

SÉCURITÉ

Bitwarden Livre Blanc de Sécurité

Afficher dans le centre d'aide:

<https://bitwarden.com/help/bitwarden-security-white-paper/>

Bitwarden Livre Blanc de Sécurité

Aperçu du programme de sécurité et de conformité de Bitwarden

Avec l'augmentation du travail à distance et l'utilisation d'Internet plus élevée que jamais auparavant, la demande de créer et de maintenir des dizaines (sinon des centaines) de comptes en ligne avec des identifiants et des mots de passe est stupéfiante.

Les experts en sécurité recommandent que vous utilisiez un mot de passe différent, généré aléatoirement, pour chaque compte que vous créez. Mais comment gérez-vous tous ces mots de passe ? Et comment maintient-on une bonne hygiène de mot de passe à travers une organisation ?

La gestion efficace des mots de passe est une ressource fortement sous-utilisée dans l'entreprise. Dans le [Rapport Under the Hoodie 2020 de Rapid7](#), ils notent que la gestion des mots de passe et les contrôles secondaires tels que l'authentification à deux facteurs sont "gravement insuffisants, conduisant à des compromissions 'faciles'". La réutilisation ou le partage de mots de passe de manière non sécurisée rend l'entreprise vulnérable.

Pour apporter du changement dans une organisation, les équipes de sécurité et d'informatique doivent éduquer les employés sur les meilleures pratiques. En ce qui concerne la gestion des mots de passe, l'une des façons les plus simples d'encourager et de soutenir une bonne hygiène des mots de passe est de déployer une solution de gestionnaire de mots de passe dans votre lieu de travail.

Bitwarden est la manière la plus facile et la plus sûre de stocker tous vos identifiants, mots de passe et autres informations sensibles tout en les gardant commodément synchronisés entre tous vos appareils.

Bitwarden fournit les outils pour créer, stocker et partager vos mots de passe tout en maintenant le plus haut niveau de sécurité.

La solution, le logiciel, l'infrastructure et les processus de sécurité de Bitwarden ont été conçus dès le départ avec une approche de défense en profondeur à plusieurs niveaux. Le programme de sécurité et de conformité Bitwarden est basé sur le système de gestion de la sécurité de l'information ISO27001 (ISMS). Nous avons défini des politiques qui régissent nos politiques de sécurité et nos processus et nous mettons constamment à jour notre programme de sécurité pour qu'il soit conforme aux exigences légales, industrielles et réglementaires applicables aux services que nous vous fournissons en vertu de notre [Contrat de Conditions de Service](#).

Bitwarden se conforme aux directives de sécurité des applications standard de l'industrie qui comprennent une équipe d'ingénierie de sécurité dédiée et incluent des revues régulières du code source de l'application et de l'infrastructure informatique pour détecter, valider et remédier à toute vulnérabilité de sécurité.

Ce livre blanc fournit un aperçu des principes de sécurité de Bitwarden ainsi que des liens vers des documents supplémentaires qui fournissent plus de détails dans des domaines spécifiques.

Principes de Sécurité de Bitwarden

Protection des Données de l'Utilisateur

Bitwarden utilise les mesures de sécurité clé suivantes pour protéger les données des utilisateurs.

Cryptage de bout en bout : verrouillez vos mots de passe et vos informations privées avec le cryptage de bout en bout AES-CBC 256 bits, le hachage salé et PBKDF2 SHA-256. Toutes les clés cryptographiques sont générées et gérées par le client sur vos appareils, et tout le chiffrement est effectué localement. Voir plus de détails dans la section Dérivation de Hachage du Mot de Passe.

Chiffrement à connaissance zéro : Les membres de l'équipe Bitwarden ne peuvent pas voir vos mots de passe. Vos données restent cryptées de bout en bout avec votre courriel individuel et votre mot de passe principal. Nous ne stockons jamais et ne pouvons pas accéder à votre mot de passe principal ou à vos clés cryptographiques.

Note

La sortie de mi-2021 de [la récupération de compte](#) a introduit une nouvelle paire de clés publiques/privées RSA pour toutes les organisations. La clé privée est ensuite cryptée avec la clé symétrique préexistante de l'organisation avant d'être stockée. La paire de clés est générée et cryptée côté client lors de la création d'une nouvelle organisation, ou pour une organisation existante lors de :

- Navigation vers l'écran Gérer → Personnes.
- Mises à jour de tout sur l'écran Paramètres → Mon Organisation.
- Mises à niveau d'un type d'organisation à un autre.

Partage de mot de passe sécurisé : Bitwarden permet le partage et la gestion sécurisés de données sensibles avec les utilisateurs de toute une organisation. Une combinaison de cryptage asymétrique et symétrique protège les informations sensibles lorsqu'elles sont partagées.

Code open source et code disponible à la source :

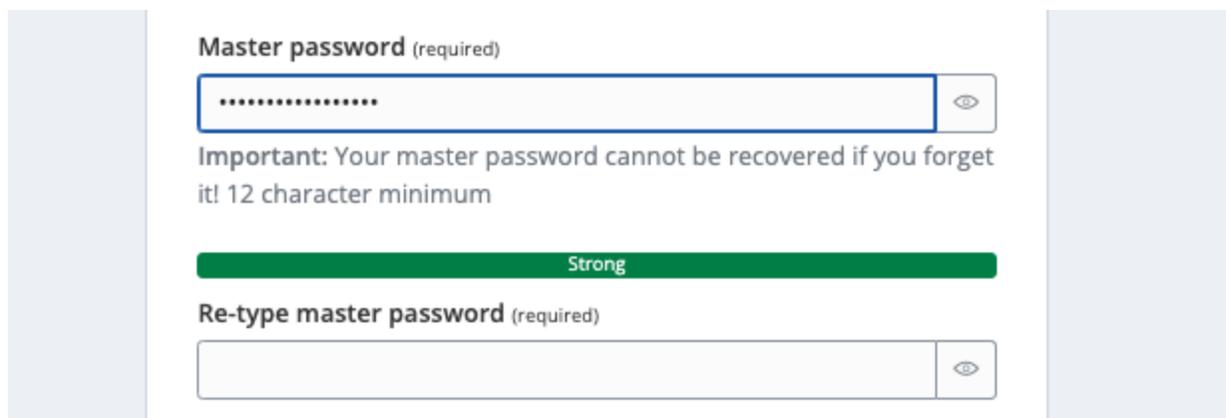
Le code source de tous les produits logiciels Bitwarden est hébergé sur [GitHub](#) et nous invitons tout le monde à examiner, auditer et contribuer à la base de code Bitwarden. Le code source de Bitwarden est audité par des cabinets d'audit de sécurité tiers de bonne réputation ainsi que par des chercheurs indépendants en sécurité. De plus, le [Programme de Divulgence de Vulnérabilités Bitwarden](#) recrute l'aide de la communauté de hackers chez HackerOne pour rendre Bitwarden plus sûr.

