KEEPER®

Company Overview and Solutions Guide

REV JAN 2025

Keeper Security is privately held and was founded in 2011 by **Darren Guccione** (CEO & Co-founder) and **Craig Lurey** (CTO & Co-founder). Keeper is headquartered in Chicago, Illinois with offices in El Dorado Hills, California (Software Development); Cork, Ireland (EMEA Business Sales); Tokyo, Japan (APAC Business Sales); and Cebu, Philippines (International Customer Support); serving millions of individuals and thousands of organizations worldwide.

About Keeper

Keeper is the leading provider of zero-trust privileged access management software that secures and manages access to your critical resources including servers, web apps, databases and workloads. As a cloud-native, zero-knowledge platform, Keeper delivers enterprise password management, secrets management, connection management, zero-trust network access and remote browser isolation in one easy-to-use interface. Keeper's solutions for personal users, MSPs and businesses use the same technology and security as their enterprise platform.

92% of IT and security professionals report cyber attacks are more frequent today than one year ago.

Source: Keeper Security, The Future of Defense: IT Leaders Brace for Unprecedented Cyber Threats report, 2024

Zero-Knowledge Security Model

Keeper is one of the few cybersecurity platforms that uses a zero-knowledge security model, with full end-to-end encryption and a unique data segregation framework to protect against cyber attacks and data breaches.

Encryption and decryption occur on the device level, upon a user logging in to 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 Advanced Encryption Standard (AES) 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.

KEEPER

Compliance & Audits

SOC 2

Customer vault records are protected using stringent and tightly monitored internal control practices. Keeper has been certified as SOC 2 Type 2 compliant for over ten years in accordance with the AICPA Service Organization Control framework. SOC 2 compliance helps ensure user vaults are kept secure through the implementation of standardized controls as defined in the AICPA Trust Service Principles framework.

ISO Certified

Keeper is ISO 27001, 27017 and 27018 certified, covering the Keeper Security Information Management System and Cloud Infrastructure, which supports the Keeper Enterprise Platform. Keeper's ISO certifications include the management and operation of the digital vault and cloud services, cloud security controls, data privacy controls, software and application development, and protection of digital assets for both the digital vault and cloud services.

FIPS 140-3 Validated

Keeper utilizes FIPS 140-3 validated encryption modules to address rigorous government and public sector security requirements. Keeper's encryption has been certified by the NIST Cryptographic Module Validation Program (CMVP) and validated to the FIPS 140 standard by accredited third-party laboratories. Keeper uses FIPS 140-3 validated encryption that has been issued certificate #4743 under the NIST CMVP.

FedRAMP Authorized **StateRAMP Authorized**

Keeper Security Government Cloud (KSGC) is KSI's password management and privileged access management 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. 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.

For a full list of Keeper Security Compliance & Audits please visit Keepersecurity.com/security.

Zero-Trust, Zero-Knowledge Privileged Access Management

Keeper's revolutionary PAM platform enables organizations to achieve full visibility, security, control and reporting across every user on every device in an organization. KeeperPAM™ secures and manages access to your critical resources, including servers, web apps, databases and workloads. Every user and device in an enterprise is authenticated and authorized with monitoring, threat tracking and reporting. As a cloud-native, zero-knowledge platform, KeeperPAM combines enterprise password management, secrets management, connection management, zero-trust network access and remote browser isolation in one easy-to-use interface. By implementing zero-trust architecture, enforcing least privilege principles and offering advanced monitoring and management tools, KeeperPAM helps organizations:

- Comply with regulatory standards
- Protect against data breaches and credential theft
- Simplify and secure user access
- Reduce administrative burden on IT staff
- Enhance overall security posture while increasing operational efficiency
- Mitigate risk to critical data if a data breach occurs

This unified platform not only safeguards critical infrastructure but also streamlines processes, reduces risks associated with privileged accounts and supports the organization's compliance and audits.

Enterprise password management - Protect, discover, share and rotate passwords, passkeys and confidential data in a zero-knowledge vault with role-based access controls, auditing and compliance. A simple approach to storing passwords, passkeys and files for every employee on every device. When paired with SSO integration, users receive a passwordless experience.

Secrets management - Integrate CI/CD pipelines, DevOps tools, custom software and multi-cloud environments into a fully-managed, zero-knowledge platform to secure infrastructure secrets and reduce secrets sprawl. Provides scheduled or on-demand rotation of service account credentials.

Zero-trust network access - Establish cloud and self-hosted privileged sessions, create tunnels, power zero-trust infrastructure access and secure remote database access without a VPN.

Remote Browser Isolation - Secure internal web-based applications, cloud apps and BYOD devices from malware, prevent data exfiltration and control browsing sessions with full auditing, session recording and password autofill.

Admin Console - Manage and deploy Keeper to users, integrate with identity providers, monitor activity and establish role-based enforcement policies.

Control Plane - Orchestrate and monitor the various components and activities related to privileged access, session management, policies and workflow.

Business Solutions

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 integral PAM functionality into one unified solution.

