



Implement least-privilege access policies, eliminate standing admin rights and enable Just-in-Time (JIT) access at both the process and machine levels with endpoint privilege management across Windows, Linux and macOS endpoints.

Robust privileged access controls are essential for organizations to strengthen their security posture, ensure operational efficiency and meet regulatory compliance requirements.

Keeper Endpoint Privilege Manager secures endpoints through lightweight agents that remove standing admin rights while enabling temporary, policy-based privilege elevation only when necessary. The system enforces customizable security policies through JIT access with optional approval workflows and Multi-Factor Authentication (MFA) enforcement.

Privileged actions can be executed either through ephemeral accounts, which are automatically provisioned and deprovisioned for each session, or by temporarily elevating privileges on standard user accounts. Organizations may choose either method depending on their security posture and operational needs.

Keeper Endpoint Privilege Manager works across Windows, macOS and Linux environments while providing visibility through a centralized dashboard that logs all elevation activities for auditing and compliance.

Benefits of Keeper Endpoint Privilege Manager

Security

Eliminates standing admin rights and enables JIT elevation only for approved applications to reduce attack surfaces and improve security.

Compliance

Provides comprehensive audit trails of privilege usage and ensures adherence to regulatory requirements through documented administrative access control.

User experience

Allows users to complete necessary tasks without IT delays through automated privilege elevation for approved applications.

Operational efficiency

Reduces help desk workload by automating approvals for routine administrative tasks.

Scalability

Enables organizations to efficiently enforce least-privilege policies and manage privileged access across thousands of Windows, macOS and Linux endpoints from a centralized platform.

Auditability and visibility

Gives insight into elevation activity, approvals and endpoint policy enforcement with detailed logging and integration into SIEM tools for faster incident response.

Learn more
keepersecurity.com

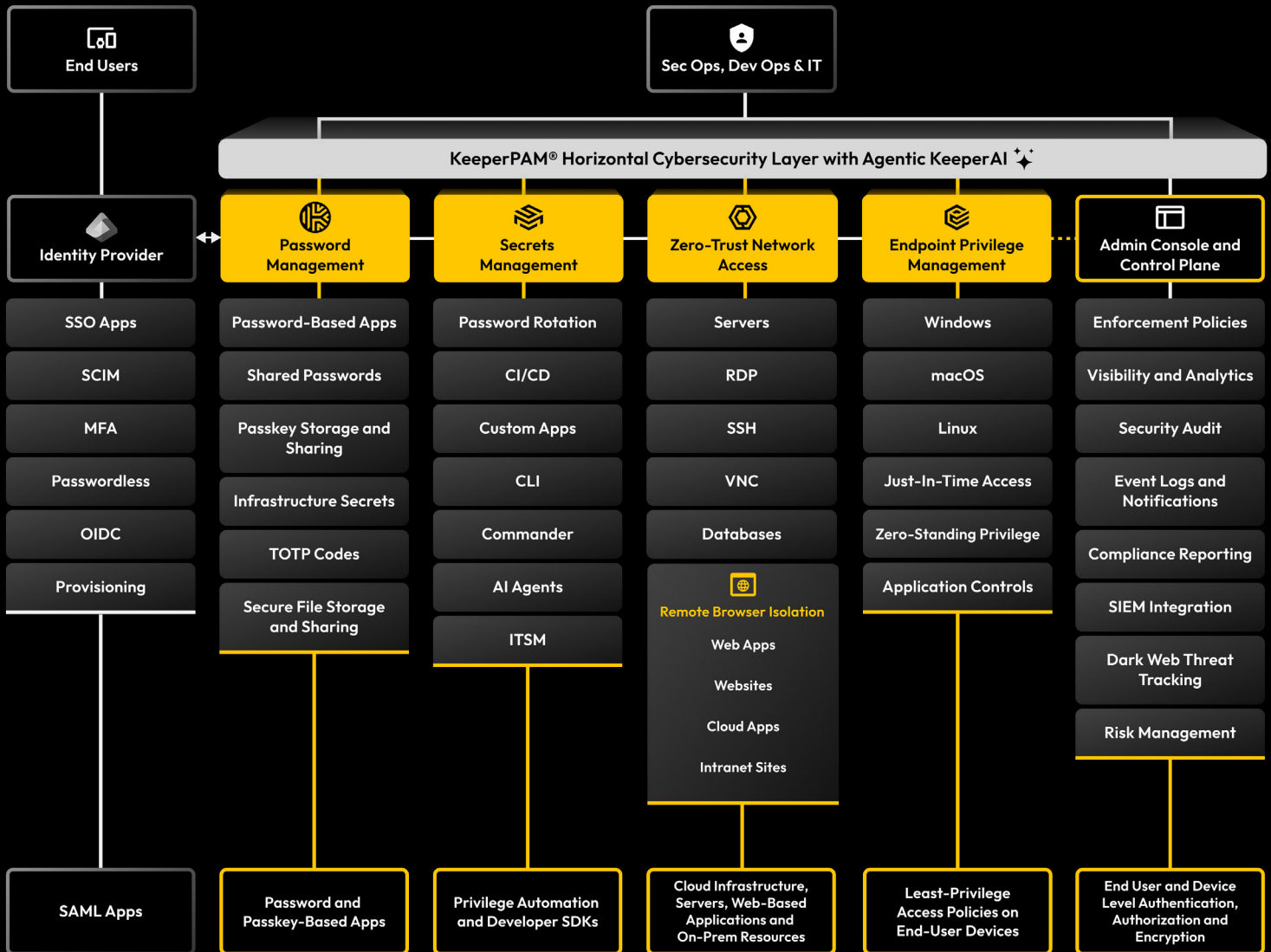
Request a demo
keeper.io/demo

Partner inquiries
partners@keepersecurity.com



About Keeper Security

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 privileged access management.



Extend zero trust to endpoints

Keeper Endpoint Privilege Manager enhances the KeeperPAM zero-trust architecture by providing precise control over privilege elevation directly on user endpoints. While KeeperPAM secures user access to systems, Keeper Endpoint Privilege Manager enforces what users can do once connected, minimizing risk from over-privileged accounts and lateral movement.

How Keeper elevates privileges

- 1. Policy** - If an application or process requires elevation, the Keeper agent checks the relevant policy.
- 2. Approval** - If approval is required, the request is routed to an admin via the Admin Console or Command Line Interface (CLI).
- 3. MFA Option** - If no approval is needed, the elevation proceeds automatically. MFA enforcement is an optional additional step.