CYBERARK®

WHITEPAPER

The Problem with Password Managers:

Workforce Credentials Need Enterprise-Grade Protection

Table of Contents

Why Workforce Credentials Need Stronger Protection

You likely have security-first controls in place to protect the credentials of privileged users. But what about the credentials used by the rest of your organization? A system admin may hold the keys to your IT kingdom, but a Salesforce admin holds the keys to your customers' data. Attackers will gladly take both forms of credential — they're not so into labels these days.

In today's threat landscape, any user can become privileged in the right circumstances, based on the resources they've gained access to. Consider this: More than half (52%) of organizations' workforces have access to sensitive corporate data,[1] such as financial records, HR information and intellectual property. In many cases, employees access these resources through the applications they use to perform their jobs. In fact, the average worker accesses more than 30 apps and accounts.[2]

The problem: many of the apps used by your workforce do not leverage modern identity protocols. In these cases, the commonly used safeguards standing in between attackers and your sensitive resources are passwords, which are often:

- Easy to guess and not in keeping with password strength requirements
- Reused across corporate apps, personal apps and social media
- Stored unsafely in spreadsheets, sticky notes and web browsers
- Passed from one user to another through email, messaging apps and more

These lax password behaviors all fall into the "human element," which Verizon's 2022 Data Breach Investigations Report links to 82% of breaches. Attackers routinely exploit these practices to breach an organization's network and seek ways to heighten their access. From there, they work toward devastating outcomes, from mounting cyberattacks to stealing confidential data.

We've reached the point where all workforce users' passwords should be protected with the same security-first approach that organizations apply to privileged users' credentials. But many of the traditional tools enterprises often use can't enable this level of protection.

READ ON TO LEARN ABOUT:

- Trends in password-based threats
- Limitations of single sign-on and standard password managers
- Advice on five ways to not only manage but also secure workforce passwords

[1,2] Identity Security Threat Landscape Report, 2022, CyberArk

The Problem With Passwords (and traditional tools for managing them)

Your workforce relies on business applications to contribute to key enterprise goals. But the tediousness of signing into every app every time becomes a productivity blocker. Password fatigue is real. It's unrealistic to expect employees to memorize dozens of passwords and make sure they're complex enough to stump attackers. And in the face of obstacles, workers will seek shortcuts.

When frequently used business applications are accessed outside of an enterprise's security controls, organizations lack the ability to:

- Track access activity
- Control password complexity
- Revoke access to applications when no longer needed

Granted, many organizations are trying to educate their workforce users on ways to avoid unsafe password habits. But even when employees try to exercise a base level of protection — such as using a web-based app's built-in browser password manager — attackers can still find their credentials.

SSO is a start — but not the final answer

Single sign-on (SSO) is often a baseline safeguard for organizations looking to address password risks. SSO solutions can release users from the need for a VPN, with simplicity that prevents workers from being tempted to take shortcuts. However, many business apps do not use modern identity protocols and cannot integrate with SSO. In these cases, the user must authenticate using passwords that can be easily guessed, stolen or obtained through social engineering attacks like phishing.

PASSWORD RISKS SURGE AS WORKERS GAIN MORE ACCESS TO SENSITIVE RESOURCES

30%

increase in stolen credentials from 2017 to 2022.[3]

921

password attacks occur per second, a 74% increase from 2021.[4]

80%>

basic web application attacks attributed to stolen credentials.[5]

30

number of applications and accounts accessed by the average employee.[6]

52%>

organizations' workforces have access to sensitive corporate data.[7]

[3] Data Breach Investigations Report, 2022, Verizon
[4] Digital Defence Report, 2022, Microsoft
[5] Data Breach Investigations Report, 2022, Verizon
[6,7] Identity Security Threat Landscape Report, 2022, CyberArk

Can SSO be an effective part of a defense-in-depth strategy? Yes, when paired with other controls and solutions, such as an adaptive form of multi-factor authentication or MFA (more about that later). Its limitations, however, mean security professionals can't consider SSO the beginning *and* end of their protection plans.

… But a standard password manager is also inadequate

To bridge the gap caused by password risks, many companies turn to traditional password managers. These tools are often designed for consumer use, offering a streamlined way for individuals to generate and manage passwords. Rather than having to remember a distinct password for each app, users can memorize a single master password — with the tool taking care of the rest, behind the scenes.

