

SECURITY

Compliance, Audits, and Certifications

A decorative graphic consisting of numerous thin, light blue wavy lines that create a sense of motion and depth, filling the lower half of the page.

View in the help center:

<https://bitwarden.com/help/is-bitwarden-audited/>

Compliance, Audits, and Certifications

Bitwarden is a global company with customers located all over the world. Our business is to help customers protect, store, and share their sensitive data. We prioritize protecting the personal data of our customers and their end-users as paramount to our company mission. Bitwarden complies with industry standards, and conducts comprehensive annual audits that are shared transparently with our customers and users. Our open source approach puts us in a unique position, where our software is viewed and scrutinized by a globally engaged community.

Privacy

For our privacy policy, visit bitwarden.com/privacy.

GDPR

Bitwarden is GDPR compliant. We use applicable, approved information transfer mechanisms where required, such as EU Standard Contractual Clauses (SCCs), or the EU - U.S. Data Privacy Framework.

Bitwarden uses Standard Contractual Clauses pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

CCPA

Bitwarden is compliant with the California Consumer Privacy Act (CCPA).

Data Privacy Framework (DPF)

Bitwarden complies with the Data Privacy Framework (DPF), previously called Privacy Shield, which defines the safe transfer of personal data

HIPAA

Bitwarden is HIPAA compliant and annually undergoes a third-party audit for HIPAA Security Rule compliance.

ISO 27001

Bitwarden is ISO 27001 certified and in compliance with ISO 27001 control sets surrounding data security.

Third party security audits

Bitwarden regularly conducts comprehensive third-party security audits with notable security firms. These annual audits include source code assessments and penetration testing across Bitwarden IPs, servers, and web applications.

2024 Web App and Network Security Assessment

Bitwarden completed a dedicated source code audit and penetration test of the web app and related network components by security firm Fracture Labs.

[Read the report.](#)

2024 Mobile Apps and SDK Security Assessment

Bitwarden completed a dedicated source code audit and penetration test of the mobile apps and SDK by security firm Cure53.

[Read the report.](#)

2023 Bitwarden Web App Security Assessment Report

Bitwarden completed a dedicated source code audit and penetration test of the web app by security firm Cure53.

[Read the report.](#)

2023 Bitwarden Desktop App Security Assessment Report

Bitwarden completed a dedicated source code audit and penetration test of the desktop app by security firm Cure53.

[Read the report.](#)

2023 Bitwarden Core App & Library Security Assessment Report

Bitwarden completed a dedicated source code audit and penetration test of the core application and library by security firm Cure53.

[Read the report.](#)

2023 Bitwarden Browser Extension Security Assessment Report

Bitwarden completed a dedicated source code audit and penetration test of the browser extension by security firm Cure53.

[Read the report.](#)

2023 Network Security Assessment

Bitwarden completed a network security assessment and penetration test by security firm Cure53.

[Read the report.](#)

2022 Security Assessment

Bitwarden completed a dedicated source code audit and penetration test by security firm Cure53.

[Read the report.](#)

SOC 2 Type 2 and SOC 3

Bitwarden has completed [SOC Type 2 and SOC 3 compliance](#). For more information, see the blog post [Bitwarden achieves SOC 2 certification](#).

2022 Network Security Assessment

Bitwarden completed a network security assessment and penetration test by security firm Cure53.

[Read the report.](#)

2021 Network Security Assessment

Bitwarden completed a thorough network security assessment and penetration test by auditing firm [Insight Risk Consulting](#).

[Read the report.](#)

2021 Security Assessment

Bitwarden completed a dedicated source code audit and penetration test by the security firm Cure53.

[Read the report.](#)

2020 Network Security Assessment

Bitwarden completed a thorough security assessment and penetration test by auditing firm [Insight Risk Consulting](#). For more information, please see the blog post [Bitwarden 2020 Security Audit is Complete](#).

[Read the report.](#)

2018 Security Assessment

Bitwarden completed a thorough security audit and cryptographic analysis by security firm [Cure53](#). For more information, please see the blog post [Bitwarden Completes Third-party Security Audit](#).

[Read the report.](#)

Open source codebase

Codebase on GitHub

Bitwarden is focused on open source software with the entirety of the codebase available on [github.com](#). See our codebase at [github.com/bitwarden](#), or learn more on [our open source page](#).

Licensing

Source code in Bitwarden repositories are covered by one of two licenses, the [GNU Affero General Public License \(AGPL\) v3.0](#) and the [Bitwarden License v1.0](#). Refer to these links to learn more about what is included in and permitted by each license.

Cloud hosting

The Bitwarden cloud service is hosted on Microsoft Azure. Please visit [Microsoft Azure Compliance Offerings](#) for more detail.

Security information

Zero knowledge encryption

Bitwarden takes a zero knowledge encryption approach to password management, meaning every piece of information in your vault is encrypted. For more information on this approach, please see the blog post [How End-to-End Encryption Paves the Way for Zero Knowledge](#).

Vault security in Bitwarden

For more information on how Bitwarden vaults are protected, including options for Bitwarden client applications, please see the blog post [Vault Security in the Bitwarden Password Manager](#).

Bug bounty program

Bitwarden also interacts with independent security researchers through our public bug bounty program on [HackerOne](#).