Confidentialité dès la conception : Bitwarden stocke toutes vos connexions dans un coffre-fort crypté qui se synchronise sur tous vos appareils. Comme elle est entièrement cryptée avant même de quitter votre appareil, vous seul avez accès à vos données. Même l'équipe de Bitwarden ne peut pas lire vos données (même si nous le voulions). Vos données sont scellées avec un chiffrement AES-CBC 256 bits, un hachage salé, et PBKDF2 SHA-256.

Audit de sécurité et conformité : Open source et audité par une tierce partie, Bitwarden se conforme aux réglementations AICPA SOC2 Type 2 / Privacy Shield, GDPR et CCPA.

Mot de passe principal

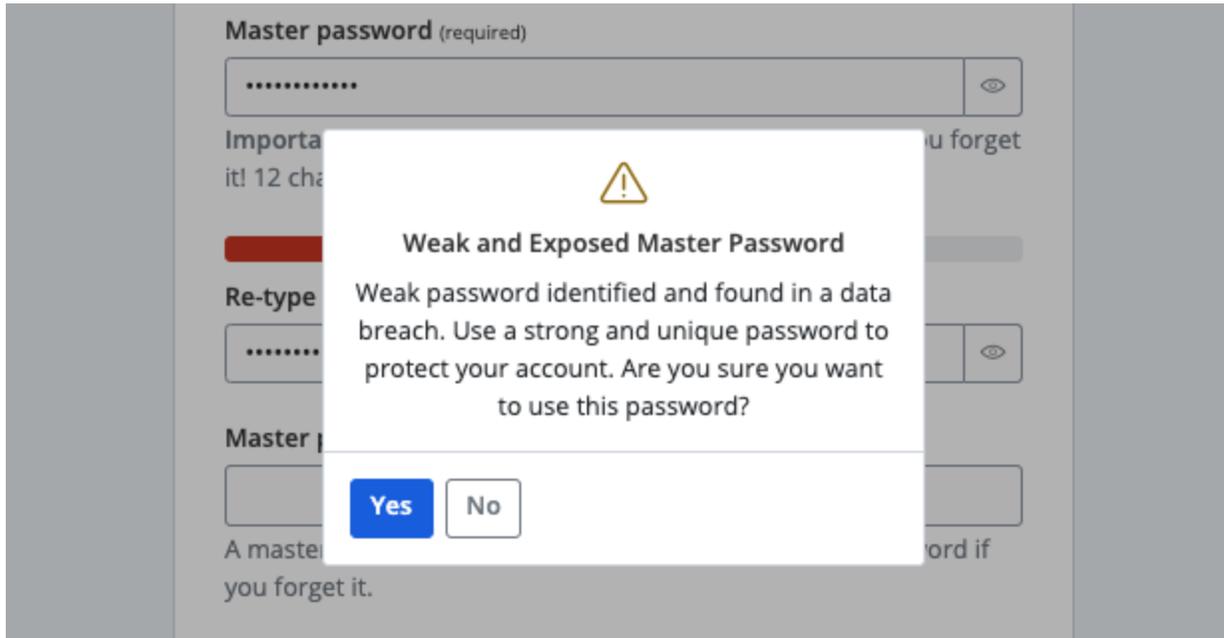
La protection des données utilisateur dans Bitwarden commence au moment où un utilisateur crée un compte et un mot de passe principal. Nous recommandons vivement d'utiliser un mot de passe principal fort pendant le processus d'intégration. Bitwarden comprend un indicateur de force du mot de passe comme guide qui évaluera et affichera la force globale du mot de passe principal entré pour encourager un mot de passe principal fort.



The screenshot shows a web form for creating a Bitwarden account. It features a 'Master password (required)' input field with a strength indicator below it. The strength indicator is a green bar labeled 'Strong'. Below the strength indicator is a 'Re-type master password (required)' input field. The form is set against a light blue background.

