



Guide: Top Password Managers for UK Businesses



1Password



NordPass®



DASHLANE



KEEPER



Zoho
Vault

LastPass...

bitwarden



For businesses in the UK, cybersecurity is more critical than ever. Password managers help protect sensitive information, streamline login processes, and reduce the risk of cyberattacks.

With a variety of password managers on the market, it's essential to choose the one that best fits your business's needs.

Here's a comparison of the most popular options available for UK businesses, including pros and cons to help guide your decision...

1Password

Overview: 1Password offers a streamlined user experience with powerful features, including customisable user permissions and dedicated customer support. It's a strong choice for teams seeking an easy-to-navigate, highly secure option.

Pros:

- **Excellent User Interface:** Clean and easy to use for all employees.
- **Security Features:** Offers data encryption and supports advanced authentication methods.
- **Team Permissions:** Admins can set specific permissions for individual team members.
- **Activity Logs:** Track who is accessing which credentials and when.

Cons:

- **Higher Pricing:** One of the more costly options, which may not be ideal for smaller businesses.
- **Limited Integrations:** Fewer integrations compared to other options like LastPass.

Best For: Teams seeking high security with easy-to-use, customisable controls.



1 out of 3

people have fallen victim
to a data breach due to a
weak password

SMB Guide



Overview: Keeper's business solution focuses on scalability, making it ideal for growing businesses. It offers customisable options and robust support for team and user management.

Pros:

- **Scalable:** Can grow with your business, suitable for small teams to enterprise-level organisations.
- **User-Friendly:** Simple interface that reduces training time.
- **Breach Monitoring:** Alerts users about breaches involving their credentials.
- **Compliance Support:** Provides tools for meeting various compliance standards.

Cons:

- **Costly:** Higher price tag, particularly for premium features.
- **Limited Free Trial:** Offers a short trial period, which may not be enough for thorough testing.

Best For: Growing businesses that need scalability and tools for compliance monitoring.

LastPass...|

Overview: LastPass is one of the most well-known password managers, offering robust features for teams and enterprises. It provides centralised admin control and advanced security measures, making it popular among small to medium-sized businesses.

Pros:

- **Ease of Use:** Intuitive design suitable for all users.
- **Admin Console:** Enables IT teams to manage passwords, monitor security, and enforce policies.
- **Multi-Factor Authentication (MFA):** Adds an extra layer of security.
- **Shared Vaults:** Ideal for team collaboration.

Cons:

- **Recent Security Concerns:** LastPass faced a few high-profile security issues, which may raise concerns for some businesses.
- **Pricing:** May be expensive for very small teams or start-ups.

Best For: Small to medium-sized teams that need a reliable, easy-to-manage password manager.

60%

of users reuse passwords across multiple accounts, significantly increasing security risks.



Overview: Bitwarden offers a more budget-friendly solution, making it especially appealing for startups and SMEs. It's open-source, which means it's highly transparent and customisable.

Pros:

- **Cost-Effective:** One of the most affordable options with no compromise on security.
- **Open-Source:** Allows for greater transparency and trust in security practices.
- **Self-Hosting Option:** Businesses can host it on their servers for added control.
- **Cross-Platform Support:** Works on nearly every device and browser.

Cons:

- **Limited Support:** Not as robust in terms of customer support options compared to premium services.
- **Less Intuitive Interface:** The UI is not as user-friendly as competitors like LastPass and 1Password.

Best For: Cost-conscious businesses looking for a secure, transparent, and flexible password manager.



Overview: Dashlane provides strong security and excellent usability. It also includes a built-in VPN, making it a great choice for companies prioritising privacy and data protection.

Pros:

- **Integrated VPN:** Adds an extra layer of security for remote workers.
- **Easy Deployment:** Simple setup and maintenance, even for non-technical users.
- **Secure Sharing:** Enables secure sharing of passwords and other sensitive data.

Cons:

- **Limited Customisation:** Fewer admin control options compared to other solutions.
- **Price:** Costs may be high for businesses needing premium features like the VPN.

Best For: Businesses prioritising both password management and privacy features, especially those with remote teams.

"Password" and "123456" continue to dominate as the most frequently used passwords, despite their extreme vulnerability 🙊



Overview: Zoho Vault offers a secure, easy-to-use password manager with an emphasis on collaboration features. It's particularly suitable for smaller businesses seeking an integrated, secure system without a large investment.

Pros:

- **Budget-Friendly:** Provides a range of pricing plans to suit various business sizes.
- **Easy Collaboration:** Supports secure sharing within teams.
- **Integration with Zoho Products:** Works well within the Zoho ecosystem, making it ideal for Zoho users.
- **Role-Based Access Control:** Facilitates secure sharing by setting access permissions.

Cons:

- **Less Known in Market:** Has a smaller footprint and may lack some of the brand trust of larger providers.
- **Limited Advanced Features:** May not have the depth of features needed for larger enterprises.

Best For: Small to medium businesses already using the Zoho ecosystem or looking for an affordable, collaborative password manager.



Overview: NordPass Business, developed by the team behind NordVPN, offers powerful security tools with easy-to-use functionality. It's designed to help businesses securely manage passwords and sensitive information.

Pros:

- **Encryption:** Zero-knowledge encryption ensures no one but the user can access their data.
- **User-Friendly:** Easy onboarding with intuitive user experience and simple deployment for teams.
- **Monitoring:** Password health reports that help businesses identify weak or reused passwords.
- **Breach Monitoring:** Multi-factor authentication and data breach scanning.
- **Cost Effective:** Affordable pricing compared to premium options.

Cons:

- **Limited Advanced Features:** Limited advanced features in comparison to LastPass or Keeper.
- **Limited Integration:** Less integration with third-party tools than some competitors.

Best For: Businesses that need a simple, secure password manager with a focus on encryption and ease of use.

Conclusion

Choosing the right password manager can be a game-changer in securing your business's digital assets.

Each of these password managers offers a unique set of features tailored to different needs. LastPass and 1Password are excellent for ease of use, while Bitwarden stands out for its affordability. Keeper and Dashlane are ideal for businesses seeking scalability and privacy, respectively.

Ultimately, your choice will depend on the specific requirements, budget, and scale of your business.

Need help choosing the right Password Manager?

With so many options, finding the best password manager for your business can feel overwhelming. At Somerbys IT, our team specialises in helping businesses secure their data and optimise digital security.

Contact us today to discuss your needs and let us help you find the perfect solution for your team.

0333 456 4431 | info@somerbysit.co.uk

Dock 3
75 Exploration Drive
Leicester, LE4 5NU

