UBINODES

Review:
13 Password Managers

Review: 13 Password managers.

Our primary security focus revolves around robust password management and encryption. Creating strong passwords requires finding a balance between length and complexity, as short and easily remembered passwords are more vulnerable to compromise. It's crucial to strike a balance where passwords are accessible to you but difficult for potential attackers to guess.

The encryption method used depends on the application, with the most important consideration being secure storage. Adopting a layered security approach when creating and managing passwords is essential. In an interconnected world, vulnerabilities can arise from multiple sources, so deploying multiple defences becomes necessary for comprehensive protection.

Taking proactive steps to protect yourself also helps safeguard the organization from threat actors. With cyber-attacks on the rise, it's vital to establish safeguards. Consider using one of the safe and user-friendly password management tools listed below to enhance password protection. Our goal is to provide you with the knowledge to avoid and mitigate attack risks, aligning with Ubinodes' work style and flow.

Our specifications sheet:

Security:

- Resistance to state-sponsored criminals (note 1)(note 2).
- Open-source (note 3).
- Administration of users.
- Access and activity logs: To know when and by whom passwords are accessed.
- IP restrictions: To restrict access of our vaults to only pre-approved IP addresses.

Accessibility:

- Multi-platform (note 4).
- Intuitive: Anyone and everyone can use it from a teenager to a 70-year-old.

1Password (01/13)

1Password is a password manager for individuals, families and businesses with lots of classic features and a few unique ones.

1.1 1Password-Pros:

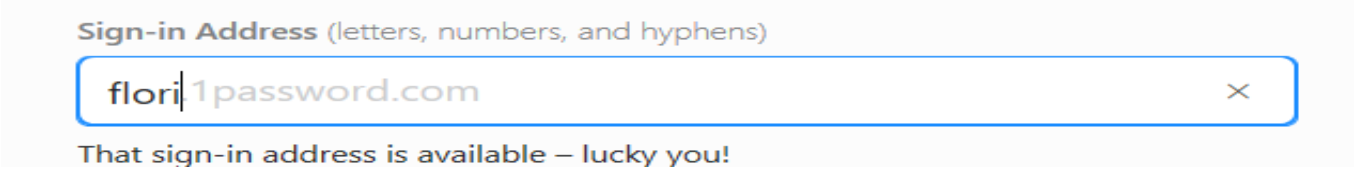
- Ensure secure password and document sharing
- User activity reporting
- Streamlined group permissions administration,
- Employ personalized access URLs that are challenging for third parties to find, activate

- Travel Mode to remove sensitive information during travel,
- Implement secret keys for user authentication.

1.2 1Password-Cons:

- Implement a complex login procedure.
- Lack user-restricted access.
- Subscription cost: $3 per user per month, with a family plan available at $5 per user/month.
- Provide offline access, considering the sensitivity to device theft (note 1).

1.3 1Password-Screenshots:



Bitwarden (02/13)

The product securely stores network users' passwords in an encrypted vault, offering easy and safe management. Bitwarden software is available on both mobile and PC, supporting Linux, MacOS, Windows, and Android operating systems. The software is traditionally open source and free for a single user, with a slight increase to $5 per month for each user in larger organizations. Passwords are encrypted using AES-256 bit encryption and support the SHA-256 hashing algorithm.

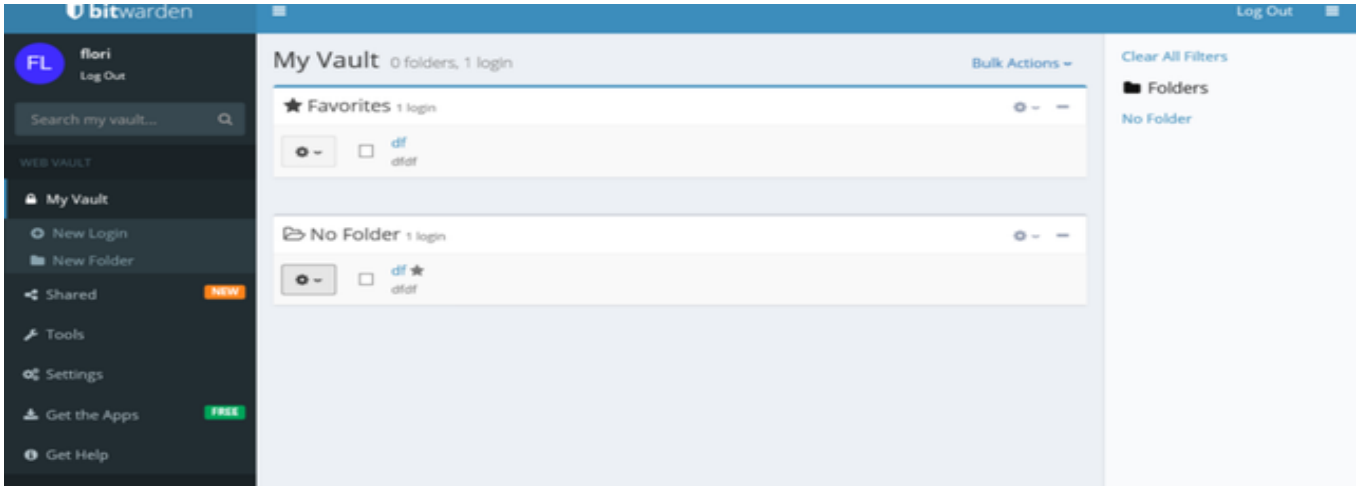
2.1 Bitwarden-Pros:

- Facilitates password sharing.
- Encrypts the login page.
- Operates as a cloud solution.
- Open-source.
- Allows the disabling of auto-fill for login credentials.
- Supports Two-Factor Authentication (2FA) and Time-Based One-Time Passwords (TOTP).
- Includes 1 GB of encrypted file storage.