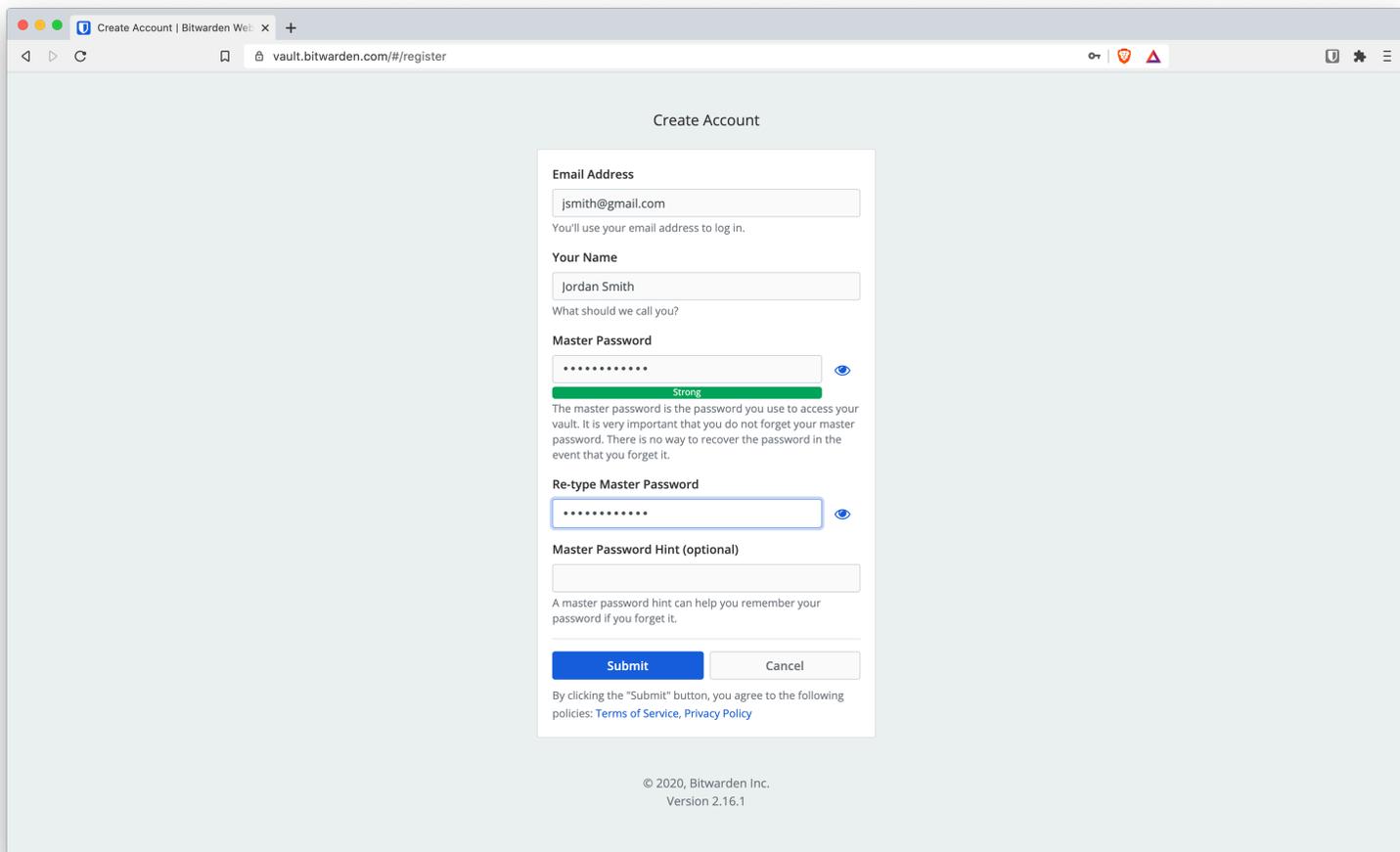
Créez un compte Bitwarden

Si vous essayez de vous inscrire avec un mot de passe faible, Bitwarden vous informera que le mot de passe principal choisi est faible. Lorsque vous créez un compte Bitwarden, vous aurez également la possibilité de vérifier les brèches de données connues pour le mot de passe principal en utilisant HIBP.



Avertissement de mot de passe principal faible

Utiliser un mot de passe principal fort est pour votre propre bénéfice en matière de sécurité car c'est le jeton que vous utilisez pour accéder à votre coffre sécurisé, où vos éléments sensibles sont stockés. Vous êtes responsable de la sécurité de votre compte pendant que vous utilisez le service Bitwarden. Nous proposons des mesures supplémentaires, telles que l'identifiant en deux étapes, pour vous aider à maintenir la sécurité de votre compte, mais le contenu de votre compte et sa sécurité dépendent de vous.



Choisissez un mot de passe principal fort

Lire la suite : [Cinq meilleures pratiques pour la gestion des mots de passe et 3 conseils du NIST pour garder vos mots de passe en sécurité](#)

Outils Utiles : [Outil de Test de la Force du Mot de Passe Bitwarden](#) et [Générateur de Mot de Passe Bitwarden](#)

Il est très important que vous n'oubliez jamais votre mot de passe principal. Le mot de passe principal est effacé de la mémoire après utilisation et n'est jamais transmis sur Internet aux serveurs de Bitwarden, il n'y a donc aucun moyen de récupérer le mot de passe dans le cas où vous l'oubliez.

Cela signifie également que personne de l'équipe Bitwarden ne peut jamais voir, lire ou déchiffrer pour accéder à vos véritables données. Vos données sont entièrement cryptées et/ou hachées avant de quitter jamais votre appareil local. C'est une étape critique que Bitwarden prend pour vous protéger, vous et vos données.

Après avoir créé votre compte et spécifié votre mot de passe principal, Bitwarden génère ensuite plusieurs clés qui sont utilisées pour protéger les données de votre compte.

Note

Au milieu de 2021, Bitwarden a introduit la [récupération de compte](#) pour les plans Entreprise. Avec cette option, les utilisateurs et les organisations ont la possibilité de mettre en œuvre une nouvelle politique permettant aux administrateurs et aux propriétaires de réinitialiser les mots de passe pour les utilisateurs.

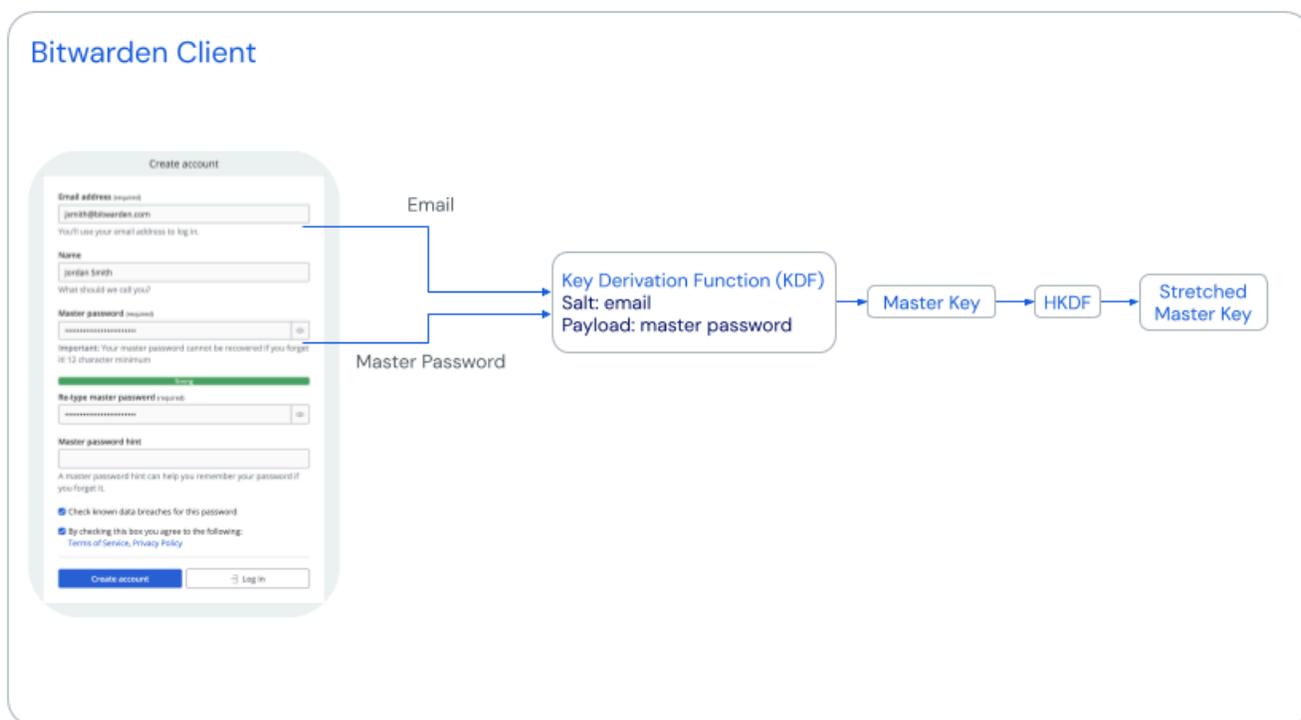
Aperçu du processus de hachage, de dérivation de clé et de chiffrement du mot de passe principal

