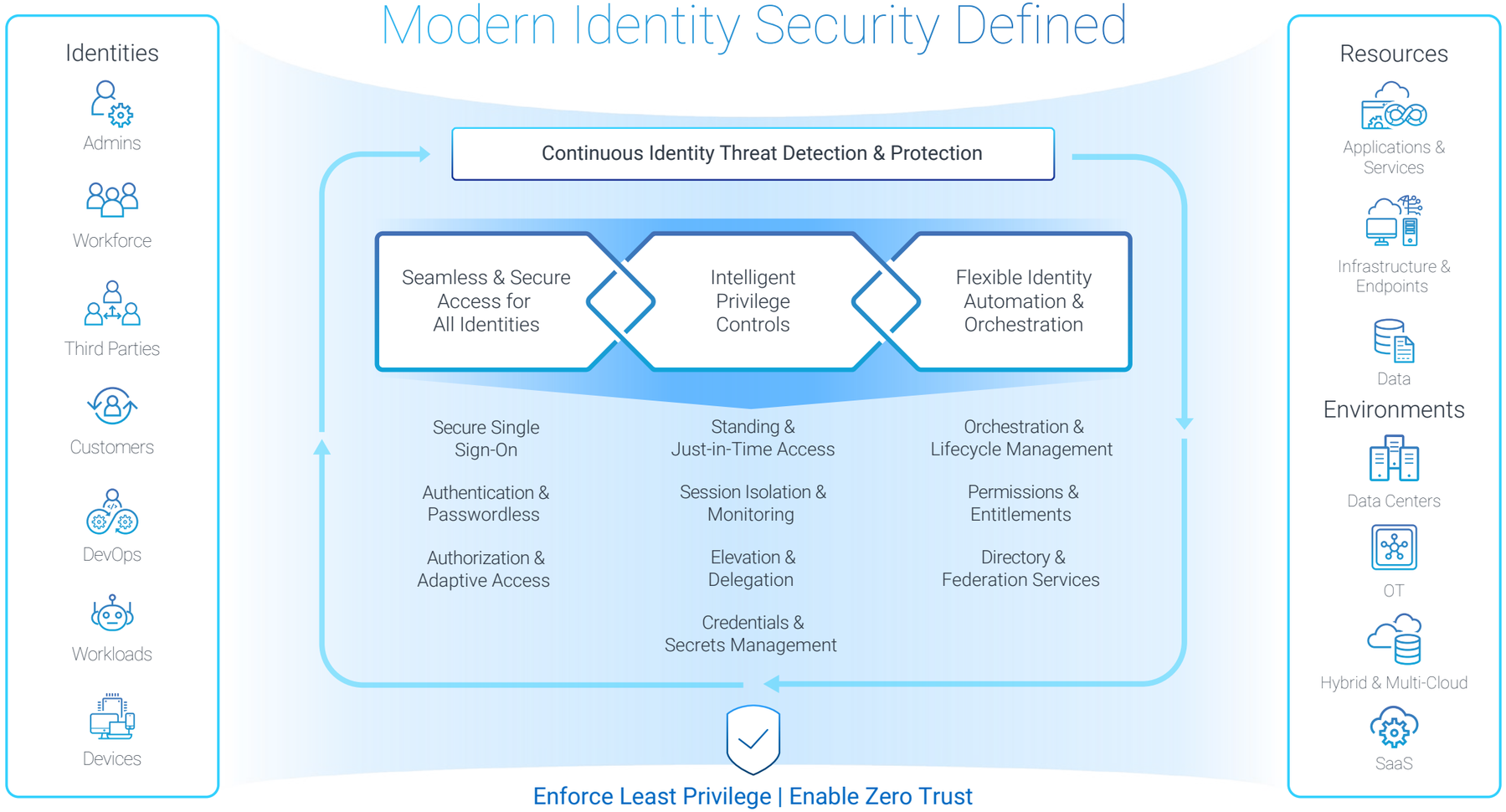
Many organizations are finding themselves in a situation in which their products were added together in piecemeal, out of urgency. In turn, these solutions are often siloed from each other. These challenges speak to the importance of building an integrated Identity Security model. This is an approach that brings together the controls found in key categories — such as Access Management and Identity Management — and allows them to complement one another.

A modern Identity Security model includes the following components:

1. **Seamless and secure access for all identities**
2. **Intelligent privilege controls**
3. **Flexible identity automation and orchestration**
4. **Continuous threat detection and prevention**

CYBERARK®
The Identity Security Company

Modern Identity Security Defined



Enforce Least Privilege | Enable Zero Trust

Conclusion

Whether you're doing preliminary research on vendors who can meet your needs or you're about to enter the room where you'll advocate a new solution to the board, we hope this buyers guide is helpful to you.

Could your security architecture benefit from some of the capabilities described in this eBook? **Learn about** CyberArk solutions for Access Management and Identity Management.

If you'd like to learn more about how to adopt an Identity Security approach that infuses privilege controls across the board to protect every type of identity, visit our website.

VISIT NOW

Schedule a Meeting

If you'd like to meet with a CyberArk team member to discuss your organization's needs, you can reach out to us.

SCHEDULE A MEETING

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., 12.22 Doc. TSK-2673

CYBERARK®
The Identity Security Company