destiny
Business & Technology Consulting SM
Education Solutions

Easily reduce cyber security threats by 80% - Talk with us to receive discounts on retail pricing

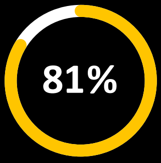
KEEPER
Cybersecurity Starts Here

DATASHEET

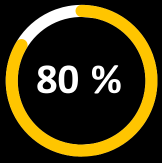
Keeper Enterprise

Your biggest security threat walks in your door every day.

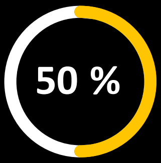
Employees use weak passwords, reuse them across accounts and forget them.



of data breaches are due to weak, default or stolen passwords [1]



of people use the same password for everything [2]



of help desk calls are password related [3]

Security

The most advanced security perimeter is easily bypassed by weak passwords. Employee password habits can only be improved with insight into password usage and compliance. Keeper solves this by providing comprehensive reporting, auditing and notifications.

Compliance

Every cybersecurity framework from NIST to ISO and PCI to HIPAA requires access tracking, least-privilege controls and audit logs. Keeper enables role-based controls and visibility into shared credentials. Access logs to Keeper vaults can be audited for compliance or forensics.

Microsoft Active Directory Synchronization

Keeper® AD Bridge synchronizes to MicrosoftActive Directory or Open LDAP. This enables rapid user provisioning and automatically adds Nodes (organizational units), Users, Roles and Teams. Keeper enables role-based access control and the ability to track roles as people move throughout the organization. This includes automatically locking vaults of employees that leave.

Two-Factor Authentication

Keeper supports Two-Factor Authentication (2FA) including SMS, Keeper DNA® (smartwatch tap), TOTP (e.g. Google Authenticator and Authority), FIDO U2F (e.g. Yubikey), Duo and RSA SecurID. 2FA may be enforced through role-based controls.

Support Costs

Drastically reduce help desk costs related to password issues. Forrester found that several large companies have allocated over $1 million annually for password-related support.

Productivity

Save employees time, frustration and eliminate the need for them to reuse and remember passwords. Keeper will generate strong, random passwords and automatically fill them for users. The Keeper vault, with a responsive and intuitive UI, is available to employees from any device and location. Everything Keeper does is geared towards quick user adoption and security. Keeper is published in 21 languages for global use.

Automate Back-End Password Rotation

Keeper® Commander SDK provides IT admins and developers with command-line tools and Python source code to perform password management, password rotation and vault functionality. Eliminate hard-coded or plaintext back-end passwords. Connectors include Unix, Windows and AD logins; Oracle, Microsoft SQL, MySQL, Postgres and Dynamo databases; and AWS password and API access keys.

Zero-Knowledge Architecture

All encryption and decryption is done on the user's device. PBKDF2 with 100,000 rounds is used for deriving a key from the user's master password. Each record is encrypted using AES-256 with a different and unique key that is randomly generated client-side. RSA encryption is used for secure record sharing between users and teams. Keeper's infrastructure sync's encrypted ciphertext between devices. Key pinning is enforced between client and server. All data in transit and at rest is always encrypted - it cannot be viewed by Keeper Security employees or any outside party.

Email Auto-Provisioning

Large organizations such as universities can provision Keeper vaults to thousands of users with a domain match on email addresses. With minimum administration, large-scale deployment can be accomplished using an existing email channel or portal.

Support for Subsidiaries, Departments, Offices and Branches

Keeper was created to support nodes and organizational units to accommodate any-sized organization across all major industries. The Keeper Administrator can structure password management policies by role, team and organizational unit. Thus, different divisions, branches, brands and office locations of an organization can all be protected with Keeper, while having different access rights, permissions and policies for enforcing secure password management across the organization. Each organization may utilize multiple Keeper Administrators with fine-grained permissions over their users, roles and teams.

Keeper Integrates with Leading SSO Solutions

Keeper® SSO Connect integrates into your IdP and is the perfect solution for applications that don't support SAML protocols. Keeper also provides users with privileged access, a secure vault to store all of their non-SSO passwords, digital certificates, encryption keys and API access keys.

ADFS
Microsoft Azure
okta
G Suite
JumpCloud
amazon web services
CAS
IBM Security
Ping Identity
onelogin
Centrify
f5

Enterprise Password Management Solutions can help Manage Password Costs and Realize Compelling ROI.

- Forrester[4]

7 Data Breach Incident Report [2] Keeper Survey of 1000 Internet Users in 2017 [3] Gartner Group [4] *Forrester Report: Best Practices: Selecting, Deploying and Managing Enterprise Password Managers ©*

destiny
Business & Technology Consulting SM
Education Solutions

destinycorp.com
info@destinycorp.com
860-721-1684