bitwarden | SECURITY PAPER

Overview of Bitwarden Security and Compliance Program

With remote work on the rise and internet usage higher than ever before, the demand to create and maintain dozens (if not hundreds) of online accounts with logins and passwords is staggering.

Security experts recommend that you use a different, randomly generated password for every account that you create. But how do you manage all those passwords? And how does one maintain good password hygiene across an organization?

Effective password management is a heavily underutilized resource in the enterprise. In the 2020 Under the Hoodie Report by Rapid7, they note that password management and secondary controls such as two-factor authentication are “severely lacking, leading to ‘easy’ compromises.” Reusing or sharing passwords in an insecure manner leaves the enterprise vulnerable.

To bring change at an organization, security and IT teams must educate employees about best practices. In regards to password management, one of the easiest ways to encourage and support good password hygiene is to deploy a password management solution across your workplace.

Bitwarden is the easiest and safest way to store all of your logins, passwords, and other sensitive information while conveniently keeping them synced between all of your devices.

Bitwarden gives the tools to create, store, and share your passwords while maintaining the highest level of security.

Bitwarden’s solution, software, infrastructure, and security processes have been designed from the ground up with a multi-layered, defense-in-depth approach. The Bitwarden Security and Compliance Program is based on the ISO27001 Information Security Management System (ISMS). We defined policies that govern our security policies and processes and continually update our security program to be consistent with applicable legal, industry, and regulatory requirements for services that we provide to you under our Terms of Service Agreement.

Bitwarden complies with industry-standard application security guidelines that include a dedicated security engineering team and include regular reviews of application source code and IT infrastructure to detect, validate, and remediate any security vulnerabilities.

This white paper provides an overview of Bitwarden security principles as well as links to additional documents that provide more detail in specific areas.

Bitwarden Security Principles

User Data Protection

Bitwarden utilizes the following key security measures to protect user data.

End-to-end encryption: Lock your passwords and private information with end-to-end AES-CBC 256 bit encryption, salted hashing, and PBKDF2 SHA-256. All cryptographic keys are generated and managed by the client on your devices, and all encryption is done locally. See more details in the Password Hashing Derivation section.

Zero knowledge encryption: Bitwarden team members can not see your passwords. Your data remains encrypted end-to-end with your individual email and Master Password. We never store and cannot access your Master Password or your cryptographic keys.

Secure password sharing: Bitwarden enables secure sharing and management of sensitive data with users across an entire organization. A combination of Asymmetric and Symmetric encryption protects sensitive information as it is shared.

Open source and source available code: The source code for all Bitwarden software products is hosted on GitHub and we welcome everyone to review, audit, and contribute to the Bitwarden codebase. Bitwarden source code is audited by reputable third-party security auditing firms as well as independent security researchers. In addition, The Bitwarden Vulnerability Disclosure Program enlists the help of the hacker community at HackerOne to make Bitwarden more secure.

Privacy by design: Bitwarden stores all of your logins in an encrypted vault that syncs across all of your devices. Since it's fully encrypted before it ever leaves your device, only you have access to your data. Not even the team at Bitwarden can read your data (even if we wanted to). Your data is sealed with AES-CBC 256 bit encryption, salted hashing, and PBKDF2 SHA-256.

Security Audit & Compliance: Open source and third-party audited, Bitwarden complies with AICPA SOC2 Type 2 / Privacy Shield, GDPR, and CCPA regulations.

Master Password

User data protection in Bitwarden begins at the moment a user creates an account and a Master Password. We highly recommend using a strong Master Password during the onboarding process. Bitwarden includes a Password Strength Meter as a guide that will assess and display the overall strength of the Master Password being entered to encourage a strong Master Password.

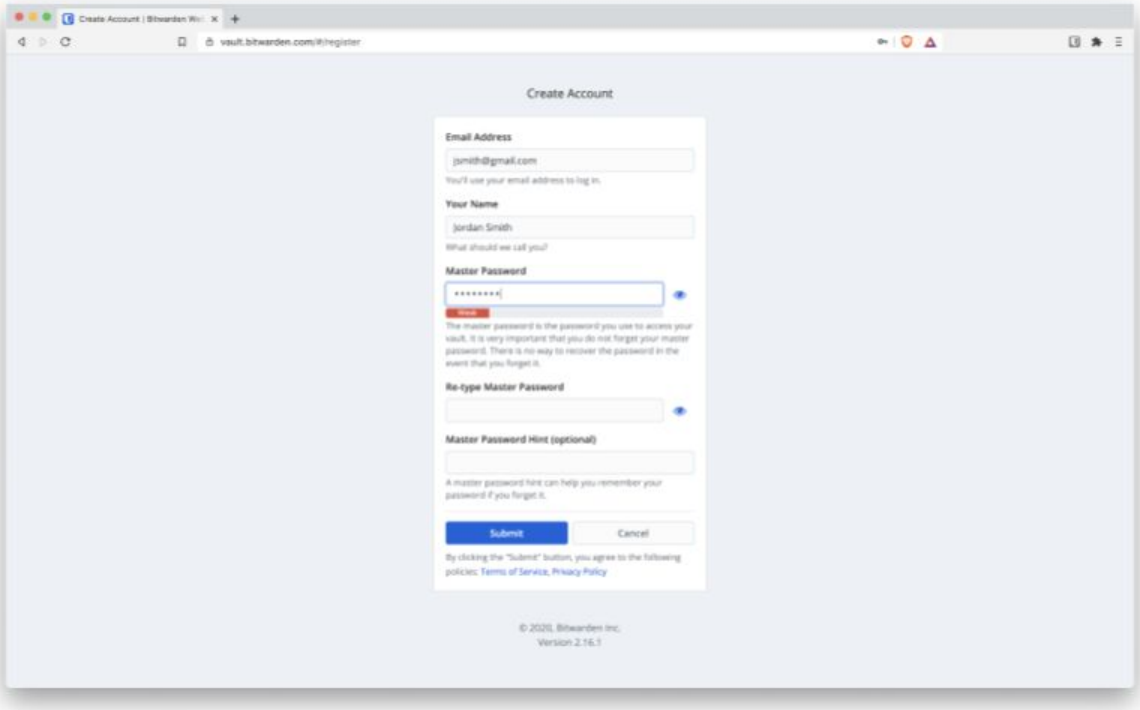

Figure: Create a Bitwarden Account

If you attempt to sign up with a weak password, Bitwarden will notify you that the Master Password chosen is weak.

