

Choosing a Workforce Password Management Solution

See How Idira Workforce Password Management Aligns with Gartner® Insights

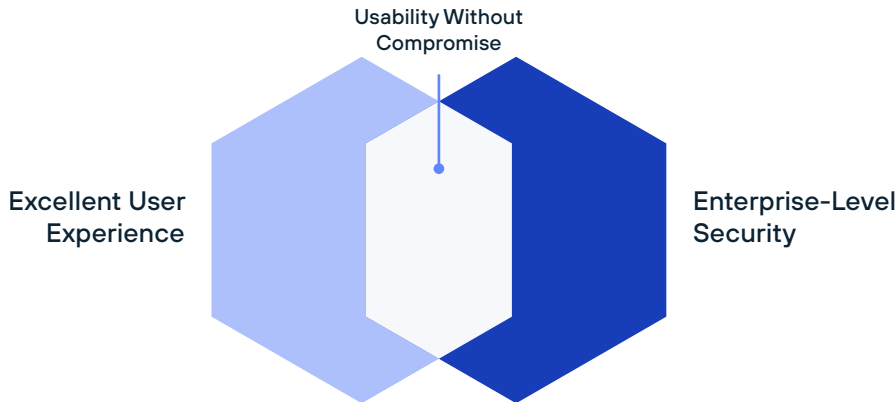
A workforce password manager (WPM), also known as an enterprise password manager, is an enterprise-designed solution that addresses both the security risks of compromised credentials and the challenges of managing passwords for employees and IT teams. A WPM secures and simplifies access to applications that don't support federation and can't be accessed through corporate single sign-on (SSO) solutions. WPM solutions should be part of an identity security platform to maximize value and ensure the longevity of the tool.¹

1. *Buyer's Guide for Workforce Password Management Tools* (Gartner subscription required), Nayara Sangiorgio, Gartner, January 4, 2025. GARTNER is a trademark of Gartner, Inc. and its affiliates.

Marrying Usability with Security

According to Gartner®, as stated in their research, “A WPM tool offers clear value by reducing user friction and increasing password security, but selecting the most suitable tool in a market crowded with functionally similar options is challenging.”²

To successfully implement an enterprise password management solution, it must offer enterprise-level defense with a user-first design. You need the buy-in from your IT security team to prove the solution is not vulnerable to attacks. And, you need buy-in from your end users who must adopt the tool, which must boost their productivity, not impede it.



Cautions Against Consumer Password Managers

Many organizations rely on personal password managers or browser-native, password-saving tools, like Chrome and Edge, to store and autofill credentials. While these solutions might offer convenience to the end user, they fall short of meeting enterprise security, compliance, and control requirements—leaving businesses exposed to unnecessary risk.

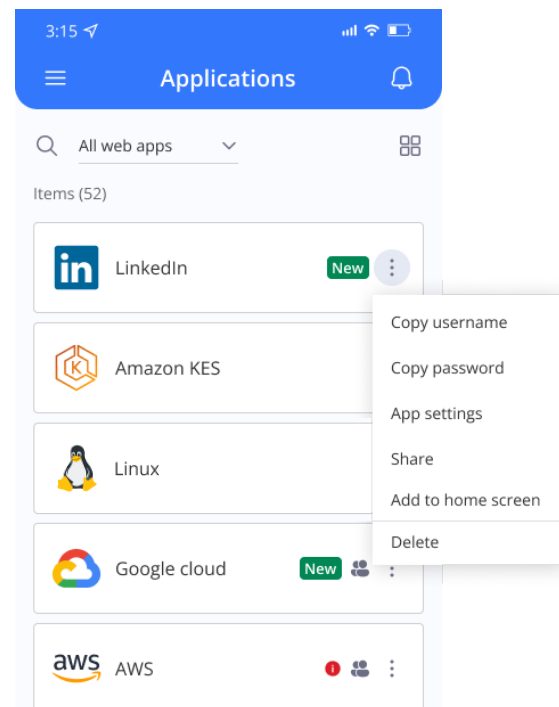
Personal password managers are built for individuals, not enterprises. They lack the centralized visibility, policy enforcement, and integration capabilities that IT and security teams need to protect workforce credentials. And, a personal password manager marketed as an enterprise solution is no different. Employees using personal password managers might store corporate credentials alongside personal ones, increasing the risk of data exposure if an account is compromised. Additionally, IT teams have no way to enforce company-wide security policies or revoke access when employees leave.

Browser-native password managers introduce similar risks. While convenient, they are designed for consumer use, storing passwords on local devices in a way that makes them vulnerable to malware, phishing attacks, and unauthorized access. They also provide little to no administrative oversight, meaning security teams have no control over how employees store and share business-critical credentials.



Employees handling numerous accounts and passwords can benefit from a workforce password management tool. The tool simplifies password management and enhances security, thereby strengthening the organization’s overall security posture.”³

—Gartner



2–3. Gartner, *Workforce Password Management Tools*.

