Data Sheet

KEEPER CONNECTION MANAGER

Keeper Remote Browser Isolation

Securely isolate web browsing activities from end-user devices – mitigating cybersecurity threats by hosting browsing sessions in a controlled remote environment.

Challenges

All organizations need to provide access to applications and websites while ensuring security and efficiency. Keeper's Remote Browser Isolation mitigates cybersecurity threats by hosting browsing sessions in a controlled remote environment and isolating web browsing activities from end-user devices, without the need for a VPN.

Employees require access to websites and tools, but VPNs are increasingly difficult to set up and maintain and often give access to far too much, especially for contractors and vendors. VPNs frequently lack the ability to lock down access to a pre-approved list of URLs, preventing you from guaranteeing that only authorized activity is occurring.

Furthermore, ensuring security, compliance and auditing requirements are met causes strain for administrators and organizations as a whole. Many solutions try to meet these needs with a combination of tools, but this only adds complexity and frustration for users, reducing adoption and increasing security risks.

Solution

Remote Browser Isolation within Keeper Connection Manager solves the complexity and security dilemma with a modern, agentless solution that provides security, ease of use and streamlined access to applications and websites without the headaches experienced in today's distributed remote work environments.

Remote Browser Isolation provides true zero-knowledge security with private browser sessions that do not carry customer data. Web browsing is simplified with secure access to sites through an up-to-date Chromium browser, regardless of the user's local browser version, which prevents data exposure risks if a device is compromised. All browsing activity flows through the customer's KCM container, never through Keeper's servers.

Integrated directly with Keeper Password Manager, credentials are autofilled for seamless access and enhanced security.

Make compliance a breeze with fully recorded website interactions, ensuring proper interactions, reducing insider risk and streamlining the audit process.

Core Benefits and Features

- Web-based access with end-to-end encryption
- Recorded web sessions
- Controlled web browsing
- Password autofill
- Secure access without a VPN
- Zero-knowledge security
- Zero-trust framework
- Role-based access controls
- Multi-factor authentication
- Admin control
- Co-browsing

About Keeper Security

Keeper Security is transforming cybersecurity for people and organizations 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 organizations 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.

