What Makes Keeper the Best Solution To Protect & Manage Your Passwords and Privileged Accounts

Keeper Security is fanatical about data protection and security, standing above any other password manager and PAM solution for a number of reasons:

Security

- Designed with zero-trust and zero-knowledge security from the ground up, across all client applications, to cover multi-cloud and distributed remote work environments.
- The most robust security model and infrastructure in the industry with the largest number of certifications and authorizations, including FedRAMP and StateRAMP Authorization.
- Enables SSO integration with Keeper SSO Connect that authenticates and provisions users into their Keeper Vaults using any SSO identity provider.
- All of Keeper's user-facing applications perform encryption on-device, with all the usability benefits of a cloud-based platform.

Ease of Deployment and Management

- Built specifically for MSPs – multi-tenant structure to centralize management, improve scalability, enable security isolation and simplify reporting and billing.
- Offer privileged access management and enterprise password management to MCs. They can start with only password management and then add on PAM later. Both are accessed via the same end-user vault.
- Automatically provision users via SCIM, SAML or AD.
- PAM is deployed via a lightweight, containerized gateway in the target environments, eliminating agents and on-prem complexity.
- Integrates with your IAM tech stack, such as IdP, SSO, SIEM, CI/CD and MFA.
- Manage every MC from a centralized Admin Console to establish role-based enforcement policies, monitor activity and set up integrations.

Ease of Use and Functionality

- MCs use one platform for all their access needs. Keeper is accessible via a web vault and native apps across Windows, macOS, Linux, iOS and Android.
- Log in with MFA for one-click, passwordless access to servers, databases, web apps and SaaS platforms.
- Securely share credentials with individuals or teams by using shared folders. Access can be revoked at any time.
- Manage privileged sessions across any protocol (RDP, SSH, MySQL, etc.) with full auditing, session logging and flexible access through UI, CLI or isolated web browsing.
- Automate password rotation to lock down service accounts.

Core Capabilities

- Password Management: Protect and manage an organization's passwords, passkeys and confidential files.
- Secrets Management: Protect API keys, CI/CD pipelines, developer tools and eliminate secrets sprawl.
- Session Management: Provide passwordless remote access to any resource using a web browser.
- Database Management: Control access to databases, either on-prem or cloud, using interactive UI sessions, CLI sessions, or tunneling with your favorite front-end tools.
- Remote Browser Isolation: Lock down internal web-based apps, cloud apps and admin panels, prevent data exfiltration and control browsing sessions with auditing, session recording and password autofill.
- SSH Key Management: Protect SSH keys in an encrypted vault with automated rotation, privileged sessions, SSH agent and Git commit signing.
- Admin Console: Manage and deploy Keeper to users, integrate with identity providers, monitor activity and establish role-based enforcement policies.
- Control Plane: Orchestrate and monitor the various components and activities related to privileged access, session management, policies and workflow.

Credibility

- Keeper has the longest-standing SOC 2 Type 2, ISO 27001 and TRUSTe certification in the industry.
- Keeper holds 10+ US utility patents on its technology.
- Over 300,000 5-star ratings across review sites.

For more information on KeeperMSP, contact your sales rep.

© 2025 Keeper Security, Inc.