Company Overview and Solutions Guide
About Keeper

Keeper is the leading provider of zero-trust and zero-knowledge security cloud services spanning secrets management, privileged access, secure remote infrastructure access, and encrypted messaging. 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.
Zero-Knowledge Security Model

Keeper is one of the few cybersecurity platforms that use a zero-knowledge security model, which utilizes a unique encryption and data segregation framework to protect against a remote data breach.

Encryption and decryption occur on the device level, upon a user logging into their Keeper vault. Each individual record stored in the user’s vault is encrypted with a random 256-bit AES key that is generated on the user’s device. The data remains encrypted after it leaves the user’s device, transmits over the internet, and is stored in the Keeper vault.

This means that no one – not even Keeper’s own employees – can access our users’ master passwords, the encryption keys used to decrypt their data, or the contents of their Keeper vaults. The data can only be decrypted by the end-user, on their device, using their Master Password or Elliptic Curve private key.

The method of encryption that Keeper uses is a well-known, trusted algorithm called AES (Advanced Encryption Standard) with a 256-bit key length. Keeper uses PBKDF2 with HMAC-SHA256 to convert the user’s Master Password to a 256-bit encryption key with a minimum of 100,000 rounds. Sharing of secrets between users uses Elliptic Curve Cryptography for secure key distribution.

Keeper’s SSO Cloud capability provides authentication against a SAML 2.0 identity provider, while retaining full Zero-Knowledge encryption with the user’s vault.
Compliance & Audits

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). Keeper is the first and only password manager and secrets management solution to be listed on the FedRAMP marketplace.
Commercial Solutions

Zero-Trust Password Management

The zero-trust security framework is centered around three core principles: assume breach, verify explicitly and ensure least privilege access. Without comprehensive password security, zero-trust falls apart.

Keeper’s enterprise password manager (EPM) enables organizations to implement zero-trust network access while dramatically reducing administrative overhead, improving reliability and performance, and enhancing employee productivity. It administrators get the tools they need to establish and enforce robust password security throughout the organization, verify users and devices, and manage role-based access control (RBAC), least-privilege access, and other security policies, such as multi-factor authentication (MFA).
## Business Solutions

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keeper Business</td>
<td>Keeper Business provides companies 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 RBAC and controlled credential sharing.</td>
</tr>
<tr>
<td>Keeper Enterprise</td>
<td>Keeper Enterprise includes everything in Keeper Business and adds single sign-on (SSO) SAML 2.0 authentication, automated team management, advanced MFA (DUO &amp; 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.</td>
</tr>
<tr>
<td>Keeper Security Government Cloud (KSGC)</td>
<td>Powered by AWS GovCloud, KSGC is the first and only password and secrets management platform listed on the FedRAMP marketplace. KSGC protects organizations of all sizes, from small municipalities and institutions to large federal agencies and campuses, enabling them to mitigate risk, prevent cyberattacks, and simplify compliance with HIPAA, FINRA, SOC, ITAR, and more.</td>
</tr>
<tr>
<td>KeeperMSP</td>
<td>Designed specifically for managed service providers (MSPs), KeeperMSP enables MSPs to solve their customers’ password management and security issues while generating additional passive revenue by offering them Keeper’s top-rated EPM as a service. KeeperMSP allows managed service providers to 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, MFA, SIEM event reporting, and regulatory and industry compliance.</td>
</tr>
<tr>
<td>Advanced Reporting and Alerts Module (ARAM)</td>
<td>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.</td>
</tr>
<tr>
<td>BreachWatch® for Business</td>
<td>Keeper BreachWatch scans the dark web, gives end users 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.</td>
</tr>
<tr>
<td>Keeper SSO Connect®</td>
<td>Keeper SSO Connect® is a SAML 2.0 service that seamlessly and quickly integrates with your existing SSO solution, enhancing and extending it with zero-knowledge password management and encryption. Keeper SSO Connect deploys rapidly in any data environment: on-prem, hybrid cloud, single cloud, or multi-cloud. SSO integration with Keeper uses Elliptic Curve cryptography to preserve zero-knowledge.</td>
</tr>
</tbody>
</table>
## Infrastructure Secrets Management

**Keeper Secrets Manager**

Keeper Secrets Manager is a cloud-based, zero-trust, zero-knowledge solution for eliminating “secrets sprawl” and securing privileged credentials and infrastructure secrets, such as SSH and API keys, database passwords, and certificates. Keeper Secrets Manager ensures that all servers, CI/CD pipelines, developer environments, and source code pull secrets from an encrypted API endpoint. Keeper Secrets Manager seamlessly integrates into any environment, with no additional hardware or cloud-hosted infrastructure required, and out-of-the-box integrations with Github Actions, Kubernetes, Ansible, and a wide variety of other DevOps tools.

