



of data breaches are due to weak, default or stolen passwords<sup>1</sup>



of people reuse passwords across business and personal accounts<sup>2</sup>



of people share passwords with colleagues to access accounts<sup>2</sup>

### **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 Business with Simple, 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.

### **Cost Savings 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™.

### **Key Features**

- Encrypted vault for each employee
- Enhanced protection with two-factor authentication
- Secure file storage and sharing
- Password generator
- Cloud-based, OS and device independent
- Admin console with reporting, auditing and analytics
- Fast deployment with AD/LDAP provisioning
- 24x7 support

### **Key Benefits**

- Prevent password-related data breaches and cyberthreats
- Strengthens compliance
- Boost employee productivity
- Enforce password policies and procedures
- Reduce help desk costs
- Minimal training, fast time-to-security
- Improve employee security awareness and behavior

## The Keeper Difference

- 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 and HIPAA 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

## Keeper Third-Party Attestations and Certifications



Gartner Peer Insights  
4.7 out of 5 stars



Trustpilot  
9.3 out of 10 stars



G2 Crowd  
Spring 2019 Enterprise Leader  
4.7 out of 5 stars



PCMag  
Editor's Choice  
4.5 out of 5 stars

### Sources

<sup>1</sup> Verizon Data Breach Report 2017

<sup>2</sup> Ponemon Insitute, 2019