THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Keeper Security Passes 100,000 Enterprise Customers

Keeper announced it now serves over 100,000 enterprise organizations, marking a milestone in the shift toward consolidated identity security platforms.

CONTROL FRAMEWORK

Consolidation Trend Accelerates

Enterprises are replacing fragmented password managers, privileged access tools, and MFA apps with single-pane-of-glass identity platforms that can be orchestrated by AI agents.

CONTROL FRAMEWORK

Unified Architecture

Keeper's platform combines password vaulting, privileged access management, and zero-trust verification into a shared data store and policy engine, reducing integration overhead.

→ Password vault with end-to-end encryption

→ Privileged Access Management module

→ Zero-trust verification layer

→ Central policy engine for all secrets

CONTROL FRAMEWORK

Agentic Enablement

The platform exposes REST and GraphQL APIs that AI-driven agents can call to retrieve, rotate, and provision credentials automatically, supporting DevSecOps pipelines.

CONTROL FRAMEWORK

Security Impact

By centralising secrets, organizations eliminate duplicate credential stores, lower phishing risk, and enforce consistent MFA and least-privilege policies.

CONTROL FRAMEWORK

Migration Blueprint

A typical consolidation follows three phases: 1) Inventory existing identity tools, 2) Map secrets to Keeper vaults, 3) Enforce unified policies and decommission legacy solutions.

EXECUTIVE TAKEAWAY

Executive Takeaway

Adopting Keeper's unified identity platform enables enterprises to streamline secret management, empower AI agents, and strengthen overall security posture as the agentic era unfolds.