Création de Compte Utilisateur

Lorsque le formulaire de création de compte est soumis, Bitwarden utilise la fonction de dérivation de clé basée sur le mot de passe 2 (PBKDF2) avec 600 000 tours d'itération pour étirer le mot de passe principal de l'utilisateur avec un sel de l'adresse de courriel de l'utilisateur. La valeur salée résultante est la clé maîtresse de 256 bits. La clé maîtresse est également étendue à 512 bits de longueur en utilisant la fonction de dérivation de clé basée sur HMAC-Extract-and-Expand (HKDF). La Clé Principale et la Clé Principale Étirée ne sont jamais stockées sur les serveurs de Bitwarden ou transmises à ceux-ci.

Note

Dans la version 2023.2.0, Bitwarden a ajouté Argon2id comme option alternative à PBKDF2. [En savoir plus.](#)



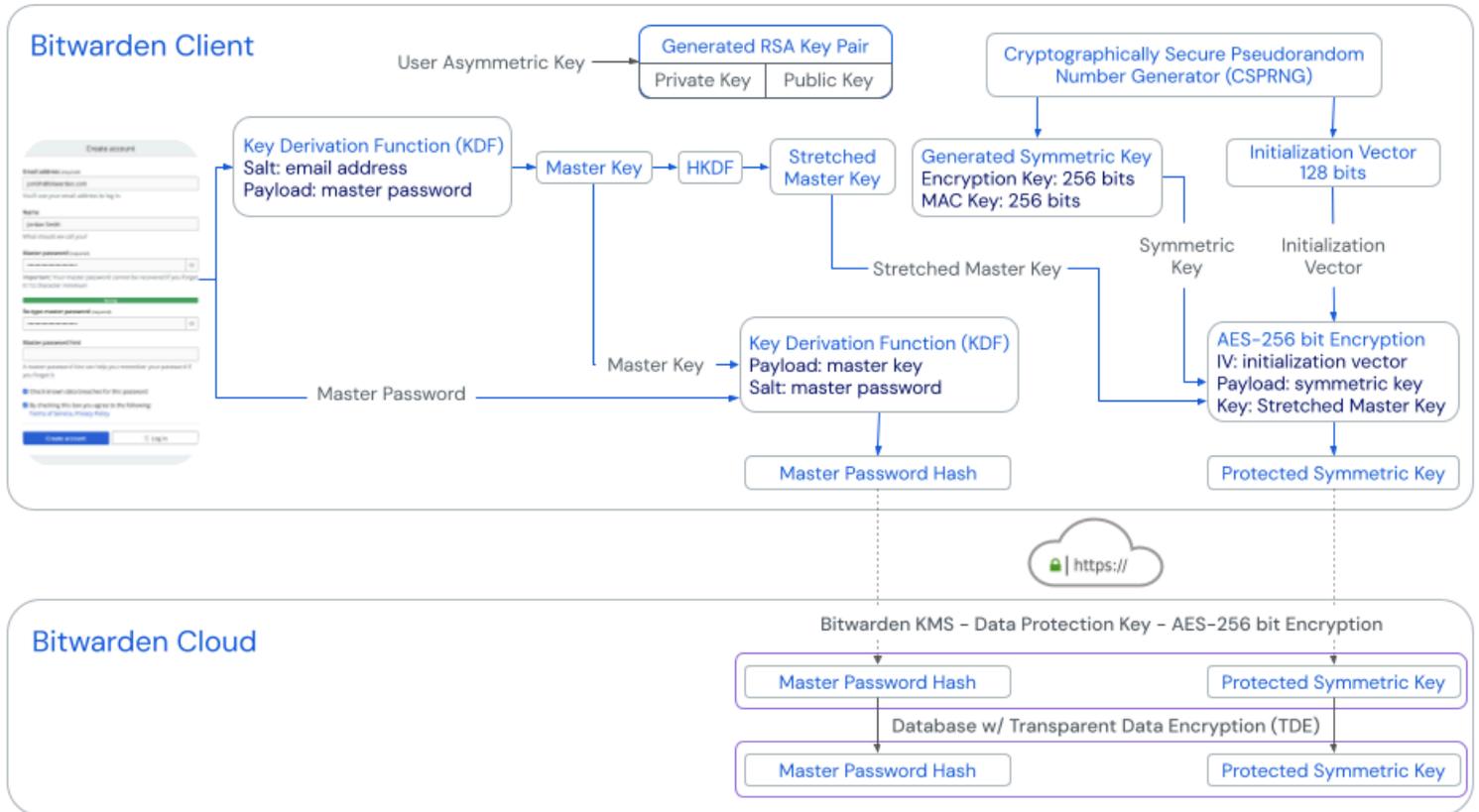
Dérivation de clé basée sur le mot de passe

De plus, une clé symétrique de 512 bits et un vecteur d'initialisation sont générés à l'aide d'un générateur de nombres pseudo-aléatoires cryptographiquement sécurisé (CSPRNG). La clé symétrique est cryptée avec le cryptage AES-256 bits en utilisant la clé maîtresse étirée et le vecteur d'initialisation. La clé résultante est appelée la Clé Symétrique Protégée. La Clé Symétrique Protégée est la clé principale associée à l'utilisateur et envoyée au serveur lors de la création du compte, et renvoyée aux applications client Bitwarden lors de la synchronisation.

Une clé asymétrique est également générée (paire de clés RSA) lorsque l'utilisateur enregistre son compte. La paire de clés RSA générée est utilisée si et quand l'utilisateur crée une organisation, qui peut être créée et utilisée pour partager des données entre les utilisateurs. Pour plus d'informations, référez-vous à [Partage de Données Entre Utilisateurs](#).

