

RESOURCE CENTER

Bitwarden Reviewer's Guide

Get the full interactive view at
<https://bitwarden.com/ja-jp/resources/bitwarden-reviewers-guide/>



Introducing Bitwarden

This guide is intended for consumer tech journalists and reviewers evaluating Bitwarden for product reviews, comparison pieces, or broader stories around credential management and security. It outlines key user workflows and differentiators to support quick impressions and in-depth evaluations.

Estimated time to review Bitwarden Password Manager:

- Quick walkthrough (15 - 30 minutes):
 - A hands-on introduction to the core Bitwarden experience: [account creation](#), [importing credentials](#), [autofill testing](#), and [syncing across mobile and desktop](#).
 - Ideal for usability and feature-overview coverage.
- In-depth evaluation (45 - 90 minutes):
 - A more comprehensive look at key value adds for individuals, teams, families: testing secure sharing with [Bitwarden Send](#), [creating and storing passkeys](#), exploring the [password generator](#), and reviewing mobile/desktop parity.
 - Suitable for reviewers looking to highlight everyday security features or compare top password managers.

Table of Contents

[Product strengths and trust differentiators](#)

[Your passwords, anywhere you need them](#)

[More than passwords](#)

[What sets Bitwarden apart](#)

[User profiles: Who is Bitwarden for?](#)

[How to get started](#)

[Community-driven innovation](#)

Product strengths and trust differentiators

Bitwarden empowers individuals, teams, and businesses to manage credentials and sensitive information across devices with simplicity and security. Trusted by over 10 million users worldwide, Bitwarden combines strong encryption, seamless UX, and trusted open-source transparency.

Check out the [Bitwarden Security Whitepaper](#).

Built on trust and transparency

- Bitwarden is the only widely adopted password manager that is fully open source across its core platform, mobile and desktop apps, browser extensions, and command-line interface (CLI) — allowing anyone to inspect the code and contribute.

End-to-end encryption

- All data is encrypted locally before it leaves the device. Bitwarden uses **256-bit AES** with zero-knowledge encryption. Bitwarden cannot see your data, and neither can anyone else.
- The master key to access encrypted data is in the hands of the user. Master passwords are protected using **PBKDF2** or **Argon2** to resist brute-force attacks.

Third-party audits

- Multiple **annual security audits** by independent firms, such as Cure53, ensure that Bitwarden is secure at every layer.

Public security documentation

- Bitwarden shares detailed [security whitepapers](#), [public roadmaps](#), and documentation about how the products work.
- The code is available publicly on [GitHub](#) for anyone to inspect.

Security architecture at a glance

- Encryption: Zero-knowledge, end-to-end encryption with AES-256, Argon2 or PBKDF2 protection
- [Compliance](#): SOC 2 Type II, ISO/IEC 27001 certified, and aligned with GDPR, HIPAA, and CCPA
- Hosting flexibility: Bitwarden supports both cloud-hosted and [self-hosted deployment](#)

Your passwords, anywhere you need them

Bitwarden is available on every major platform:

- **Desktop:** Windows, macOS, Linux
- **Mobile:** iOS, Android
- **Browser Extensions:** Chrome, Firefox, Safari, Edge, Brave, Vivaldi, and more
- **CLI:** Secure access for DevOps, IT admins, and power users
- **Self-host:** The Bitwarden server can be self-hosted on your own architecture on a variety of platforms, accessible by the other Bitwarden clients.

Autofill everywhere

- Log into websites with [one tap](#) or a quick [keyboard shortcut](#). Bitwarden autofills credentials while protecting them with end-to-end encryption.

Sync across devices

- Your vault syncs automatically across all logged-in devices so users always have access when needed.

Biometric login

- Supports Face ID, Touch ID, Windows Hello, and Android biometric authentication.

More than passwords

Bitwarden securely stores a wide range of sensitive information:

- Logins
- Credit cards
- Secure notes
- Identities

Password generator

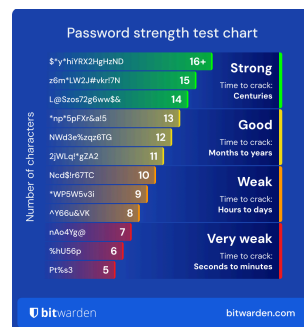
Create secure passwords, passphrases, and usernames using customizable criteria.

