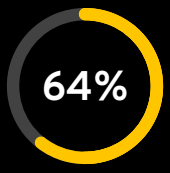
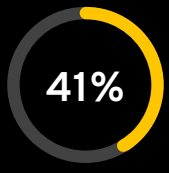
Education Industry: Cybersecurity is More Vital Than Ever

cybersecurity incidents were reported by the education sector in 2019[1]



don't believe their existing IT infrastructure will protect them against cyberattacks in the next 12-18 months[2]



of higher education cybersecurity incidents and breaches were caused by social engineering attacks[3]

The Education Security Challenge

Out of 17 major industries, education ranks last in cybersecurity preparedness[4]. The education industry has vulnerable data, including personal information about staff and students at every level, from K-12 to higher education. The sudden shift to remote learning this year has caused a drastic increase in the number of cyberattacks for education institutions and those studying remotely. This means exposure from connecting to unsecured networks while large amounts of data are being shared outside of a more controlled educational facility.

How Keeper Helps

Keeper's business password management solutions give school IT administrators complete visibility into employee, student, and parent usage of school-related login credentials, enabling them to monitor password use across the entire network and enforce policies such as strong passwords, 2FA, and other security protocols. Keeper also helps secure remote learning and home-schooling environments by enforcing role-based access to internal systems while Keeper auto-fill feature helps prevent phishing attacks by only auto-filling credentials on sites stored in the Keeper Vault.

Email Auto-Provisioning

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

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 and folders and records can be securely shared and revoked. The vault of an administrator or staff member who leaves can be automatically locked and be securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

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 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.

Microsoft Active Directory

Synchronization Keeper® AD Bridge synchronizes to Microsoft Active 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.

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 and 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.

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.

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.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **https://keepersecurity.com.**

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

TRUSTe CERTIFIED PRIVACY · AICPA SOC · AICPA SOC 2 · ISO 27001 · PCI DSS COMPLIANT · Privacy Shield Framework

Keeper Awards and Recognition

2020 Enterprise Leader
4.7 out of 5 stars

Editors' Choice
4.5 out of 5 stars

Gartner Peer Insights
4.9 out of 5 stars

Spiceworks
5 out of 5 stars

[1] PurpleSec [2] PurpleSec [3] Cybercrime Magazine [4] Cision