Un hachage de mot de passe principal est également généré en utilisant PBKDF-SHA256 avec une charge utile de clé principale et avec un sel du mot de passe principal. Le hachage du mot de passe principal est envoyé au serveur lors de la création du compte et de

l'identifiant, et est utilisé pour authentifier le compte utilisateur. Une fois atteint le serveur, le hachage du mot de passe principal est à nouveau haché en utilisant PBKDF2-SHA256 avec un sel aléatoire et 600 000 itérations. Un aperçu du processus de hachage du mot de passe, de dérivation de clé et de chiffrement est montré ci-dessous.



Hachage du mot de passe Bitwarden, dérivation de clé et chiffrement

Identifiant de l'utilisateur | Authentification de l'utilisateur | Accès aux Données du coffre de l'utilisateur

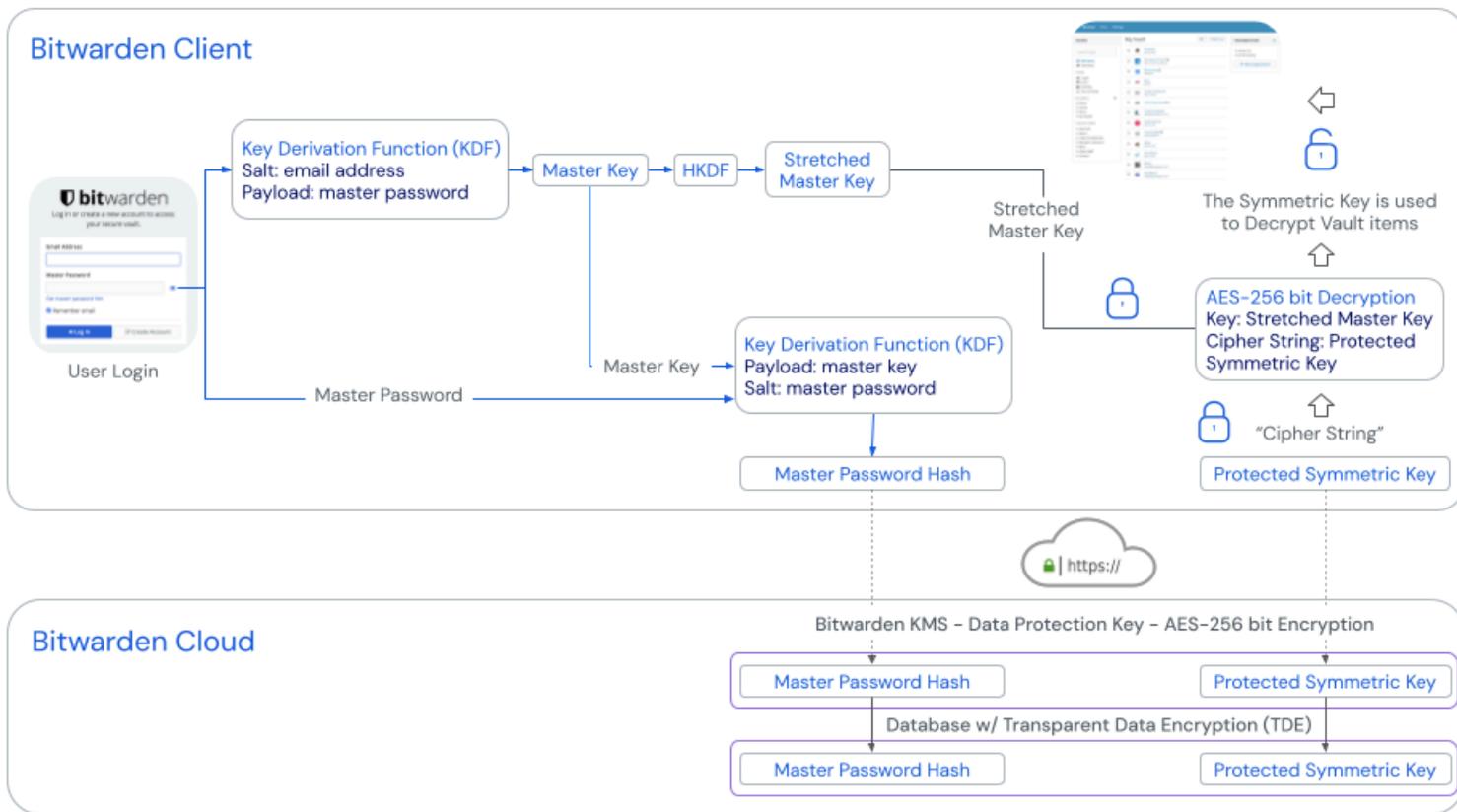
Il vous est demandé de d'abord entrer votre adresse de courriel et votre mot de passe principal afin de vous [connecter](#) à votre compte Bitwarden.

Ensuite, Bitwarden utilise la fonction de dérivation de clé basée sur le mot de passe 2 (PBKDF2) avec un défaut de 600 000 tours d'itération pour étirer votre mot de passe principal avec un sel de votre adresse de courriel. La valeur salée résultante est la clé maîtresse de 256 bits. Un hachage de la clé principale est envoyé au serveur lors de la création du compte et de l'identifiant, et est utilisé pour authentifier le compte utilisateur.

Note

Dans la version 2023.2.0, Bitwarden a ajouté Argon2id comme option alternative à PBKDF2. [En savoir plus.](#)

La clé maîtresse est également étendue à 512 bits en utilisant la fonction de dérivation de clé basée sur HMAC et d'expansion (HKDF). La Clé Symétrique Protégée est déchiffrée en utilisant la Clé Maître Étirée. La clé symétrique est utilisée pour déchiffrer les éléments du coffre. Le déchiffrement est entièrement effectué sur le client Bitwarden car votre mot de passe principal ou votre clé principale étirée n'est jamais stockée sur ou transmise aux serveurs Bitwarden.



Un aperçu de l'identifiant utilisateur

Nous ne conservons pas le mot de passe principal stocké localement ou en mémoire sur le client Bitwarden. Votre clé de chiffrement (Clé Symétrique) est conservée en mémoire pendant que l'application est déverrouillée. Ceci est nécessaire pour déchiffrer les données dans votre coffre. Lorsque le coffre est verrouillé, cette donnée est purgée de la mémoire. Après une certaine période d'inactivité sur l'écran verrouillé, nous rechargeons les processus de l'application pour nous assurer que toutes les adresses mémoire gérées restantes sont également purgées. Nous faisons de notre mieux pour garantir que toute donnée qui pourrait être en mémoire pour le fonctionnement de l'application n'est conservée en mémoire que tant que vous en avez besoin et que cette mémoire est nettoyée chaque fois que l'application est verrouillée. Nous considérons que l'application est complètement sûre lorsqu'elle est dans un état verrouillé.

