

CyberArk Workforce Password Manager



Protect Your Passwords and Simplify Access

SOLUTION BRIEF

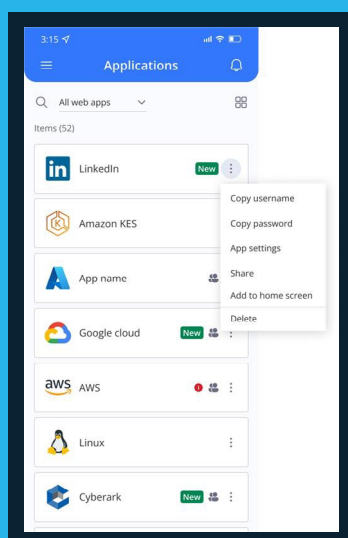
86%

of breaches involve stolen credentials

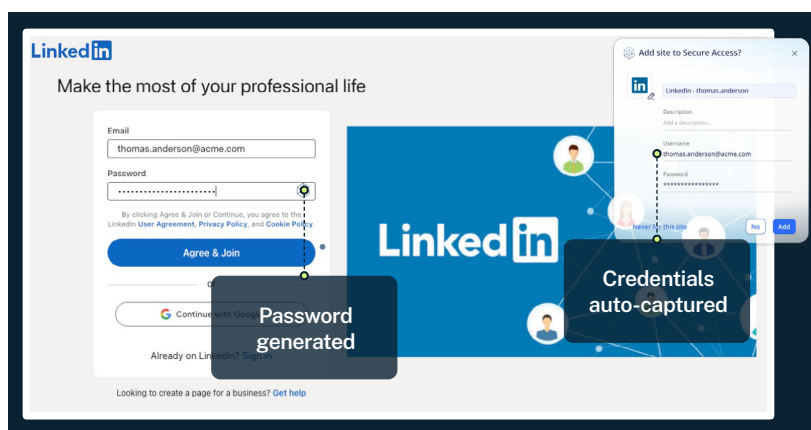
Google Cloud, Threat Horizons, 2023

“Work passwords and personal passwords should be kept separate, with employees storing their personal password data in their own personal vaults. PPM [Personal Password Manager] 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.”

- Gartner® Buyer's Guide for Workforce Password Management Tools, Nayara Sangiorgio, 2025



CyberArk allows seamless access for users on mobile devices.



Protect Business Credentials with Enterprise-Grade Security

CyberArk Workforce Password Manager (WPM) is an enterprise-focused password management solution designed to help businesses secure user credentials while simplifying employee access. Unlike consumer-grade solutions or built-in browser solutions, CyberArk employs the highest security standards in the industry and ensures IT teams maintain visibility and control over credentials while delivering a seamless experience for users.

What You Can Achieve with a Workforce Password Manager

- **Mitigate credential-based attacks:** Prevent unauthorized access by securing passwords in a vault with industry-leading encryption.
- **Eliminate password frustration for end users:** Enable effortless logins and intuitive UI with auto-fill capabilities and one-click app access.
- **Ensure IT visibility & control:** Gain oversight of access and sharing, enforce policies, and prevent the use of compromised credentials.
- **Measure and track risk posture:** View password insights, access reports and assess and address risks.
- **Seamless integration:** Extend identity security beyond passwords with CyberArk's broader security ecosystem.

The Hidden Costs of Password Resets

Beyond security risks, inefficient password management imposes significant operational burdens for both IT and employees and significant costs for companies.

Nearly

21%

of users reset a password weekly and 15% say they reset a password daily ¹

\$70

The cost to a company for each password reset ²

Generate a secured password

x&jQQpp@

Medium

Password

Passphrase

Characters 4

☒ Uppercase ☒ Numbers
☒ Lowercase ☒ Symbols

Exclude Example: A, a, 0, 1

Use password

CyberArk generates strong passwords, allowing organizations to align to NIST standards.