2.2 Bitwarden-Cons:

- No recovery option in case of main password loss.
- Lacks an activity log for user monitoring.
- Does not provide IP address restricting/whitelisting.
- No reporting feature.
- Pricing: $3 per user per month for basic features, with additional offerings including a personal use premium plan at $10 per year and a team plan at $5 per user per month.

2.3 Bitwarden-Screenshots:



Dashlane (03/13)

Unlike the previous product, Dashlane operates on a subscription basis as a password manager, supporting standard operating systems such as MacOS, Windows, iOS, and Android. In addition to password management, Dashlane functions as a digital wallet, with encryption based on the SHA-256 algorithm. The software, available in 12 languages, provides two-factor authentication and VPN integration, catering to organizations of any size.

Contrary to the Wall Street Journal's assertion that "Neither Dashlane nor a hacker (or government agency) ... could access your data without knowing your master password," this claim is inaccurate. (note 1).

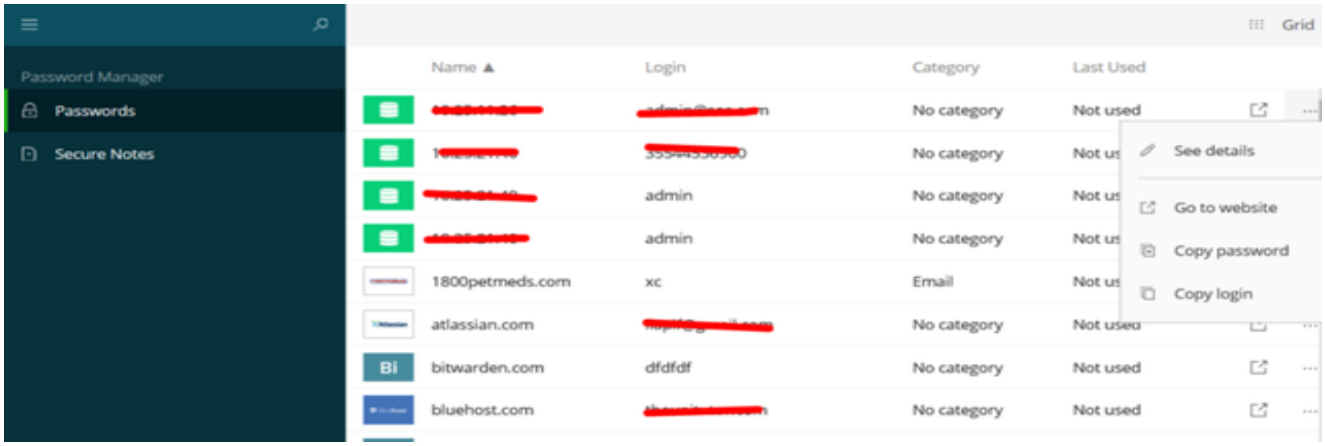
3.1 Dashlane-Pros:

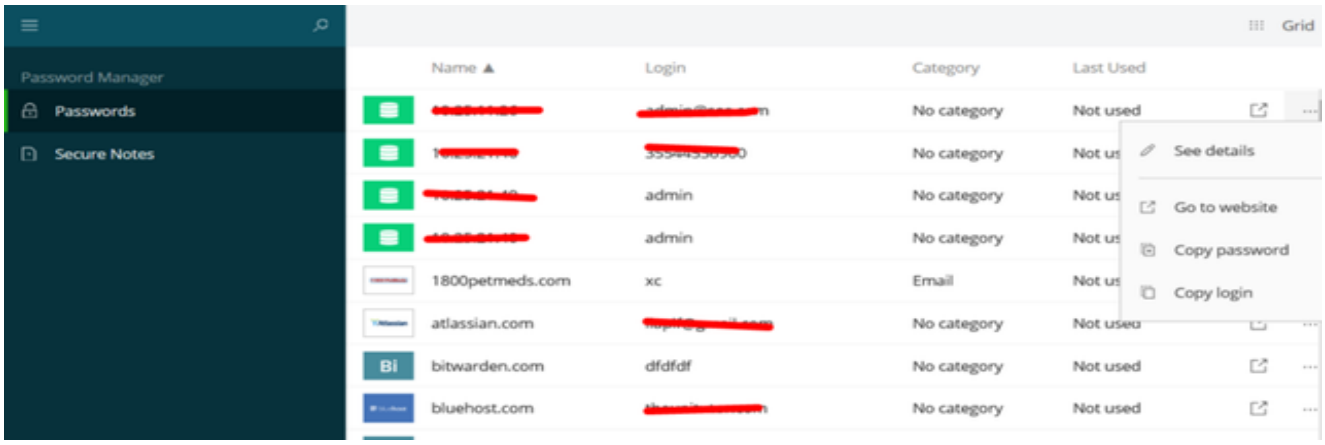
- Provides login reporting.
- Enables secure password sharing, with a limit of 5 for free accounts and unlimited for business plans.
- Allows the disabling of auto-login and autofill.
- Offers a free option, with a business plan priced at $4 per user per month.
- Supports Two-Factor Authentication (2FA).
- Utilizes 2FA to secure connections to new devices.
- Facilitates secure data sharing between users using asymmetric encryption.
- Ensures user data protection even in the event of Dashlane server compromise.

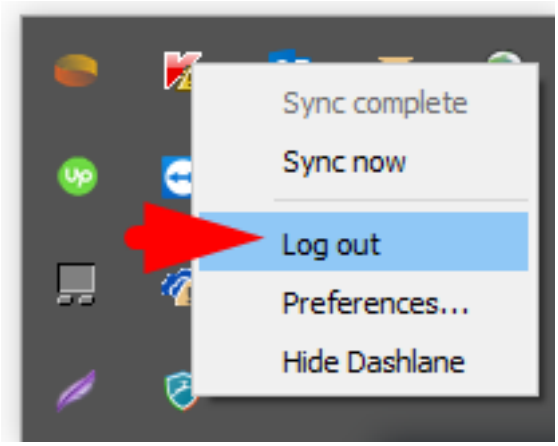
3.2 Dashlane-Cons:

Password management must be conducted through a locally installed app, heightening the risk of unauthorized access from a lost or stolen device (note 1). Manual logout is mandatory after each session.