Protection supplémentaire des données utilisateur lors de l'activation de l'identifiant en deux étapes

La connexion en deux étapes (également appelée authentification à deux facteurs ou 2FA) est une couche de sécurité supplémentaire pour votre compte, conçue pour garantir que vous êtes la **seule** personne qui peut accéder à votre compte, même si quelqu'un découvrirait votre mot de passe principal.

Comme meilleure pratique, nous recommandons à tous les utilisateurs d'activer et d'utiliser l'identifiant en deux étapes dans leur compte Bitwarden. Lorsque l'identifiant en deux étapes est activé, vous devez compléter une étape secondaire lors de la connexion à Bitwarden (en plus de votre mot de passe principal). Par défaut, on vous demandera de compléter cette étape secondaire à chaque fois, cependant il y a une option "Se souvenir de moi", qui enregistrera votre statut 2FA, afin que vous puissiez vous connecter sans 2FA la prochaine fois sur cet appareil particulier pour une durée allant jusqu'à 30 jours.

Note : Changer votre mot de passe principal ou désautoriser des sessions vous obligera à ré-authentifier 2FA, que vous ayez sélectionné "Se souvenir de moi" précédemment ou non.

Bitwarden prend en charge l'identifiant en deux étapes en utilisant les méthodes suivantes :

Plans Gratuits

- En utilisant une application d'authentification (par exemple, [2FAS](#), [Ravio](#), ou [Aegis](#))
- FIDO2 WebAuthn (toute clé certifiée FIDO2 WebAuthn)
- Courriel

Fonctionnalités Premium – incluses dans les plans Familles, Équipes et Entreprise

- Duo Security avec Duo Push, SMS, appel téléphonique, et clés de sécurité U2F
- YubiKey (tout appareil de la série 4/5 ou YubiKey NEO/NFC)

Vous pouvez activer plusieurs méthodes d'identifiant en deux étapes. Si vous avez activé plusieurs méthodes d'identifiant en deux étapes, l'ordre de préférence pour la méthode par défaut qui est affichée lors de la connexion est le suivant : FIDO U2F > YubiKey > Duo > Application d'authentification > Courriel. Vous pouvez cependant passer manuellement à n'importe quelle méthode et l'utiliser lors de l'identification.

Il est très important que vous ne perdiez jamais vos codes de récupération d'identifiant en deux étapes. Bitwarden propose un modèle de sécurité de protection de compte qui ne prend pas en charge les utilisateurs perdant leur mot de passe principal ou les codes de récupération de l'identifiant en deux étapes. Si vous avez activé la connexion en deux étapes sur votre compte et que vous perdez l'accès à vos codes de récupération de connexion en deux étapes, vous ne pourrez pas vous connecter à votre compte Bitwarden.

Note

Au milieu de 2021, Bitwarden a introduit la [récupération de compte](#) pour les plans Entreprise. Avec cette option, les utilisateurs et les organisations ont la possibilité de mettre en œuvre une nouvelle politique de sécurité permettant aux administrateurs et aux propriétaires de réinitialiser les mots de passe des utilisateurs.

Changement du mot de passe de l'utilisateur

Votre mot de passe principal ne peut être modifié que depuis le [Coffre Web](#). Pour des instructions spécifiques sur comment changer votre mot de passe utilisateur, consultez cet [article](#) d'aide Bitwarden.

Régénérer la Clé de Chiffrement de Votre Compte

Lors d'une opération de changement de mot de passe, vous avez également la possibilité de régénérer (changer) la clé de chiffrement de votre compte. Régénérer la clé de chiffrement est une bonne idée si vous pensez que votre précédent mot de passe principal a été compromis ou que les données de votre coffre Bitwarden ont été volées à partir de l'un de vos appareils.

Warning

La régénération de la clé de chiffrement de votre compte est une opération délicate, c'est pourquoi ce n'est pas une option par défaut. Une rotation de clé implique de générer une nouvelle clé de chiffrement aléatoire pour votre compte et de **régénérer toutes les données du coffre** en utilisant cette nouvelle clé. Voir les détails supplémentaires dans cet [article](#).

Protection des Données en Transit

Bitwarden prend la sécurité très au sérieux lorsqu'il s'agit de gérer vos données sensibles. Vos données ne sont jamais envoyées au Cloud Bitwarden sans être d'abord cryptées sur votre appareil local.

De plus, Bitwarden utilise TLS/SSL pour sécuriser les communications entre les clients Bitwarden et les appareils des utilisateurs vers le Cloud Bitwarden. L'implémentation TLS de Bitwarden utilise des certificats X.509 de 2048 bits pour l'authentification du serveur et l'échange de clés, ainsi qu'une suite de chiffrement robuste pour le chiffrement en masse. Nos serveurs sont configurés pour rejeter les chiffrements et protocoles faibles.

Bitwarden met également en œuvre des en-têtes de sécurité HTTP tels que la sécurité de transport strict HTTP (HSTS), qui forcera toutes les connexions à utiliser TLS. Cette couche supplémentaire de protection avec HSTS atténue les risques d'attaques par déclassé et de mauvaise configuration.

Protection des Données au Repos

Bitwarden crypte toujours et/ou hache vos données sur votre appareil local avant qu'elles ne soient envoyées aux serveurs cloud pour synchronisation. Les serveurs Bitwarden sont uniquement utilisés pour stocker et synchroniser les données cryptées du coffre. Il n'est pas possible d'obtenir vos données non cryptées des serveurs cloud de Bitwarden. Plus précisément, Bitwarden utilise le chiffrement AES 256 bits ainsi que PBKDF-SHA256 pour sécuriser vos données.

AES est une norme en cryptographie et est utilisée par le gouvernement américain et d'autres agences gouvernementales à travers le monde pour protéger les données top-secrètes. Avec une mise en œuvre appropriée et une clé de chiffrement forte (votre mot de passe principal), AES est considéré comme inviolable.