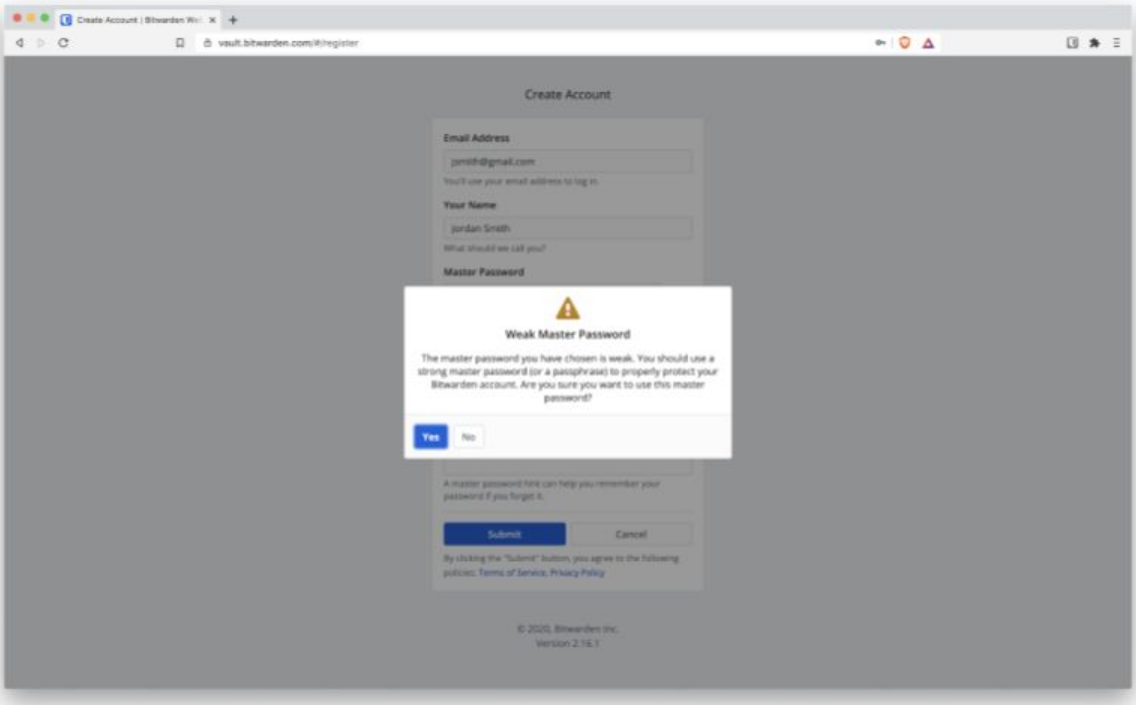

Figure: Weak Master Password Warning

Using a strong Master Password is for your own security benefit because it is the token you use to access your secure Vault, where your sensitive items are stored. You are responsible for keeping your account secure while you use the Bitwarden service. We offer additional measures, such as two-step login, to help you maintain your account's security, but the content of your account and its security are up to you.

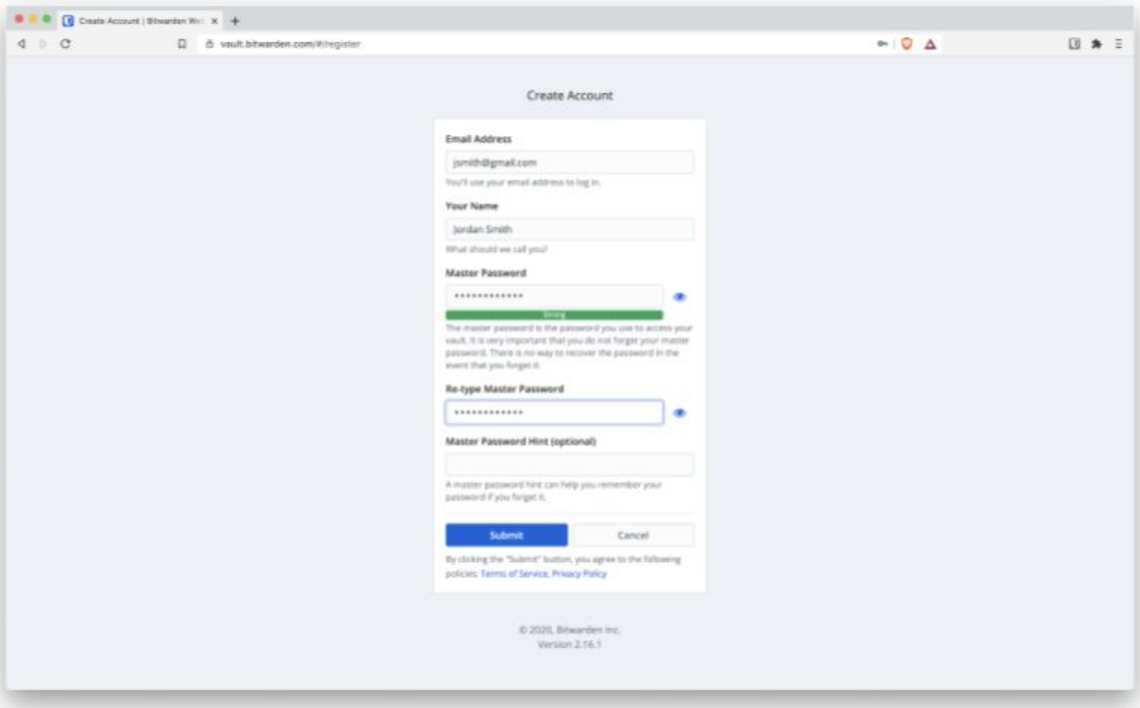

Figure: Choose a Strong Master Password

Read More: Five Best Practices for Password Management and 3 tips from NIST to keep your passwords secure

Helpful Tools: Bitwarden Password Strength Testing Tool and Bitwarden Password Generator

It is very important that you never forget your Master Password. The Master Password is cleared from memory after usage and never transmitted over the Internet to Bitwarden servers, therefore there is no way to recover the password in the event that you forget it.

This also means no one from the Bitwarden team can ever see, read, or reverse engineer to get to your real data. Your data is fully encrypted and/or hashed before ever leaving your local device. This is a critical step that Bitwarden takes to protect you and your data.

After creating your account and specifying your Master Password , Bitwarden next generates several keys that are used in protecting your account's data.

Overview of the Master Password Hashing, Key Derivation, and Encryption Process

User Account Creation

When the Create Account form is submitted, Bitwarden uses Password-Based Key Derivation Function 2 (PBKDF2) with 100,000 iteration rounds to stretch the user's Master Password with a salt of the user's email address. The resulting salted value is the 256 bit Master Key. The Master Key is additionally stretched to 512 bits in length using HMAC-based Extract-and-Expand Key Derivation Function (HKDF). The Master Key and Stretched Master Key are never stored on or transmitted to Bitwarden servers.