3.3 Dashlane-Screenshots:







Encryptr (04/13)

Discontinued: https://spideroak.support/hc/en-us/articles/115003945666-Encryptr-End-of-Life

Keeper (05/13)

Keeper is a great tool for keeping your website passwords and financial info safe. It works as a cloud service, meaning it operates from servers in the cloud. You can use it on your

computer or phone, whether you have Linux, MacOS, Windows, or Android. There are different plans for students, families, personal use, businesses, and bigger companies.

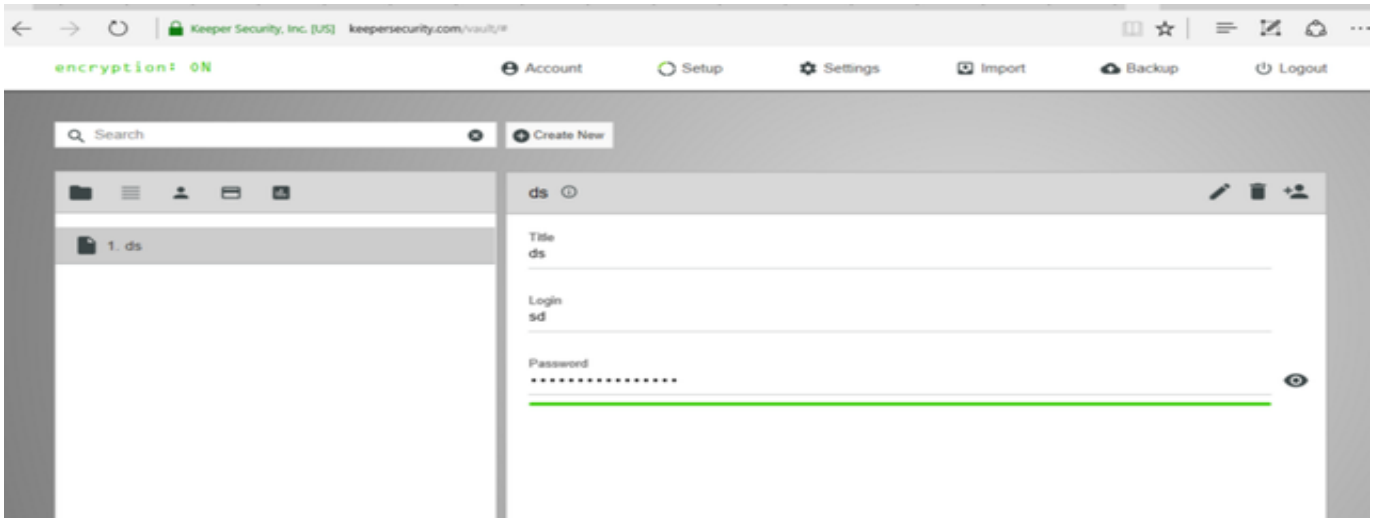
5.1 Keeper-Pros:

- Encrypted access,
- Access and activity tracking,
- Secure password sharing,
- Recovery account for emergency access,
- Main password vaults not stored locally,
- Cloud solution,
- Two-factor authentication, including Yubikey.

5.2 Keeper-Cons:

- Lacks reporting
- IP address restricting/whitelisting
- Offers very basic console features.
- Priced at $30 per user per year for basic functionality.

5.3 Keeper-Screenshots:



Lastpass (06/13)

LastPass is a user-friendly password manager with both free and highly affordable options. The company emphasizes robust encryption algorithms, offering a password manager accessible through major browsers and apps from prominent app stores.

6.1 Lastpass-Pros:

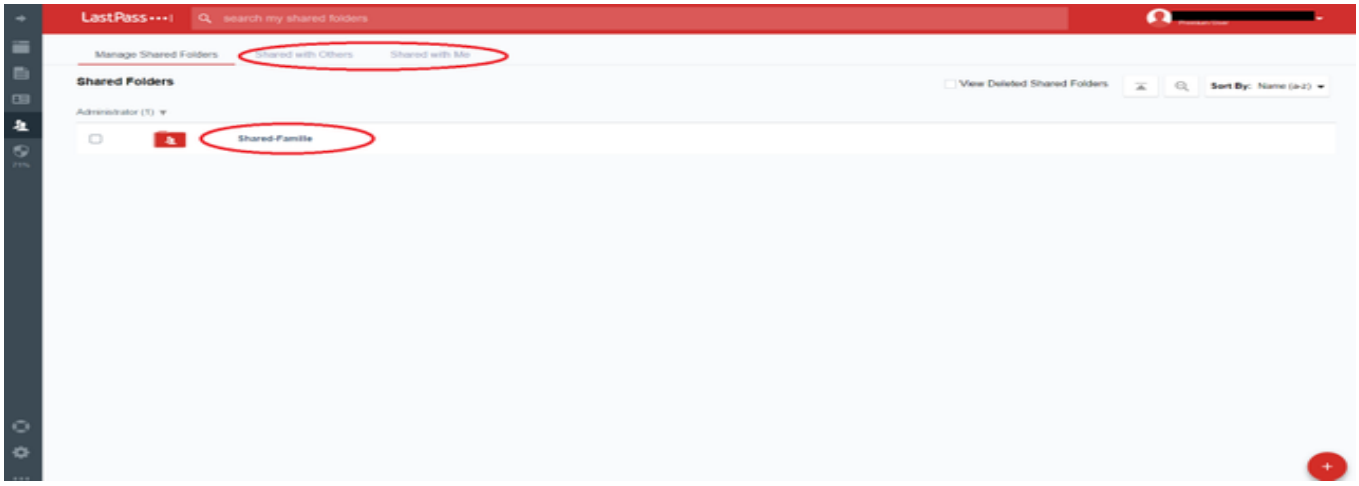
- Two-factor authentication provided.
- Enables password sharing.
- Includes a form filler option.
- Allows note storage.

