KEEPER
Cybersecurity Starts Here™

DATASHEET

Professional Services Industry Brief

Cyberattacks Threaten the Reputations of Professional Services Firms

2nd
most common target for ransomware attacks[1]

42%
of law firms have experienced a security breach[2]

56%
of law firms do not use file encryption[3]

273%
increase in large-scale data breaches in one year[4]

Cybercriminals Want Your Clients' Data

In the normal course of their business, law firms, accountants, M&A advisors, and other business consultants handle and store highly confidential personal and business information belonging to clients, including digital intellectual property, patent applications, financial records, tax filings, mergers and acquisitions information, and details of lawsuits. These professional services firms also rely heavily on digital technology to communicate with clients, collaborate with colleagues, and manage projects and client files.

As a result, professional services firms are vulnerable to highly-targeted cyberattacks where the perpetrators are seeking to steal specific information. If client data is compromised, the professional services firm's obligation to safeguard this information is thrown into question, and the firm's reputation can suffer significant damage. Yet many professional services firms are not adequately securing their employee passwords or their client data, even as they implement new digital channels, automation, and remote work technologies that expand their potential attack surface.

Keeper gives professional services firms the visibility and control they need to prevent password-related cyberattacks by enabling IT administrators to manage employee password usage and systems access throughout the data environment.

Keeper Helps You Protect Your Clients' Confidential Data and Maintain Regulatory & Industry Compliance

Professional services firms must comply with a number of regulatory and industry compliance standards regarding client privacy protections and systemic cyber risk mitigation. While specific compliance requirements are dependent on area of expertise, common mandates that professional services firms face include:

- Sarbanes-Oxley (SOX): Anti-fraud controls that apply to public companies and companies eyeing a potential initial public offering (IPO).
- Payment Card Industry Data Security Standard (PCI DSS): Security standards for handling payment card information.
- Statement on Standards for Attestation Engagements No. 18 (SSAE-18): Monitors and enforces controls around the applications and application infrastructure that impact financial reporting.

Keeper simplifies compliance monitoring and reporting by giving IT administrators full visibility and control over employee password usage and role-based systems access throughout their data environments, with customizable audit logs and event reporting.

Secure More than Just Passwords with Keeper Secure File Storage

In addition to securing employee passwords, Keeper helps professional services companies prevent data loss by allowing them to store sensitive files, documents, digital certificates, private keys, photos, and videos in a highly secure, encrypted digital vault. Employees can securely share files with colleagues with confidence, knowing that only the intended recipients can access the shared files.

Keeper uses PBKDF2 to derive authentication keys based on the user's Master Password, then generates individual record-level AES-256 encryption keys locally on the device to encrypt each stored file. Keeper's cloud only holds the encrypted ciphertext of each file. Sharing between users is performed using PKI to ensure that only the recipient of a shared file can decrypt it. Keeper's zero-knowledge encryption methods ensure that only the user can access and decrypt their stored files.

Defend Against Third-Party Vendor Breaches with BreachWatch™

Even if your password security is solid, your firm could be compromised through one of your vendors. With remote workforces having rapidly expanded, cybercriminals are taking advantage of the myriad of SaaS solutions that businesses are deploying to enable their remote workforces.

Keeper's BreachWatch for business protects your organization against third-party vendor breaches. BreachWatch for business doesn't depend on public breach notifications. It scans Dark Web forums and notifies organizations in real-time if any employee passwords have been compromised. This allows IT administrators to force password resets right away, minimizing the risk of cybercriminals using them to breach company systems.

IT Admin Insight

Every employee is provided with a secure digital vault. A security dashboard in the Admin Console provides an overview of weak passwords, password reuse, and 2FA enforcement, along with Role Based Access Control (RBAC) to enforce least privilege policies. Administration may be delegated according to department or by team leader, and folders and records can be securely shared and revoked. If an administrator or employee leaves the company, their vault can be automatically locked and securely transferred. Access logs to Keeper vaults can be audited for compliance or forensics.

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.

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 access controls (RBAC).

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 synchonizes 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 OpenLDAP. This enables rapid user provisioning and automatically adds Nodes (organizational units), Users, Roles, and Teams. Keeper enables 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.**

Keeper Third-Party Attestations and Certifications

[1] CIO Dive [2] FindLaw [3] CNBC