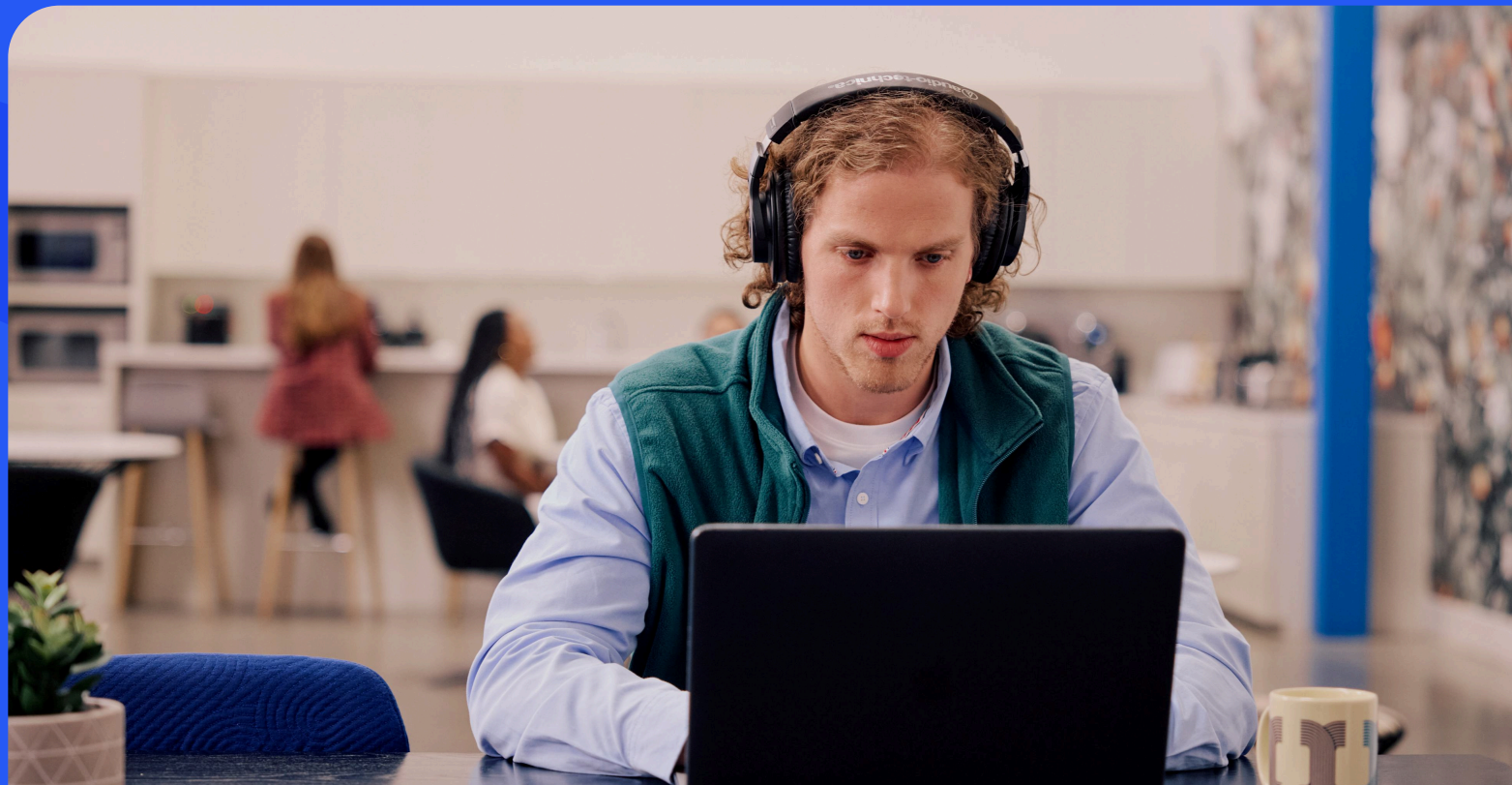
1Password

Small business. Big security risks.

This new approach to access security can lower risk and increase productivity for SMBs.



Introduction

If you work in IT at an SMB, you're all too familiar with wearing too many hats while having too little time. From hardware to applications, data, security, compliance, and more, you're responsible for ensuring the business operations run smoothly and securely without impeding employee productivity.

