

# Closing the Workforce Password Management Gap in the Enterprise

By Khizar Sultan, Vice President, Identity Solutions,  
Palo Alto Networks

## The Pervasive Workforce Password Problem

For IT and security teams, password-related chaos is constant with endless resets, weak and reused credentials, and risky employee habits. Opportunistic attackers don't miss any opportunity to take full advantage of these challenges. A staggering 7,000 password attacks occur every second, driving up enterprise security risks and IT costs.<sup>1</sup>

Meanwhile, workforce users are fed up. They are expected to remember dozens of unique, strong passwords as they navigate various tools and resources to do their jobs. It's simply unrealistic. This practice has led nearly half of workers (49%) to reuse the same login credentials for multiple work-related applications, and 36% to use the same credentials at home and work.<sup>2</sup>

While credential reuse is understandable, it creates immense risk. Some workers have taken matters into their own hands by self-selecting a consumer password manager, exacerbating shadow IT issues. Many employees admit to bypassing cybersecurity policies to make their lives easier. They also go as far as jotting down passwords on sticky notes and in notebooks, only for them to become easily lost and just as easily found by others. Digital-savvy employees simply save them as notes in their phones. Despite their good intentions, they can inadvertently create risk by storing credentials on local, unencrypted files, like spreadsheets, or within insecure browser-based password managers like Chrome or Firefox.

Unfortunately, AI has taken password-stealing methods, like phishing, to new levels, making it easier than ever to infiltrate user devices with malware, find and extract stored passwords, and send them straight to the attacker. These advanced approaches can lead to unauthorized access to sensitive accounts and data, posing significant security risks.

The answer is to eliminate passwords altogether, which is where the world is heading. But today, passwords are a reality, and protecting them is a shared responsibility. Many studies show that cybersecurity education is essential for improving employee behavior and password habits. More important is providing a solution that makes it easy for workers to securely manage and share credentials for work.

## The Changing Nature of Identity: Privilege Is Everywhere

For a long time, the standard approach to workforce access security has centered around basic controls like authentication via single sign-on (SSO). But this type of authentication ignores the reality of the modern worker and the changing nature of identity. That is, the average employee can be a low-risk user one minute, and in the next minute, depending on their task, they can have access to a highly privileged account.

More than half of organizations' workforce users have access to sensitive corporate data that's frequently accessed through business applications. Almost all employees have some kind of sensitive or privileged access, meaning your sensitive enterprise data and resources might be one weak password away from getting into the wrong hands. Unfortunately, SSO can protect only certain business applications. Many tools, like those used for collaboration, banking, and shipping, don't support federation and can be accessed only with individual usernames and passwords. This lack of federation makes it difficult for IT and security teams to effectively track access activity, control password complexity, and revoke access to apps users no longer need.

### The Plight of Passwords

**\$70** the cost to a company for each password reset.<sup>3</sup>

**65%** of employees have bypassed security policies to make their lives easier and boost their productivity.<sup>4</sup>

**86%** of breaches involve stolen credentials, an attacker's favorite target.<sup>5</sup>

1. *Microsoft Digital Defense Report 2024*, Microsoft, October 2024.

2. *CyberArk 2024 Employee Risk Survey*, CyberArk, December 2024.

3. *Innovation Insight: Workforce Password Management Tools*, Gartner®, March 18, 2024.

4. *CyberArk, 2024 Employee Risk Survey*.

5. *Threat Horizons*, Google Cloud, August 2023.

---

## Not All Password Managers Are Created Equal

To fill these security gaps, many organizations turn to business versions of personal password manager tools. Most popular offerings, however, stop at the point of managing passwords. They're unable to deliver the enterprise-level security capabilities that IT and security teams need to protect their organizations from identity-based threats such as the following examples.

### Visibility and Control Over End-User Activity

Unable to show how apps are accessed and passwords are shared, these tools can exacerbate the risks caused by employees' DIY password management approaches. For instance, in many cases, users can still choose to save passwords in their browsers, a key entryway for attackers targeting endpoints.

### Sophisticated Integrations

Workforce password management tools must integrate with and support numerous identity and access management (IAM) systems as well as the enterprise browser to be most effective. Yet, many password managers on the market today lack sophisticated integration capabilities, making it impossible to provide extended protections at critical points such as login, continuous authentication after the login, and throughout browser sessions.

### Proven Security Track Record

In recent years, several popular personal password managers have suffered data breaches—both directly and indirectly—that compromised users' personal data and put sensitive information at risk. These incidents underscore the need for a tool that can fulfill or exceed data protection requirements and is backed by an experienced vendor with a proven security track record.

## Best Practices for Closing the Enterprise Password Security Gap

Because attackers can often exploit employee credentials as though they are privileged, organizations must secure all credentials with privileged controls. This approach includes employing the highest level of security in how passwords are stored, shared, created, and managed, without requiring more effort from employees. By embracing these four strategic best practices, organizations can create a user-friendly experience that their workforce will use and stick to, while also ensuring the security, control, and visibility they need.