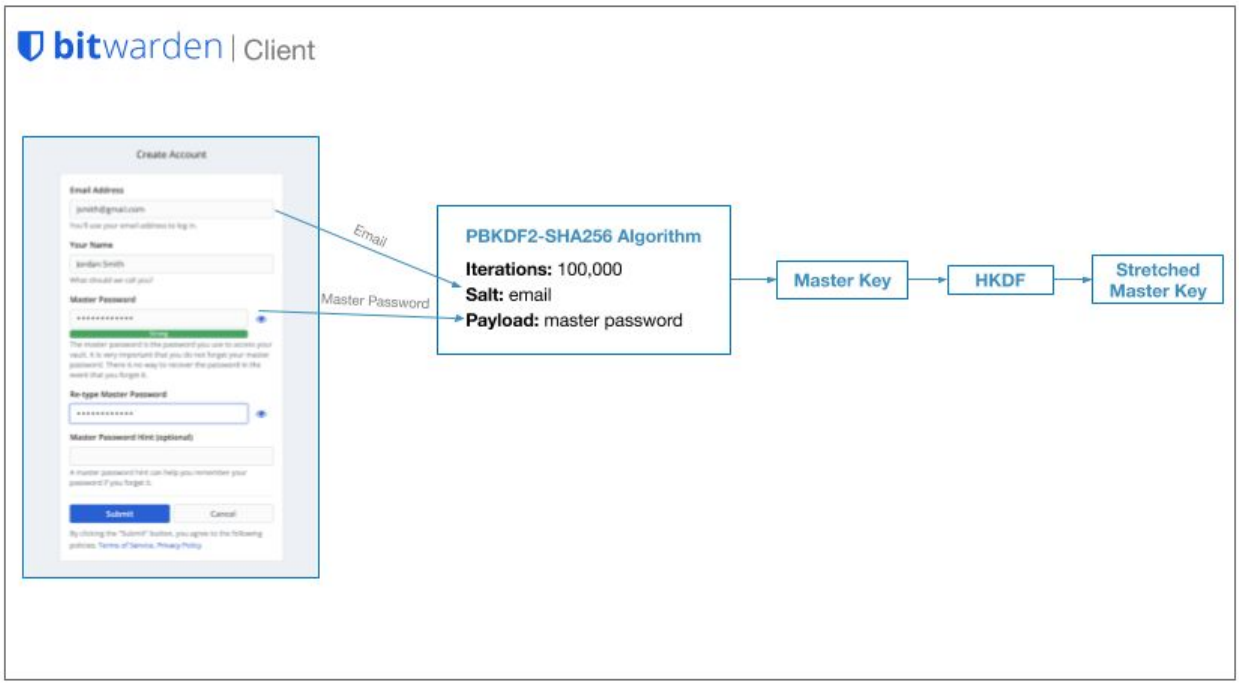

Figure: Password-based key derivation

In addition, a 512-bit Symmetric Key and an Initialization Vector is generated using a Cryptographically Secure Pseudorandom Number Generator (CSPRNG). The Symmetric key is encrypted with AES-256 bit encryption using the Stretched Master Key and the Initialization Vector. The resulting key is called the Protected Symmetric Key. The Protected Symmetric Key is the main key associated with the user and sent to the server upon account creation, and sent back to the Bitwarden Client apps upon syncing.

An asymmetric key is also generated (RSA key pair) when the user registers their account. The Generated RSA Key Pair is used if and when the user creates an Organization. Organizations can be created and used to share data between users. When you create an organization, an Organization Symmetric key is generated using a Cryptographically Secure Pseudorandom Number Generator (CSPRNG). The Organization Symmetric Key is encrypted using the public key from your Generated RSA Key Pair. The private key from your Generated RSA Key Pair is encrypted with your Generated Symmetric Key using AES-256.

Please refer to Sharing Data Between Users for additional details. Below is a diagram showing the various keys that are generated when creating a Bitwarden user account.

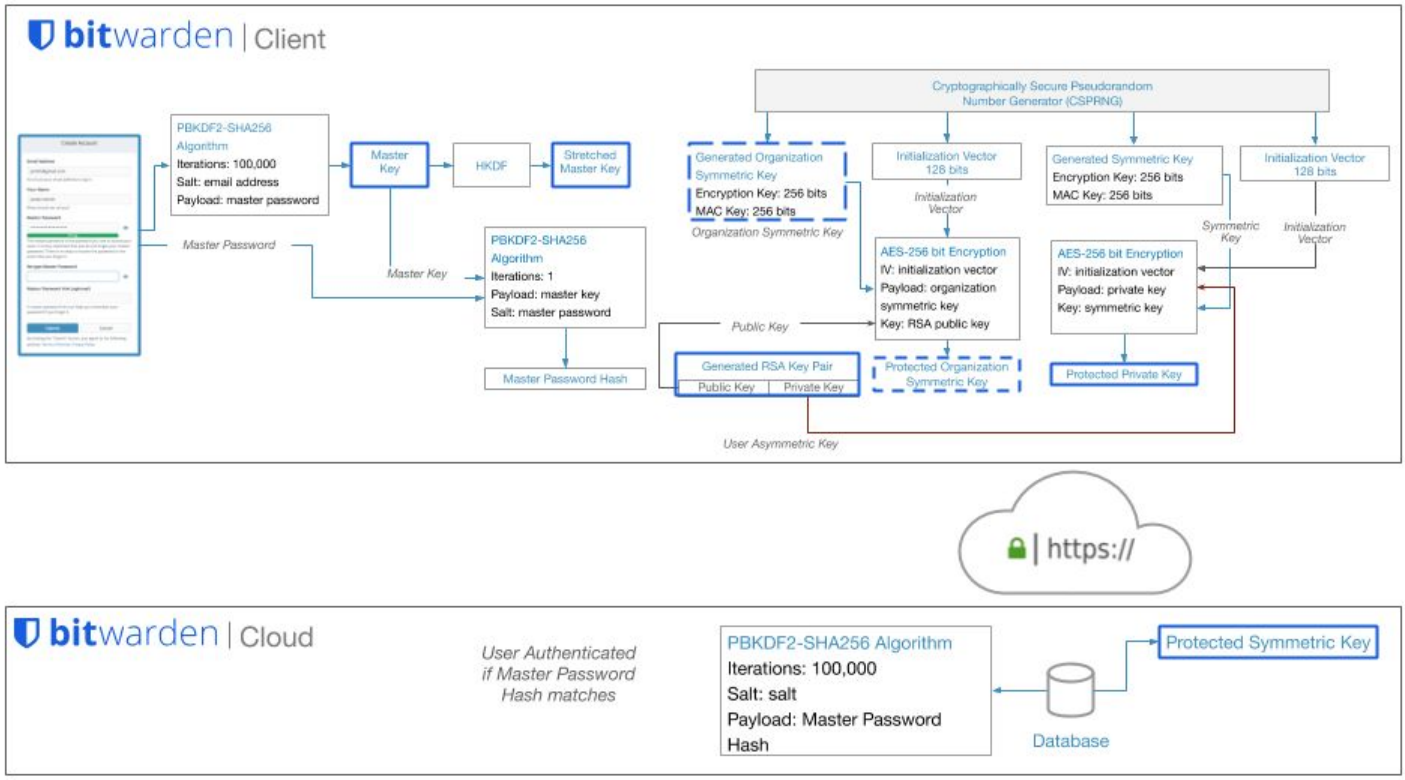

Figure: Overview of the various keys created when registering a new Bitwarden account

A Master Password hash is also generated using PBKDF-SHA256 with a payload of Master Key and with a salt of the Master Password. The Master Password hash is sent to the server upon account creation and login, and used to authenticate the user account. Once reaching the server, the Mater Password hash is hashed again using PBKDF2-SHA256 with a random salt and 100,000 iterations. An overview of the password hashing, key derivation, and encryption process is shown below.

