1Password

GUIDE

What to consider when choosing a password manager for your business

A step-by-step guide

Introduction

Learn how to choose the password manager that fits your business's budget, privacy, and security needs. Packed with tips, strategies, and a scoring template, this guide has everything you need to pick a solution that works for you and your team members.

In this guide you'll find:

- Why your team needs a password manager.
- What to ask stakeholders.
- Which goals can be reached.
- How to evaluate a password manager.
- A scoring template to compare password managers.

If you still have questions when you get to the end of this guide, reach out to our team! We're happy to help answer any questions you might have about password managers.

Why your team needs a password manager

The first step to choosing a password manager is understanding *why* you need one, and the *value* it can add to your business.

1. Improved security

A password manager keeps your business secure by making it easy for everyone to use strong, unique passwords. It gives your team a secure and convenient way to share those passwords, and helps you keep track of accounts and secrets – even if someone leaves the business unexpectedly.

2. Security oversight

The best password managers include dashboards that help you monitor your organization's security. They'll flag potential security risks so you can quickly take action before any attackers exploit them.

3. Build a culture of security

82% of breaches are traced back to a human element like weak or reused passwords. A password manager will help everyone develop better security habits, be mindful of potential threats, and set a good example for new hires.

4. Increase productivity

A password manager can reduce the time your IT team spends manually setting up users, managing permissions, and resetting passwords. According to Forrester's Total Economic Impact™(TEI) report, businesses can save up to $286,000 simply by increasing the efficiency of their IT support and operations.

Password managers save team members time by autofilling their work logins. Companies that adopt one save over 1,400 employee hours per year that would have been spent typing out credentials or waiting for password resets*.

* Information from Forrester's Total Economic Impact™ (TEI) report.

STEPS TO TAKE WHEN CONSIDERING A PASSWORD MANAGER

Step 1: Identify your stakeholders

Consulting the right people in the early stages of your research will help you choose a password manager that meets everyone's needs. Here's a list of teams you should consider talking to, and some questions to help you understand what they need from a password manager.

Identify your stakeholders

IT

- How much time do you spend resetting passwords each week?
- Which of our existing tools would a password manager need to integrate with?
- How often do you have to reach out to colleagues who have left our company for login credentials?

Finance

- Do you need a secure way to share information with external partners?
- Would the team benefit from a way to share credit card and other payment details, especially if someone isn't in the office while making a purchase?

HR

- Do you feel that logins with access to sensitive employee information are secure with our current password management system?
- Would you benefit from more control over who has access to which logins, with an easy way to grant permission to new hires?
- Could a centralized place to securely store shared logins be helpful to your team?

Developers

- Would your team benefit from a secure way to manage infrastructure secrets like API tokens, application keys, and private certificates?
- Would you be interested in a password manager that can securely store and autofill SSH keys?

Legal

- Do you need a secure way to share confidential documents or contracts?
- Would it be helpful to know when someone accesses a specific login?
- Would you benefit from granular permission settings to ensure everyone only has access to the things they need?

Now that you have a clearer idea of how other teams in your business could benefit from a password manager, you can start defining your goals.

Step 2: Define your goals

If your goal is simply to have a more secure workplace, then adding a password manager to your security stack is a great option. But the benefits of a password manager go far beyond making your workplace more secure.

Building on why you need a password manager, you can use this list to define the goals you hope a password manager will help you achieve. They could be as simple as freeing up your team's time with faster logins, or being proactive when a breach might occur.

Define your goals

Security

- A secure way to store passwords.
- Encourages everyone to use strong, unique passwords.
- Identify passwords that have been compromised.
- Share passwords and other digital secrets with anyone.
- Give users the minimum level of access needed to perform their job.
- Easier to revoke access when someone leaves the company.
- Protects accounts not covered under SSO (Single Sign-On).

Working process / productivity

- Free-up IT time by reducing the need for password resets.
- Increase employee productivity by streamlining login process and credential sharing.
- Autofill helps teams sign in faster.
- Access to login information or secure documents whenever you need it.

Security oversight

- See which password policies are being followed.
- See who accesses shared credentials.
- Overview of your company's security health.
- Know when company-owned domains have been breached.
- Identify weak, reused, or compromised passwords.

Now that you know how the teams in your business could benefit from a password manager and you've outlined the goals for your company, it's time to take a closer look at choosing a password manager that will help you achieve those goals and meet your team's needs.

STEPS TO TAKE WHEN CONSIDERING A PASSWORD MANAGER

Step 3: How to evaluate a password manager

There are more than a few password managers on the market, and all of them promise to keep your team's information safe. Evaluate different options with the mindset of every team being able to stay secure, while sharing sensitive information.

Of course, while a password manager is most effective when your entire team is using it, sometimes that's not yet an option. You can always start small by only rolling a password manager out to a few teams, and then scale over time.

