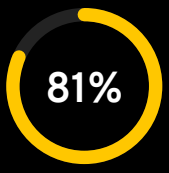
KEEPER
Cybersecurity Starts Here

DATASHEET

Higher Education Industry Brief

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]

Securing Educational Institutions

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.

Instill password security best practices in our future leaders. Save staff and students time, frustration by eliminating the need for reusing and remembering 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.

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 clientside. RSA encryption is used for secure record sharing between users and teams. Keeper's infrastructure syncs 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.

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

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 while maintaining a zero-trust and zero-knowledge framework. 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 an administrator or staff member that leaves can be automatically locked and securely transferred. Access logs to Keeper vaults can be audited for compliance or forensic reports.

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.

Flexible Provisioning

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.

Simple to Deploy & Use

Keeper takes only minutes to deploy, requires minimal ongoing management, and scales to meet the needs of any size organization, from a small municipality to a large federal agency. IT administrators can easily and quickly provision Keeper vaults to all of their users with a domain match on email addresses.

With minimal administration, a large-scale deployment can be accomplished using an existing email channel or portal. Keeper integrates seamlessly into any data environment — single cloud, multi-cloud, or hybrid — and any security stack. It works with online services and apps, including legacy LOB apps, and it integrates into any SSO deployment.

About Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-trust, zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage, advanced reporting and messaging. Named PC Magazine's Best Password Manager & Editors' Choice and awarded the Publisher's Choice Cybersecurity Password Management InfoSec Award, Keeper is trusted by millions of people and thousands of organizations to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2 (Type 1 and 2) and ISO 27001 Certified and is also listed for use by the Federal government through the System for Award Management (SAM). Keeper protects organizations of all sizes across every major industry sector.

Integration 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 · AICPA SOC · PCI DSS Compliant · TRUSTe Certified Privacy

Keeper Awards and Recognition

2021 Enterprise Leader
4.7 out of 5 stars

Editors' Choice
4.5 out of 5 stars

Gartner Peer Insights
4.6 out of 5 stars

Spiceworks
4.9 out of 5 stars

[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