ABOUT KEEPER

Keeper is a market-leading, top-rated zero-knowledge security and encryption platform for preventing password-related data breaches and other cyberthreats. Millions of consumers and thousands of businesses worldwide trust Keeper to mitigate the risk of password-related cyberattacks.

Keeper Security is privately-held and was founded in 2011 by Darren Guccione (CEO & Co-founder) and Craig Lurey (CTO & Co-founder). Keeper has four offices located in Chicago (Headquarters), California (Software Development), Ireland (EMEA Business Sales) and the Philippines (International Customer Support), serving over one million customers worldwide.

81% of breaches are due to weak password security
WHY ZERO-KNOWLEDGE?

Keeper is one of the few cybersecurity platforms that uses a zero-knowledge security model, which utilizes a unique encryption and data segregation framework to protect against a remote data breach. In a zero-knowledge model, the service provider has no knowledge as to what is stored on its servers. Because Keeper employs the zero-knowledge model, we have no way of accessing any of our users’ master passwords, nor can we access our customers’ encryption keys to decrypt their data.

Password Security Is a Critical Part of any Modern Identity and Access Management Stack

If employees are engaging in insecure password practices, such as using weak passwords, reusing passwords across accounts, and not using multi-factor authentication (2FA) wherever it’s supported, identity and access management (IAM) falls apart. Using Keeper, organizations can establish and enforce robust password security throughout the organization, including the use of strong, unique passwords for all accounts and multi-factor authentication (MFA). Keeper also makes it easy to manage role-based access control (RBAC), least-privilege access, and other security policies.
BUSINESS DATA POINTS

71% of breaches are financially motivated¹

94% of SMBs globally have experienced a cyberattack within their companies’ lifetime²

72% of malware was delivered by email³

95% of cybersecurity breaches are due to human error⁴

Sources: ¹² Verizon ³ Ponemon ⁴ Cybint
**Keeper Business**

Keeper Business provides IT administrators with complete visibility into employee password practices, allowing them to enforce company password policies, monitor employee compliance, and generate audit trails and reports. Keeper also securely manages the lifecycle of privileged account credentials with role-based access control (RBAC) and controlled credential sharing.

**Keeper MSP**

Designed specifically for managed security providers (MSPs), KeeperMSP enables MSPs to solve their customers’ password management and security issues by offering them password management as a service. With KeeperMSP, managed service providers can independently provision, manage, and monitor multiple customers from a central admin dashboard, with robust reporting and auditing tools to enforce security and compliance requirements such as RBAC, 2FA, SIEM event reporting, and regulatory and industry compliance.

**BreachWatch® For Business**

Keeper BreachWatch scans the dark web and provides end-users with up-to-date risk assessments of passwords directly in their vaults, and provides administrators with a summary view of breached password status across the organization.

**KeeperChat® for Business**

KeeperChat provides the highest level of privacy, security, organization and storage for text messaging. KeeperChat is super fast, easy to use and far more secure, much like our password management products, zero-knowledge means only the user has the ability to decrypt and access their information on their device.

**Advanced Reporting and Alerts Module (ARAM)**

ARAM takes Keeper’s reporting capabilities to the next level with enterprise-grade, customizable reporting and alerting functionality, allowing administrators to monitor any size user population, view focused, summary trend data, and receive real-time notifications of risky or unusual behaviors.

**Keeper Enterprise**

Keeper Enterprise includes everything in Keeper Business and adds single sign-on (SAML 2.0) authentication, automated team management, advanced two-factor authentication, (DUO & RSA), Active Directory and LDAP sync, SCIM and Azure AD provisioning, email auto-provisioning, command line provisioning, and developer APIs for password rotation and backend integration.
CONSUMER DATA POINTS

- 39% of consumers use the same password for every online service.
- 70% of consumers have more than 10 password-protected online accounts; 30% have “too many to count.”
- 53% of people admit they use the same password for different accounts.
- 84% of online adults in the U.S. primarily keep track of their passwords by memorizing or writing them down.

WHAT MAKES KEEPER FOR CONSUMERS STAND OUT?

Keeper’s password manager stores all of your passwords in a secure digital web vault that you can easily access from any device, running any operating system, and with almost any browser. It autofills your login credentials on all of your websites and apps. You can easily protect your web vault with the multi-factor authentication (2FA) of your choosing.

To access your Keeper web vault on desktop and laptop computers (Windows, Mac, and Linux), you can use the Keeper desktop app or our browser extension, which works in all modern browsers. On mobile devices, download the Keeper app for iOS or Android. Real-time sync ensures that you’re always accessing the most current version of your Keeper vault, no matter which device you’re using.