All features available at a very affordable price: $24 per user per year for the premium plan, while the team plan is priced at $29 per user per year. Also includes 1GB encrypted file storage.

6.2 Lastpass-Cons:

Offline mode: Vulnerable to physical theft since passwords can be stored on devices for offline access, although this can be disabled in the settings (note 1). Potentially susceptible to brute force attacks as all data is stored in user browsers, presenting a vulnerability exploitable by hackers.

6.3 Lastpass-Screenshots:



Myki (07/13)

A relatively new password manager with lots of advanced features but some basic vulnerabilities.

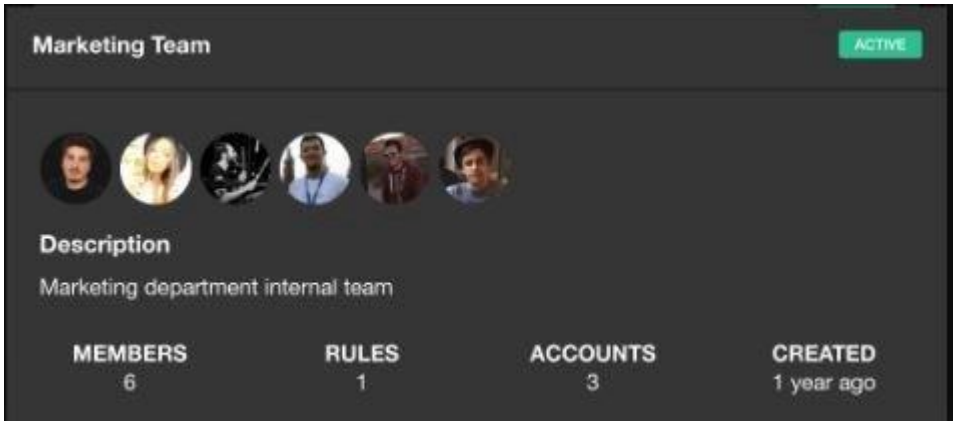
7.1 Myki-Pros:

- Cost-effective for teams at $48 per 100 users per year.
- Provides provisional accounts,
- Facilitates management and access restrictions for multiple members simultaneously.
- Offers geographical access restrictions, allowing mapping to limit team members' account access.
- Incorporates IP address restricting/whitelisting
- Time-based access control.
- Features Browser Activity Monitoring (BAM) for real-time insights into users' interactions, down to their keystrokes, aiding in detecting malicious activity.
- Includes account sharing functionality to grant access without sharing credentials and supports two-factor authentication.

7.2 Myki-Cons:

- Provides solely mobile app access, exposing vulnerability to device theft.
- Local storage of passwords on phones heightens susceptibility to device theft.
- The web interface is still under development,
- UI lacks polish.
- The digital wallet auto-fill feature is also susceptible to theft.

7.3 Myki-Screenshots:



PassworkMe (08/13)

PassworkMe is a team-oriented password manager designed for companies and startups, with hosting based in the Netherlands.

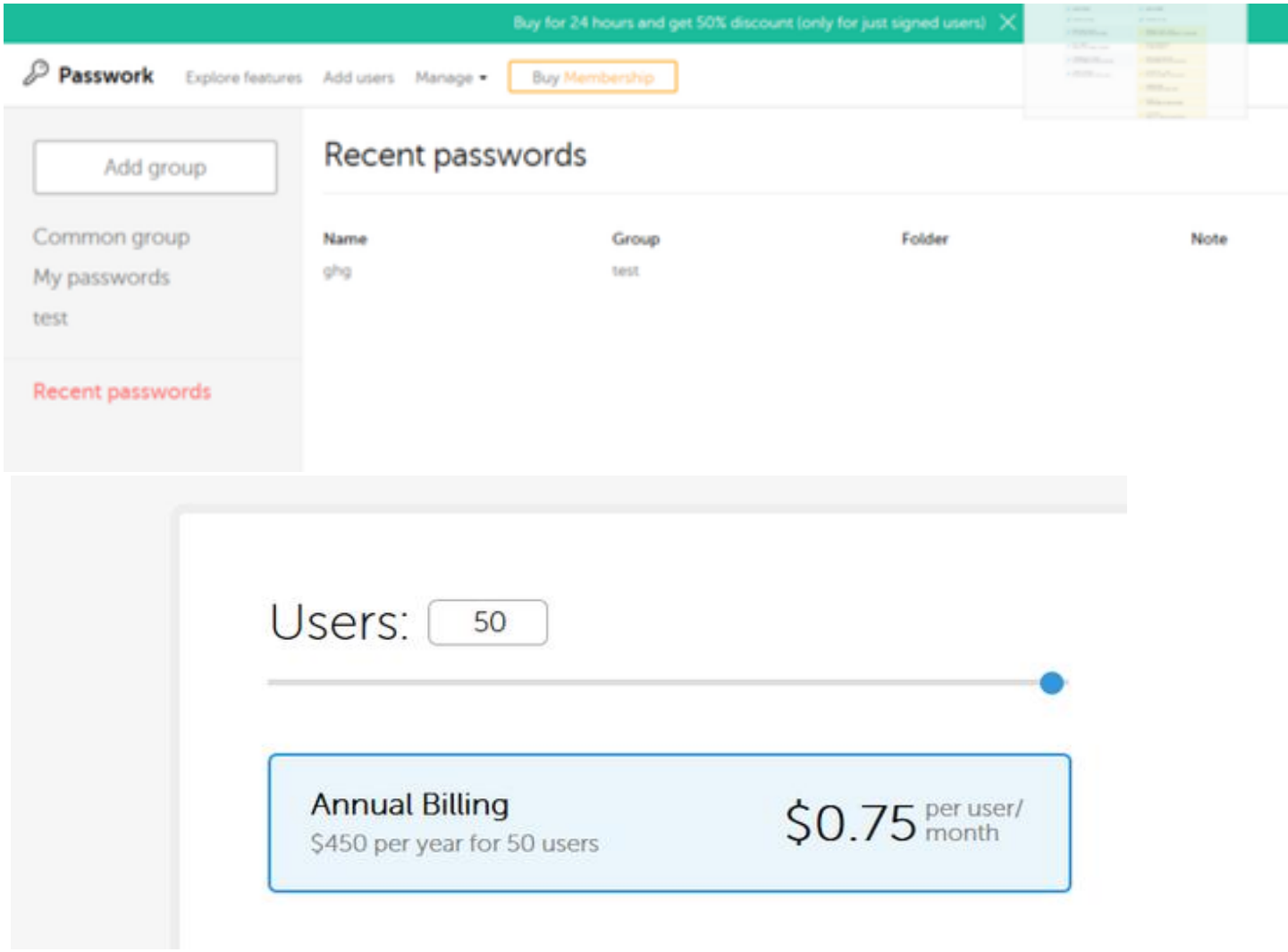
8.1 PassworkMe-Pros:

