

Protect passwords, passkeys, credentials and secrets...

Protect against ransomware attacks...

Enable secure sharing of credentials and secrets...

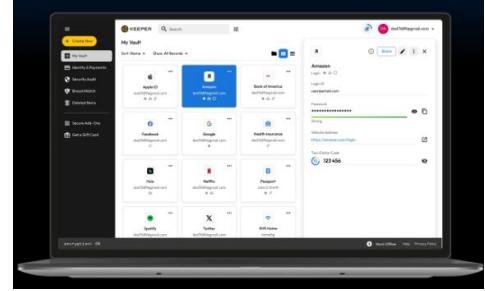
Mitigate risk of data breaches...

Bolster security and privacy...

Strengthen compliance standards...



Keeper is the most secure cybersecurity and password management platform for preventing password-related data breaches and cyberattacks.



- Stores and manages your passwords, credentials, files, and private data.
- Creates random, high-strength passwords for all logins and stores them in a secure vault.
- Saves time, frustration, and eliminates the need to reset, reuse, and remember passwords.
- Each of your employees get a private, encrypted vault for storing and managing their passwords, credentials, files and private data that can be accessed anywhere and on any device.
- Enables secure, granular and controlled sharing of credentials, secrets, and vaults among internal employees and teams, as well as external contractors and partners.
- Protects against ransomware attacks with robust administration, controls and visibility over strong password security, and real-time dark web monitoring.
- Supports role-based controls, delegated admin, MFA, auditing, SIEM event reporting, and requirements for industry compliance with HIPAA, DPA, FINRA, GDPR and more.

Zero-Trust Password Management to Protect Your Workforce, Devices and Data

Zero-trust is a security model that enforces secure access to everything by everyone. All users and devices are authenticated and authorized before being granted access to critical networks, applications and data. It is a comprehensive framework that ensures maximum security without sacrificing performance and user experience.

Dark Web Monitoring

Keeper continuously compares your passwords to current scans of stolen credentials from data breaches, malware-infected devices, and other underground sources. Alerts are immediately sent to users and administrators when compromised passwords are found. These early warnings allow users and administrators to take action before becoming victims of account takeover, ransomware or online fraud.