Once inside your Keeper web vault, you view and edit all of your website login credentials, including your 2FA codes, as well as share records with other Keeper users. Custom fields let you add other important information about your Keeper records, such as answers to security questions. You can also use your Keeper web vault to store other important information, such as the password to your home WiFi network, the security code for your alarm system, or PINs for desktop or mobile devices.

Keeper is designed to be as user-friendly as possible. If you do have a question or need help, we maintain an extensive self-help library of user guides and videos on our website. Need to talk to someone? Our customer support team is always a message away, 24/7.
Other Reasons that Customers Choose Keeper

Your Keeper vault can store all of your digital assets, not just your passwords! Keeper’s Secure File Storage is your digital safety deposit box, a secure place to store critical documents so that you can immediately find and access them when you need them. Use it to store insurance and loan paperwork, vaccination and other healthcare records, deeds and titles, bank account statements, passport photos, and more. You can also use Keeper Secure File Storage for backups of family photographs and videos, so that your priceless memories are kept safe for both your current family and future generations to enjoy.

Speaking of families, in addition to our personal plans for individual consumers, Keeper offers Family plans that cover up to five members of a household, making it easy for household members to share passwords, 2FA codes, documents, and files.

Trusted by millions of users worldwide, Keeper maintains a rating of “Excellent” on Trustpilot, 4.5/5 on Google Play, and 4.9/5 on the iOS App Store. We’ve also been named PCMag’s Best Password Manager of the Year for three years running.

Data Protection

Keeper’s proprietary zero-knowledge encryption methods ensure that only the user can access and decrypt their stored passwords and files. Nobody else can access your Keeper vault - not even Keeper’s own employees!

To protect your passwords and 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 record. 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. But you don’t have to worry about this, it’s all completely transparent to you as an end-user.

In the event of an emergency, what happens to the passwords and files in your Keeper vault? Keeper Emergency Access lets you choose up to five trusted family members and friends to be granted access to your Keeper vault should you not access it for a period of time that you specify.
CONSUMER SOLUTIONS

Keeper Unlimited
Keeper Personal users store their passwords in a private, encrypted digital vault that can be accessed from anywhere, using any device, running any operating system. Keeper autofills login credentials across websites and apps, which makes it easy to use a strong, unique password for every online account. In addition to passwords, Keeper can securely store payment card information, along with sensitive files, documents, photos, and videos. It even stores 2FA codes.

Keeper Family
Keeper Family plans extend all the great features of Keeper Personal to up to five users in a household, with easy and secure sharing features so that family members can share passwords, files, payment cards, and more.

BreachWatch®
Keeper BreachWatch scans the dark web and provides end-users with up-to-date risk assessments of passwords directly in their vaults, and provides administrators with a summary view of breached password status across the organization.

KeeperChat®
KeeperChat is one of the world’s most secure messaging platforms for consumers. KeeperChat is super fast, easy to use and far more secure, much like our password management products, zero-knowledge means only the user has the ability to decrypt and access their information on their device.
RATINGS & AWARDS

Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice for two consecutive years and is the winner of four G2 awards for Best Software and four InfoSec Award for Best Product in Password Management for SMB and Best Product for SMB Cybersecurity. Keeper is SOC-2, FIPS 140-2 and ISO 27001 Certified and is listed for use by the U.S. federal government through the System for Award Management (SAM).

Publisher's Choice Cybersecurity Password Management
Cutting Edge Chief Executive of the Year

Best Password Manager of the Year & Editors' Choice 2019 & 2020
Editors' Choice 2018 & 2019

Best Product in Password Management
Best Product for SMB Cybersecurity
Publisher's Choice for Chief Executive of the Year
Most Innovative CTO of the Year

Gartner Peer Insights
Spiceworks
Editors' Choice
2021 Enterprise Leader

4.9 out of 5 stars
5 out of 5 stars
4.5 out of 5 stars
4.7 out of 5 stars
KEEPER LEADERSHIP

The Keeper leadership team is committed to customer success. We have deep expertise in cybersecurity software, cloud computing and mobile device technologies.

Darren Guccione  
CEO & Co-Founder

Craig Lurey  
CTO & Co-Founder

Amy Lindenmeyer  
CFO

Mark Cravotta  
CRO

Lauren Word  
Human Resources Manager

Nikki Jamison  
Associate Corporate Counsel

Steve Beckmeier  
Sr. Director of Inside Sales, North America

Rainer Enders  
VP of Engineering

Patrick Tiquet  
VP of Security & Architecture

Gene Dias  
VP of Technology

Sean Elder  
Global Director of Customer Success

Mitch Rosen  
Global Director of Solutions Engineering
OFFICE LOCATIONS

Keeper Security is a global company headquartered in Chicago, IL, with offices in El Dorado Hills, California (Software Development), Cork, Ireland (EMEA Business Sales), and Cebu, Philippines (International Customer Support).