Enpass vs Keeper: Key Differences for IT Decision-Makers

Choosing a password manager for your organization isn't just about storing passwords, it's about how much control you have over your data, how easily it fits into your existing setup, and how confidently you can scale without worrying about compliance or cost.

This quick comparison highlights the key differences between **Enpass** and **Keeper.**

Features	Enpass	Keeper
Data Location	Your Microsoft 365 or Google Workspace	Keeper Servers
Data Sovereignty	🟢 You control your data location	🔴 No control on data location
Data Decentralization	🟢 Users' data is stored only on their devices and their Microsoft 365 or Google Work accounts	🔴 All users' data of every Keeper customer is stored on Keeper's servers.
Immune to Mass Breaches	🟢 Yes	🔴 No, one single breach can provide access of all users' data to the hacker
Maintenance Overheads	No overheads. Enpass leverages your existing Microsoft 365 or Google Workspace setup.	No Overheads
Supported MFA Levels	Up to 4	Upto 3
Admin Control	🟢	🟢
Password Sharing	🟢	🟢
Security Audit Dashboard	🟢	🟢
Access Recovery	🟢	🟢

Policy Enforcement	🟢	🟢
Group Based Policies	🟢	🟢
IdP Integration	🟢	🟢
Single Sign On (SSO)	🟢	🟢
SCIM Provisioning	🟢	🟢
SIEM Integration	🟢	🟢
Emergency Access	🟢	🟢
Encrypted File Attachments	🟢	🟢
Built-in TOTP	🟢	🟢
App Platforms	Windows, Mac, Linux, iOS, Android	Windows, macOS, Linux, iOS, Android
Browser Extensions	Chrome, Firefox, Edge, Brave, Safari, Vivaldi, Opera	Chrome, Firefox, Edge, Safari, Opera, Brave
Free Family Plan for Employees	🟢	🟢

Ready to secure your organization?

With Enpass, you stay in control. No vendor lock-in, no centralized risk. You get the enterprise features you expect, **without the headaches of self-hosting** or relying on a vendor's infrastructure. Just secure, compliant, and flexible password management built around your infrastructure.

Start your free trial at https://www.enpass.io/business   📞 **Contact Sales at** https://www.enpass.io/contact