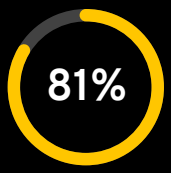
KEEPER
Cybersecurity Starts Here

DATASHEET
Industry Brief

Higher Education

Education data breach cost per record (40% higher than industry average)[1]

of people reuse passwords[2]



of breaches started with weak or stolen passwords[2]

Security Education

The point of higher education is the open exchange of knowledge. However, some knowledge should not be shared: personal information, census data, and secret research are examples. Unfortunately, administration, staff and students alike use weak passwords, reuse them across accounts and forget them.

Install password security knowledge in our future leaders. Save staff and students 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 users from any device and location. Everything Keeper does is geared towards quick user adoption and security.

Support Costs

Beyond increasing security, Keeper drastically reduces help desk costs. Up to 50% of help desk calls are password related.[3] Those calls cost $31 each, potentially adding up to hundreds of thousands of dollars annually.

Two-Factor Authentication

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

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.

IT Admin Insight

Every user is provided a secure digital vault. A security dashboard in the Admin Console provides an overview of weak passwords, password reuse and two-factor authentication enforcement. Keeper enables role-based access controls to enforce least-privilege policies. Administration may be delegated to department or team leaders. Folders and records can be securely shared and revoked. The vault of a administration or staff member that leaves can be automatically locked and be securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

> **"Enterprise Password Management Solutions can Help Manage Password Costs and Realize Compelling ROI."**
>
> - Forrester[4]

Thousands of Organizations Trust Keeper

THE UNIVERSITY OF ALABAMA
THE UNIVERSITY OF IOWA
UNIVERSITY of MARYLAND
THE OHIO STATE UNIVERSITY

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.

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.

Azure AD Sync (SCIM) & Provisioning API

Keeper supports the ability to seamlessly provision users and teams from Microsoft Azure AD or other identity platforms using the SCIM protocol. Keeper also supports API-based, command-line provisioning through the use of Keeper® Commander SDK. The Keeper Commander SDK is open source Python code that is available for download from Keeper's Github Repository.

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

Keeper Third-Party Attestations and Certifications

GSA Schedule 70 Contract 47QTCA18D00C9 · TRUSTe Certified Privacy · AICPA SOC · PCI DSS Compliant

[1] IBM/Ponemon Cost of Breach 2017 [2] Verizon 2018 Data Breach Incident Report [3] Gartner Group [4] Forrester Report: Best Practices: Selecting, Deploying and Managing Enterprise Password Managers

Business Sales

Americas & APAC
+1 312 829 2680

United Kingdom
+44 20 3405 8853

Germany & DACH
+49 89 143772993

Ireland
+353 21 229 6020

EMEA
+353 21 229 6011

Netherlands
+31 20 262 0932

Iberia & Italy
+34 919 01 65 13

Sweden & Nordics
+46 8 403 049 28

keepersecurity.com

sales@keepersecurity.com

Support

Consumer
+1 312 971 5702

Business (Americas & APAC)
+1 312 226 4782

Business (EMEA)
+353 21 229 6019