PBKDF-SHA256 est utilisé pour dériver la clé de chiffrement à partir de votre mot de passe principal. Ensuite, cette clé est salée et hachée pour l'authentification avec les serveurs Bitwarden. Le nombre d'itérations par défaut utilisé avec PBKDF2 est de 600 001 itérations sur le client (ce nombre d'itérations côté client est configurable à partir des paramètres de votre compte), puis 100 000 itérations supplémentaires lorsqu'il est stocké sur nos serveurs (pour un total de 700 001 itérations par défaut).

Note

Dans la version 2023.2.0, Bitwarden a ajouté Argon2id comme option alternative à PBKDF2. [En savoir plus.](#)

Certaines données cryptées, y compris la clé symétrique protégée d'un utilisateur et le hachage du mot de passe principal, sont également cryptées de manière transparente au repos par l'application, ce qui signifie qu'elles sont cryptées et décryptées à nouveau lorsqu'elles entrent et sortent de la base de données Bitwarden.

Bitwarden utilise également le chiffrement de données transparent Azure (TDE) pour se protéger contre la menace d'activité malveillante hors ligne en effectuant le chiffrement et le déchiffrement en temps réel de la base de données, des sauvegardes associées et des fichiers de journal de transactions au repos.

En savoir plus : [Comment le chiffrement de bout en bout ouvre la voie à la connaissance zéro](#) et [Quel chiffrement est utilisé](#)

Se connecter avec des clés de passe et maintenir un cryptage de bout en bout

En plus du mot de passe principal, les utilisateurs peuvent choisir de déverrouiller leurs coffres avec une clé de passe. Ce processus utilise une norme de pointe et une extension pour WebAuthn appelée la fonction pseudo-aléatoire ou PRF, qui tire le matériel clé d'un authentificateur. Avec PRF, les clés dérivées sont utilisées dans le chiffrement et le déchiffrement des données stockées dans le coffre du gestionnaire de mots de passe Bitwarden et dans Bitwarden Secrets Manager, en maintenant un chiffrement de bout en bout, sans connaissance préalable.

Lorsqu'une clé de passe est enregistrée pour se connecter à Bitwarden :

1. Une **paire de clés publique et privée de passkey** est générée par l'authentificateur via l'API WebAuth. Cette paire de clés, par définition, constitue votre clé de passe.
2. Une **clé symétrique PRF** est générée par l'authentificateur via l'extension PRF de l'API WebAuthn. Cette clé est dérivée d'un **secret interne** unique à votre clé de passe et d'un **sel** fourni par Bitwarden.

3. Une **paire de clés publique et privée PRF** est générée par le client Bitwarden. La clé publique PRF crypte votre **clé de chiffrement de compte**, à laquelle votre client aura accès en vertu d'être connecté et déverrouillé, et la **clé de chiffrement de compte cryptée par PRF** résultante est envoyée au serveur.
4. La **clé privée PRF** est cryptée avec la **clé symétrique PRF** (voir Étape 2) et la **clé privée PRF cryptée** résultante est envoyée au serveur.
5. Votre client envoie des données aux serveurs Bitwarden pour créer un nouvel enregistrement de clé de passe pour votre compte. Si votre clé de passe est enregistrée auprès du support pour le chiffrement et le déchiffrement du coffre, cet enregistrement comprend :
 - Le nom de la clé de passe
 - La clé publique de passe-partout
 - La clé publique PRF
 - La clé de chiffrement de compte cryptée par PRF
 - La clé privée cryptée par PRF

Votre clé privée de passkey, qui est nécessaire pour accomplir l'authentification, ne quitte jamais le client que sous un format crypté.

Lorsqu'une clé de passe est utilisée pour se connecter et, spécifiquement, pour déchiffrer les données de votre coffre :

1. En utilisant la cryptographie à clé publique de l'API WebAuthn, votre demande d'authentification est affirmée et confirmée.
2. Votre **clé de chiffrement de compte cryptée PRF** et **clé privée cryptée PRF** sont envoyées du serveur à votre client.
3. En utilisant le même **sel** fourni par Bitwarden et le **secret interne** unique à votre clé de passe, la **clé symétrique PRF** est recréée localement.
4. La **clé symétrique PRF** est utilisée pour déchiffrer votre **clé privée PRF chiffrée**, ce qui donne votre **clé privée PRF**.
5. La **clé privée PRF** est utilisée pour déchiffrer votre **clé de chiffrement de compte cryptée PRF**, ce qui donne votre **clé de chiffrement de compte**. Votre clé de chiffrement de compte est utilisée pour déchiffrer les données de votre coffre.

Comment les Éléments du Coffre sont Sécurisés

Toutes les informations (Identifiants, Cartes de paiement, Identités, Notes) associées à vos données stockées dans le coffre sont protégées par un cryptage de bout en bout. Les éléments que vous choisissez de stocker dans votre coffre Bitwarden sont d'abord stockés avec un élément appelé un objet Cipher. Les objets de chiffrement sont cryptés avec votre Clé Symétrique Générée, qui ne peut être connue qu'en déchiffrant votre Clé Symétrique Protégée à l'aide de votre Clé Maître Étirée. Cette encryption et déryption sont entièrement réalisées sur le client Bitwarden car votre mot de passe principal ou clé principale étirée n'est jamais stockée sur ou transmise aux serveurs Bitwarden.

Rapports sur la santé des chambres fortes

Tous les plans payants de Bitwarden sont livrés avec des rapports de santé du coffre pour les individus et les organisations.

Pour les coffres individuels, les individus ont accès à ce qui suit :

- Rapport sur les mots de passe exposés

- Rapport sur les mots de passe réutilisés
- Rapport sur les mots de passe faibles
- Rapport sur les sites Web non sécurisés
- Rapport 2FA Inactif
- Rapport de Brèche de Données

Pour les utilisateurs professionnels, un ensemble similaire de rapports existe pour les éléments du coffre de l'organisation.