Keeper Business Password Manager

Keeper Business Password Manager 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)

Powered by AWS GovCloud, Keeper Security Government Cloud is a FedRAMP and StateRAMP Authorized password management and privileged access management platform. KSGC protects organizations of all sizes, from small municipalities and institutions to large federal agencies and campuses, enabling them to mitigate risk, prevent cyber attacks and simplify compliance with HIPAA, FINRA, SOC, ITAR and more.

KeeperMSP

KeeperMSP is a powerful multi-tenant, zero-knowledge platform designed exclusively for MSPs that enables you to protect your Managed Companies (MCs) and your MSP from unauthorized access and data breaches. MSPs can offer both an enterprise password manager and a full Privileged Access Management solution to MCs to protect standard users and privileged users alike. Provisioning and management are handled through a centralized admin console, providing MSPs with streamlined control while ensuring robust privacy and security for all users.

Powerful Add-Ons for Superior Team Protection

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 summary trend data and receive real-time notifications of risky or unusual behaviors. All event data can be logged into third party SIEMs.

BreachWatch® for Business

Keeper BreachWatch constantly scans users' Keeper Vaults for passwords exposed on the dark web and sends immediate alerts. A summary view of breached password statuses across the organization is available to admins.

Compliance Reports

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.

KeeperChat® for Business

KeeperChat provides the highest level of privacy, security, organization and storage for private messaging. KeeperChat is super fast, easy to use and far more secure than other secure 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 devices.

Keeper SSO Connect®

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.

Consumer Solutions

Store unlimited credentials and access them from any device

Keeper's password manager stores all of your passwords, passkeys 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 Vault on desktop and laptop computers (Windows, Mac, and Linux), you can use the Keeper desktop app, browser extension or web vault. 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 or with non-Keeper users via One-Time Share. 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.

Consumer Solutions

Keeper Unlimited

Keeper Unlimited 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. KeeperFill 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, sensitive files, documents, photos and videos. It even stores MFA codes.

Keeper Family

Keeper's family plan extends all the great features of Keeper Unlimited to up to five users in a household, with easy and secure sharing capabilities so that family members can share passwords, files, payment cards and more. Family members cannot access each other's passwords unless they're shared, and 10GB of Secure File Storage is included with a subscription.

Secure File Storage

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 needed. Use it to store insurance and loan paperwork, vaccination and other healthcare records, deeds and titles, bank account statements, photos and more.

BreachWatch®

Keeper BreachWatch scans the dark web and alerts users if any of their credentials are found so that they can take immediate action.

KeeperChat®

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. KeeperChat is free for all personal users.

Industry Reviews and Awards

Apple App Store
4.9 out of 5 stars

Google Play Store
4.6 out of 5 stars

SoftwareReviews
8.9 out of 10

GetApp
4.7 out of 5 stars

G2
Keeper Password Manager
4.6 out of 5 stars

Gartner Peer Insights
Enterprise Password Management
4.6 out of 5 stars

PCPro (UK)
Recommended
5 out of 5 stars

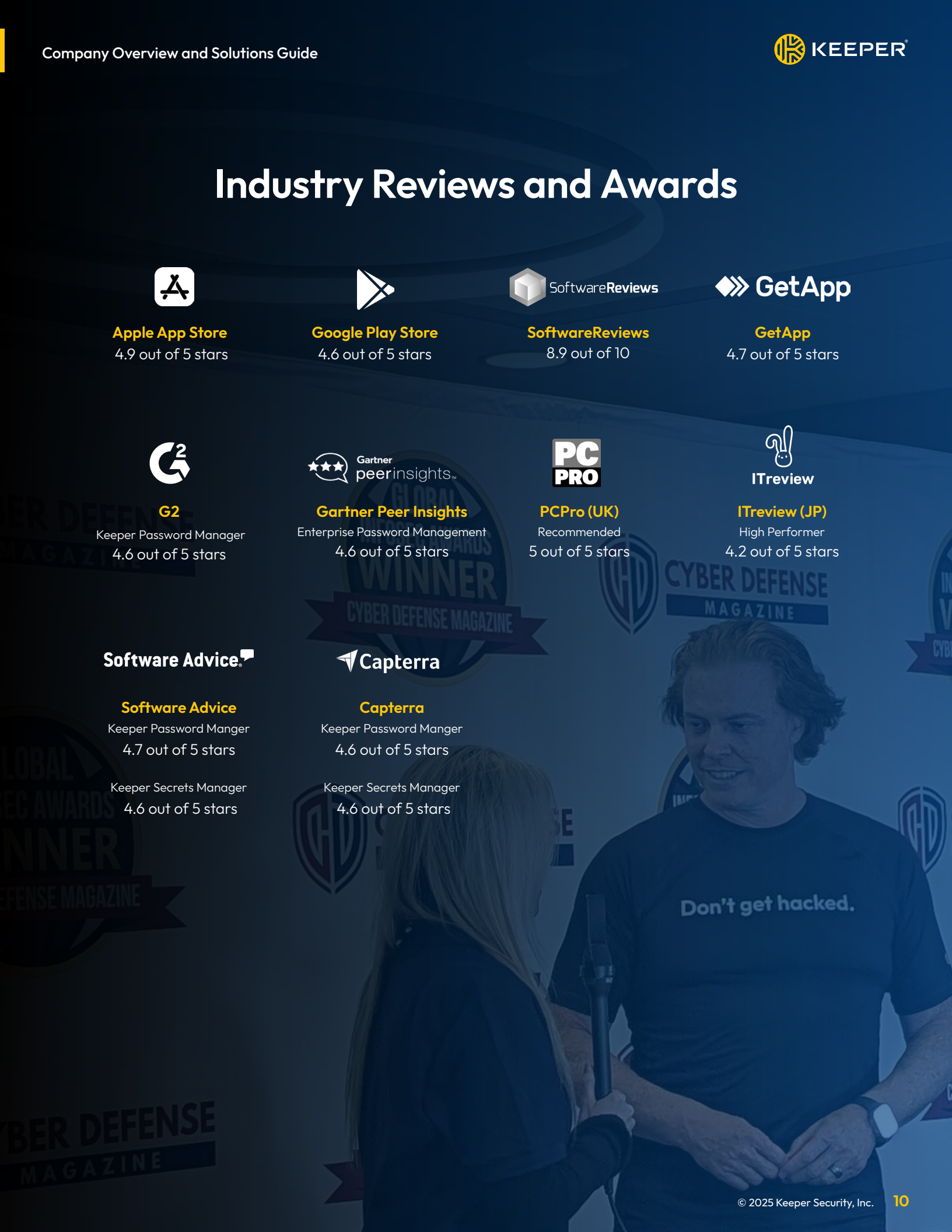
ITreview (JP)
High Performer
4.2 out of 5 stars