- RSA encrypted access.
- Priced at $18 per user per year.
- Flexible vaults are not stored locally.
- Password vaults are not stored locally.
- Includes IP address restricting/whitelisting.
- Facilitates secure password sharing.

8.2 PassworkMe-Cons:

- Limited to 50 users.
- Lacks emergency access.
- No user restrictions.

8.3 PassworkMe-Screenshots:



Roboform (09/13)

RoboForm claims the title of the world's top password manager and secured the second spot for our organization. Here's why:

9.1 Roboform-Pros:

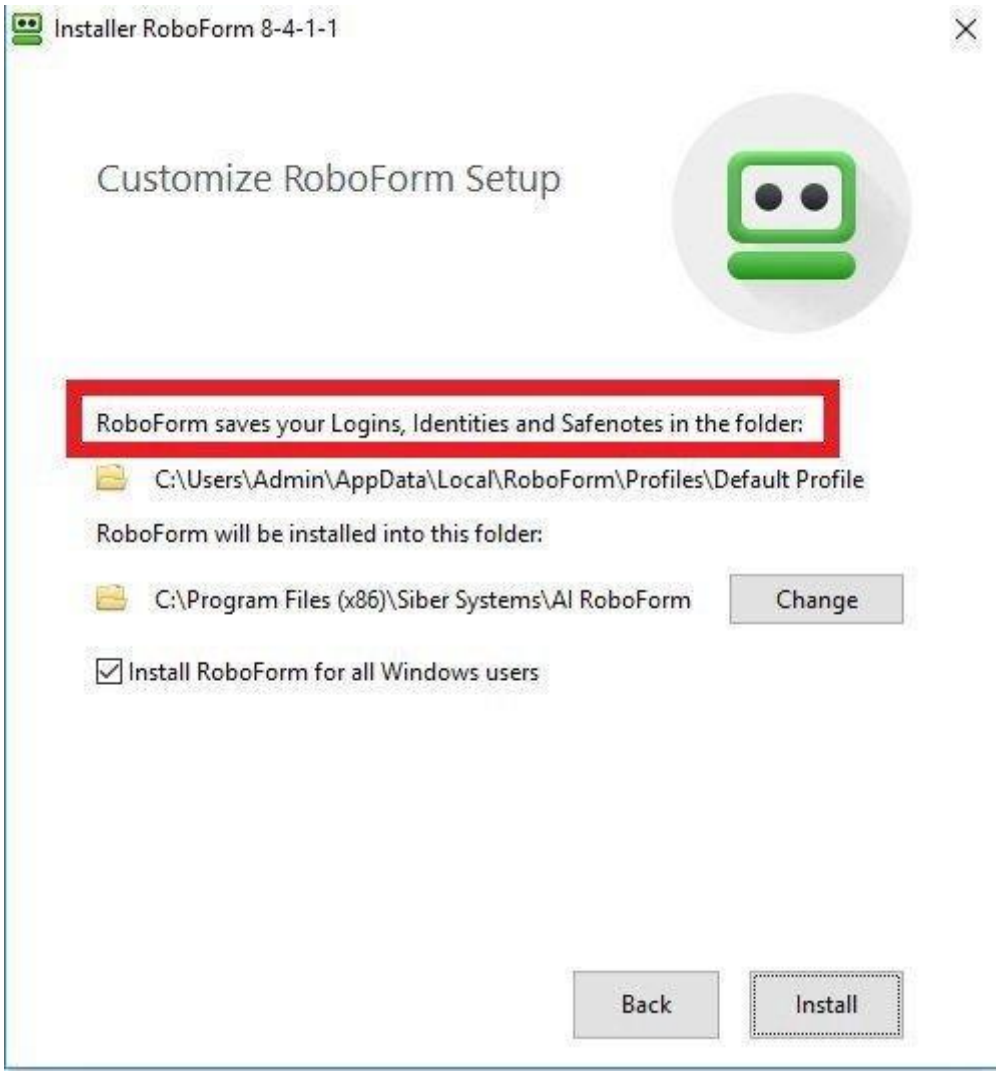
- Enforces robust user policies.
- Features user-friendly interfaces.
- Includes IP address whitelisting.
- Incorporates a web session timeout feature.
- Provides a one-time password authentication option.
- Allows administrators to limit the number of password changes.
- Offers user login reports.
- Employs end-to-end encryption for password sharing.