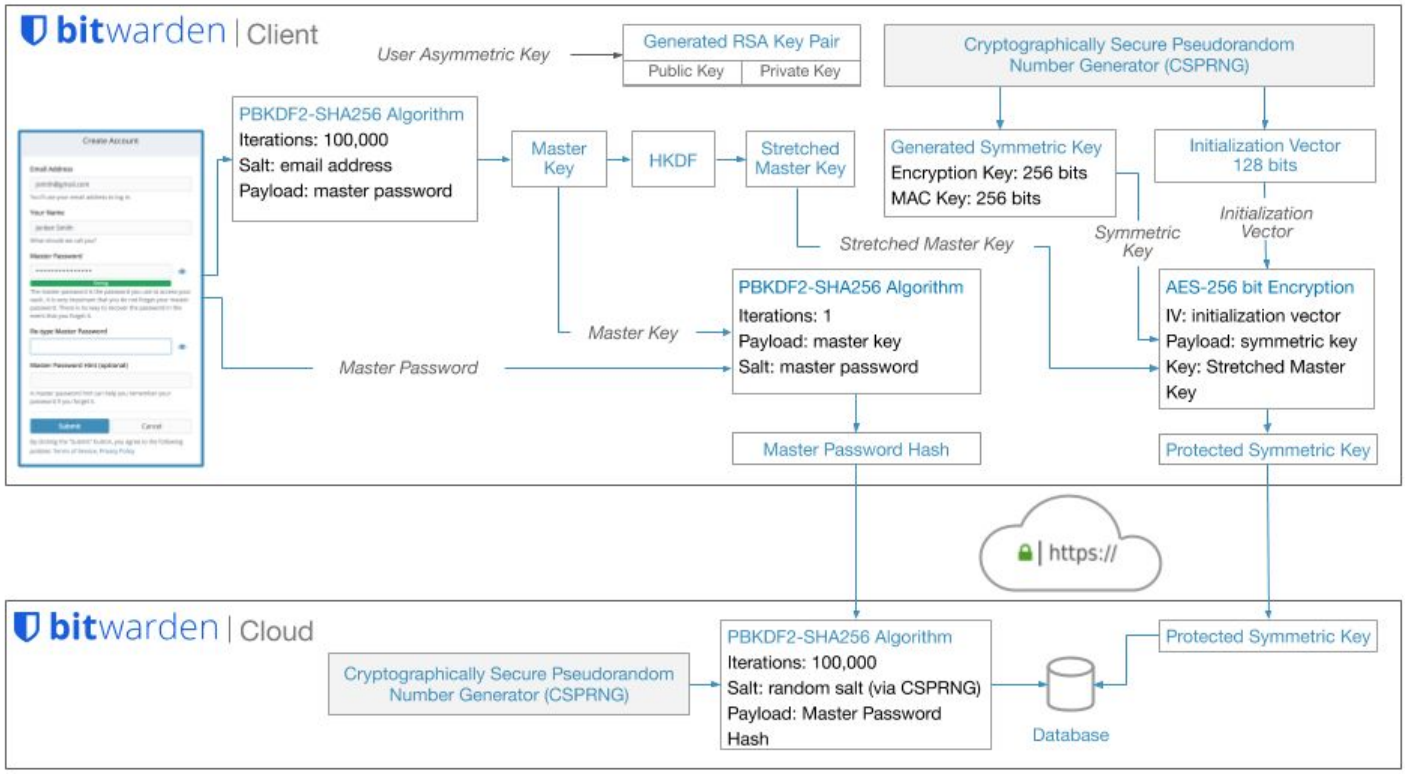

Figure: Bitwarden password hashing, key derivation, and encryption

User Login | User Authentication | Access to User Vault Data

You are required to first enter your Email Address and Master Password in order to log in to your Bitwarden account.

Next, Bitwarden uses Password-Based Key Derivation Function 2 (PBKDF2) with a default of 100,000 iteration rounds to stretch your Master Password with a salt of your Email Address. The resulting salted value is the 256 bit Master Key. A hash of the master key is sent to the server upon account creation and login, and used to authenticate the user account.

The Master Key is additionally stretched to 512 bits in length using HMAC-based Extract-and-Expand Key Derivation Function (HKDF). The Protected Symmetric Key is decrypted using the Stretched Master Key. The Symmetric Key is used to decrypt Vault Items. The decryption is done entirely on the Bitwarden Client because your Master Password or Stretched Master Key is never stored on or transmitted to Bitwarden servers.

