1Password.com

How to choose a good Password Manager for your business

The Basics

Password managers like 1Password are only secure if your team are actually using them, so the basics are really important. A password manager needs to automatically save your passwords, generate stronger ones and fill them accurately everywhere you need them. You also want your password manager to store more than passwords, things like secure notes and identities.

	1PASSWORD
Includes apps and extensions on Mac, Windows, iOS, Android and all major browsers.	👍
Stores anything you need to secure. Passwords, notes, identities and credit cards.	👍

Security

This is the most important section. Your choice of password manager should tick every box with confidence. Security is an ongoing task and you need to trust your choice to treat your information with the utmost respect.

	1PASSWORD
The operators of the service have no ability to see or learn what sites and services users have logins for, nor when they use those.	👍
Data stored on the server should be impossible to crack in the event of a server compromise.	👍
The operators of the service have no ability to see or learn user passwords.	👍

The security of the service should have multiple layers of encryption and not rely on the secrecy of TLS or SSL.	👍
No secrets should be transmitted during the login process.	👍
The login process also guarantees the authenticity of the server you are logging into.	👍
The service uses multi-factor authentication as an additional factor that's beneficial to its security.	👍
The service should encourage and incentivise security researchers and undergo formal penetration testing.	👍

Distributing to your team

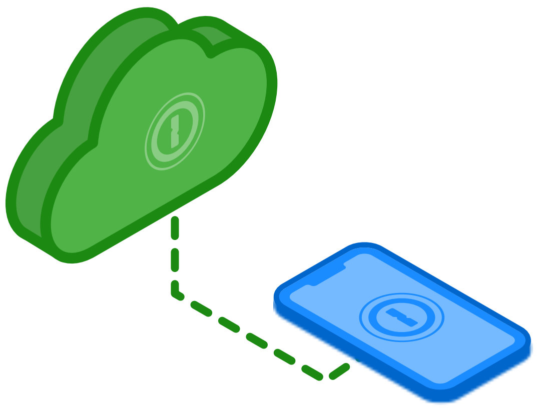
Getting the right credentials to the right people is a key part of password management. Your password manager should have tools that scale to your business — from a vault to share with a team,to advanced sharing with groups and active directory.

	1PASSWORD
Advanced permissions for sharing	👍
Active Directory support for managing a large number of users	👍
Sharing data among users should be managed in a way that doesn't give those who control the server the ability to set up unapproved sharing.	👍

Privacy and Compliance

The information a password manager does have should be kept to themselves not used to remarket or be sold to third parties. The 1Password service will never share, sell or use your details for marketing or market research.

	1PASSWORD
Service should be SOC and GDPR compliant.	👍
Service should be designed to not acquire any user data other than the complete minimum needed to operate the service. “Privacy by Design.”	👍
No data or metadata is passed to third parties or used for internal advertising.	👍



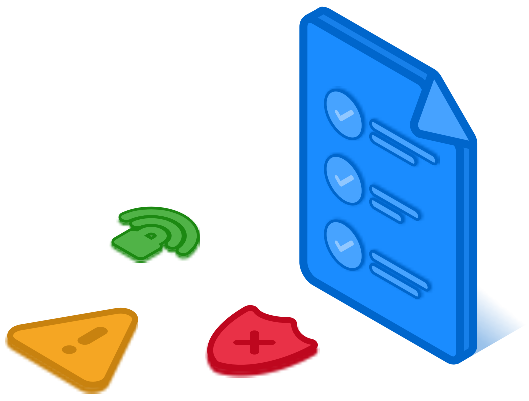
The Cloud

It’s a popular buzzword, and with that comes several questions, but remember the cloud is another server which means it needs to be secure, audited and trusted. 1Password uses Amazon Web Services which has a number of protections and is regularly security tested.

	1PASSWORD
Each session should be encrypted with a key unique to that session (independently of TLS).	👍
Requests to the server should not be reusable if captured.	👍
The security architecture of the system should be well-documented and open to public and expert scrutiny.	👍
TLS, to the extent it is used as an additional layer of security, should be configured to require up-to-date and strict versions.	👍

Auditing and Reporting

Whether you are auditing your own security or reporting on the security of your team, 1Password gives you all the information you need. 1Password's Watchtower is the most comprehensive suite of tools to protect and update passwords at risk. You get alerts based on weak, compromised, vulnerable and duplicate passwords in addition to other security recommendations.



1Password's business reporting allows you to get feedback on your team's security. You can look at a team member's specific usage of a password, how much they use 1Password, and what they have access to. You can report on an individual or the entire team — handy for keeping an eye on security.

	1PASSWORD
Alerts when an account is compromised in a breach.	👍
Diagnoses weak and reused passwords	👍
Reports on team members usage of specific accounts	👍

Get started with 1Password now

Try 1Password Business free for 30 days and keep your business secure.

Try 1Password FREE