- Facilitates the importation of browser bookmarks.
- Competitively priced at $25 per user per year for a business account.

9.2 Roboform-Cons:

- Restricts password sharing to paid accounts.
- Requires most actions to be performed through installed software.
- Stores data locally.
- Poses challenges for users in terms of management.

9.3 Roboform-Screenshots:



Safe in Cloud (10/13)

SafeInCloud is another leading password manager known for its simplicity, user-friendliness, and compatibility across major platforms and devices.

10.1 SafeInCloud-Pros:

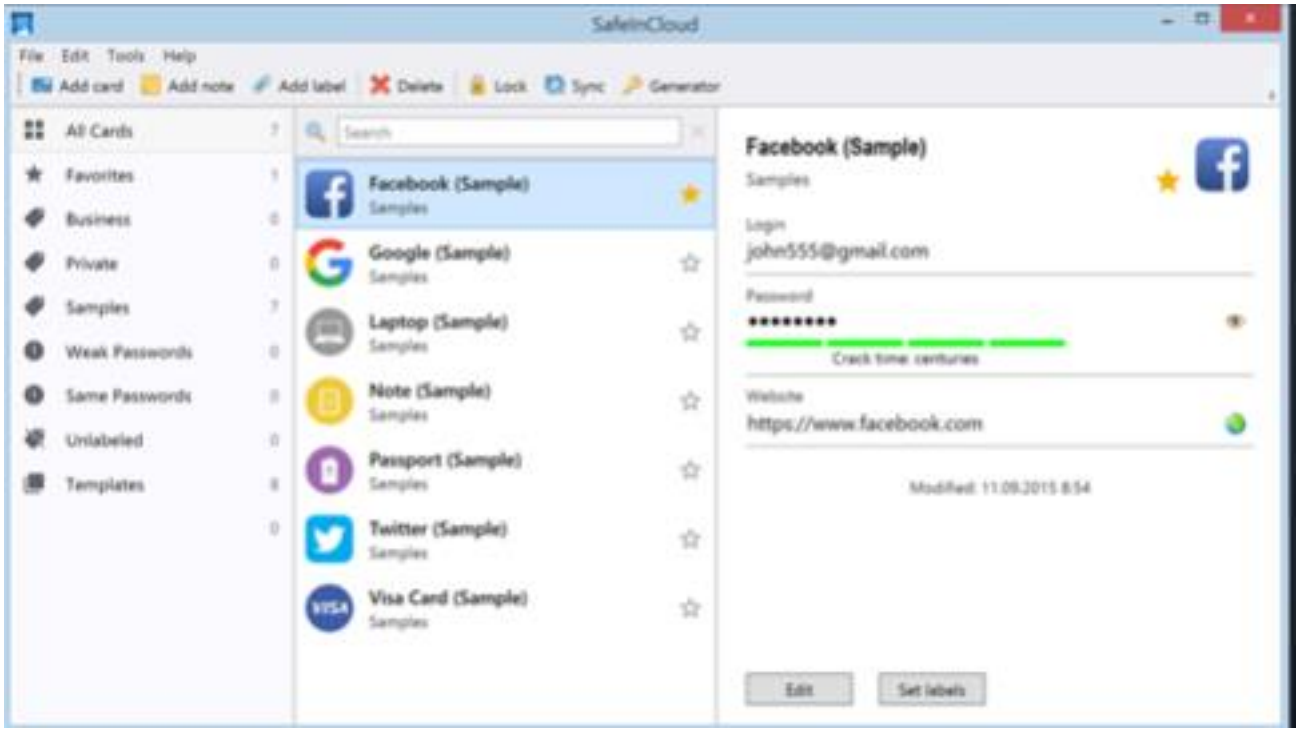
- Free.

- Facilitates password sharing.
- Includes a password generator and strength indicator.
- Offers cloud synchronization.
- Employs strong AES-256 encryption.
- Supports fingerprint authentication.

10.2 SafeInCloud-Cons:

- Standalone solution: Requires local installation on devices.
- Lacks access or activity tracking.
- Automatically deletes the database if incorrect passwords are entered five times.

10.3 SafeInCloud-Screenshots:



Sticky Password (11/13)

Sticky Password is a good password management option for personal use. However, it's not ideal for teams, especially those in high-risk countries. While originally designed for personal use, Sticky Password plans to add a new sharing feature soon. This feature will allow selected accounts to be shared among Sticky Password users, making it more suitable for working teams.