Software Advice
Keeper Password Manger
4.7 out of 5 stars

Keeper Secrets Manager
4.6 out of 5 stars

Capterra
Keeper Password Manger
4.6 out of 5 stars

Keeper Secrets Manager
4.6 out of 5 stars



2024 Analyst Recognition

EMA

Keeper Security's zero-trust Privileged Access Management (PAM) solution, KeeperPAM®, was recognized as a Value Leader by the IT and data management analyst research and consulting firm Enterprise Management Associates (EMA) in its 2024 PAM Radar™ Report, following the same recognition in 2023:

- KeeperPAM was identified as a leading PAM provider for product strength and cost-efficiency.
- The 2024 PAM Radar™ Report highlights Keeper's success in providing an easy-to-deploy platform with broad functionality.
- As a cloud-hosted SaaS solution, the report notes that KeeperPAM requires no on-premises infrastructure deployments, and because it's agentless and clientless, no additional software is needed.

Leaders are identified based on their product's characteristics in five categories: architecture and integration, functionality, deployment and administration, cost advantage and vendor strength.

GigaOm

Keeper Security is recognized as a Leader in the GigaOm Radar Report for Enterprise Password Management, earning the highest marks of any vendor for overall value in 2024. This marks the third consecutive year Keeper has earned this prestigious accolade, and highest ranking on the report, underscoring its commitment to providing cutting-edge cybersecurity solutions. The GigaOm report evaluates 13 leading password management solutions, focusing on key features, business criteria and emerging technologies.

- Keeper scores high across all of the decision criteria, and distinguishes itself with its relentless pursuit of innovation and growth, particularly through its zero-trust Privileged Access Management (PAM) solution, KeeperPAM.
- Additionally, the report highlights Keeper's secrets management, seamless integration with Identity Providers (IdP) and strong compliance features as significant competitive advantages.

2024 Awards

SC Awards Europe

Best Security Company

Fortress Cybersecurity Awards

Zero Trust

Teiss Awards

New product of the year

Cybersecurity Excellence Awards

Cybersecurity Research

Best Identity and Access Management

Best Privileged Access Management

Best CEO

Best CTO

Best Cybersecurity Company

Most Innovative Cybersecurity Company

Best Zero-Trust Security

Global Cybersecurity Visionary

Reseller Choice Awards

Best Password Management

Strategic Investors

Insight Partners

Insight Partners is a leading global venture capital and private equity firm investing in high-growth technology and software ScaleUp companies that are driving transformative change in their industries. Founded in 1995, Insight Partners has invested in more than 800 companies worldwide with over $90B in regulatory assets under management. Insight's mission is to find, fund and work successfully with visionary executives, providing them with practical, hands-on software expertise to foster long-term success. Across its people and its portfolio, Insight encourages a culture around a belief that ScaleUp companies and growth create opportunity for all. For more information on Insight and all its investments, visit **insightpartners.com**.

Summit Partners

Founded in 1984, Summit Partners is a global alternative investment firm that is currently managing more than $36 billion in capital dedicated to growth equity, fixed income, and public equity opportunities. Summit invests across growth sectors of the economy and has invested in more than 550 companies in technology, healthcare and other growth industries. Summit maintains offices in North America and Europe and invests in companies around the world. For more information, please visit **SummitPartners.com** or follow Summit on **LinkedIn**.