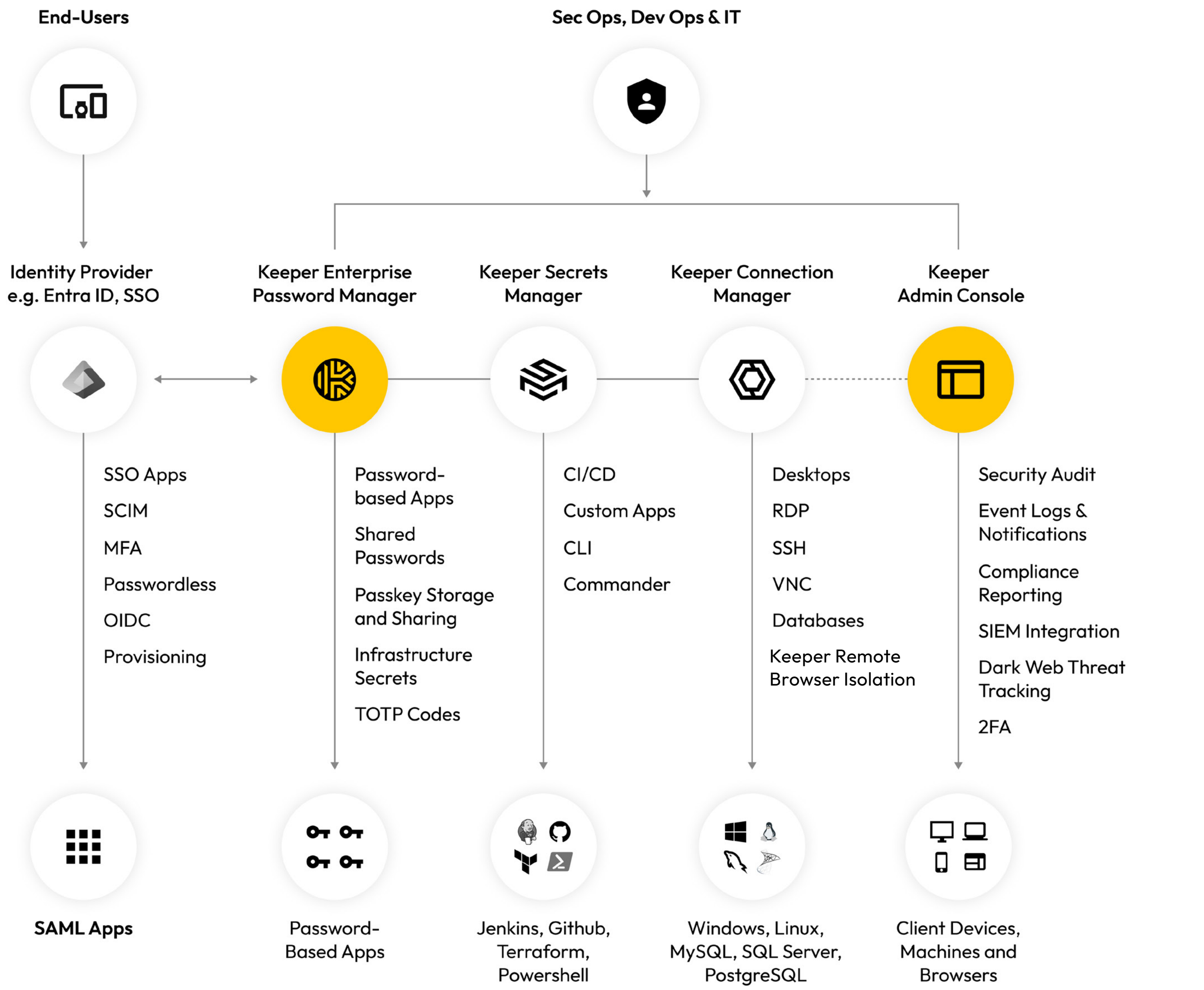
Keeper Security is backed by leading private equity firms Insight Partners and Summit Partners.

Keeper Security
Don't get hacked.

Learn more
keepersecurity.com

Start a free trial today
keepersecurity.com/connection-manager-trial.html

Keeper Privileged Access Management Platform



End-Users

Sec Ops, Dev Ops & IT

Identity Provider
e.g. Entra ID, SSO

- SSO Apps
- SCIM
- MFA
- Passwordless
- OIDC
- Provisioning

SAML Apps

Keeper Enterprise Password Manager

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

Password-Based Apps

Keeper Secrets Manager

- CI/CD
- Custom Apps
- CLI
- Commander

Jenkins, Github, Terraform, Powershell

Keeper Connection Manager

- Desktops
- RDP
- SSH
- VNC
- Databases
- Keeper Remote Browser Isolation

Windows, Linux, MySQL, SQL Server, PostgreSQL

Keeper Admin Console

- Security Audit
- Event Logs & Notifications
- Compliance Reporting
- SIEM Integration
- Dark Web Threat Tracking
- 2FA

Client Devices, Machines and Browsers

Business Value

Auditing

User activity on protected websites can be recorded for review and compliance or security purposes, ensuring proper interactions and reducing insider threats and fraud.

Access control

Access to protected websites can easily be limited by role-based access controls, even if the target website does not natively support it.

Co-browsing

Share an active view of a web page with others for cooperative work on training.

Testing

Reproducing bugs in websites and applications can be difficult. By accessing enviroments through Keeper Connection Manager (KCM), testing and quality assurance teams can ensure the steps to reproduce an issue are always recorded.

Ultimate privacy

Autofilled credentials are never seen or available to the end-user, providing the best protection against DOM inspection.