KEEPER
Cybersecurity Starts Here®

DATASHEET
Healthcare Industry Brief

The Healthcare Industry is Under Attack

of healthcare organizations have been breached in the past 5 years[1]

is the average data breach cost per record in 2019[2]

increase of healthcare email fraud attacks in the past 2 years[3]

Cybersecurity for Healthcare Organizations

As the healthcare industry ramps up operations to manage the influx of COVID-19 cases, major organizational and network system changes may leave them vulnerable to cyberattacks. Cybercriminals are already targeting the healthcare industry with phishing campaigns and ransomware attacks that can adversely impact health information technology, medical records, and patient safety.[4]

Over 93% of healthcare organizations have been breached in the past two years[5], and over 80% of data breaches are caused by compromised passwords.[6] Keeper prevents password-related breaches and ransomware by giving administrators total visibility into employee password practices, with comprehensive reports and audits. Administrators can also control employee password habits and enforce security policies such as strong, unique passwords and multi-factor authentication (MFA).

Increased Productivity

Keeper is the ultimate cybersecurity and productivity application that protects every employee, whether they are remote or on-site against password-related data breaches and cyberthreats. Not only is Keeper easy for employees to use, but it makes it easy for them to comply with organizational password security policies.

Keeper automatically generates strong, unique passwords for each account; stores them in a secure vault that employees can access from any location and any desktop or mobile device, and auto-fills employee login credentials on all sites and apps. It even saves 2FA codes! Employees will never lose or forget another password, saving them time and hassle and eliminating reset-password help desk requests.

Two-Factor Authentication

Keeper supports multiple two-factor authentication (2FA) methods, including SMS, Keeper DNA® (smartwatch tap), TOTP (e.g., Google Authenticator and Authy), FIDO U2F (e.g. Yubikey), Duo, and RSA SecurID. 2FA may also be enforced through role-based controls.

Email Auto-Provisioning

Easily and quickly 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.

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.

HIPAA Compliance

Section 164.308(a)(5) requires "Procedures for creating, changing, and safeguarding passwords," and Section 164.312(a)(1) requires unique user identification, emergency access, and automatic log off. Section 164.312(b) addresses audit controls, including activity logs. Keeper provides every employee with a secure digital vault. Keeper generates strong, random passwords and automatically fills them for users. Keeper enables role-based access controls (RBAC) to enforce least-privilege policies. Folders and records can be securely shared, and permissions can be easily added and revoked. When an employee departs the company, their Keeper vault can be automatically locked and securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics. Keeper's zero-knowledge architecture ensures that only end-users have access to their Keeper Vault. Because Keeper Security never has access to user data, a business associate agreement (BAA) is not required for HIPAA compliance.

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 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 (RBAC) and the ability to track roles when employee positions or job duties change. This includes automatically locking vaults when employees depart the company.

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

GSA Schedule 70 Contract 47QTCA18D00C9 · HIPAA Compliant · 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] Industry Analysts [2] Cision PR Newswire [3] HIPAA Journal [4] NJCCIC [5] Herjavec Group Healthcare Cybersecurity Report 2020 [6] ZDNet