Key Features of a Workforce Password Management Solution



Work passwords and personal passwords should be kept separate, with employees storing their personal password data in their own personal vaults. PPM tools are not suitable for managing and auditing business accounts—they lack the robust security features of WPM tools. It is crucial to separate these two categories of password managers and establish clear guidance/policies to inform employees about the expectations for password management use in the organization.”⁴

—Gartner

Protecting Passwords with Idira Workforce Password Management

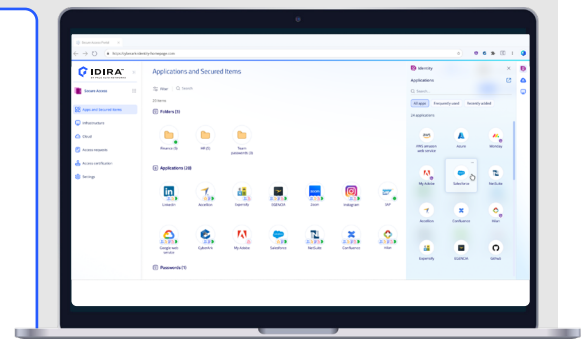
Idira™ Workforce Password Management, by Palo Alto Networks, offers an enterprise-ready password management solution with a consumer-grade user experience to secure credentials and accounts. Its tight integrations across the Idira Identity Security Platform ensure easy access for employees and include purpose-built controls for IT teams. Idira addresses both the security risks of compromised credentials and relieves password fatigue for end users.

According to Gartner

“Passwords are a constant risk to organizations because they can serve as an easy entry point for cybercriminals. The challenge of identity management is further exacerbated by poor and inefficient password management, as users are burdened with multiple passwords to manage.”⁵

How Idira Workforce Password Management Delivers

Idira Workforce Password Management provides secure storage of credentials and other sensitive items in the Idira Identity Cloud or self-hosted vault, which ensures that all password-based credentials for business applications are protected with industry-standard encryption algorithms. It enables users to launch all applications from a centralized location.



Launch all applications from a centralized location

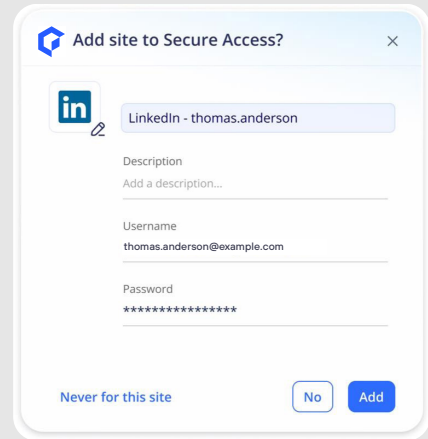
4–5. Gartner, *Workforce Password Management Tools*.

According to Gartner

"Evaluate key features: Compare the features of different vendors, focusing on critical aspects like web interface, ease of use and scalability."⁶

How Idira Workforce Password Management Delivers

Idira Workforce Password Management offers both cloud-based and on-premises deployment models, giving organizations the flexibility to choose the solution that best fits their needs. The cloud-based model offers quick deployment and automatic updates, while the on-premises model provides more control over data management.



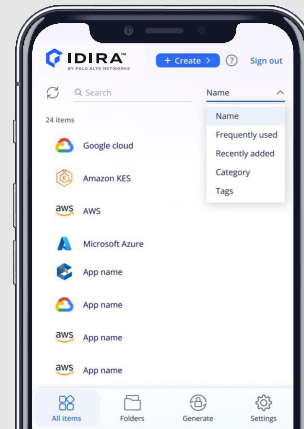
Storing credentials on-premises in the vault or securely in the cloud

According to Gartner

"Gartner clients frequently emphasize the importance of user-friendly interfaces, with user experience often being a key factor in purchasing decisions."⁷

How Idira Workforce Password Management Delivers

End users appreciate the simplicity and intuitive design Idira Workforce Password Management provides. It eliminates the struggle of remembering and keeping track of multiple passwords by providing effortless logins and instant access to applications.



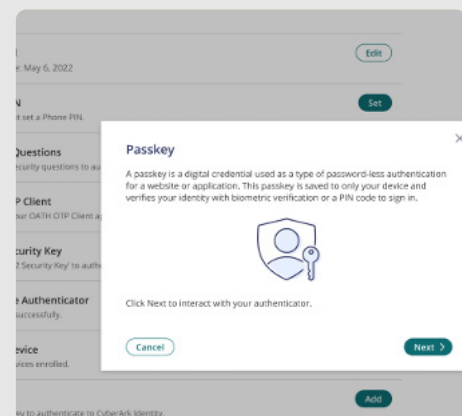
Eliminating end-user friction with an intuitive web interface

According to Gartner

"WPM tools often need to integrate with a variety of other systems to boost security posture and streamline operations."⁸

How Idira Workforce Password Management Delivers

Idira Workforce Password Management integrates seamlessly with various IAM systems, including SSO solutions, multifactor authentication (MFA) tools, and enterprise directories like Active Directory. This integration ensures that password management is streamlined and secure across the organization.