The problem is that "the rest" often doesn't account for the complex security needs of a large enterprise.

Traditional password managers tend to lack controls and functionalities that enterprises need to secure end-user credentials that are constantly targeted by attackers. For example, many of these tools:

- Support only a minimal set of multifactor authentication options, which limits a security team's ability to increase log-in difficulty for would-be attackers
- Provide rudimentary logging and reporting functionality, which makes it difficult for administrators to audit user activity in any level of detail
- Still leave room for bad password habits — in some cases, users can still choose to save passwords in their web browsers, a key entryway for attackers to access critical systems and steal data

Read on to learn about five capabilities that can help organizations apply enterprise-grade protection to workforce credentials.

Traditional password managers might be able to help reduce password fatigue at small businesses and startups with low headcounts. But what happens when they're unable to scale to protect larger enterprises dealing with a rapid proliferation of apps, identities and workforce turnover?

Don't Just Manage Passwords — Protect Them

It used to be that organizations only needed to apply controls such as credential storage and protection to highly privileged IT users. But given the amount of sensitive data everyday employees can access, it's time to think outside of categories and silos. This means adopting a holistic, risk-based approach to Identity Security and applying privilege controls across the board.

Security teams looking to improve how they safeguard workforce credentials should explore these five capabilities:

1 | Intelligent authentication

2 | Security-first storage

3 | Safe credential management and sharing

4 | End-to-end visibility

5 | Frictionless user experience

Let's look at each of these factors in turn.

WHAT IS IDENTITY SECURITY?

Centered on intelligent privilege controls, Identity Security seamlessly secures access for all identities and flexibly automates the identity lifecycle with continuous threat detection and prevention — all with a unified approach.

LEARN MORE

1. Intelligent authentication

To prevent risky password behaviors, it's essential to blend intelligent authentication with an enhanced user experience. This calls for an adaptive form of MFA that can adjust the difficulty of authentication challenges based on real-time insights on user behavior. By distinguishing typical from atypical log-in activity, an adaptive MFA solution can use what it "sees" to make decisions such as:

- Requiring extra and/or more complex authentication challenges when risk is high
- Streamlining access with fewer and/or more convenient challenges when risk is low

To support a defense-in-depth strategy, organizations can use adaptive MFA as a complement to their SSO tools and apply it to various types of access — for example, endpoints, virtual desktops, Remote Desktop Protocol and more.

2. Security-first storage

Security teams should look for ways to introduce vault-based storage for workforce credentials, with the flexibility to decide how accounts and credentials are stored, managed and retrieved. For example, an enterprise-grade tool could provide a security admin with options to automatically store new credentials in self-hosted vaults and allow users to retrieve them without connecting to a VPN.

In addition, organizations can strengthen their defense-in-depth approach by applying MFA capabilities to the solutions they use for password protection. In this case, administrators could require users to pass secondary authentication challenges before accessing credentials for individual applications.

INCREASED COMPLEXITY CALLS FOR STRONGER CONTROLS FOR SHARING AND TRANSFERRING PASSWORDS

Risks multiply when multiple employees need to use the same set of credentials for accessing a single business application. This also increases the complexity of auditing users' access activity.

Additionally, if a user leaves an organization, valuable data could be lost if others cannot access their account to particular applications.

Companies need a simple way share access, transfer ownership of credentials and audit access activity.

3. Safe credential management and sharing

Security teams need visibility and control over who can access credentials and when. This allows users to securely share credentials without revealing passwords but also grants the ability to:

- Protect privacy by controlling who can share, view and edit credentials
- Impose time limits on user access to specific apps
- Manage the transfer of credential ownership to new users

In an era of increased workforce turnover, this level of control is essential. Two-thirds of security decision-makers say the accelerated rate of workforce turnover has created security issues, such as the failure to deprovision employee access rights.[8]

