



Company Overview and Solutions Guide





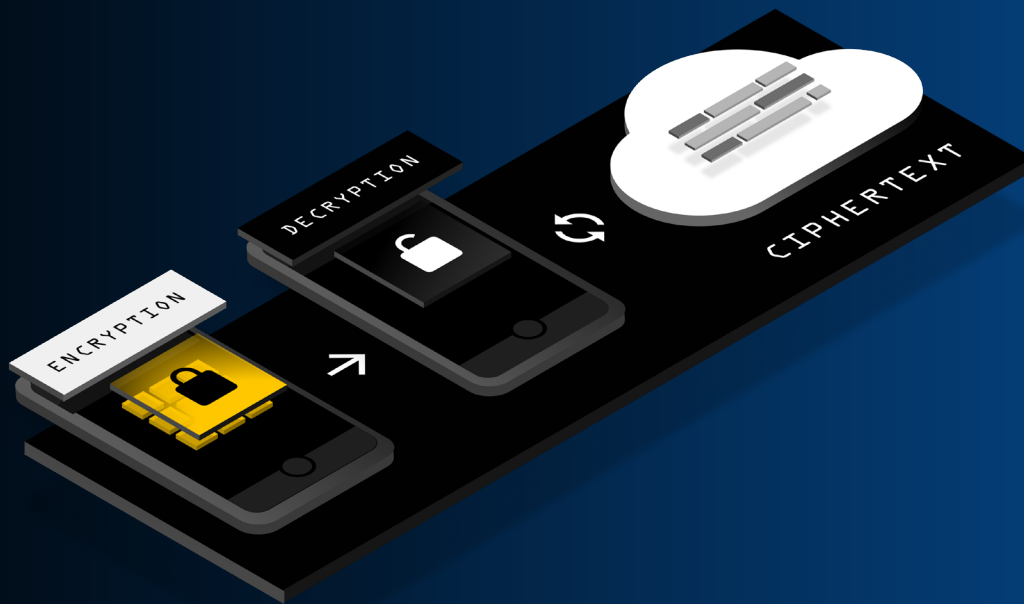
About Keeper

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.

81% of breaches are due to a failure to secure passwords, credentials and secrets.





Zero-Knowledge Security Model

Keeper is one of the few cybersecurity platforms that uses a zero-knowledge security model, with 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 1,000,000 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 Fanatical About Data Protection and Security

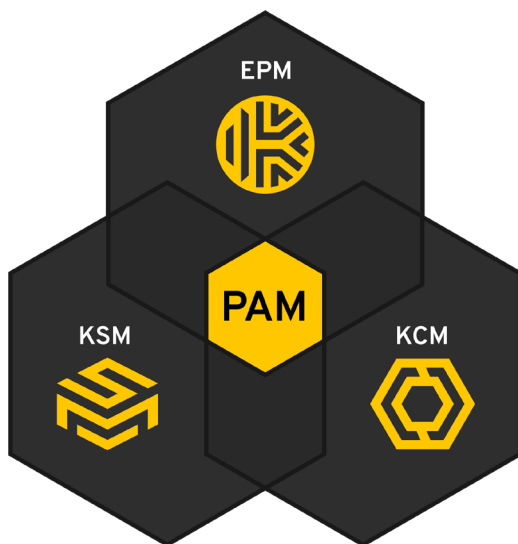
Keeper utilizes best-in-class security with a zero-trust framework and zero-knowledge security architecture to safeguard your information and mitigate the risk of a data breach.

 SOC 2	<p>Keeper is certified as SOC 2 Type 2 compliant in accordance with the AICPA Service Organization Control framework. SOC 2 certification helps ensure that your vault is kept secure through the implementation of standardized controls as defined in the AICPA Trust Service Principles framework.</p>
 ISO 27001 Certified	<p>Keeper is ISO 27001 certified, covering the Keeper Security Information Management System which supports the Keeper Enterprise Platform. Keeper's ISO 27001 certification is scoped to include the management and operation of the digital vault and cloud services, software and application development, and protection of digital assets for the digital vault and cloud services.</p>
 FIPS 140-2 Validated	<p>Keeper utilizes FIPS 140-2 validated encryption modules to address rigorous government and public sector security requirements. Keeper's encryption has been certified by the NIST CMVP and validated to the FIPS 140 standard by accredited third party laboratories. Keeper has been issued certificate #3967 under the NIST CMVP.</p>
 FedRAMP Authorized  StateRAMP Authorized	<p>Keeper Security Government Cloud (KSGC) is KSI's password management and cybersecurity platform for public sector agencies. KSGC is a FedRAMP and StateRAMP Authorized provider, hosted in AWS GovCloud (US). KSGC can be found on the FedRAMP and StateRAMP marketplaces.</p> <p>The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. federal government program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. FedRAMP enables government agencies to use modern cloud technologies, with an emphasis on security and protection of federal information and helps accelerate the adoption of secure, cloud solutions.</p>

For a full list of Keeper Security Compliance & Audits please visit [Keepersecurity.com/security](https://keepersecurity.com/security).