### 1. Security-First Password Storage and Retrieval

IT and security teams can protect against the most common identity-based attacks by adopting a security-first approach to storing workforce credentials. When evaluating solutions, look for the following capabilities:

- Centrally stores and manages all credentials in a secure vault, in the cloud or on-premises, depending on organizational needs, and protects them with strong encryption and access controls.
- Secures more than just passwords, such as notes, software license keys, PINs, serial numbers, and other sensitive items.
- Ensures that only strong passwords are used and aligns policies to NIST password guidelines.
- Includes built-in multifactor authentication (MFA) for step-up authentication or continuous authentication to reduce the risk of unauthorized access to high-risk business app credentials.

Organizations can bolster protections by enabling automated, real-time password retrieval from their chosen cloud or vault location. Inspired by just-in-time (JIT) privilege controls, this capability can help IT and security teams ensure passwords are never stored locally at endpoints, keeping them outside the reach of local device malware.

---

## 2. Effortless Logins and Instant Access

Security leaders strongly believe that optimizing the user experience is important for enabling zero trust success through IAM tools. Building upon that perspective, eliminate password-related pain and frustration for end users. Look for tools with the following capabilities:

- Simplifies access to business apps by securely autofilling credentials at login and automatically capturing them when new accounts are created.
- Generates strong, complex, and unique passwords for users whenever needed, while detecting and blocking the use of passwords that were previously involved in a data breach.
- Seamlessly integrates with SSO, corporate directories, and third-party identity providers, giving users a consistent login experience from a centralized user portal.
- Enables secure, simple credential sharing with internal teams.

Such features can help reduce password fatigue, help end users focus on what they were hired to do, and eliminate risky habits that can unwittingly create openings for bad actors.

## 3. Enterprise-Designed Visibility and Control

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 employees have accessed a specific application during a particular time.
- Restrict users from adding personal applications and block certain URLs.
- Enable or disable features such as file sharing.
- Report on credential sharing between colleagues and teams.
- Add additional security layers, or privileged controls, for certain users or apps.
- View password-related risks like aged or weak passwords.

Going a step further, protection must continue past the point of authentication. Organizations should have the ability to monitor and record all actions that occur once a user logs into a session. With increasing compliance demands, ensure any records surrounding high-risk actions taken in apps are backed up by a full audit trail.

## 4. Safe Credential Management and Sharing

IT and security teams want greater visibility and control over who can access credentials and when. By taking an enterprise-grade approach, organizations can ensure that end users, such as team managers, can securely share their credentials without revealing the actual passwords. Look for these additional capabilities that can strengthen your organization's security posture:

- Protects privacy by controlling who can share, view, and edit credentials.
- Imposes time limits on user access when sharing credentials for certain applications, such as if a manager goes on vacation and needs to grant a worker temporary access for a set number of days.
- Prevents users from saving passwords in built-in browser password managers, reducing the number of account and credential repositories.
- Manages the transfer of credential ownership to new users.

Since workforce turnover is inevitable, this level of control is essential. Look for capabilities that enable admins to transfer ownership automatically without losing the chain of custody when the primary owner leaves the organization. This approach also helps organizations onboard new users at scale without losing time or information.

## Striking the Right Balance

Securing passwords has never been more important. While personal password management tools might offer simple user experiences, they aren't equipped with the controls needed to secure the credentials of a large, complex workforce. Protecting against credential-based attacks takes a layered, end-to-end identity security approach that ensures credentials are securely stored, managed, shared, and obfuscated at login. It also means protecting them from compromise on the endpoint and from attacks that prey on weak passwords, while continuously monitoring for risk.

These multipronged security measures can't come at the user's expense. By focusing on the four best practices we've highlighted here, security decision-makers can strike an effective balance between protection and productivity, empowering end users to participate in their security.

## Protect the User's Journey with Workforce Identity Security

Enterprise security is a continuous journey, not a destination. As your organization bolsters its password protection capabilities, you can build toward a holistic identity security approach that combines a range of controls and solutions. Ultimately, this approach will enable you to secure all credentials, passwords, and secrets at every stage of an identity's access journey. It starts with initial login at the endpoint, goes to accessing SaaS apps and cloud infrastructure, and follows the entire user session.

## Enterprise Security Demands Enterprise-Grade Solutions

Idira™ Workforce Password Management, by Palo Alto Networks, is an enterprise solution that addresses both the security risks of compromised credentials and the challenges of managing passwords for employees and IT teams. This solution simplifies managing passwords, protects work accounts, and gives companies visibility and control over password security. Users can easily add application credentials to their user portal, access apps with a click of a button, and securely share credentials with internal teams. Behind the scenes, passwords are securely stored in the Idira Identity Cloud or self-hosted Idira Vault, providing security teams granular control and visibility. Further, the included MFA capabilities reduce the risk of unauthorized access to business app credentials.

To explore all the ways Idira can secure the identities across your organization, visit

[www.paloaltonetworks.com/idora](http://www.paloaltonetworks.com/idora).



3000 Tannery Way  
Santa Clara, CA 95054

Main: +1.408.753.4000  
Sales: +1.866.320.4788  
Support: +1.866.898.9087

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

idora\_closing-the-password-management-gap-in-the-enterprise\_042226