



of all breaches take place
in financial services



records stolen from
financial institutions in 2015



of data breaches are due to weak,
default or stolen passwords

Data breaches ‘breaking the bank’ for financial institutions

It should go without saying that banks and financial institutions are prime hacking targets. The industry has been pummeled in recent years as wave after wave of cyber attacks have hit this sector. High-profile, large-scale attacks, such as the one that compromised the personal information of 76 million clients at JP Morgan Chase, illustrate that banks, credit unions, credit card companies, insurance companies and investment advisory organizations need to bolster their cybersecurity defenses.

The likelihood and potential impact of cyber attacks have subsequently made cybercrime a business risk, high on most executive agendas with a clear mandate to find ways to mitigate risk in an efficient and cost effective manner.

The greatest risk of breach can be isolated to the most basic of security concepts, the “password”

It is well-documented that passwords pose the greatest security risk to organizations today; Verizon reported over 81% of data breaches are due to weak employee passwords. Data breaches can be very costly and result in escalating response costs, lost productivity, regulatory fines and tarnished brand.

Protect your organization and customers with enterprise-strength password management

Keeper is the trusted leader in password management helping organizations manage, secure and enforce strong passwords across all employee logins, applications and sites. Employees can access Keeper natively on all mobile operating systems, desktops and browsers.

Data is protected in Keeper’s zero-knowledge security architecture with world-class encryption. Zero-knowledge means that only the user has knowledge of and access to their Master Password and the encryption key that is used to encrypt and decrypt their information. Keeper uses 256-bit AES encryption, which is used to encrypt classified data designated as TOP SECRET by the U.S. Government. Keeper also supports two-factor authentication to strengthen the protection of systems storing customer data.

Key Features

- Effective and intuitive password management
- Enhanced protection with two-factor authentication
- 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

- Mitigate cyber risk
- 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

Reduce costs and improve productivity with Keeper

Password resets are a major burden on the productivity of IT departments. The #1 help desk call is for a forgotten password - Gartner estimates the annual industry cost for password resets is around \$10B per year.

Keeper provides cost savings to customers by reducing help desk calls and increasing employee productivity. Employee passwords are encrypted and stored within Keeper so employees no longer need to remember them. Keeper auto-fills login credentials across mobile applications and browsers, which greatly improves productivity. If an employee forgets their master password, Keeper allows employees to set a security question so the master password can be recovered without IT assistance.

Finally, all Keeper users have 24x7 access to Keeper's dedicated customer care team. With Keeper, those costly help desk calls will be significantly reduced and the burden of resetting passwords will become a thing of the past for the IT department.

Secure more than just passwords

Passwords are one of many confidential assets that businesses need to secure. Keeper protects your sensitive files, documents, digital certificates, private keys, photos and videos in a highly-secure, encrypted digital vault. You can securely share files with colleagues and have confidence knowing that your information is backed up in Keeper's Cloud Security Vault™.

The Keeper difference

Only Keeper...

- Provides a simple, intuitive and unified password manager and digital vault
- Has an impenetrable security architecture with rigorous 3rd party audits (SOC II Type 2 compliant)
- Delivers native applications across all major devices, operating systems and browsers
- Provides password policy visibility and enforcement
- Has a dedicated customer care team 24x7x365



Who uses Keeper?

Over 3,000 organizations trust Keeper including BlackRock, Chase, Credit Union of Ohio, Raymond James and more.