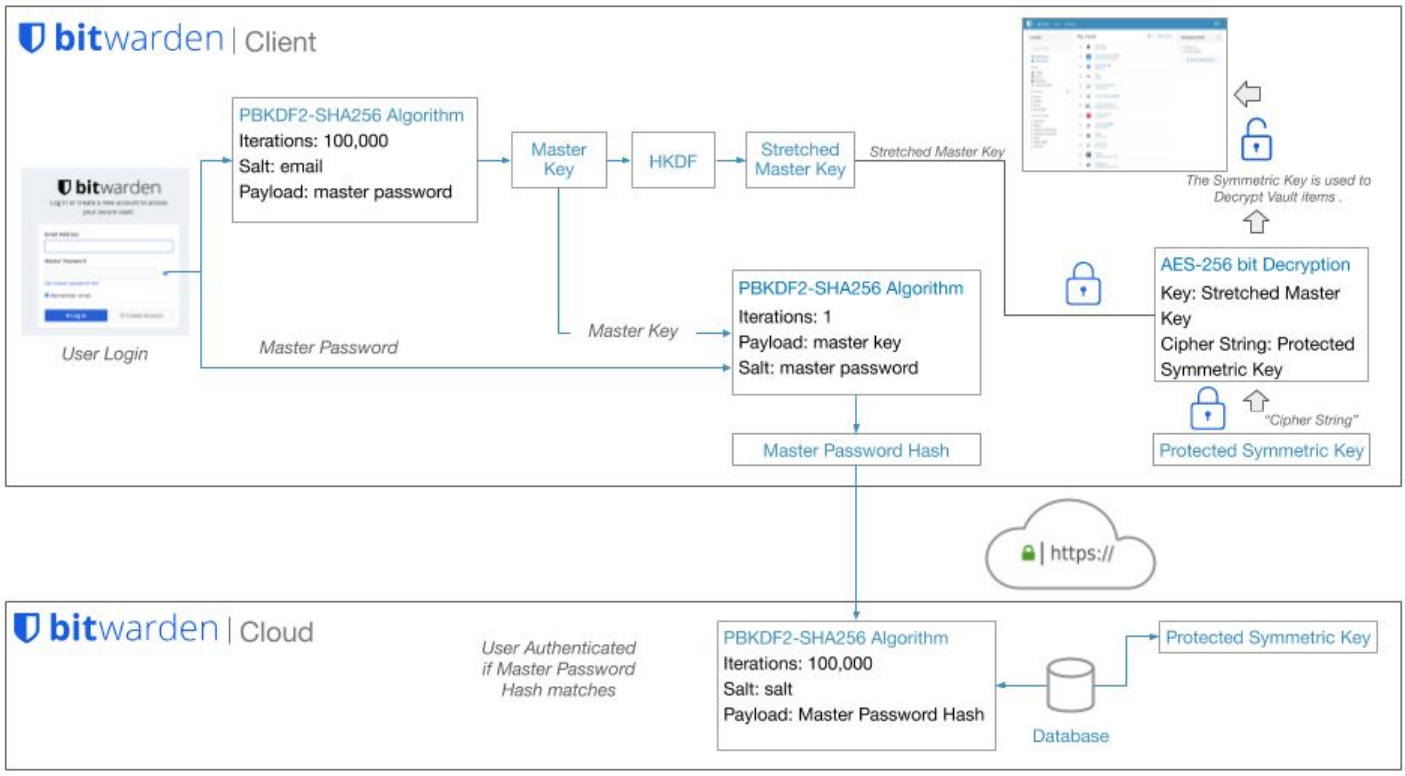

Figure: An overview of user login

We do not keep the Master Password stored locally or in memory on the Bitwarden Client. Your encryption key (Symmetric Key) is kept in memory while the app is unlocked. This is needed to decrypt data in your vault. When the vault is locked, this data is purged from memory. After a certain time frame of inactivity on lock screen, we reload the application processes to make sure that any leftover managed memory addresses are also purged. We do our best to ensure that any data that may be in memory for the application to function is only held in memory for as long as you need it and that memory is cleaned up whenever the application is locked. We consider the application to be completely safe while in a locked state.

Additional User Data Protection when enabling Two-step login

Two-step login (also called two-factor authentication or 2FA) is an extra layer of security for your account, designed to ensure that you're the **only** person who can access your account, even if someone were to discover your Master Password.

As a best practice, we recommend all users activate and use two-step login within their Bitwarden account. When two-step login is activated, you are required to complete a secondary step while logging into Bitwarden (in addition to your Master Password). By default,

you will be prompted to complete this secondary step every time, however there is a “Remember Me,” prompt which will save your 2FA status, so you can log in without 2FA the next time on that particular device for up to 30 days.

Note: Changing your Master Password or deauthorizing sessions will require you to re-authenticate 2FA, no matter if you selected "Remember Me" on it previously or not.

Bitwarden supports two-step login using the following methods:

Free Plans
- Using an Authenticator app such as Authy or Google Authenticator
- Email

Premium Features
- Duo Security with Duo Push, SMs, phone call, and U2F security keys
- YubiKey (any 4/5 series device or YubiKey NEO/NFC)
- FIDO U2F (any FIDO U2F certified key)

You can enable multiple two-step login methods. If you have multiple two-step login methods enabled, the order of preference for the default method that is displayed while logging in is as follows: FIDO U2F > YubiKey > Duo > Authenticator app > Email. You can manually switch to and use any method during login, however.

It is very important that you never lose your two-step login recovery codes. Bitwarden offers an account protection security model that does not support users losing their Master Password or two-step login recovery codes. If you have two-step login enabled on your account and lose access to your two-step login recovery codes you will not be able login to your Bitwarden account.

Changing User Password

Your Master Password can only be changed from the Web Vault. For specific steps on how to change your user password, see this Bitwarden Help article.

Rotating Your Accounts Encryption Key

During a password change operation you also have the option to rotate (change) your account’s encryption key. Rotating the encryption key is a good idea if you believe that your previous Master Password was compromised or that your Bitwarden vault’s data was stolen from one of your devices.

Warning

Rotating your account's encryption key is a sensitive operation, which is why it is not a default option. A key rotation involves generating a new, random encryption key for your account and **re-encrypting all vault data** using this new key. See additional details in this Bitwarden Help article.

Data Protection in Transit

Bitwarden takes security very seriously when it comes to handling your sensitive data. Your data is never sent to the Bitwarden Cloud without first being encrypted on your local device.

In addition, Bitwarden uses TLS/SSL to secure communications between Bitwarden clients and user devices to the Bitwarden Cloud. Bitwarden's TLS implementation uses 2048-bit X.509 certificates for server authentication and key exchange and a strong cipher suite for bulk encryption. Our servers are configured to reject weak ciphers and protocols.

Bitwarden also implements HTTP Security headers such as HTTP Strict Transport Security (HSTS), which will force all connections to use TLS. This additional layer of protection with HSTS mitigates the risks of downgrade attacks and misconfiguration.

Data Protection at Rest

Bitwarden always encrypts and/or hashes your data on your local device before it is sent to the cloud servers for syncing. The Bitwarden servers are only used for storing and synchronizing encrypted vault data. It is not possible to get your unencrypted data from the Bitwarden cloud servers. Specifically, Bitwarden uses AES 256-bit encryption as well as PBKDF-SHA256 to secure your data.

AES is a standard in cryptography and used by the U.S. government and other government agencies around the world for protecting top-secret data. With proper implementation and a strong encryption key (your Master Password), AES is considered unbreakable.

PBKDF-SHA256 is used to derive the encryption key from your Master Password. Then this key is salted and hashed for authenticating with the Bitwarden servers. The default iteration count used with PBKDF2 is 100,001 iterations on the client (this client-side iteration count is configurable from your account settings), and then an additional 100,000 iterations when stored on our servers (for a total of 200,001 iterations by default).

Learn more: How end-to-end encryption paves the way for zero knowledge and What encryption is being used

How Vault Items Are Secured

All information (Logins, Cards, Identities, Notes) associated with your stored vault data is protected with end-to-end encryption. Items that you choose to store in your Bitwarden vault are first stored with an item called a Cipher object. Cipher objects are encrypted with your Generated Symmetric Key, which can only be known by decrypting your protected Symmetric Key using your Stretched Master Key. This encryption and decryption are done entirely on the Bitwarden Client because your Master Password or Stretched Master Key is never stored on or transmitted to Bitwarden servers.

Vault Health Reports

All Bitwarden paid plans come with Vault Health reports for both individuals and organizations.

For personal Vaults, individuals have access to the following:

- Exposed Passwords Report
- Reused Passwords Report
- Weak Passwords Report
- Unsecured Websites Report
- Inactive 2FA Report
- Data Breach Report

For business users, a similar set of reports exists for Organization Vault items.

Read more: Vault Health reports

For more information on Bitwarden Event Logs and external reporting, see Event Logs

Importing Passwords and Other Secrets into Bitwarden

You can easily import your data from over 40 different services, including all the popular password manager applications, to Bitwarden. The full list of supported applications and some additional information, including troubleshooting steps for importing your data into Bitwarden, are documented in Bitwarden Help Center.