11.1 StickyPassword-Pros:

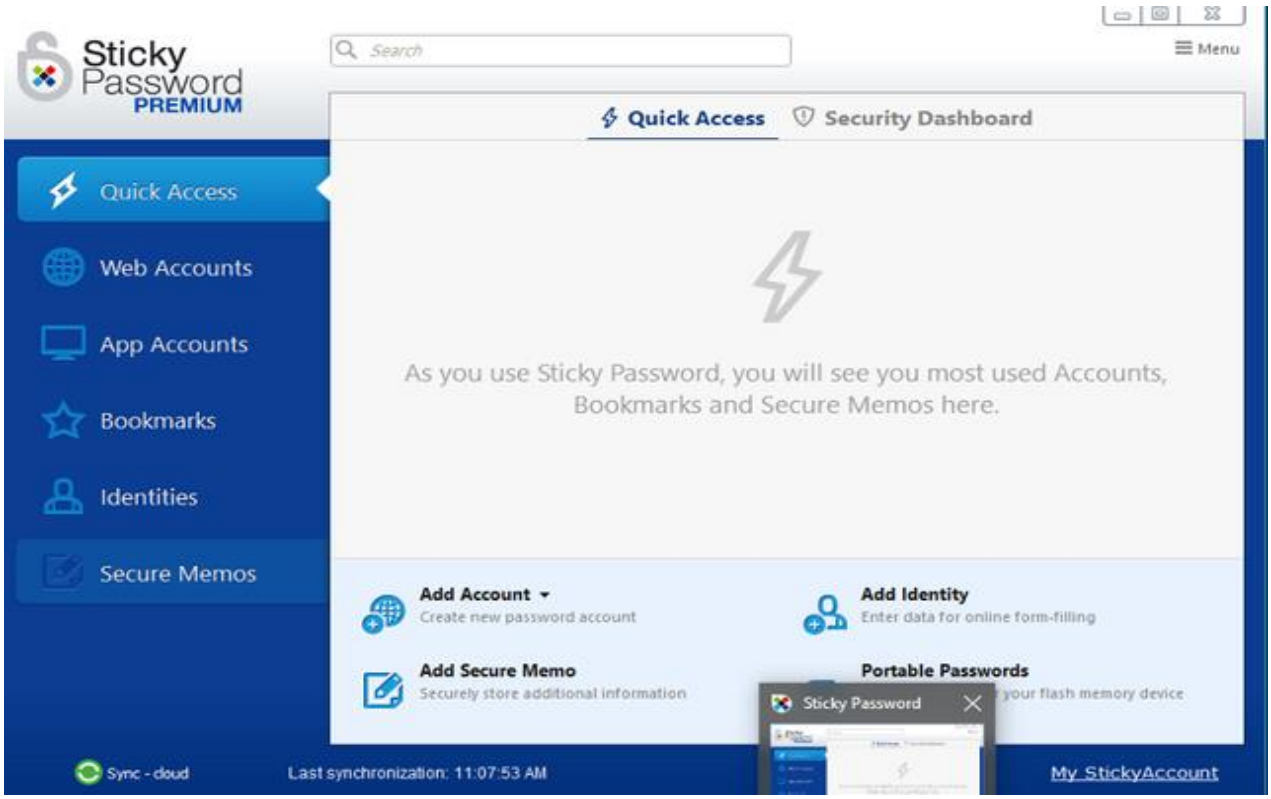
- AES-256 encryption ensures security.
- Fingerprint authentication enhances access control.
- Two-factor authentication adds protection.

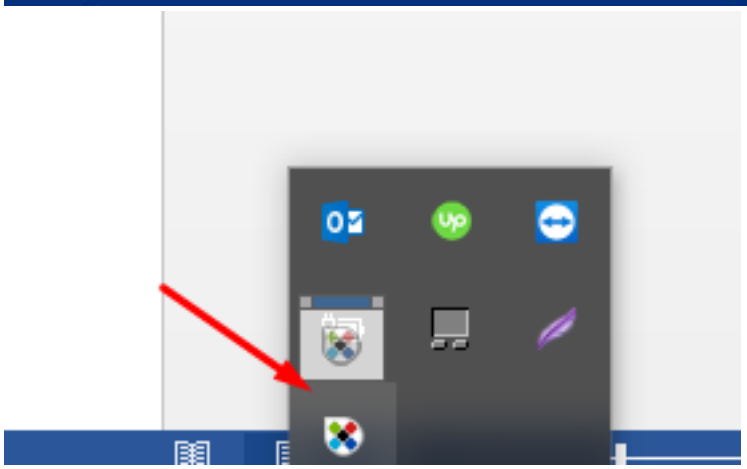
- Cloud synchronization is available with the paid package for device connectivity.
- The lifetime access fee for the paid version is $150.
- Device whitelisting enhances security.
- Form filling streamlines data entry.

11.2 StickyPassword-Cons:

- Standalone solution: locally installed on devices.
- Offline data synchronization may expose it to data theft.
- No password sharing.
- No access or activity tracking.
- Vulnerable to access from hacked emails.
- No recovery if the main password is lost.
- The application doesn't request a master password when closed and opened.

11.3 StickyPassword-Screenshots:





SuperGenPass (12/13)

SuperGenPass is a unique password solution. Instead of storing passwords locally or online, vulnerable to theft and data loss, it employs a hash algorithm. This algorithm transforms a master password into unique, complex passwords for the websites you visit.

12.1 SuperGenPass-Pros:

- It's free.
- Passwords are not stored online or offline.

12.2 SuperGenPass-Cons:

- No password sharing.
- No access or activity tracking.

- No reporting.
- No IP address restricting/whitelisting.
- Very basic console feature.
- For personal use only.

12.3 SuperGenPass-Screenshots:

ZOHO (13/13)

ZOHO provides diverse online services for businesses. Although we haven't tested all their offerings, we selected their password manager, and ultimately the one we choose. A key factor is that ZOHO Vault avoids local storage of passwords on devices or browsers. This feature ensures the invulnerability of passwords stored on ZOHO's password manager against theft and brute force attacks.

