KeeperDB™

Multi-Protocol Database Access Platform

Challenges

KeeperDB replaces legacy database tools with a visually modern, AI-powered client available as both a standalone desktop application and as a fully governed, zero-trust privileged access session inside KeeperPAM.

01

Legacy tools like DBeaver and MySQL Workbench offer outdated interfaces, no native credential integration and no biometric authentication – creating friction and security gaps for every database user.

02

Database credentials are stored in plaintext config files and keychains on endpoints, creating an uncontrolled attack surface that grows with every DBA, developer and contractor granted access.

03

Privileged database sessions go unrecorded. Without session capture, query logging and event streaming, compliance teams have no evidence of what was run, by whom, or when.

04

Access provisioning and deprovisioning are manual and slow. There is no mechanism for just-in-time access, time-limited sessions or instant revocation without a full credential rotation.

Solution

KeeperDB is a full-featured database client available in two modes. As a standalone desktop application for macOS, Windows and Linux, it replaces tools like DBeaver with a visually modern interface, biometric authentication (Face ID and Windows Hello), direct integration with Keeper Secrets Manager for credential retrieval and an embedded AI agent using the customer's preferred LLM provider.

When deployed as part of KeeperPAM, KeeperDB becomes a fully governed privileged access session: credentials never reach the endpoint, every query is session-recorded and streamed to KeeperAI for threat detection, access is controlled by zero-trust policy with just-in-time provisioning and all events integrate with SIEM and audit platforms. Both modes support PostgreSQL, MySQL/MariaDB, SQL Server, Oracle, Amazon Redshift and SQLite.

