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

01

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 or ZTNA.

02

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.

03

Furthermore, ensuring security, compliance and auditing requirements are met strains 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, preventing data exposure risks if a device is compromised. All browsing activity flows through the customer's Keeper Connection Manager container, never through Keeper's servers.

Automatically fill login and password details into isolated browser sessions without ever transmitting credentials to the user's device. This includes limiting vendor access and closely monitoring sessions through recording and keystroke logging.

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

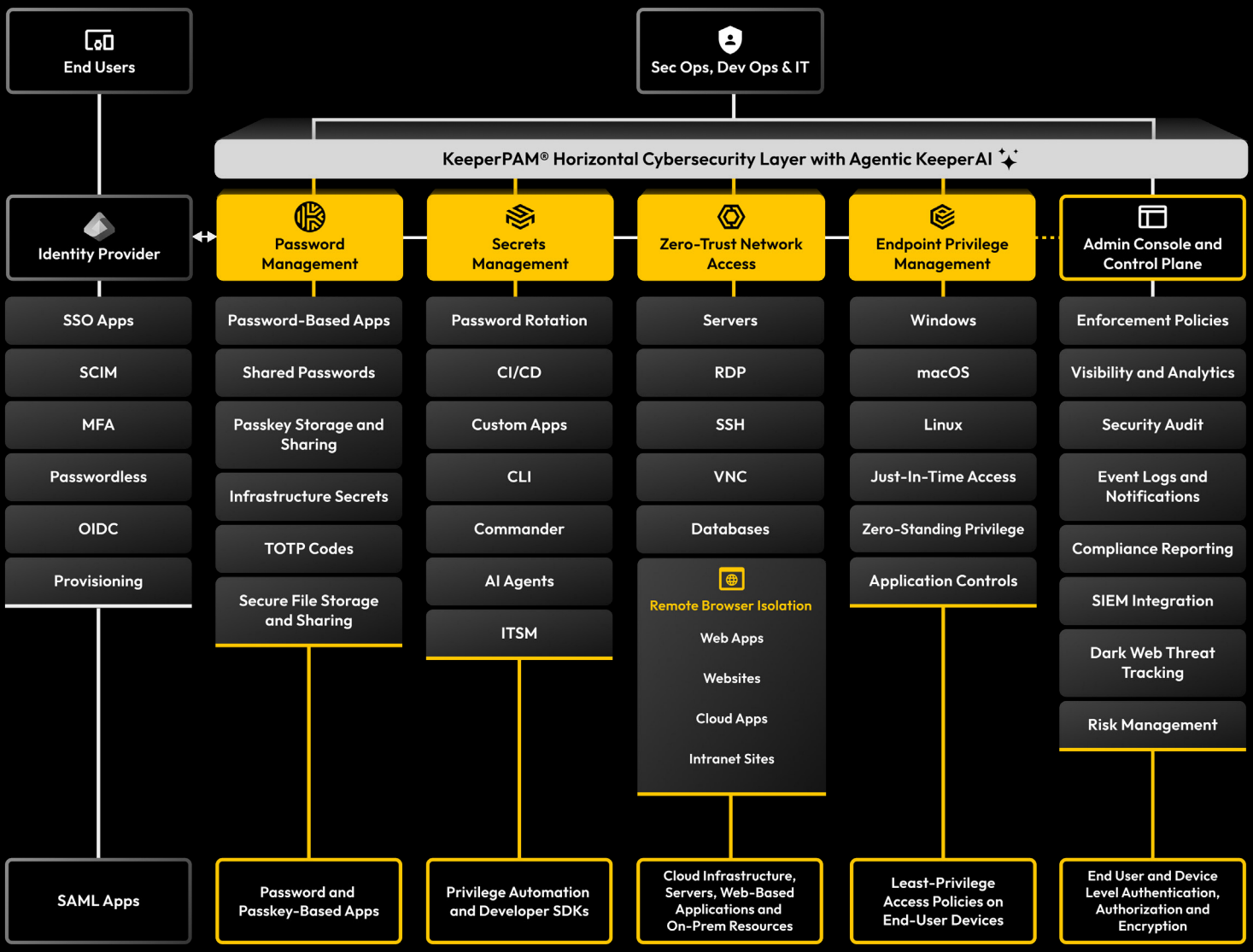
Limit actions with customizable admin restrictions, providing browsing sessions that prevent data exfiltration by prohibiting clipboard usage, file uploads and downloads and more.

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 or ZTNA
- Zero-knowledge security
- Zero-trust framework
- Role-based access controls
- Multi-factor authentication
- Admin control
- Co-browsing
- SSO-enable any web-based application
- Prevent insecure access from vendors or BYOD users
- Eliminate data exfiltration

KEEPER CONNECTION MANAGER

Keeper Privileged Access Management Platform



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.

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

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 session with others for cooperative work or training.

Ultimate privacy
Autofilled credentials are never seen or available to the end-user, providing the best protection against DOM inspection and cross-site scripting attacks.

Security teams
Test suspicious links without the need to launch a virtual machine.