

Enterprise Password Manager (EPM)

Prevent breaches, reduce help desk costs and ensure compliance.

Challenges

Weak and stolen passwords, credentials and DevOps secrets are a leading cause of data breaches. Most organizations lack visibility into these threats, and have no way to enforce security best practices across every employee, in every location, across every device, application and system. This creates a series of challenges for IT administrators:

1. An organization consists of human and machine credentials that need to be protected.
2. Distributed remote work and multi-cloud computing have made traditional IT perimeters obsolete.
3. Attack surfaces are expanding exponentially as billions of additional devices, credentials and secrets are connected to distributed networks - both on and off-premises.
4. Conventional cybersecurity solutions are heterogeneous and siloed in nature, thereby creating critical gaps in visibility, security, control, compliance and reporting.

Organizations that don't address these core challenges face a heightened risk of data breaches, compliance violations and operational friction.

Solution

Keeper Enterprise Password Manager monitors and protects every user on every device across an organization with full cloud and native-application capabilities. Keeper EPM seamlessly integrates with existing IT technology, including Security Information and Event Management (SIEM), Multi-Factor Authentication (MFA), passwordless and Identity provider (IdP) solutions.

Keeper EPM provides comprehensive authentication and encryption across every website, application and system employees interact with. Keeper EPM is easy to deploy, easy for non-technical users to adopt and is the most secure product of its kind. Keeper holds the industry's longest-standing SOC 2 Type I and II compliance, ISO 27001 certification and is FedRAMP and StateRAMP Authorized.

About Keeper Security

Keeper Security is transforming cybersecurity for people and organizations around the world.

Keeper's affordable and easy-to-use cybersecurity solutions are built on a foundation of zero-trust and zero-knowledge security to protect every user on every device. Millions of individuals and thousands of organizations rely on Keeper for best-in-class password, passkey and secrets management, Privileged Access Management (PAM), secure remote access and encrypted messaging. Our next-generation cybersecurity platform deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance.

Keeper Security is backed by leading private equity firms Insight Partners and Summit Partners.

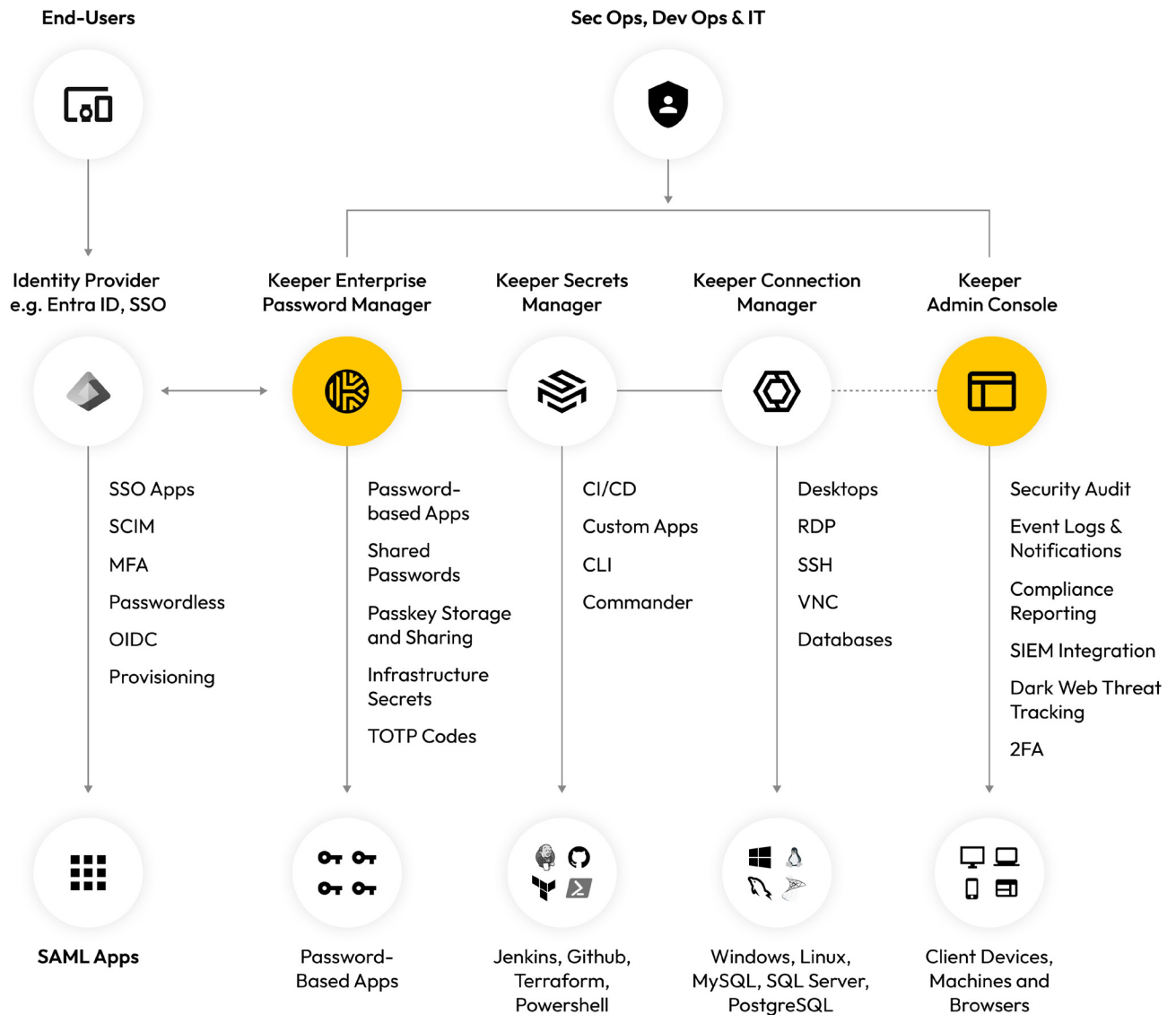
Keeper Security
Don't get hacked.

Learn more
keepersecurity.com

Start a free trial today
keepersecurity.com/start-business-trial.html



Keeper Privileged Access Management Platform



Business Value

- Prevent ransomware and credential-related cyber attacks
- Protect every user on every device from every location
- Get comprehensive visibility, enforce security best practices and controls, and streamline compliance audits
- Enhance and extend your existing Single Sign-on (SSO) deployment
- Improve employee productivity and reduce the burden of password-related tickets for your helpdesk and IT teams

Key Capabilities

- Encrypted end-user vaults
- Password and passkey storage, management and sharing
- KeeperFill® browser extension powered by KeeperAI™
- Web, desktop and mobile apps
- Dark web monitoring with BreachWatch
- Intuitive Admin Console
- Seamless provisioning and integrations
- Role-Based Access Controls (RBAC)