Native integration with adaptive MFA and the ability to respond to risks in real time

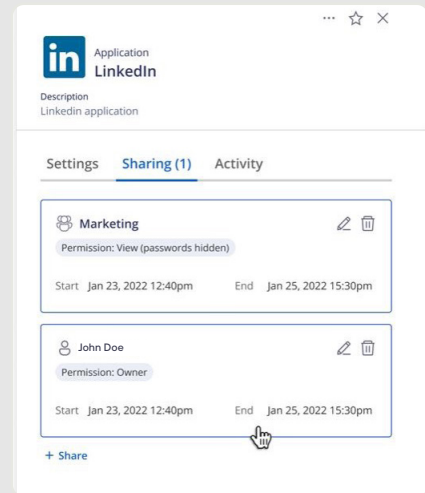
6-8. Gartner, *Workforce Password Management Tools*.

According to Gartner

"WPM tools secure and manage passwords for business end users. These solutions are designed to automate the creation, storage, retrieval, and autofill of passwords. They enable restricted sharing of business accounts and provide hygiene scores for passwords stored in the vault."⁹

How Idira Workforce Password Management Delivers

Idira Workforce Password Management offers advanced security features such as MFA, dark web monitoring, and password blocklisting. These features help organizations enhance their security posture and protect against credential-based attacks.



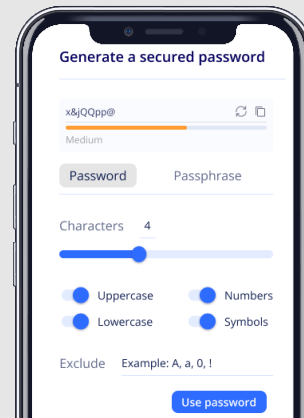
Idira credential sharing feature with admin controls for added protection

According to Gartner

"Compliance and security standards: If applicable to your organization, assess which vendors comply with relevant industry standards and regulations, such as GDPR, HIPAA, or SOC 2."¹⁰

How Idira Workforce Password Management Delivers

Idira Workforce Password Management aligns with NIST password guidelines, ensuring that all user passwords meet stringent security standards. This solution also supports compliance with other relevant industry standards and regulations.



Strong password generation and policy creation to ensure compliance

9–10. Gartner, *Workforce Password Management Tools*.

More Than a Password Manager

Idira Workforce Password Management secures credentials and other sensitive notes and files for organizations. Because it's part of the comprehensive Idira Identity Security Platform, it integrates with solutions that extend protections like session recording and monitoring, session protection controls, continuous authentication, and password replacement. Simply adopting an enterprise password manager isn't enough to solve the challenges organizations face today when securing credentials. Organizations need a complete identity security approach to secure their passwords.

Featuring end-to-end protection, Idira Workforce Password Management includes a built-in Prisma® Browser™, secure web sessions, and privileged access management (PAM), as well as SSO and MFA capabilities. Together, these features deliver continuous protection from credential theft and misuse across the entire user journey:

- **Password replacement technology:** Prisma Browser obfuscates passwords, preventing exposure to users or threats, reducing the risk of credential theft from compromised devices.
- **Protection after the login:** Secure web sessions provide session recording, real-time monitoring, and session protection to detect and mitigate risks during user sessions.
- **Adaptive authentication:** Native MFA integration adds an extra layer of protection, ensuring only authorized users gain access to sensitive resources.
- **Simplified compliance:** Audit-ready reports provide visibility into user access, credential sharing, and session activity, streamlining compliance efforts.
- **Operational efficiency:** Automating password management, enforcing security policies, and responding to threats faster through centralized management all reduce IT overhead.

Get Started

Selecting the right workforce password management solution is critical to an organization's security and efficiency. Idira Workforce Password Management both meets and exceeds Gartner's guidance, providing a robust, user-friendly, and secure solution. By choosing Idira, organizations can ensure the protection of their credentials while offering a seamless experience for their users.

Explore all the ways Idira can secure the identities across your organization. [Request a demo.](#)

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.

BONUS: How Idira Exceeds Security Standards and Protects Your Business Passwords

- No primary passwords or single point of failure.
- Industry-leading data encryption standards.
- Option to save credentials on-premises in a PAM self-hosted vault.
- FedRAMP High certified.
- Step-up authentication or continuous authentication for high-risk applications.
- Option to use WPM user experience for autofill of privileged credentials.
- Credentials are not stored on the local device.
- Optional integration with Prisma Browser.
- Optional session recording and audit trail for high-risk applications.
- 99.99% uptime.



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

© 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.
idira_wp_choosing-a-workforce-password-management-solution_042326