Enables Secure Sharing of Credentials and Secrets
Keeper allows IT Admins to enable secure, granular and controlled sharing of credentials, secrets and vaults among employees and teams.

Mitigates Risk of Data Breaches
Keeper uses a proprietary, zero-knowledge security architecture that supports on-prem, cloud and hybrid-cloud environments for client-side encryption key management.

Robust Compliance, Reporting and Auditing
Supports role-based access controls, 2FA, auditing, event reporting and industry compliance with SOX, NIST, PCI DSS, SOC 2, ISO 27001, HIPAA, DPA, FINRA and GDPR.

Protects Your Organization Against Ransomware Attacks
Keeper protects your organization against ransomware attacks using robust administration, controls and visibility over strong password security and real-time dark web monitoring.

Bolsters Security and Privacy
Each employee gets a private, encrypted vault for storing and managing their passwords, credentials, files and private client data.

Boosts Employee Productivity
Reduces help desk costs, saves employees time, reduces frustration and eliminates the need for employees to reuse and remember passwords.

A fully managed, cloud-based, zero-knowledge platform for securing infrastructure secrets such as API keys, database passwords, access keys, certificates and any type of confidential data.

- Credentials are provisioned from the vault
- Developer SDKs and CLI access
- Integrated with top CI/CD systems
- Centralized Management and RBAC
- Reports, alerts, audits, logs and SIEM integration

Instantly access your infrastructure with zero-trust security. KCM provides DevOps and IT teams with effortless access to RDP, SSH, MySQL and Kubernetes endpoints through a web browser.

- Privileged Access Management
- Agentless and clientless, web browser access
- Lightning fast, minimum latency and responsive
- Zero-trust security, IP lock, no keys exposed
- Session recording, tracking and audits
Single Sign On (SSO) Integration
Deploy Keeper through existing SAML 2.0-compatible SSO solutions with seamless authentication. Supports popular IdPs such as Microsoft Azure, ADFS, Okta and Google Workspace.

Role-Based Access Controls
Employee permissions can be fully customized through fine-grained access controls based on the role and responsibilities of team members.

Scalable User Provisioning
Keeper streamlines onboarding through an administrative console and advanced integration with Active Directory, SSO, SCIM and developer APIs.

Share with Colleagues and Teams
Securely create, share and manage both individual records and encrypted folders across teams or individual users.

Auditing, Analytics and Reporting
Keeper’s Enterprise Password Management (EPM) Platform provides visibility into password practices with robust reporting and auditing tools so you can reduce the threat of cyber breaches and maintain compliance standards.

Advanced DevOps Tools
The Keeper Commander SDK provides IT admins and developers with open source code, command-line tools and APIs to perform password management and password rotation functionality.

Unified Security, Visibility and Control for Passwords, Secrets, and Connections for Every User and Every Device
- Unified visibility, security and control
- RBAC, Dark-web monitoring, policies, compliance and reporting
- Zero-trust, zero-knowledge, hyper secure, cloud-based
- Simple adoption, fully integrated with IdM stack, automated roll-out

Top Industry Awards and Ratings
- G2 2022 Enterprise Leader 4.7 out of 5 stars
- PCMag Editors' Choice 4.5 out of 5 stars
- Gartner Peer Insights 4.5 out of 5 stars
- Spiceworks 4.9 out of 5 stars

Data Sheet
Keeper Enterprise

© 2022 Keeper Security, Inc.