How to evaluate a password manager

Here are the essential features that you should look for when evaluating a password manager:

Basic features

At their core, password managers help you securely store all of your passwords in one place. The basic features you should look for in any password manager include:

- Password storage.
- A strong password generator.
- A secure way to share passwords.
- Alerts for duplicate and weak passwords.
- Easy to use.

Additional password manager features

Security isn't just a nice-to-have – it's a critical part of any business. So you shouldn't settle for just the basics when choosing your password manager. Here are some of the most useful extras that a password manager can offer:

Act as two-factor authentication (2FA)

A password manager can act as an authenticator to retrieve and submit the necessary code when logging in, similar to filling passwords.

Protect your password manager with 2FA

Keep all of your passwords secure by adding an extra layer of protection to your password manager account by enabling 2FA.

Password sharing with anyone

Share passwords with people who don't use a password manager, or who use a different solution. Help keep your information secure when it's in motion.

File storage

Securely store your most important files, so they're always available when you need them.

Reporting dashboards

Useful analytics will help you monitor your business's overall security posture.

Security breach monitoring and alerts

Receive alerts about password breaches.

A commitment to support passkeys

The future is passwordless using passkeys, but you'll still need a secure place to store all those passkeys.

Automated provisioning

Connect your identity provider with your password manager to automate common administrative tasks.

Free family accounts

Encourage good security habits in your employees by helping them stay secure in all parts of their life.

Protect infrastructure secrets

Keep all of your company's secrets secure, including API tokens, application keys, and private certificates.

Secure travel mode

Remove vaults from your computers and mobile devices when traveling across borders.

Compatibility with software you use

People store personal details on phones and tablets as well as desktop and laptop computers. No matter which device, operating system, or browser you choose to use, your password manager should be available everywhere you are.

Cloud-based vaults

If you do use multiple devices, research the syncing capabilities. Cloud-based vaults can be accessed from any device, and many desktop-based programs allow you to set up vaults on multiple devices.

Security

A password manager is the gateway to all of your secrets – so understanding what security measures they employ to keep your data safe is an important consideration. From what they encrypt, to how they encrypt it, here are some things to consider when reviewing a password managers security:

Zero-knowledge encryption

Look for zero-knowledge policies or documentation that shows the encryption and decryption are being done locally – this means the password manager never has access to any of your passwords or secrets.

Audits

Make sure the password manager you consider is independently reviewed. Regular audits help protect against evolving threats.

Vault encryption

Your data should be guarded by tamper-proof protection – even in the event of a breach.

URL encryption

If there is a breach, this will prevent an attacker from knowing which websites you frequent, mitigating the risk of targeted phishing attempts.

Item title encryption

Protect sensitive information within item titles so attackers wouldn't know a credit card from a cookie recipe.

Vault title encryption

If your vault titles contain sensitive information, like your kids' names or confidential project titles a potential attacker couldn't read them.

Support / customer service

Even the best products available sometimes require help setting up, rolling out, or managing day-to-day tasks. Knowing you can get support when you need it is an important feature not on the feature list! Make sure you know what level of help you can expect from your chosen password manager company.

Free onboarding and training

Learn how to use the password manager and onboard your team.

Dedicated customer success

Have an account team dedicated to helping your team manage and adopt the password manager.

Support documentation

Get step-by-step help with a library of self-serve articles.

Live chat support

Get help fast with live chat tools.

Dedicated email support

Reach out with any technical or product issues and a dedicated in-house team of support experts will help.

Dedicated phone support

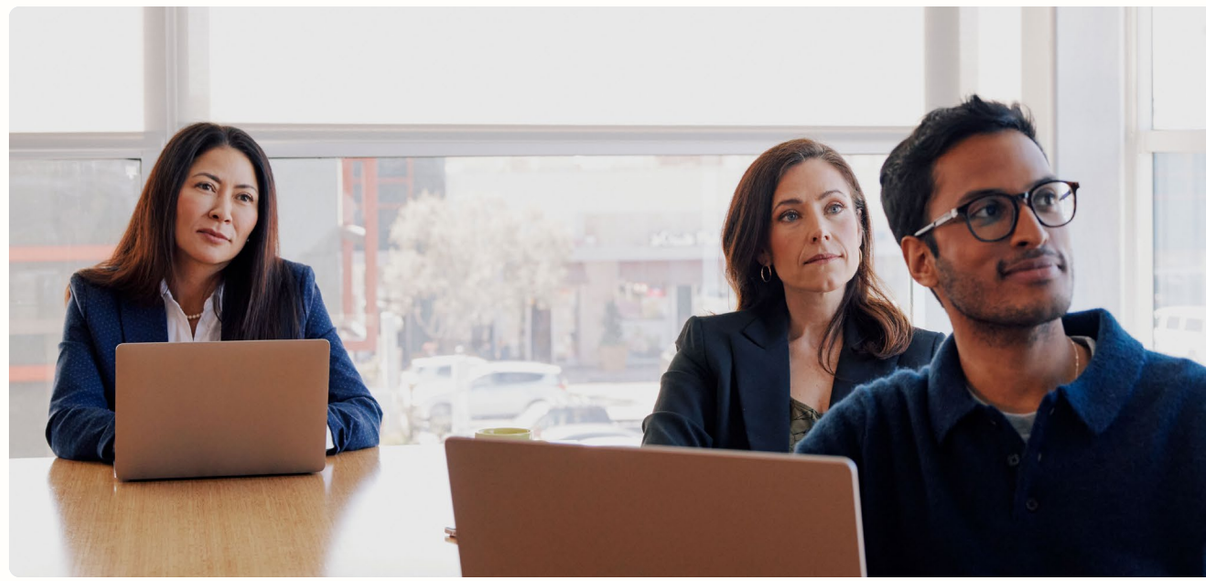
Get real-time support over the phone for quick, personalized assistance.

