Bitwarden Security and Compliance

Bitwarden envisions a world where no one gets hacked. This is reflected in a steadfast Bitwarden commitment to security, privacy, and compliance with international standards.

Get the full interactive view at
https://bitwarden.com/compliance/

bitwarden

Bitwarden privacy and product security

Third-party audited

External experts regularly review Bitwarden products, ensuring strong and trusted security.

Zero-knowledge, end-to-end encryption

Secured with strong encryption, no one has access to your vault information, not even Bitwarden!

Compliant with privacy and security standards

Get Bitwarden products quickly approved by your internal IT and security teams with industry compliance.

Trust and transparency powered by open source

An open source codebase enables the security of Bitwarden products to be easily audited by independent security researchers, notable security firms, and the Bitwarden community.

Trusted open source architecture

The Bitwarden codebase on GitHub is regularly reviewed and audited by millions of security enthusiasts and active Bitwarden community members.

Source code assessment

Bitwarden completes annual source code audits and penetration tests for each client including web, browser extension, and desktop — in addition to the core application and library.

Network security assessment

Bitwarden completes annual network security assessments and penetration tests by reputable security firms.

HackerOne bug bounty

Independent security researchers are rewarded for submitting potential security issues.

Keeping your data secure

As your password manager and credential security provider, Bitwarden utilizes trusted security measures and encryption methods to protect user data.

Zero-knowledge, end-to-end encryption

Bitwarden uses end-to-end encryption for all vault data, which only your master password can decrypt. With a zero-knowledge architecture, Bitwarden does not have the ability to read any encrypted data in your vault.

Multifactor encryption

Multifactor encryption is an additional layer of encryption that protects your stored information. This makes it practically impossible for a bad actor to break into your vault, even if they were able to gain access to your encrypted vault data.

Self-hosting options

Choose to deploy and manage Bitwarden on-premises in your private network or infrastructure with self-hosting options. Self-hosting allows customers to have more detailed control over their stored information.

Security compliance

Bitwarden adheres to industry security standards with an ISO 27001 certification, SOC2 and SOC3 certifications, and HIPAA compliance.

SOC2 and SOC3

System and Organization Controls (SOC) comprise a set of control frameworks that are used to validate an organization's security systems and policies. Bitwarden is SOC2 Type II and SOC3 certified.

HIPAA

Bitwarden is HIPAA compliant and undergoes annual third-party audits for HIPAA Security Rule compliance.

ISO 27001

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

SOC2 Reports available upon request.

Privacy compliance

Bitwarden prioritizes protecting the personal data of users and ensuring compliance with key privacy standards across the globe.

CCPA & CPRA

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

GDPR

Bitwarden complies with GDPR, current EU data protection rules, and EU Standard Contractual Clauses (SCCs).

Data Privacy Framework

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

Meet your security compliance standards with Bitwarden

Bitwarden is more than a password manager; it's a foundational tool for achieving and maintaining industry compliance with key security standards. Through secure sharing, monitoring capabilities, centralized management, and robust data protection, Bitwarden strengthens your organization's cybersecurity posture to meet compliance needs.

ISO 27001

ISO 27001, an international standard, sets the foundation for creating, maintaining, and developing information security management systems (ISMS), including data management.

SOC 2

Service Organization Control 2 (SOC 2) reports are often requested by customers and business partners of outsourced solution providers. Companies seeking SOC 2 compliance can leverage a SOC 2-compliant password manager to help meet requirements.

NERC

The North American Electric Reliability Corporation (NERC) is a non-profit international regulatory body dedicated to setting compliance standards that help reduce risks to the electricity grid and power systems serving hundreds of millions of people in the United States, Canada, and part of Mexico.

NIS2

NIS2 is a set of requirements for securing network and information systems across the EU. The directive mandates businesses identified as operators of essential services to implement appropriate measures to enhance cybersecurity and comply with legal obligations.

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) provides guidance and best practices for organizations to follow, in order to help businesses, non-profits, and other private-sector institutions to improve cybersecurity risk management.

SOX

Sarbanes-Oxley Act (SOX) compliance involves adhering to a set of security requirements designed to ensure the integrity of financial reporting.

Password Management Maturity Model

This framework helps organizations understand their password manager maturity level — based on their current operations — and identify what steps are necessary to strengthen their security and improve their existing classification.

FAQs

- **Can the Bitwarden team see my passwords?**

  No.

  Your data is fully encrypted and/or hashed before ever leaving **your** local device, so no one from the Bitwarden team can ever see, read, or reverse engineer to get to your real data. Bitwarden servers only store encrypted and hashed data. For more information about how your data is encrypted, see Encryption.

  Learn more >

- **How do you keep the cloud servers secure?**

  Bitwarden takes extreme measures to ensure that its websites, applications, and cloud servers are secure. Bitwarden uses Microsoft Azure managed services to manage server infrastructure and security, rather than doing so directly.

  Learn more >

- **Is Bitwarden audited?**

  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.

  Learn more >

- **What happens if Bitwarden gets hacked?**

  If for some reason Bitwarden were to get hacked and your data was exposed, your information is still protected due to strong encryption and one-way salted hashing measures taken on your vault data and master password.

  Learn more >

- **Where is my data stored in the cloud?**

  Bitwarden processes and stores all vault data securely in the Microsoft Azure Cloud in the US or EU using services that are managed by the team at Microsoft. Since Bitwarden only uses service offerings provided by Azure, there is no server infrastructure to manage and maintain. All uptime, scalability, security updates, and guarantees are backed by Microsoft and their cloud infrastructure. Review the Microsoft Azure Compliance Offerings documentation for more detail.

  Learn more >

- Why should I trust Bitwarden with my passwords?

  You can trust us for a few reasons:

  1. Bitwarden is **open source** software. All of our source code is hosted on GitHub and is free for anyone to review. Thousands of software developers follow Bitwarden's source code projects (and you should too!).
  2. Bitwarden is **audited by reputable third-party security firms** as well as independent security researchers.
  3. Bitwarden **does not store your passwords**. Bitwarden stores encrypted versions of your passwords that only you can unlock. Your sensitive information is encrypted locally on your personal device before ever being sent to our cloud servers.
  4. **Bitwarden has a reputation.** Bitwarden is used by millions of individuals and businesses. If we did anything questionable or risky, we would be out of business!

  Still don't trust us? You don't have to. Open source is beautiful. You can easily host the entire Bitwarden stack yourself. You control your data.

  Learn more >

- Does Bitwarden use a salted hash for my password?

  PBKDF2 SHA-256 is used to derive the encryption key from your master password, however you may choose Argon2 as an alternative. Bitwarden salts and hashes your master password with your email address **locally**, before transmission to our servers. Once a Bitwarden server receives the hashed password, it is salted again with a cryptographically secure random value, hashed again, and stored in our database.

  Learn more >

- How is my data securely transmitted and stored on Bitwarden servers?

  Bitwarden **always** encrypts and/or hashes your data on your local device before anything is sent to cloud servers for storage. **Bitwarden servers are only used for storing encrypted data.** For more information, see Storage.

  Learn more >

- What encryption is being used?

  Bitwarden uses AES-CBC 256-bit encryption for your vault data, and PBKDF2 SHA-256 or Argon2 to derive your encryption key.

  Learn more >

- What information is encrypted?

  All vault data is encrypted by Bitwarden before being stored anywhere. To learn how, see Encryption.

  Learn more >

- Where is my data stored on my computer/device?

  Data that is stored on your computer/device is encrypted and only decrypted when you unlock your vault. Decrypted data is stored **in memory** only and is **never written to persistent storage**.

  Learn more >