13.1 Zoho-Pros:

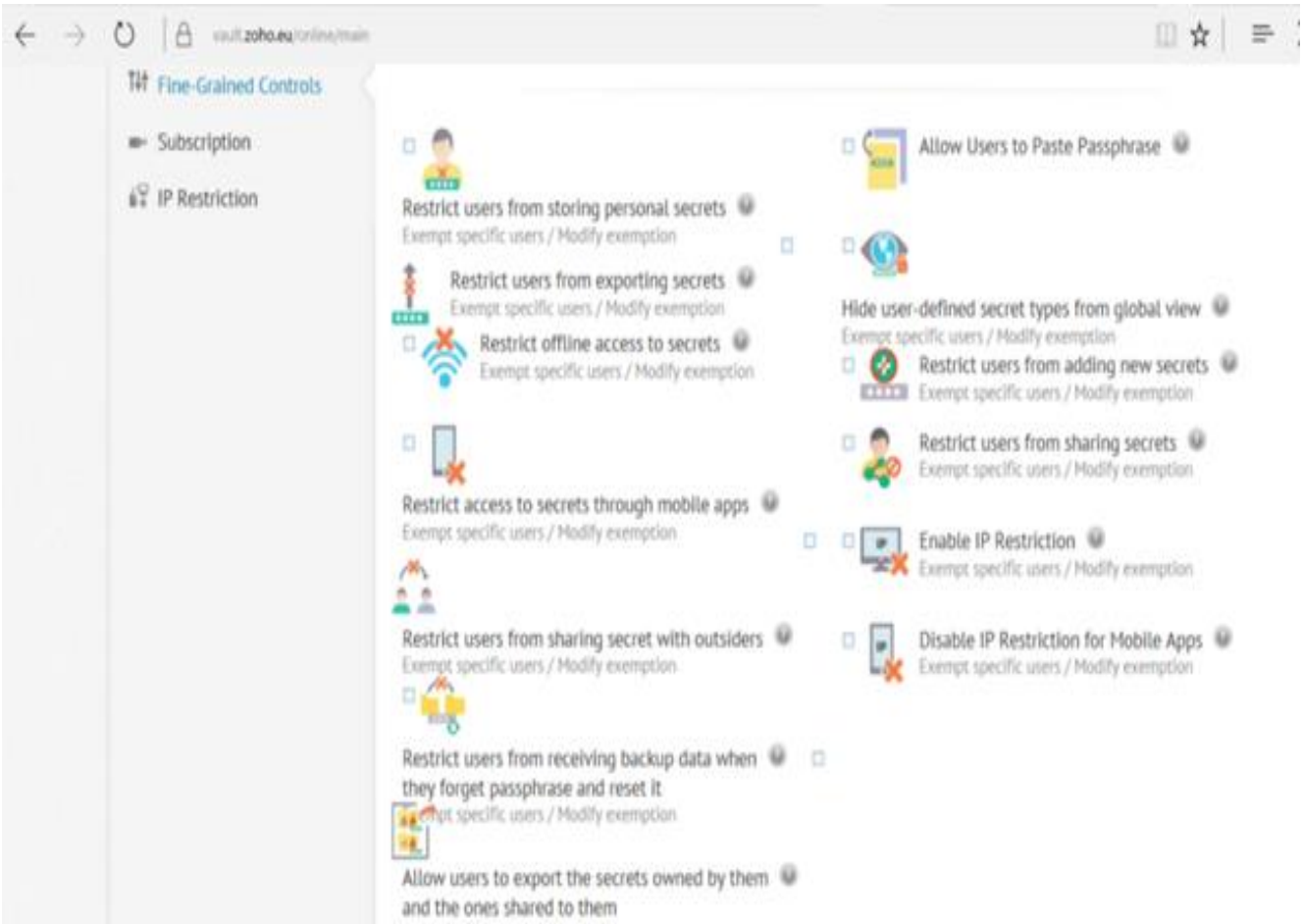
- Web encrypted access.
- Tracks password access and activities.
- Secure password sharing.
- Passwords are not stored locally on devices (note 6).
- Access can be restricted to specific IP addresses.
- Strong users access restriction policies.
- Detailed reporting on every user activity, including password sharing.

- Break glass account for emergency access.
- Also, a free option is available, but without certain features.
- Transfer/acquire ownership of passwords.
- One-click auto logon.
- Two-factor authentication.

13.2 Zoho-Cons:

- Price of the professional package: €4/user/month.

13.3 Zoho-Screenshots:



14. Notes

(1Certain software, such as Elcomsoft, is designed to crack password managers. According to their testing, only Bitwarden, Keeper, PassworkMe, Supergenpass, and Zoho demonstrated robust security. You can read more about their findings here: [Elcomsoft Blog](https://blog.elcomsoft.com/2017/08/one-password-to-rule-them-all-breaking-into-1password-keepass-lastpass-and-dashlane/).

(2) Police, prosecutors, and other officials who engage in "legal" crimes through corrupted state institutions pose a significant threat to individuals and countries. If involved in illegal activities, they can manipulate the system to cover it up, often seizing devices under false charges and gaining access to SMS and emails. To protect against these threats, it is essential to use encryption software, secure your devices, and purchase hardware from outside your operating country.

(3)Open source doesn't ensure thorough code audits for backdoors or weaknesses, yet it signals a commitment to transparency.

(4) Access passwords across devices and share specific passwords with agents globally. The solution must support iOS, Android, Windows, Linux, and Mac desktops. Windows phones and BlackBerry are excluded due to their limitations, which make finding a suitable solution nearly impossible.

(5) Zero-knowledge encryption requires storing the key on the user's device to protect against state-sponsored criminals. While this doesn't stop the provider from handing over plaintext messages to the government, it does mean that an attacker would need to actively target the user to steal their password.

(6)Upon logging into the Zoho Vault extension, all secrets are temporarily encrypted within the browser extension. When accessing secret details, editing secrets, or revealing passwords by clicking the "Show" button, the details are decrypted using the extension's passphrase and displayed in plain text.

Encrypted secret data in the extension is cleared upon logging out from Zoho Vault or when the passphrase is cleared after timeout. The browser extension supports offline access, requiring the passphrase for decryption.

The Zoho Vault browser extension incorporates an offline access feature, requiring the passphrase for decryption. In offline mode, data persists even if the passphrase is cleared because there is no two-way connection with Zoho Vault servers to fetch secrets.

Administrators can manage offline mode settings through fine-grained control. It's worth noting that these products underwent testing and review by Florjan Llapi, a Certified Ethical Hacker and System Administrator.