Price

It's hard to put a price on great security – especially because all password managers offer different plans. Some charge per user, others charge per team, some limit how many devices you can access your password manager on, and others limit how many items you can store. It's important to know that the plan you're looking at includes everything you need to keep your information safe.

Price

Price is important, but you shouldn't compromise to save a quick dollar given the ROI of a password manager.



Comparison template

Use this template to identify which password managers have the features you're looking for with the security you expect. Remember, the goal is to find the best password manager that will help you achieve your goal of protecting your business.

We've already gone ahead and pre-filled the 1Password column for you.

Basic features →
Additional password manager features →
Security →
Support / customer service →
Price →

Basic features	1Password		
Password storage	Yes		
A strong password generator	Yes		
A secure way to share passwords	Yes		
Alerts for duplicate and weak passwords	Yes		
Easy to use	Yes		

Additional password manager features	1Password		
Act as two-factor authentication (2FA)	Yes		
Protect your password manager with 2FA	Yes		
Password sharing with anyone	Yes		
File storage	1Password Business – 5GB per person		
Reporting dashboards	Yes		
Security breach monitoring and alerts	Yes		
A commitment to support passkeys	Yes		
Automated provisioning	Yes		
Free family accounts	Yes		
Protect infrastructure secrets	Yes		
Secure travel mode	Yes		
Compatibility with software you use			
Cloud-based vaults	Yes		

Comparison template (continued)

Security	1Password		
Zero-knowledge encryption	Yes		
Audits	Yes		
Vault encryption	Yes		
URL encryption	Yes		
Item title encryption	Yes		
Vault title encryption	Yes		

Price	1Password		
Zero-knowledge encryption	$7.99 USD per user/ month		

Support / customer service	1Password		
Free onboarding and training	Business customers with 21 seats and above get complimentary support		
Dedicated customer success	Business customers with 21 seats and above can get support any time.		
Support documentation	Yes		
Live chat support	Yes		
Dedicated email support	Yes		
Dedicated phone support	Yes		

Why 1Password

1Password is the world's most-trusted password manager that does more than just protect your passwords.

With industry-leading security and usability we help businesses securely manage passwords, secrets, private documents, and their most sensitive data from online threats.

Security

Security isn't just a feature, it's our foundation. Your data is end-to-end encrypted, protected by the combination of a 128-bit Secret Key and an account password – dual-key encryption that's unique to 1Password. We work with other security experts to make sure our code is rock solid – and we offer the highest bug bounty in the industry. Our security model is designed to keep everyone's information safe, even in the event of a breach.

Privacy

We can't see what you store in 1Password, so we can't use it, share it, or sell it – and neither can anyone else.

Support

As a 1Password customer, you automatically get access to our dedicated account teams to help with bespoke setup, training, and complimentary hands-on help with onboarding. We also have an extensive library of support documentation available for whenever you need it.

Unlock via Single Sign-on (SSO)

1Password integrates with your existing SSO to make authenticating and provisioning employees simple. And now, you can even use SSO to log into your 1Password account. Our approach to this integration was to keep SSO simple, but also keep your secrets yours. Simplify your security across the board with a unified experience that makes it easy for your team to work.

Reporting

See your team's security health at a glance so you can mitigate your risks and take immediate action. With 1Password Watchtower you'll be notified of exposed passwords, and when company-owned domains have been breached. And with 1Password Insights you'll be able to monitor password health, usage, and sharing – all from one integrated dashboard.

Contact us

Our team will work hand-in-hand with you to understand your unique business needs. Head to 1Password.com/business to sign up for a 14-day free trial today or contact the 1Password Sales team to find out if 1Password is the best option for your team.

Need a hand persuading your company that they should invest in a password manager?
Learn how to convince your leadership team that a password manager is necessary with our free guide.