Data Sheet

Keeper Secrets Manager (KSM)

Defend against supply chain attacks with a modern, cloud-based platform for securing infrastructure secrets such as API keys, database passwords, access keys and certificates.

Challenges

Stolen or weak DevOps secrets are a leading cause of supply chain attacks. Secrets are sprawled throughout source code, config files and CI/CD systems, which exposes organizations to hackers. This expanded attack surface creates several challenges for DevOps, Security and IT professionals:

1. Development teams often prioritize productivity over security and well-intentioned employees end up hard-coding credentials across the environment.
2. Distributed and remote workforces collaborate across regions, systems and environments – leading to heterogeneous secret storage.
3. Without centrally managed access controls, employees risk becoming over-privileged.
4. For many organizations, internal and compliance policies mandate regular credential rotation, which is only possible with comprehensive vaulting.

Organizations need a secure, easy-to-use and cost-effective way to tame secrets sprawl and enforce least-privileged access. By coordinating access, enforcing automated credential rotation and ensuring end-to-end encryption, DevOps, IT and Security teams can drastically reduce the risk of a devastating breach.

Solution

Keeper Secrets Manager provides your DevOps, IT, security and software-development teams with a cloud-based, zero-trust and zero-knowledge security platform for managing infrastructure secrets and protecting your organization's most sensitive data.

Keeper Secrets Manager centralizes your secrets to eliminate sprawl, prevent unauthorized access and provide auditing and logging. Extensive Software Development Kit (SDK) and Application Programming Interface (API) capabilities allow injecting credentials just-in-time into any programming language, which covers machine access to secrets, in addition to human access.

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.

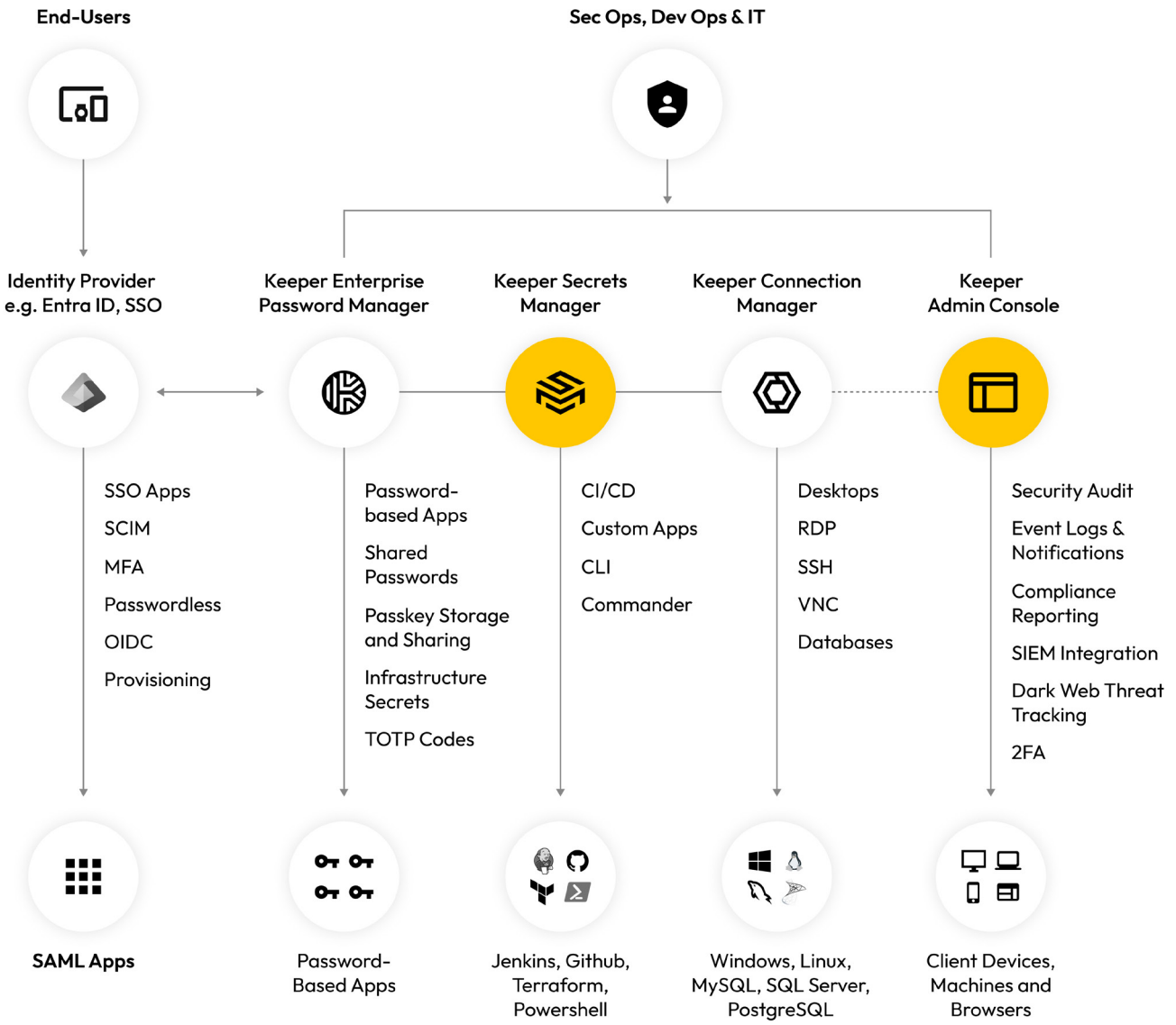
Keeper Security is backed by leading private equity firms Insight Partners and Summit Partners.

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

Secures your highly privileged systems and data
Consolidate your secrets in a unified platform and eliminate secrets sprawl by removing hard-coded credentials from source code, config files and CI/CD systems.

Flexible and fast integration
Out-of-the-box integration with all popular CI/CD platforms such as Github Actions, Jenkins and Ansible.

Easy to deploy and easy to use
Fully cloud-based, zero-trust and zero-knowledge platform that doesn't require any complex networking, storage or HA configurations.

Key Capabilities

- Automatically rotate credentials for service and admin accounts, user identities, REST-based API accounts, machines and user accounts across your infrastructure and multi-cloud environments.
- Manage access rights and permissions with role-based access controls.
- Client devices decrypt the vault secrets locally after retrieval. Keeper has no ability to decrypt stored vault data.
- Keeper Secrets Manager is a fully-managed service with unlimited scaling capacity.