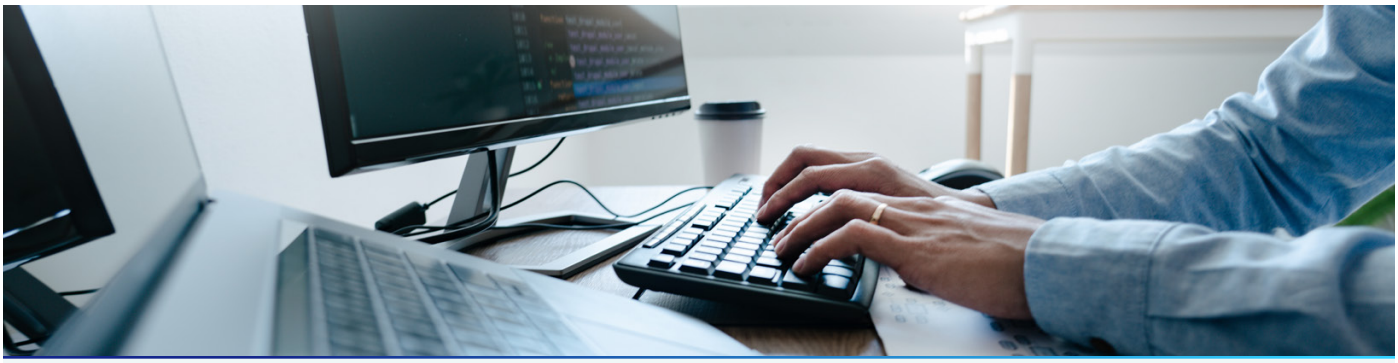
Enterprise-grade credential management and sharing lets admins transfer ownership automatically without losing the chain of custody when the primary owner leaves the organization. This approach can also help organizations onboard new users at scale without losing time or information.

4. End-to-end visibility

An enterprise-grade approach to password protection should provide real-time visibility into users' access activity. For example, security admins need the ability to determine which workforce users have accessed a specific application during a particular time – with easy-to-use reporting capabilities for auditing.

But what happens to visibility after a workforce user logs in? Security controls must continue past the point of authentication. Enterprises should look for ways to require an extra layer of protection that allows them to monitor and record all actions taking place once a user is logged in — also backed up by a full audit trail.

[8] Identity Security Threat Landscape Report, 2022, CyberArk



Nearly half (48%) of organizations have a limited ability to view data logs and audit user activity. This keeps them in the dark about potentially risky actions taken in web application sessions.[9]

Security teams need to know what's happening at and beyond the point of authentication, with the same level of controls and capabilities they apply toward monitoring, recording and protecting privileged users' access and sessions.

5. User experience

Eighty-six percent of security leaders believe that optimizing the user experience is important-to-very important for enabling Zero Trust success through Identity and Access Management tools.[10] Enterprises need an approach to managing and securing workforce passwords that can:

- Integrate easily with corporate directories and third-party identity providers
- Recognize when users are entering credentials and offer to save them in a secure, vault-based location
- Securely auto-fill credential fields for a smooth and quick log-in experience
- Generate unique and strong passwords for users whenever needed

These additional features will help reduce password fatigue and prevent workers from taking the kinds of shortcuts that can unwittingly create openings for bad actors to infiltrate your network.

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

[10] The CISO View Survey: Zero Trust and Privileged Access, 2021, CyberArk

Key Takeaways

Securing credentials for every form of identity is key to preventing breaches and attacks — especially when many business applications don't use enterprises' identity protocols or integrate with SSO. While traditional password management tools might help with improved user experiences, they aren't equipped with the controls needed to secure a large, complex workforce's credentials from attackers.

As a security decision-maker, you need to balance both sides of the equation: protection and productivity. Focusing on the following five areas can help you achieve that balance:

1 | Intelligent authentication

2 | Security-first storage

3 | Safe credential management and sharing

4 | End-to-end visibility

5 | Frictionless user experience

CyberArk Workforce Password Management is designed to enable enterprises to securely store and manage password-based credentials — as well as items such as license keys and PINs — while enforcing robust controls over business application access. The solution also provides users with seamless, one-click access to business apps and eliminates the need to save credentials in password managers or browsers.

Learn more about how **CyberArk Identity solutions** can help security teams safeguard their organizations against the risks highlighted in this piece, while enabling productivity among workforce users.

Read about the **CyberArk Identity Security Platform**, which is designed to bring together these controls and capabilities in a unified, risk-based approach that secures all identities.

About CyberArk

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.

CYBERARK®