If you are exporting your sites from the LastPass.com Web Vault, please refer to the specific information on this Help note Import your data from LastPass.

Sharing Data between Users

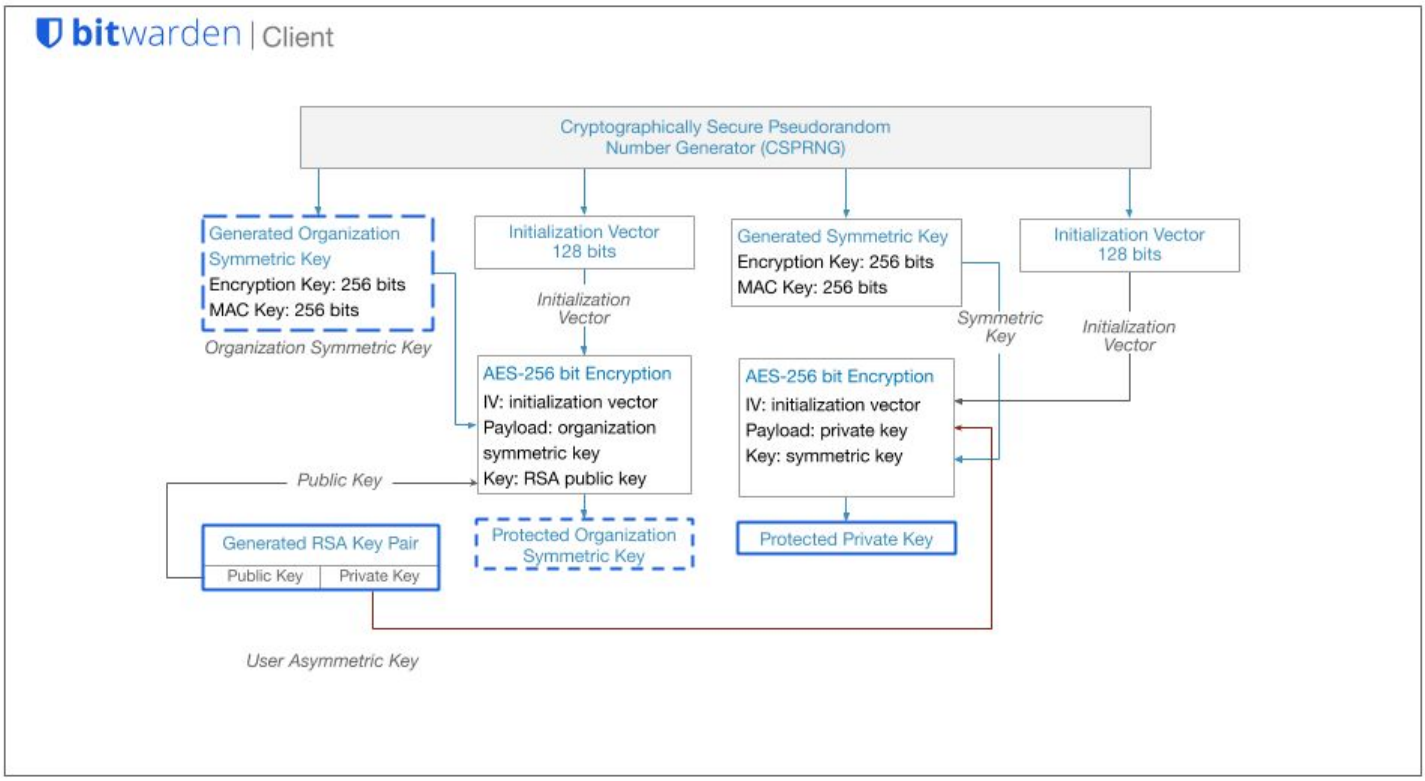

Figure: Organization Symmetric Key and User Asymmetric key, which is the RSA Key Pair

Collaboration is one of the leading benefits of using a password manager. In order to enable sharing, you need to first create an Organization. A Bitwarden Organization is an entity that relates users together that want to share items. An Organization could be a family, team, company, or any other type of group that desires to share data.

An individual user account can create and/or belong to many different Organizations, allowing you to manage your items from a single account.

You can create a new Bitwarden Organization from the Web Vault or request that an Administrator of an existing Organization send you an invite.

When you create an Organization, an Organization Symmetric key is generated using a Cryptographically Secure Pseudorandom Number Generator (CSPRNG). The Organization Symmetric Key is encrypted using the public key from your Generated RSA Key Pair. The private key from your Generated RSA Key Pair is encrypted with your Generated Symmetric

Key using AES-256. The Generated RSA Key Pair and Generated Symmetric Key were created when you first signed up and registered your account.

Read More: What are Organizations?

Access Controls and Managing Bitwarden Collections

As your Organization's use of Bitwarden grows, it helps to have users who can manage Collections independently, without requiring access to everything within the Organizational Vault.

Managing Collections and Groups is a simple way to separate, grant, or limit access to Vault items in Bitwarden, thereby controlling user visibility of resources.

A complete list of roles and access control is documented in the User Types and Access Control section of Bitwarden Help Center.

Read more: How to manage Collections

Event Logs

Event logs contain time-stamped, detailed information about what actions or changes have occurred within an Organization. These logs are helpful with researching changes in credentials or configuration and very useful for audit trail investigation and troubleshooting purposes.

Additional information on Event Logs is documented in Bitwarden Help Center. Event logs are available for Teams and Business plans only.

To gather more data, plans with API access can use the Bitwarden API. API responses will contain the type of event and relevant data.

SIEM Integration and External Systems

For Security Information and Event Management (SIEM) systems like Splunk, when exporting data from Bitwarden, a combination of data from the API and CLI may be used to gather data.

This process is outlined in the help center note on **Organization event logs** under SIEM and External Systems Integrations.

Account Protection and Avoiding Lockout

Today, Bitwarden offers account protection with a security model that does not support users losing their passwords or two-step login recovery codes.

Bitwarden cannot reset user passwords nor can Bitwarden disable two-step login if it has been enabled on your account.

Warning
Users who lose their Master Password, or who lose their two-step login recovery code, will need to delete their account and start over.

To mitigate these potential issues, Bitwarden recommends the following for account protection and lockout avoidance.

Master Password
Identify a way for you to retain and be able to recover your Master Password should you forget it. This may include writing it down and placing it in a safe, or safe place.

Use a Master Password hint
If helpful, use the Master Password hint provided by Bitwarden at sign up. Or set up a hint at any time via the Settings in the Web Vault.

Organization management
For Organizations, have multiple Administrators who can access and manage the Organization.

Two-step login recovery code
If you choose or are required by your Organization to set up two-step login, be sure to access and retain your recovery code and store that in an equally safe place as your Master Password.

Bitwarden Cloud Platform and Web Application Security

Bitwarden Architecture Overview

Bitwarden processes and stores all data securely in the Microsoft Azure cloud 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, and security updates, patching, and guarantees are backed by Microsoft and their cloud infrastructure.