But while employees will typically let you know when they need a new computer, it's uncommon for someone to create an IT ticket requesting better security. If anything, employees can often see security as a productivity-draining hindrance to work around if necessary. Making matters worse, remote and hybrid work has exacerbated the challenges of securing your company. It's harder than ever to manage or even get visibility into the devices and applications that your teams are using.

Big risks for SMBs

The pressure to secure all of your company's data, employees, apps, and devices can be overwhelming. Especially when you face:

- Limited bandwidth to prioritize security against competing IT responsibilities.
- Difficulty getting employees to comply with security practices.
- Lack of visibility into the unmanaged apps and devices brought in by employees.

But the risks of not prioritizing security are too big to ignore.

Challenges to address	Potential consequences
80% of employees use non-sanctioned shadow IT	70% of cyber attacks target small businesses
Stolen credentials are the leading entrypoint for hackers to gain access to systems.	$5.53M is the average cost of a data breach when remote employees are involved
88% of SMB breaches involve ransomware, and the average ransomware payment in 2025 was $115,000.	1 in 5 SMBs said they would go out of business if an attack cost them as little as $10,000. 1 in 5 SMBs said they would go out of business if an attack cost them as little as $10,000.

These challenges and consequences are driven by two seemingly conflicting obstacles:

- Employees are increasingly working with unmanaged applications that use weak or reused credentials, introducing risk and potential exposure for your company.
- On the other hand, you need to ensure employees have the tools and applications they need to be productive and make the company successful – even if that includes shadow IT.

The even bigger question – how do you do both in a way that's manageable and doesn't impact your overall security posture?

Making security *access*-able

The only way to enable your team to use the tools and devices they need, and not overwhelm yourself in the process, is to streamline how employees access those tools. By addressing the access problem, you'll be able to:

1. Provide the flexibility your team needs while still maintaining security.
2. Drive adoption of secure access practices across your organization.
3. Improve the overall security posture of your organization.

Looking for practical steps you can take to address these challenges? Head over to 1Password's checklist for data breach prevention.

Flexible, yet secure

Each member of your organization uses a variety of tools to get their job done, but are all of those tools managed and secure? Finding ways to secure the tools that employees use, even if you don't manage them directly, is the only way to ensure that any data or information related to each tool is protected.

The easiest way to tackle this problem is to protect the point of access: credentials. By securing logins and passwords, you can ensure that any app your team uses is secure from the get-go. Even better, with a tool like a password manager, you remove the need for employees to memorize every password, meaning they can use strong, unique passwords for every account.

With the right password manager, you can even simplify the process of onboarding new employees. By creating groups for different departments and levels, new team members can have access to everything they need from day one. Having employees assigned to groups also makes offboarding departing employees as simple as revoking their access to group credentials.

> *The easiest way to tackle this problem is to protect the point of access:* ***credentials.***

Go with the workflow

One common challenge facing IT teams is increasing employee adoption of security tools. The key is to find solutions that actually improve the lives of your users, instead of making them harder. Password managers are a great example of a tool that improves security while improving productivity. For example, they can:

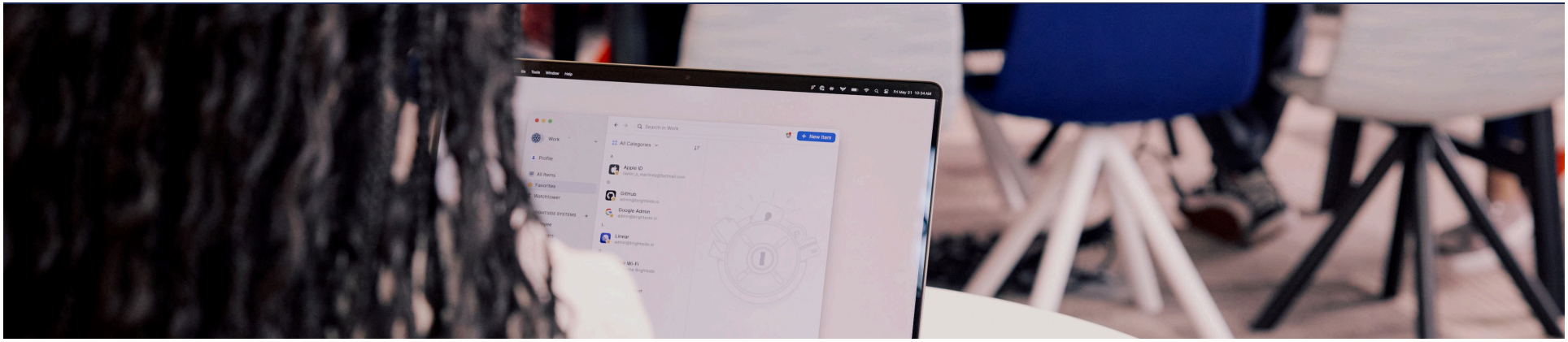
- Simplify and standardize the password process and ensure high security.
- Make it easy to share and manage credentials between teams that use shared accounts, like primary bank accounts in finance, or social media accounts in marketing.
- Significantly reduce the number of password reset requests.

