Data Sheet

KEEPER CONNECTION MANAGER

Keeper Connection Manager (KCM)

Provides agentless, clientless and secure remote access to RDP, SSH, database and Kubernetes endpoints through a web browser.

Challenges

Organizations of all sizes need to provide secure and reliable access to IT infrastructure, databases and back-end websites. However, legacy remote access solutions often result in limited scalability, high administrative overhead, end-user frustration and serious security gaps.

1. Virtual Private Networks (VPNs) typically provide too much access, especially for contractors, vendors and occasional-use employees.
2. VPNs do not protect against cookie tracking, viruses or other malware.
3. VPNs are expensive and notoriously difficult for IT personnel to configure and maintain, as well as for end-users to use.
4. Some solutions rely on combinations of agents, clients and distributed bastion servers, increasing system complexity and impairing user adoption.

Employees need to establish secure, reliable and easy-to-use remote connections from anywhere to minimize the risk of unauthorized access to sensitive assets.

Solution

Keeper Connection Manager solves the complexity and security dilemma with a modern, agentless solution that provides the security, ease of use and speed required in today's distributed, remote work environments.

Keeper Connection Manager is designed to operate on the Principle of Least Privilege. Access rights are delegated through users and groups, which are automatically created by the Keeper Connection Manager packages and through strict file permissions.

All traffic passes through a secure, authenticated gateway. Desktops are never exposed to the public Internet. Following zero-trust principles, only authorized and authenticated connections are allowed.

About Keeper Security

Keeper Security is transforming cybersecurity for people and organisations around the world.

Keeper's affordable and easy-to-use cybersecurity solutions are built on a foundation of zero-trust and zero-knowledge security to protect every user on every device. Millions of individuals and thousands of organisations rely on Keeper for best-in-class password, passkey and secrets management, Privileged Access Management (PAM), secure remote access and encrypted messaging. Our next-generation cybersecurity platform deploys in minutes and seamlessly integrates with any tech stack to prevent breaches, reduce help desk costs and ensure compliance.

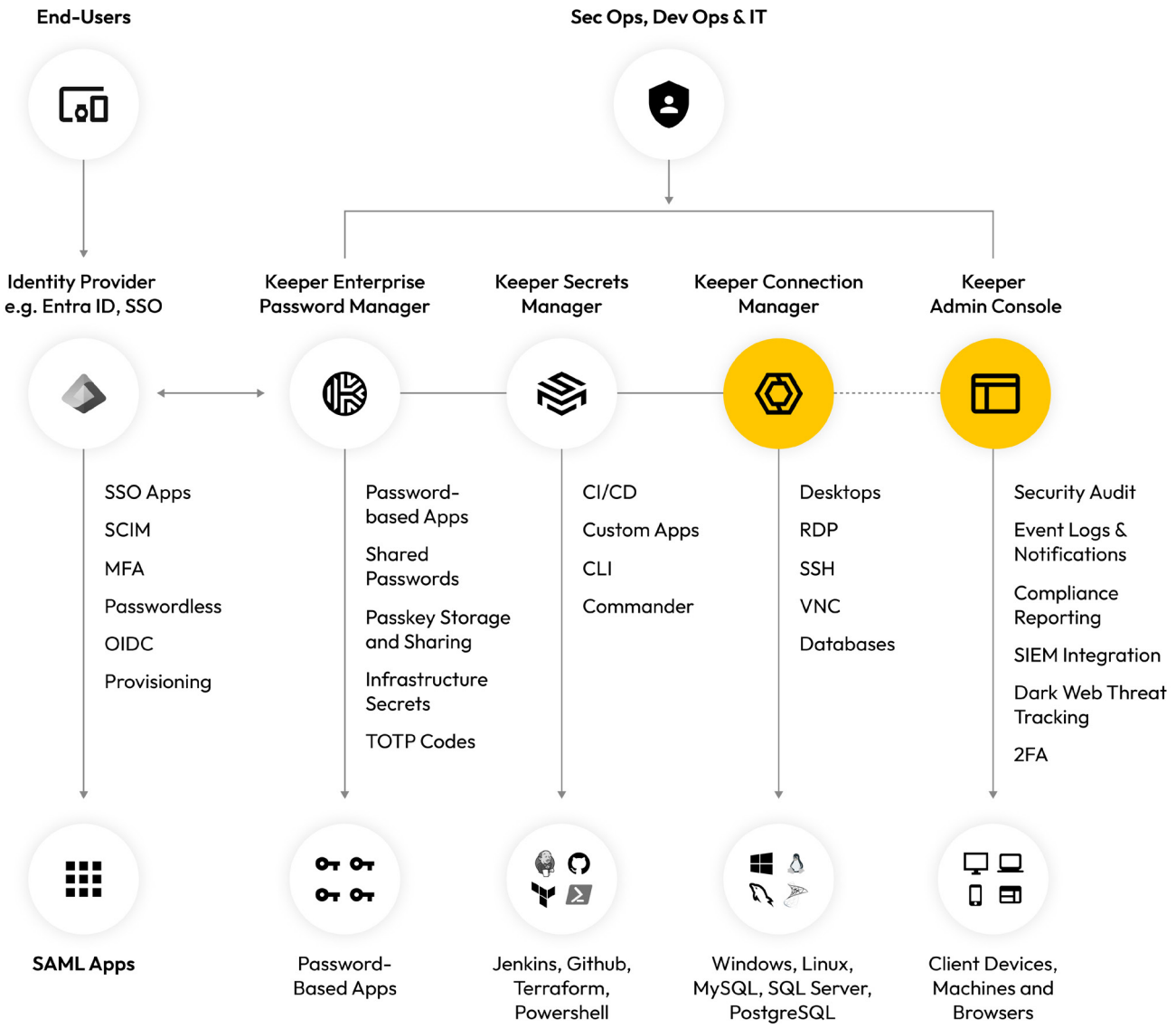
Keeper Security is backed by leading private equity firms Insight Partners and Summit Partners.

Keeper Security
Don't get hacked.

Learn more
keepersecurity.com

Start a free trial today
keepersecurity.com/start-business-trial.html

Keeper Privileged Access Management Platform



Business Value

Remote Browser Isolation
Mitigate cybersecurity threats by hosting browsing sessions in a remote, controlled environment.

Remote Database Access
Protect proprietary data and PII with secure remote database access.

Secure Remote Infrastructure Access
Establish secure remote connections from anywhere without exposing credentials.

Privileged Account Session Management
Meet compliance requirements with audited and recorded sessions.

Key Capabilities

- Web-Based Access with End-to-End Encryption
- Multi-Factor Authentication
- Agentless Access (No VPN Required)
- Multiple Data Stores
- Zero-Knowledge Security
- Zero-Trust Framework
- Role-Based Access Control (RBAC) Policy Engine
- Event Monitoring and Session Recording
- Passwordless Authentication
- Multi-Protocol Support
- Integration with Keeper Secrets Manager