Security Updates and Patching

The team at Microsoft manages OS patching on two levels, the physical servers and the guest virtual machines (VMs) that run the Azure App Service resources. Both are updated monthly, which aligns to the monthly Microsoft's Patch Tuesday schedule. These updates are applied automatically, in a way that guarantees the high-availability SLA of Azure services.

Read More: Patching in Azure App Service or SLA for App Service

For detailed information on how updates are applied, read here

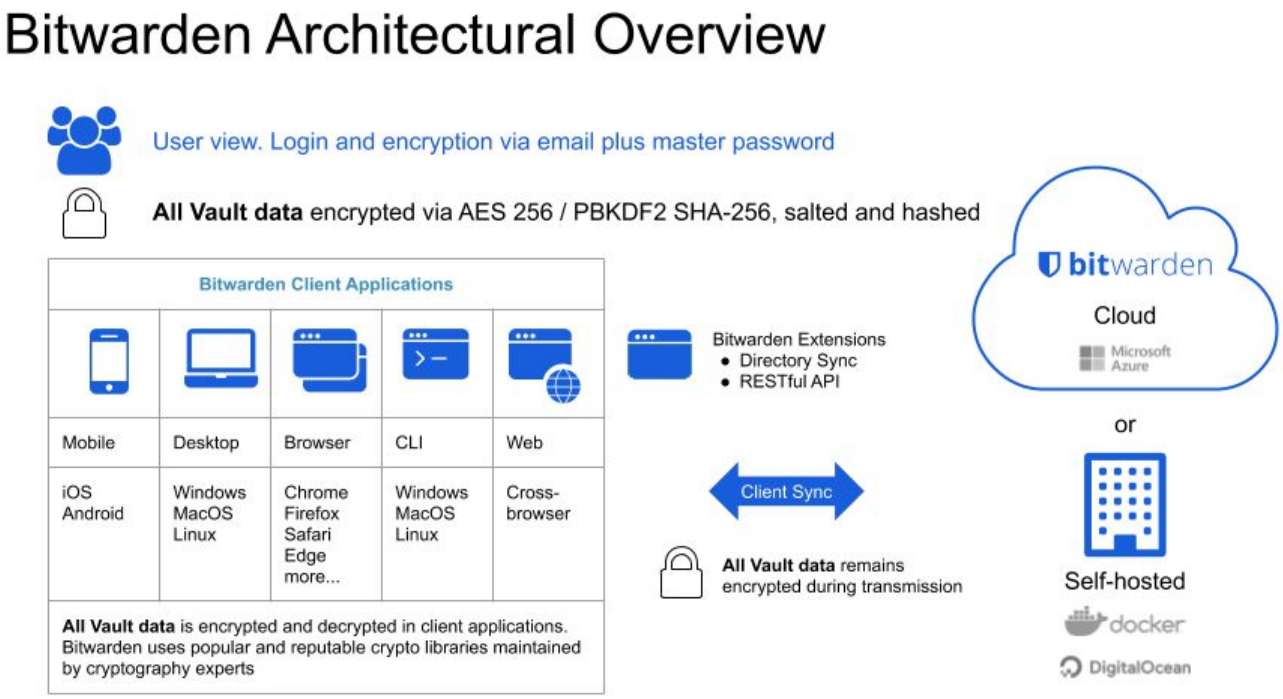

Figure: An overview of the Bitwarden architecture

Bitwarden Access Controls

Bitwarden employees have significant training and expertise for the type of data, systems, and information assets that they design, architect, implement, manage, support, and interact with.

Bitwarden follows an established on-boarding process to ensure that the appropriate level of access is assigned and maintained. Bitwarden has established levels of access that are appropriate for each role. All requests including any access change requests need to be

reviewed and approved by the manager. Bitwarden follows a least-privilege policy that grants employees the minimum level of access required to complete their duties. Bitwarden follows an established off-boarding process through Bitwarden Human Resources that revokes all access rights upon termination.

Software Lifecycle and Change Management

Bitwarden evaluates changes to platform, applications, and production infrastructure to minimize risk and such changes are implemented following the standard operating procedures at Bitwarden.

Change Request items are planned based on roadmap and submitted to engineering at this point. Engineering will review and evaluate their capacity and assess the level of effort for each change request item. After review and evaluation, they will formulate what they are going to work on for a specific release. CTO provides details of the release through communication channels and management meetings and the development life cycle begins for that release.

High-level development, release, testing, and approval process:

- Developing, building and iterating using pull requests in GitHub
- Get features to a point where they are testable
- Engineering performs functional testing of the feature and/ or product as they are developing and building
- Unit testing build is automated as part of Bitwarden Continuous Integration (CI) pipelines
- Some testing also performed by Customer Success team
- Director of Engineering assists with review and helps to formalize the process including documentation updates
- CTO Provides Final Go / No-Go Approval

Meeting Attendance: To ensure successful review, approval implementation and closure of change requests, each core Operation and IT service staff should be represented during the meeting to review and discuss the change request.

Emergency Deployment / hotfixes get escalated priority, and review and approval of the change is received from a manager or director prior to the change being made and is subsequently reviewed, communicated and closed during the next scheduled change meeting. This is normally in a service outage, system down or in an urgent outage prevention situation.

Control of Production Systems

Bitwarden maintains documented runbooks for all production systems, that cover deployment, update, and troubleshooting processes. Extensive alerts are set up to notify and escalate in the case of issues.

Baseline Configurations

Bitwarden processes and stores all data securely in the Microsoft Azure cloud 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, and security updates and guarantees are backed by Microsoft and their cloud infrastructure.

Azure Service Configurations are leveraged by Bitwarden to ensure applications are configured and deployed in a repeatable and consistent manner.

Bitwarden Platform Key Management Procedures

Keys and other secrets utilized by the Bitwarden platform itself, include credentials for the Bitwarden cloud provider accounts. All such keys are generated, securely stored, and rotated as needed, in accordance with industry-standard practices. Bitwarden uses an internal Bitwarden vault for secure storage and backup of sensitive keys or other secrets utilized by the Bitwarden platform. Access control to the Bitwarden vault leverages User Types and Access Control.

Data Types and Data Retention

Bitwarden processes two kinds of user data to deliver the Bitwarden Service: (i) Vault Data and (ii) Administrative Data.

(i) Vault Data

Vault Data includes all information stored within accounts to the Bitwarden Service and may include Personal Information. If we host the Bitwarden Service for you, we will host Vault Data. Vault Data is encrypted using secure cryptographic keys under your control. Bitwarden cannot access Vault Data.

Data Retention of Vault Data: You may add, modify, and delete Vault Data at any time.

(ii) Administrative Data

Bitwarden obtains Personal Information in connection with your account creation, usage of the Bitwarden Service and support, and payments for the Bitwarden Service such as names, emails address, phone and other contact information for users of the Bitwarden Service and the number of items in your Bitwarden Service account ("Administrative Data"). Bitwarden uses Administrative Data to provide the Bitwarden Service to you. We retain Administrative Data for as long as you are a customer of Bitwarden and as required by law. If you terminate your relationship with Bitwarden, we will delete your Personal Information in accordance with our data retention policies.