Commercial Solutions

Next-Gen, Zero-Trust, Zero-Knowledge
Privileged Access Management (PAM) Platform



KeeperPAM™

Keeper's cybersecurity PAM (privileged access management) SaaS-based platform enables organizations to achieve full visibility, security, control and reporting across every user on every device in an organization.

The platform enables zero-trust and zero-knowledge security and compliance by unifying three integral products into one platform.



82% of breaches involve the human element - with the majority due to stolen or weak passwords, credentials and secrets.¹



Enables organizations to securely manage, protect, discover, share and rotate passwords with full control and visibility to simplify auditing and compliance.



Delivers a fully-managed, cloud-based solution to secure infrastructure secrets such as API keys, database credentials, access keys and certificates.



Provides an agentless remote desktop gateway for instant privileged session management, remote infrastructure access and secure remote database access to RDP, SSH keys, database and Kubernetes endpoints – no VPN required.





KeeperPAM Addresses the Key Pain Points and Requirements in Organizations to Prevent Data Breaches

- | | |
|--|--|
|  Password Management |  Password Discovery |
|  Password Sharing |  Single Sign-On Security |
|  Password Rotation |  Passwordless Authentication |
|  Secrets Management for DevOps |  Credential Governance & Controls |
|  Privileged Session Management |  SSH Key Management |
|  Remote Infrastructure Access |  Secure Remote Database Access |
|  Zero-Trust, Zero-Knowledge Security |  Industry Compliance & Reporting |








Products and Solutions

Protect Your Organization	
 KeeperPAM	Keeper’s patented PAM platform enables organizations to achieve complete visibility, security, control and reporting across every user on every device in any organization. The platform is cloud-based, enables zero-trust and zero-knowledge security, and meets compliance mandates by unifying three integral solutions into one unified solution.
 Keeper Password Manager for Business	Keeper Password Manager for 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.
 Keeper Enterprise Password Manager	Keeper Enterprise Password Manager includes everything in Keeper Business and adds single sign-on (SSO) SAML 2.0 authentication, automated team management, advanced MFA (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.

 Keeper Security Government Cloud (KSGC)	<p>Powered by AWS GovCloud, Keeper Security Government Cloud is a FedRAMP and StateRAMP Authorized password management and cybersecurity platform. 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.</p>
 KeeperMSP	<p>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.</p>
 Keeper Secrets Manager (KSM)	<p>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</p>
 Keeper Connection Manager (KCM)	<p>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.</p>

Powerful Add-Ons for Superior Team Protection

 Advanced Reporting and Alerts Module (ARAM)	<p>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.</p>
 BreachWatch® for Business	<p>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.</p>
 Compliance Reports	<p>Keeper Compliance Reports allow Keeper Administrators to monitor and report the access permissions of privileged accounts across the entire organization, in a zero-trust and zero-knowledge security environment. Keeper Compliance Reports supports audits for Sarbanes Oxley (SOX) and other regulations that require access-control monitoring and event auditing. On-demand compliance reports can be forwarded to automated compliance systems and external auditors.</p>
 KeeperChat® for Business	<p>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.</p>
 Keeper SSO Connect®	<p>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.</p>

Consumer Solutions

What makes Keeper stand out for consumers?

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.

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!

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.



Consumer Subscription Packages

 Keeper Unlimited	<p>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.</p>
 Keeper PlusBundle	<p>The Keeper PlusBundle includes all of the great features of Keeper Unlimited plus BreachWatch® dark web monitoring, and Secure File Storage.</p>
 Keeper Family Unlimited / Keeper Family PlusBundle	<p>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.</p>
 Secure File Storage	<p>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.</p>
 BreachWatch®	<p>Keeper BreachWatch scans the dark web and alerts consumers if any of their credentials are found on cybercrime forums.</p>
 KeeperChat®	<p>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.</p>
 One-Time Share	<p>Keeper "One-Time Share" provides time-limited secure sharing of a record to anyone without having to create a Keeper account. One-Time Share is the most secure way to send confidential information without exposing it over email, text message or messaging.</p>

Top Industry Ratings, InfoSec Awards & User Reviews



Gartner Peer Insights
4.7 out of 5 stars



Spiceworks
4.9 out of 5 stars



Editors' Choice
4.5 out of 5 stars



2023 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

[Learn More](#)



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

[Learn More](#)



- 🏆 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](#)



[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



Nikita Word
HR Director



Nikki Jamison
General Counsel



Rainer Enders
VP of Engineering



Gene Dias
VP of Technology



Patrick Tiquet
VP of Security & Architecture



Sean Elder
VP of Global Customer Success



Steve Beckmeier
Sr. Director of Inside Sales,
North America



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



Des Donohoe
Director of Sales, EMEA



Paula Johnson
Director of Talent Acquisition



Andrea Restrepo
Director of Enterprise Sales



Daniel Searls
Director of Customer Success,
EMEA



Anne Cutler
Director of Global
Communications



Max Scholle
Director of Digital Marketing



Brad Cain
Director of B2B Growth
Marketing



Tess Kostiner
Director of Affiliate Marketing



Zane Bond
Head of Product



John Twomey
Director of Finance, EMEA



Tingting Gong
Director of Consumer Support



Paul Aiello
Global Director of B2B Support

Office Locations

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