Secure sharing with Bitwarden Send

[Send encrypted text or files](#) with anyone using expiring links with access controls.



Bitwarden password security: At work, at home, and on the go!



What sets Bitwarden apart

Feature	Bitwarden
Trusted open source	☑ Yes
End-to-end, zero-knowledge encryption	☑ Yes
Unlimited items synced across unlimited devices	☑ Yes
Transparent security audits	☑ Yes
Secrets management	☑ Bitwarden Secrets Manager
Passkey developer SDK	☑ Passwordless.dev

Explore [Bitwarden Secrets Manager](#) for securing developer and DevOps teams.

User profiles: Who is Bitwarden for?

Bitwarden is built for anyone looking to secure and streamline their digital life, from individuals to enterprises. Example use cases include:

- **Security-conscious users** seeking trusted, open source alternative to built-in tools
- **Families** managing shared logins for school, streaming, etc.
- **Travelers** needing secure access across multiple locations and devices
- **Freelancers** managing multiple client credentials
- **IT teams** enforcing policy-driven credential management

How to get started

1. Sign up:

- Create a free individual account at bitwarden.com. Bitwarden offers Free, Premium (for individuals), Family, Teams, and Enterprise plans. [Compare plans here](#) for the right fit.
- The solution guides new users through a simple, intuitive onboarding process, highlighting key steps like vault creation and fundamental security practices.

Explore the Bitwarden
[password generator](#).

2. Download the apps:

- Mobile: iOS / Android
- Desktop: macOS / Windows / Linux
- Browser extensions: Chrome, Safari, Firefox, Edge, and more
- [Command Line Interface](#) (CLI): For advanced users and developers
 1. **What to note:** Bitwarden apps work seamlessly across platforms. Unlike Apple Keychain or Google Password Manager, Bitwarden is platform-agnostic, fully open source, and built for portability and trusted transparency.

3. Explore your vault:

- Import credentials from browsers or other password managers (e.g., Chrome, LastPass, Dashlane, or 1Password) or generate new ones using the Bitwarden [password generator](#).
- The web vault and desktop app include robust import tools with field mapping support.

4. Testing the browser extension:

- Most users interact with Bitwarden through the [browser extension](#), which combines convenience with strong security, enabling users to manage credentials within the browser workflow.
- Reviewers should test the following features:
 1. Autofill accuracy and form recognition
 2. Quick search and vault access
 3. Editing entries, TOTP, folders, and custom fields
 4. Security controls: vault timeout, app lock, biometric unlock

5. Try advanced features:

- Enable [two-factor authentication](#) (2FA) (TOTP or hardware keys)
- Test [biometric unlock](#) or [PIN unlock](#) on supported devices
- Save and sync a passkey to experience cross-device synchronization

6. Sync and export options:

- Bitwarden supports [encrypted vault exports](#) for users who want an extra layer of control over their data
- The vault can be accessed offline through locally cached data, ensuring availability without an internet connection

- Cross-platform syncing ensures credentials are always available across mobile, desktop, browser environments

7. **Test sharing use cases:**

- For Teams or Family plan reviewers, explore shared collections to simulate access control and permission management in a shared vault environment.
- Use [Bitwarden Send](#) to share a note or password securely.

Community-driven innovation

The Bitwarden mission is rooted in trust, inclusion, and responsible community-driven innovation. It empowers users while prioritizing security and privacy.

- 10M+ users in 180+ countries
- 50,000+ business customers
- Leader in G2 [Enterprise Grid Report](#)
- Leader in [Software Reviews](#) Data Quadrant and Emotional Footprint reports

About Bitwarden

Bitwarden equips enterprises and individuals with the power to securely manage and share information online with trusted open source security solutions. With a password manager for everyone, users can easily manage their entire online identity anywhere. Bitwarden Secrets Manager and Passwordless.dev enhance developer secrets security and streamline passkey development for end users and workforce authentication. Founded in 2016, Bitwarden serves over 50,000 businesses and more than 10 million users worldwide across 180 countries in 50+ languages. The company is headquartered in Santa Barbara, California. Learn more at bitwarden.com.

Press resources

[Video Overview](#)

[Product Page](#)

[Media Kit](#)

[Brand Guidelines](#)

Questions:

press@bitwarden.com