As Jan Van der Kolk, the IT Manager at Dovetail, put it, “1Password helps us maintain our security culture as we scale and grow. It’s important to have one tool across the business that we can rely on for everyone to safely store and share credentials.” He went on to say that, “We no longer get any IT requests for resetting passwords. With a lot of people and tools, that time adds up.”

Posture check! Is your access secure?

Securing access is a foundational step in improving your overall security posture, especially when it comes to the tools that you don't know about. The worst-case scenario is your team is creating accounts in multiple places and using simple or easy-to-crack passwords. These practices inherently open your organization up to unnecessary risk.

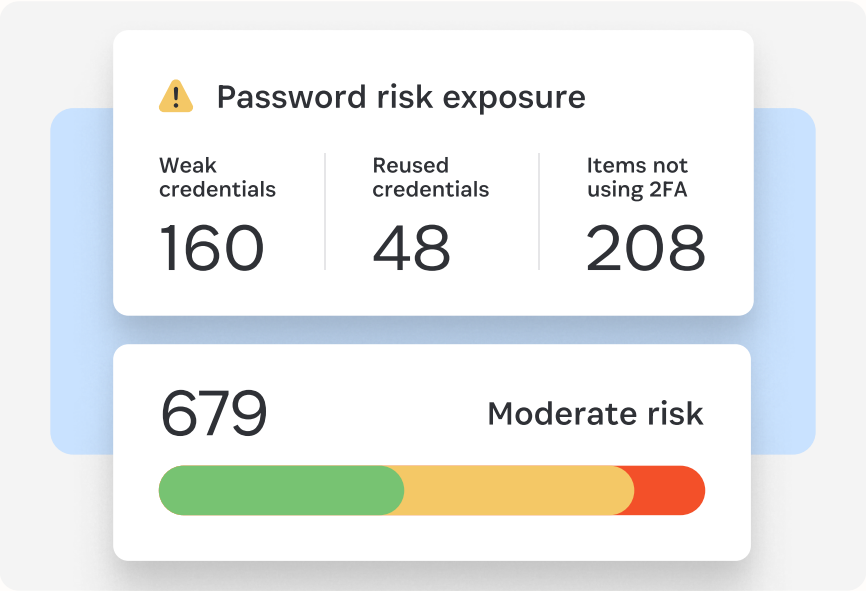
Standardizing how you approach and enforce access management practices across your organization can help protect you from attacks like phishing and stolen credentials, among others.



How 1Password helps solve the access problem

1Password makes strong security easy while providing the visibility needed to keep your company safe. Save time and take back control, all while securing your business. With 1Password you can:

- Provide employees secure access to any tool from any device or location.
- Enable employees to autofill and securely share logins, two-factor codes, security questions, and much more so the secure thing is always the easy thing.
- Identify which of your team's passwords are being reused or have been caught in a data breach.



Conclusion

1Password

We've seen that employees will find ways to work around security systems that interrupt their workflows, unintentionally exposing their company to risk. It's up to IT teams to adapt to how and where their team is getting work done. Productivity and security don't have to be a "one or the other" option.

That's why over 175,000 businesses rely on 1Password's Enterprise Password Manager to secure their business. With 1Password, companies are able to secure every sign-in, regardless of where your workforce is. 1Password is built with your team in mind, ensuring they're secure without slowing them down.

Learn more about 1Password for small and mid-size businesses.

© 2025 AgileBits Inc. All Rights reserved. 1PASSWORD, the Key Hole Logo and other trademarks owned by AgileBits Inc.