KEEPER
Cybersecurity Starts Here™

DATASHEET

Financial Services Industry Brief

$18M avg. cost of a financial services data breach[1]

20 number of days it takes to resolve a single phishing attack password for everything[2]

81% of data breaches are due to weak, default or stolen passwords[3]

Who uses Keeper? Thousands of organizations trust Keeper including Chase, Credit Union of Ohio, Raymond James, Quest Federal Credit Union and more.

Data Breaches 'Breaking the Bank' for Financial Institutions

Banks, credit unions and other financial institutions are prime targets for cybercriminals and the industry has been pummeled in recent years by wave after wave of cyberattacks. A recent report from Deloitte notes that cybersecurity continues to be a risk, and that cyberattacks from state actors are a growing threat to the industry.[4] For credit unions, small staff and lean budgets lead to increased risk.

Help Meeting Financial Services Compliance

Financial services reporting requires access tracking, least-privilege controls and audit logs. Keeper enables role-based controls and visibility into shared credentials. Access logs to Keeper vaults can be audited for compliance or forensics, making reporting much easier for IT managers at financial institutions.

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.

Reduce Support Costs

Drastically reduce help desk costs related to password issues. Forrester found that several large companies have allocated over $1 million annually for password-related support.

Increase Productivity

Save employees 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 employees from any device and location. Everything Keeper does is geared towards quick user adoption and security. Keeper is published in 21 languages for global use.

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.

Key Features

- Enhanced protection with two-factor authentication (2FA)
- Secure file storage and sharing
- Cloud-based, OS and device independent
- Admin console with reporting, auditing and analytics
- Fast deployment with AD/LDAP provisioning
- 24x7 support

Key Benefits

- Maintain regulatory compliance
- Increase employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimal training, fast time-to-security
- Improve employee security awareness and behavior

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 client-side. RSA encryption is used for secure record sharing between users and teams. Keeper's infrastructure syncs encrypted ciphertext between devices. All data intransit 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.

For Financial Institutions, Support for Departments, Offices and Branches

Keeper was created to support nodes and organizational units to accommodate any-sized institution. The Keeper Administrator can structure password management policies by role, team and organizational unit. Thus, different divisions, branches, and office locations can all be protected with Keeper, while having different access rights, permissions and policies for enforcing secure password management across the institution. Each business unit may utilize multiple Keeper Administrators with fine-grained permissions over their users, roles and teams.

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 Schedule70 Contract 47QTCA18D00C9 · TRUSTe CERTIFIED PRIVACY · AICPA SOC · PCI DSS COMPLIANT · HIPAA COMPLIANT

[1,2] Cost of Cyber Crime Study: Financial Services, Accenture Security, 2018

[3] 2018 State of Cybersecurity in Small and Medium Size Businesses, Ponemon Institute

[4] 2019 Banking and Capital Markets Outlook, Deloitte Center for Financial Services

Business Sales

Americas & APAC	**Ireland**	**Iberia & Italy**
+1 312 829 2680	+353 21 229 6020	+34 919 01 65 13
United Kingdom	**EMEA**	**Sweden & Nordics**
+44 20 3405 8853	+353 21 229 6011	+46 8 403 049 28
Germany & DACH	**Netherlands**	
+49 89 143772993	+31 20 262 0932	

Support

Consumer
+1 312 971 5702
Business (Americas & APAC)
+1 312 226 4782
Business (EMEA)
+353 21 229 6019

keepersecurity.com   sales@keepersecurity.com