When you use the Site or communicate with us (e.g., via email) you will provide, and Bitwarden will collect certain Personal Information such as:
- Name
- Business name and address
- Business telephone number
- Email address
- IP-address and other online identifiers
- Any customer testimonial you have given us consent to share.
- Information you provide to the Site's Interactive Areas, such as fillable forms or text boxes, training, webinars or event registration.
- Information about the device you are using, comprising the hardware model, operating system and version, unique device identifiers, network information, IP address, and/or Bitwarden Service information when interacting with the Site.
- If you interact with the Bitwarden Community or training, or registered for an exam or event, we may collect biographical information and the content that you share.
- Information gathered via cookies, pixel tags, logs, or other similar technologies.

Please refer to the Bitwarden Privacy Policy for additional information.

Logging, Monitoring, and Alert Notification

Bitwarden maintains documented runbooks for all production systems, that cover deployment, update, and troubleshooting processes. Extensive alerts are set up to notify and escalate in the case of issues. A combination of manual and automated monitoring of the Bitwarden Cloud infrastructure provides a comprehensive and detailed view of system health as well as proactive alerts on areas of concern. Issues are surfaced quickly so that our infrastructure team can effectively respond and mitigate problems with minimal disruption.

Business Continuity / Disaster Recovery

Bitwarden employs a full range of disaster recovery and business continuity practices from Microsoft Azure that are built into the Bitwarden Cloud. This includes high availability and backup services for our application and database tiers.

Threat Prevention and Response

Bitwarden performs vulnerability assessments on a regular basis. We leverage third-party tools and external services, including: OWASP ZAP, Mozilla Observatory, OpenVAS, and others are used to do internal assessments.

Bitwarden uses Cloudflare in order to provide a WAF at the edge, better DDoS protection, distributed

availability and caching. Bitwarden also uses proxies within Cloudflare for better network security and
performance of its services and sites.

Bitwarden is open source software. All of our source code is hosted on GitHub and is free for anyone to review. Bitwarden source code is audited by reputable third-party security auditing firms as well as independent security researchers. In addition, The Bitwarden Vulnerability Disclosure Program enlists the help of the hacker community at HackerOne to make Bitwarden more secure.

Auditability and Compliance

The Bitwarden Security and Compliance Program is based on the ISO27001 Information Security Management System (ISMS). We have defined policies that govern our security policies and processes and continually update our security program to be consistent with applicable legal, industry, and regulatory requirements for services that we provide to you under our Terms of Service Agreement.

Bitwarden complies with industry-standard application security guidelines that include a dedicated security engineering team and include regular reviews of application source code and IT infrastructure to detect, validate, and remediate any security vulnerabilities.

External Security Reviews
Third-party security reviews and assessments of applications and/or the platform are performed at a minimum of once per year.

Certifications
Bitwarden certifications include:
- SOC2 Type II (renewed annually)
- SOC3 (renewed annually)

According to the AICPA, the use of the SOC 2 Type II report is restricted. For SOC 2 report inquiries, please contact us.

Read More: Bitwarden achieves SOC2 certification

The SOC 3 report provides a summary of the SOC 2 report that can be distributed publicly. According to the AICPA, SOC 3 is the SOC for service organizations report on trust services criteria for general use.
Bitwarden makes a copy of our SOC 3 report available here.

These SOC certifications represent one facet of our commitment to safeguarding the security and privacy of customers, and compliance with rigorous standards. Bitwarden also performs a regular cadence of audits on our network security and code integrity.

Read more: Bitwarden 2020 security audit is complete and Bitwarden completes third-party security audit

HTTP Security Headers

Bitwarden leverages HTTP Security headers as an additional level of protection for the Bitwarden web application and communications. For example, HTTP Strict Transport Security (HSTS) will force all connections to use TLS, which mitigates the risks of downgrade attacks and misconfiguration. Content Security Policy headers provide further protection from injection attacks, such as cross-site scripting (XSS). In addition, Bitwarden implements X-Frame-Options: SAMEORIGIN to defend against clickjacking.

Threat Model and Attack Surface Analysis Overview

Bitwarden follows a risk-based approach to designing secure services and systems which include threat modeling and attack surface analysis to identify threats and develop mitigation to them. The risk and threat modeling analysis extends to all areas of Bitwarden platform including the core Bitwarden Cloud Server application and the Bitwarden Clients such as Mobile, Desktop, Web Application, Browser and/or Command Line Interfaces.

Bitwarden Clients

Users primarily interact with Bitwarden through our client applications such as Mobile, Desktop, Web Application, Browser and/or Command Line Interfaces. The security of these devices, workstations, and web browsers is critical, because if one or more of these devices are compromised an attacker may be able to install malware such as a keylogger which would capture all information entered on these devices including any of your passwords and secrets. You, as the end-user and/or device owner, are responsible for ensuring that your devices are secured and protected from non-authorized access.

HTTPS TLS and Web Browser Crypto End-to-End Encryption

The Bitwarden Web client runs in your web browser. The authenticity and integrity of the Bitwarden Web client depends on the integrity of the HTTPS TLS connection by which it is delivered. An attacker capable of tampering with the traffic that delivers the web client could deliver a malicious client to the user.

Web browser attacks are one of the most popular ways for attackers and cyber criminals to inject malware or inflict damage. Attack vectors on the web browser might include:

- An element of **Social Engineering, such as Phishing,** to trick and persuade the victim to take an action that compromises the security of their user secrets and account.
- Web Browser attacks and Browser Extension / Add-On Exploits: A malicious extension designed to be able to capture user secrets as they are typed on the keyboard.
- Attacks on Web Applications through the Browser: Clickjacking, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).

Bitwarden leverages HTTP Security headers as an additional level of protection for the Bitwarden web application and communications.

Code Assessments

Bitwarden is an open source password manager. All of our source code is hosted and publicly available on GitHub for review. Bitwarden source code has been and continues to be audited annually by reputable third-party security auditing firms as well as independent security researchers. In addition, The Bitwarden Vulnerability Disclosure Program enlists the help of the hacker community at HackerOne to make Bitwarden more secure.

Read more: Bitwarden Security FAQs
Bitwarden Threat Prevention and Response
Bitwarden Security and Compliance Assessments, Reviews, Vulnerability Scans, PenTesting

Conclusion

This overview of the Bitwarden Security and Compliance program is offered for your review. Bitwarden's solution, software, infrastructure, and security processes have been designed from the ground up with a multi-layered, defense-in-depth approach.

The Bitwarden Security and Compliance Program is based on the ISO27001 Information Security Management System (ISMS). We defined policies that govern our security policies and processes and continually update our security program to be consistent with applicable legal, industry, and regulatory requirements for services that we provide to you under our Terms of Service Agreement.

If you have any questions, please contact us.