

A Look at Enpass Business Features: Your Data. Your Cloud. Your Way.

All password managers do the same thing, but Enpass is different in one big way—Data Sovereignty. It's not just about managing passwords; it's about where your data resides. Unlike traditional password managers that force you to store your data on their servers, Enpass ensures you stay in control.

Your data remains within your existing infrastructure, primarily on your Microsoft 365 or Google Workspace—without requiring self-hosting.

This feature list breaks down what makes Enpass secure, scalable, compliant and easy to deploy.



Vaults and Data Management

Feature	Description
Data location – Microsoft 365 and Google Workspace	Password vaults are stored in users' existing Microsoft 365 or Google Workspace accounts
Unlimited passwords, passkeys and file storage	No restrictions on the number of credentials you can store.
Unlimited vaults	Unlimited vaults for business, personal and sharing data.
Password and file sharing	Share passwords and files with colleagues safely.
Access recovery	Recover access for employees when they forget their Master Passwords.
Work as TOTP authenticator	Save and autofill one-time codes generated in Enpass.
Data import and export	Easily bring in data from other password managers or export it when needed.
Automatic data deletion on user offboarding	Data is automatically deleted from user's devices when they leave organization.



Policy Creation, Control and Enforcement

Feature	Description
Administrative controls	Easily manage users & groups, define password policies, all from one place.
Security audit dashboard	Get an overview of organization-wide password health, identifying at-risk users having weak, reused, and compromised passwords.

Dark web monitoring	Detects and highlights passwords exposed in data breaches.
Policy enforcement	Enforce security rules across users or teams.



Integrations

Feature	Description
Microsoft 365 and Google Workspace	Users' data is stored only in your trusted Microsoft 365 or Google Workspace.
Single Sign-on (SSO)	Leverage SAML-based SSO with existing IdP like Entra ID, Google Workspace, Okta and others.
Automatic user provisioning via SCIM	Supports automatic user provisioning via SCIM from your IdP such as Entra ID, Okta and others.
SIEM integration	Integrates with SIEM platforms like Azure Sentinel to stream event logs and alerts for improved security visibility.
UEM/MDM configuration for deployment	Supports managed app configurations for seamless deployment via your UEM or MDM platform.



Security and Monitoring

Feature	Description
Multi-factor authentication (MFA)	Up to 4 factors: Login and multi-factor authentication of your Google Workspace or Microsoft 365 account, Enpass master password, and Enpass keyfile (optional).
Event and audit logs	Keep an audit trail of changes in your Enpass environment.
Phishing protection	Alerts users if they attempt to enter credentials on suspicious websites.
Zero-knowledge architecture	We don't even have your encrypted data on our servers. It goes beyond zero knowledge. Only you have access to your data.
AES 256-bit encryption	All credentials are encrypted with 256-bit AES using a key derived from 320,000 rounds of PBKDF2-HMAC-SHA512.
Biometric login	Unlock Enpass app with biometric on your device.
Third-party security audits	Regular reviews by external firms to ensure security compliance.

Certifications	Certified to ISO 27001:2022 standards, audited for SOC 2 Type II and Compliant with GDPR.
----------------	---



Platform Compatibility

Feature	Description
Native applications	Available on iOS, Android, Windows, macOS, and Linux.
Smartwatch support	Apple Watch and Wear OS smartwatch.
Browser extension support	Compatible with Chrome, Edge, Firefox, Safari, Brave, Vivaldi, and Opera.



Support

Feature	Description
24/7/365 technical support	Round-the-clock help available through email.
Personalized onboarding and training	Tailored onboarding and training designed for your needs.
Account manager (a real human to support you)	Your go-to person for questions, setup or issues.

Ready to secure your organization?

With Enpass, you stay in control. No vendor lock-in, no centralized risk. It's secure, compliant, and designed to fit seamlessly into your existing infrastructure.

Start your free trial at <https://www.enpass.io/business>

Contact Sales at <https://www.enpass.io/contact>