Learn more
keepersecurity.com

Request a demo
keeper.io/demo

Partner inquiries
partners@keepersecurity.com

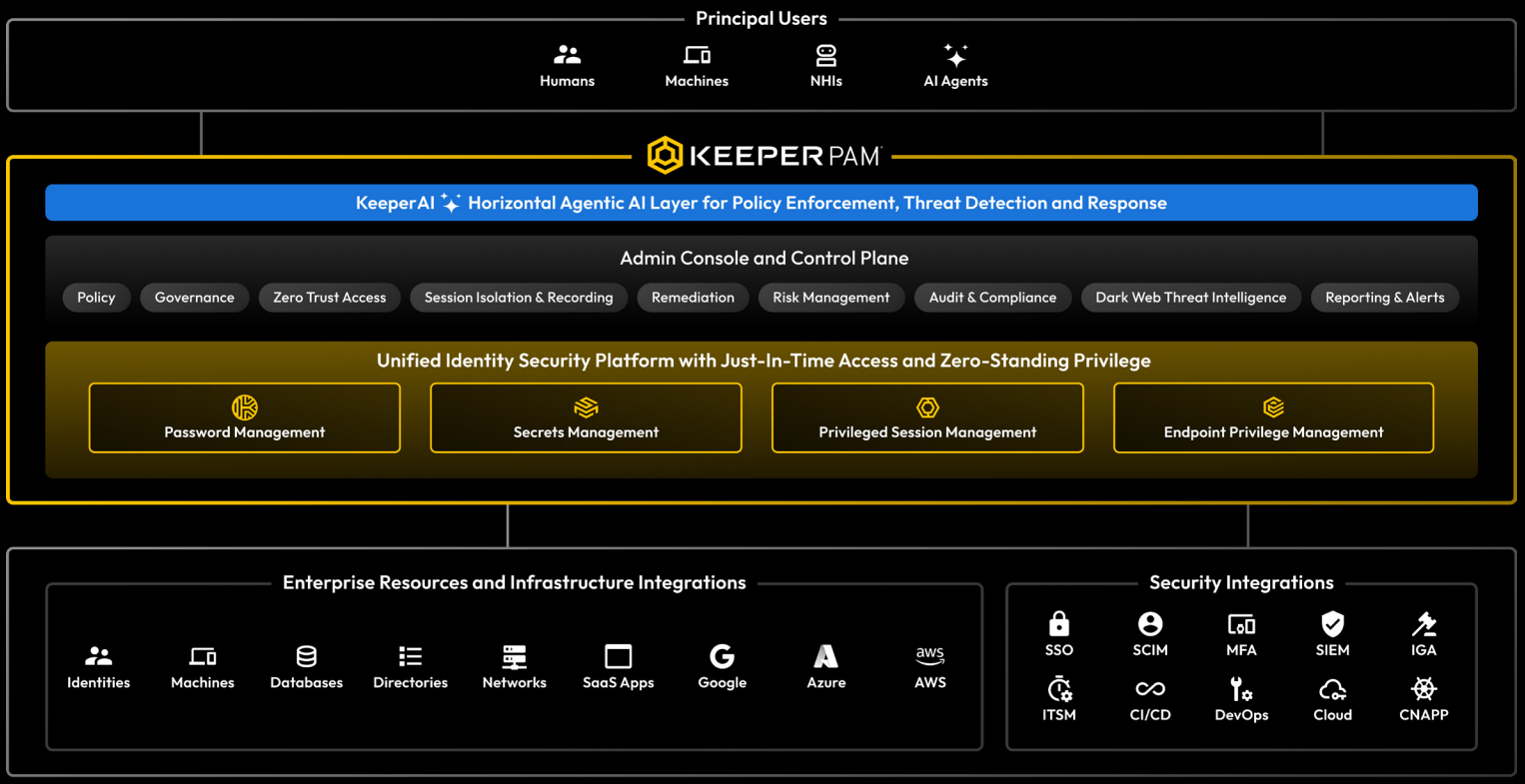
About Keeper Security

Keeper Security is the global leader in zero-trust and zero-knowledge cybersecurity, protecting passwords, passkeys, secrets, endpoints and privileged access for thousands of organizations and millions of users worldwide.

KEEPER PAM

DATA SHEET

The Zero-Trust, AI-Enabled Identity Security Platform



Business Value

Standalone Desktop App

- Replaces DBeaver, MySQL Workbench and other legacy database tools with a visually modern UI and full functional parity
- Biometric authentication via Face ID and Windows Hello – no master password, no stored credentials on disk
- Direct Keeper Secrets Manager integration retrieves database credentials from the vault at connection time
- Built-in AI agent supports any customer-hosted or cloud LLM – write queries in natural language, generate and refine SQL and chart results
- Multi-protocol support across PostgreSQL, MySQL/MariaDB, SQL Server, Oracle, Redshift and SQLite in a single client

Utilized in KeeperPAM

- Credentials are decrypted in the Keeper Gateway and never written to any endpoint – zero credential exposure
- Full privileged session recording: every query, result set and AI-generated statement is captured in a tamper-evident audit trail
- Just-in-time access with ephemeral accounts requestable from Slack, Jira, ServiceNow and Teams – instant revocation with no credential rotation
- KeeperAI continuously analyzes session activity for anomalous queries and data exfiltration attempts in real time
- All events stream to SIEM, ARAM and third-party audit platforms for centralized compliance reporting

Key Capabilities

- **Query editor and SQL notebook:** Syntax highlighting, autocomplete, multi-statement execution, destructive query confirmation and a persistent scratchpad
- **AI agent:** Natural language to SQL, autonomous and supervised modes, chart generation and performance triage – all using the customer's preferred LLM provider
- **Biometric authentication:** Face ID and Windows Hello for passwordless login
- **KSM credential integration:** Retrieve credentials directly from Keeper Secrets Manager at connection time – no local storage
- **Real-time performance monitor:** Process list, blocking chains, lock analysis and one-click session termination across all supported engines
- **Zero-trust access (PAM):** Credentials injected at the Gateway; client receives a proxied connection with no credential visibility
- **Session recording (PAM):** Full screen and query capture, indexed and searchable, stored in Keeper's zero-knowledge vault
- **KeeperAI threat detection (PAM):** Anomalous query detection, exfiltration alerts and AI-assisted remediation guidance
- **JIT provisioning (PAM):** Time-limited ephemeral accounts requestable from Slack, Jira, Teams and ServiceNow
- **Tunnel support (PAM):** Use a locally installed native client with Gateway-side credential injection and full session recording