KEEPER PAM

Privileged access for people, machines and AI agents

A cloud-native privileged access management platform built on zero-knowledge encryption. KeeperPAM secures credentials, secrets, endpoints and privileged sessions through one unified control plane, with no infrastructure changes and no inbound network access required.

One platform for privileged access

Password and passkey management	Securely store, manage and share passwords, passkeys and sensitive records in an encrypted vault with Role-Based Access Controls (RBAC) and auditing.
Secrets management	Protect API keys, service accounts, certificates and other machine secrets across CI/CD, infrastructure-as-code, Kubernetes and AI-agent workflows.
Privileged session management	Provide credential-free access to servers, databases, web applications, cloud consoles and other privileged resources with session monitoring and recording.
Endpoint privilege management	Remove standing local administrator privileges and grant time-limited elevation based on policy across Windows, macOS and Linux endpoints.
Remote access and database management	Securely access infrastructure through browser-based sessions, passwordless database connections and encrypted tunnels.

Privileged access capabilities

Automated rotation - Rotate passwords, SSH keys, database credentials, API keys, tokens and service account credentials across cloud and on-premises environments.

Discovery - Discover machines, databases, directories, accounts and credentials across on-premises, AWS and Azure environments, then import managed resources into the Keeper Vault.

Privileged sessions - Secure access through RDP, SSH, VNC, Telnet, Kubernetes, HTTPS and supported database protocols, including MySQL, PostgreSQL and SQL Server.

KeeperDB - Connect to supported databases directly from the Keeper Vault, run queries and manage database sessions without exposing database credentials to users.

Encrypted tunnels - Connect approved native tools, such as MySQL Workbench, SQL Server Management Studio, pgAdmin and PuTTY, through encrypted TCP tunnels without requiring a VPN.

Just-In-Time (JIT) access - Grant time-limited access that expires when sessions end, for both database access and endpoint privilege elevation.

KeeperAI - Analyze privileged session activity in real time, identify suspicious behavior and support automated responses, including session termination based on policy.

Deployment

KeeperPAM is accessed through the Keeper Vault. For access to resources inside a private network, customers deploy Keeper Gateway in the relevant cloud or on-premises environment. The Gateway uses outbound connectivity to Keeper Cloud and does not require inbound firewall rules or bastion hosts.

Security architecture and controls

Identity and access controls - Enforce SSO, MFA, RBAC, least-privilege policies, time-limited access, approval workflows and detailed audit logging.

Monitoring and response - Record and replay privileged sessions, send security events to supported SIEM platforms and use KeeperAI to identify and respond to suspicious session activity.

Zero-knowledge architecture - Vault data is encrypted and decrypted on the user's device. Keeper stores encrypted data and cannot access customers' plaintext vault contents.

End-to-end encrypted access - Connections between users, Keeper Gateway and target resources are protected with zero trust controls and end-to-end encryption.

© 2026 Keeper Security, Inc. | Rev. 10.2026