Data Sheet

KEEPER® SECRETS MANAGER

Defend against cyber attacks by 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, exposing organizations to hackers. This expanded attack surface creates several challenges for DevOps, Security and IT professionals.

01

Productivity is prioritized over security and well-intentioned employees end up hard-coding credentials across the environment.

02

Modern, distributed workforces collaborate across regions, systems and environments, leading to higher risk potential without proper controls in place.

03

Without centrally managed access controls, employees risk becoming over-privileged, opening threat vectors and reducing compliance.

04

Often 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 store secrets and enforce least-privileged access. By coordinating access, enforcing automated credential rotation and ensuring end-to-end encryption, teams can drastically reduce the risk of a devastating breach.

Solution

Keeper Secrets Manager allows your teams to integrate CI/CD pipelines, DevOps tools, custom software and multi-cloud environments into a fully managed, zero-knowledge and zero-trust platform to secure infrastructure secrets and reduce secrets sprawl. Keeper Secrets Manager centralizes 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, covering machine and human access to secrets.

Don’t get hacked.

Learn more
keepersecurity.com

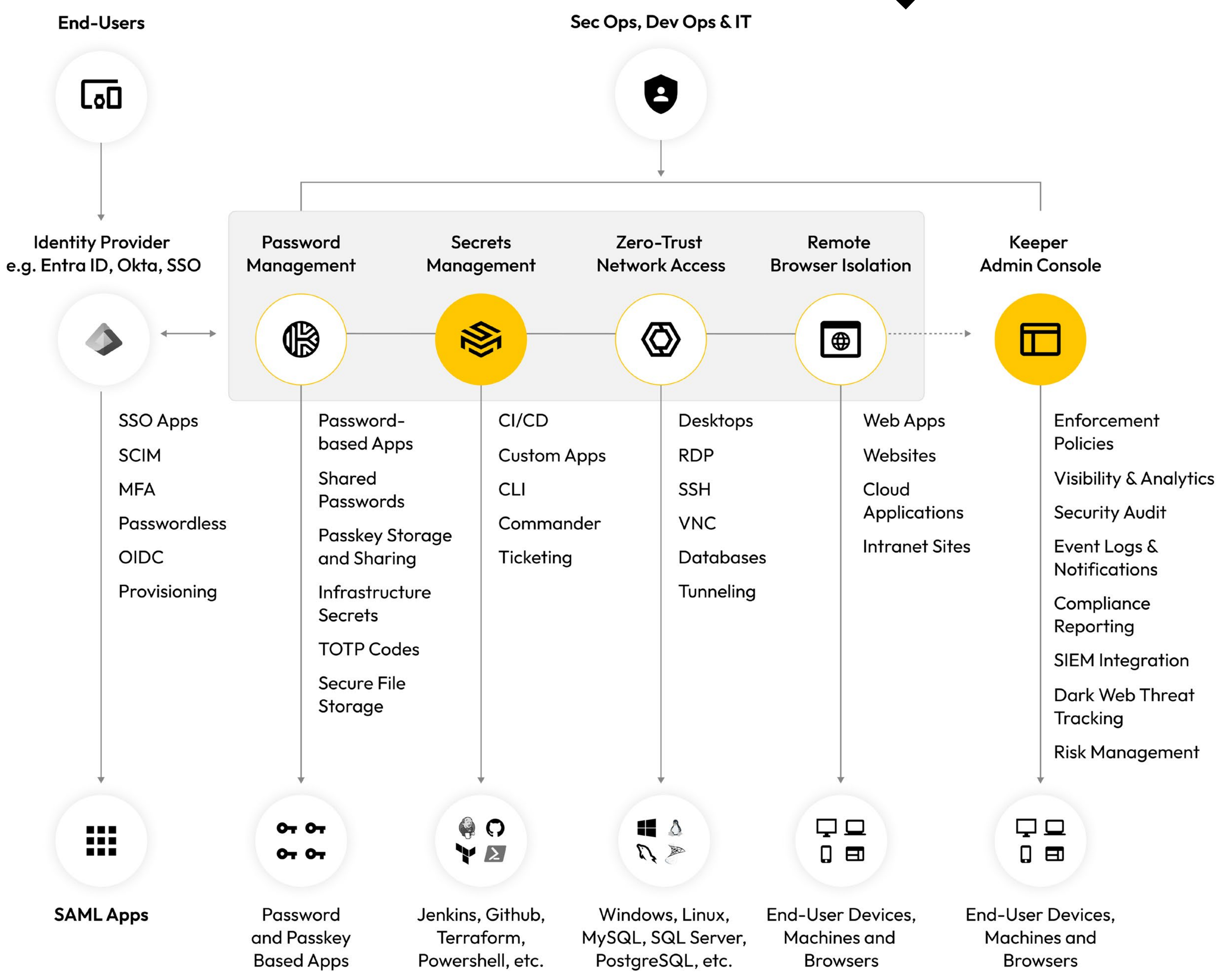
Request a demo
keeper.io/ksm

About Us

Keeper Security is transforming cybersecurity for people and organizations globally. Keeper’s intuitive solutions are built with end-to-end encryption to protect every user, on every device, in every location. Trusted by millions of individuals and thousands of organizations, Keeper is the leader for password, passkey and secrets management, privileged access, secure remote access and encrypted messaging.

KEEPER SECRETS MANAGER

Keeper Privileged Access Management Platform



End-Users

Sec Ops, Dev Ops & IT

Identity Provider e.g. Entra ID, Okta, SSO
- SSO Apps
- SCIM
- MFA
- Passwordless
- OIDC
- Provisioning

SAML Apps

Password Management
- Password-based Apps
- Shared Passwords
- Passkey Storage and Sharing
- Infrastructure Secrets
- TOTP Codes
- Secure File Storage

Password and Passkey Based Apps

Secrets Management
- CI/CD
- Custom Apps
- CLI
- Commander
- Ticketing

Jenkins, Github, Terraform, Powershell, etc.

Zero-Trust Network Access
- Desktops
- RDP
- SSH
- VNC
- Databases
- Tunneling

Windows, Linux, MySQL, SQL Server, PostgreSQL, etc.

Remote Browser Isolation
- Web Apps
- Websites
- Cloud Applications
- Intranet Sites

End-User Devices, Machines and Browsers

Keeper Admin Console
- Enforcement Policies
- Visibility & Analytics
- Security Audit
- Event Logs & Notifications
- Compliance Reporting
- SIEM Integration
- Dark Web Threat Tracking
- Risk Management

End-User Devices, Machines and Browsers

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