## Zero-Trust Remote Infrastructure Access

**Keeper Connection Manager (KCM)**

Keeper Connection Manager provides IT and DevOps teams with fast, passwordless, and hyper-secure remote access to servers and desktops without a VPN. Users can access their desktops using any modern web browser, with no need to install or configure agents or client software. Powered by Apache Guacamole and integrated into Keeper’s zero-trust, zero-knowledge security and encryption architecture, KCM offers distributed teams a fast and seamless remote desktop experience without sacrificing stability or security. KCM is also fully integrated into Keeper Secrets Manager for managing privileged sessions.

**With Keeper Connection Manager you can:**

- Replace VPNs by providing access through a secure bastion
- Provide browser based access to Virtual Desktop Infrastructure (VDI)
- Allow third-party vendor access without exposing any passwords
- Restrict access to sensitive assets and record all sessions
- Ensure MFA and SSO is required in front of legacy systems and databases
- Provide access to a thick client without software installation
- Grant engineers access to sensitive systems based on roles or groups

## Zero-Knowledge Encrypted Messaging

**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 than other text messaging solutions. KeeperChat utilizes the same zero-knowledge architecture as the rest of our solutions, ensuring that only KeeperChat users have the ability to decrypt and access their messages on their device.
Consumer Solutions
What makes Keeper for Consumers stand out?

Store an unlimited number of passwords & access them from any device
Keeper’s password manager stores all of your passwords and MFA codes in a secure digital web vault and auto-fills your login credentials on all of your websites and apps.

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.

Stay organized with custom fields and custom record types
Once inside your Keeper web vault, you can view and edit all of your website login credentials, including your MFA 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. Additionally, Custom Record Types allow you to use your Keeper web vault to store and organize other important information, such as payment cards, the password to your home WiFi network, the security code for your alarm system, or PINs for desktop or mobile devices.

Emergency access
In the event of an emergency, what happens to the passwords and files in your Keeper vault? Keeper Emergency Access lets consumers choose up to five trusted contacts to be granted access to their Keeper vault should they not access it for a period of time that they specify.

Easy to install; easy to use
Keeper is designed to be as user-friendly as possible. If you ever 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.

Enterprise-grade data protection – for consumers
Keeper’s consumer solutions utilize the same proprietary zero-knowledge encryption as our commercial products, putting enterprise-grade security into the hands of consumers. Only the user can access and decrypt their stored passwords and files. Nobody else can access our users’ Master Passwords, encryption keys, or vault contents - not even Keeper’s own employees!
## Consumer Subscription Packages

<table>
<thead>
<tr>
<th>Plan</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keeper Unlimited</td>
<td>Keeper Personal allows users to store their passwords in a private, encrypted digital vault that can be accessed from anywhere, using any device, running any operating system. Keeper auto-fills 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 MFA codes.</td>
</tr>
<tr>
<td>Keeper PlusBundle</td>
<td>The Keeper PlusBundle includes all of the great features of Keeper Unlimited, plus BreachWatch® dark web monitoring, and Secure File Storage.</td>
</tr>
<tr>
<td>Keeper Family Unlimited / Keeper Family PlusBundle</td>
<td>Keeper’s Family plans extend all the great features of Keeper Unlimited/Keeper PlusBundle 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.</td>
</tr>
<tr>
<td>Secure File Storage</td>
<td>Store more than just passwords in your Keeper Vault. 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.</td>
</tr>
<tr>
<td>BreachWatch®</td>
<td>Keeper BreachWatch scans the dark web and alerts consumers if any of their credentials are found on cybercrime forums.</td>
</tr>
<tr>
<td>KeeperChat®</td>
<td>The world’s most secure messaging platform for consumers, KeeperChat is super fast, easy to use, and utilizes the same zero-knowledge architecture as our award-winning password manager. This ensures that only you have the ability to decrypt and access your messages on your devices.</td>
</tr>
</tbody>
</table>
The World’s Top-Rated Password Manager

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. 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.

Gartner Peer Insights
4.6 out of 5 stars

Spiceworks
4.9 out of 5 stars

Editors’ Choice
4.5 out of 5 stars

2021 Enterprise Leader
4.7 out of 5 stars

Editor’s Choice CEO of the Year
Editor’s Choice CTO of the Year
Editor’s Choice Data Security
Next Gen PAM for Cloud Infrastructure
Market Leader Passwordless Authentication
Hot Company Secrets Management
Next Gen Zero Trust

Hot Company in IAM
Most Innovative in Endpoint Security
Cutting Edge in Security Company of the Year

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

Learn More
Learn More
Learn More
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

Kerrie Carroll
CHRO

Lauren Word
Human Resources Manager

Nikki Jamison
Associate Corporate Counsel

Rainer Enders
VP of Engineering

Gene Dias
VP of Technology

Patrick Tiquet
VP of Security & Architecture

Steve Beckmeier
Sr. Director of Inside Sales, North America

Sean Elder
Sr. Director of Global Customer Success

Marcia Dempster
Sr. Director of Channel Sales, Americas

Mitch Rosen
Global Director of Solutions Engineering

Ibrahim Lamdouar
Director of Engineering

Tyson Cutler
Director of Quality Assurance

© 2022 Keeper Security, Inc.
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).