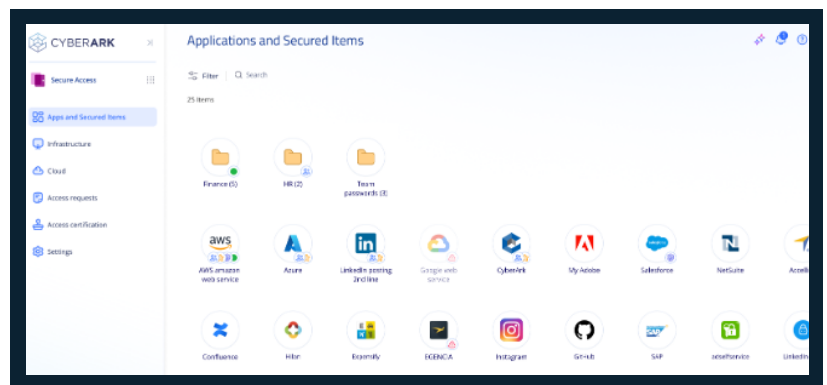
CyberArk Workforce Password Manager Key Capabilities

Enterprise-Grade Security

- Secure storage of business credentials, files or notes with centralized IT oversight.
- Enforce password policies, including strength requirements, to comply with NIST 800-63B guidance.
- Protect against credential theft with risk-based security controls, compromised credential checks, and multi-factor authentication (MFA).

Effortless Employee Access

- Automatically save and autofill credentials for fast, secure logins.
- Easy one-click access to apps and customizable features in the user portal.



Users have one-click access to all applications including SSO applications.

Enterprise Visibility, Control and Insights

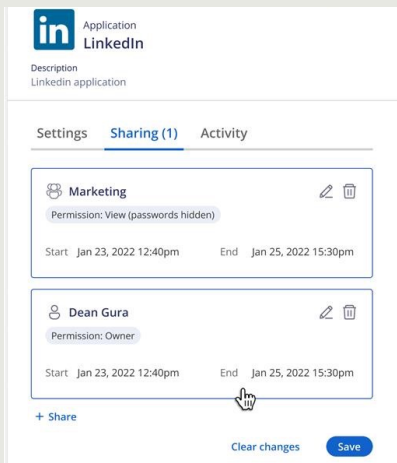
- Admin dashboards for tracking password usage and sharing.
- Customizable access policies to enforce password hygiene and comprehensive audit reporting.
- Proactive security alerts for weak or compromised credentials.
- Continuous risk intelligence and monitoring for a stronger security posture.

¹ ExpressVPN, 2022

² Gartner, Innovation Insight: Workforce Password Management Tools, Nayara Sangiorgio, 18 March 2024.

USE CASES

- Integrate password management with your identity security stack — IAM and PAM solutions.
- Share account credentials securely within the organization.
- Securely store and share more than just passwords — including API keys, notes, files and other secrets.
- Integrate with the CyberArk PAM Vault for critical applications and privileged users.
- Meet requirements to store business credentials on-premises or in the cloud.
- Adopt and enforce strong password policies.



CyberArk allows users to securely share credentials, while hiding the plain-text password.

More Than a Password Manager — A Security-First Identity Solution

CyberArk WPM is more than a password manager. Protecting passwords requires a holistic approach, not a point solution. WPM is a key part of a **comprehensive identity security strategy** that protects credentials across the enterprise. Securing credentials and accounts is what we do best, and WPM was purpose-built to meet the needs of the entire workforce.

With CyberArk, you can safeguard business credentials by leveraging your existing PAM Vault, offer native access inside a secure enterprise browser, enable recording and monitoring for sensitive web sessions, increase assurance with continuous authentication and more. Businesses gain layered protection with CyberArk that goes far beyond traditional password storage.

Why CyberArk?

CyberArk Workforce Password Manager was purpose-built for enterprises. With advanced security controls, IT governance capabilities, and seamless integrations, it delivers the protection businesses need without compromising user experience.

Protect Your Business Passwords with CyberArk Today.

Learn more about [Workforce Password Management](#) or sign up for a [free trial](#) to see CyberArk Workforce Password Manager in action.