Lire plus:[Coffre Health rapporte](#)

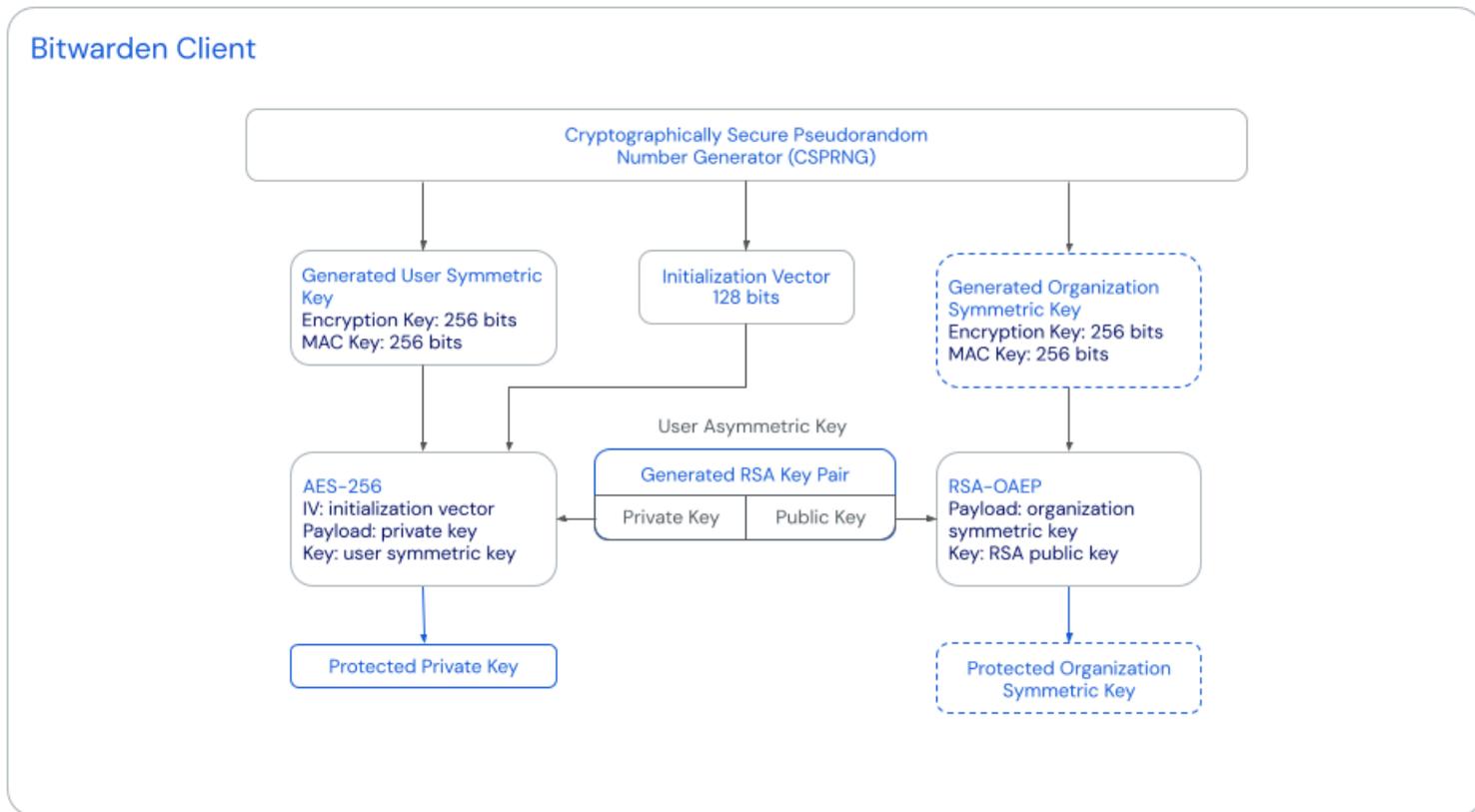
Pour plus d'informations sur les journaux d'événements Bitwarden et le rapport externe, voir [Journaux d'événements](#).

Importer des mots de passe et d'autres secrets dans Bitwarden

Vous pouvez facilement importer vos données de plus de 40 services différents, y compris toutes les applications populaires de gestionnaire de mots de passe, vers Bitwarden. La liste complète des applications prises en charge et certaines informations supplémentaires, y compris les étapes de dépannage pour importer vos données dans Bitwarden, sont documentées dans [le Centre d'aide Bitwarden](#).

Si vous exportez vos sites à partir du coffre Web LastPass.com, veuillez vous référer aux informations spécifiques sur cette note d'aide [Importer vos données de LastPass](#).

Partage de Données Entre Utilisateurs



Protection et échange de clés d'organisation

La collaboration est l'un des principaux avantages de l'utilisation d'un gestionnaire de mots de passe. Pour permettre le partage, vous devez d'abord créer une Organisation. Une organisation Bitwarden est une entité qui relie ensemble des utilisateurs qui souhaitent partager des éléments. Une organisation peut être une famille, une équipe, une entreprise ou tout autre type de groupe qui souhaite partager des données.

Un compte utilisateur individuel peut créer et/ou appartenir à de nombreuses organisations différentes, vous permettant de gérer vos éléments à partir d'un seul compte.

Vous pouvez créer une nouvelle organisation Bitwarden à partir du coffre Web ou demander à un administrateur d'une organisation existante de vous envoyer une invitation.

Lorsque Vous Créez une Organisation

Lorsque vous créez une Organisation, une clé symétrique d'Organisation est générée à l'aide d'un Générateur de Nombre Pseudo-Aléatoire Cryptographiquement Sécurisé (CSPRNG). Cette clé symétrique de l'Organisation est ce qui est utilisé pour déchiffrer les Données du coffre détenues par l'Organisation, donc partager des Données avec les membres de l'Organisation nécessite de fournir un accès sécurisé à celle-ci. La clé symétrique brute de l'organisation n'est jamais stockée sur les serveurs de Bitwarden.

Dès que la clé symétrique de l'Organisation est générée, RSA-OAEP est utilisé pour chiffrer la clé symétrique de l'organisation avec la clé publique RSA du créateur de l'Organisation. Une paire de clés RSA est générée pour chaque utilisateur lors de la création du compte, qu'ils soient membre d'une organisation ou non, donc cette clé existera déjà avant la création de l'organisation.

Note

La clé privée RSA, dont l'utilisation est décrite ci-dessous, est stockée cryptée avec la clé de cryptage du compte de l'utilisateur, donc les utilisateurs doivent être complètement connectés pour y accéder.

La valeur résultante de cette opération est appelée la clé symétrique de l'organisation protégée et est envoyée aux serveurs Bitwarden.

Lorsque le créateur de l'organisation, ou tout membre de l'organisation, se connecte à son compte, l'application client utilise la clé privée RSA déchiffrée pour déchiffrer la clé symétrique de l'Organisation protégée, ce qui donne la clé symétrique de l'Organisation. En utilisant la clé symétrique de l'organisation, les données du coffre appartenant à l'organisation sont déchiffrées localement.

Quand les utilisateurs rejoignent une organisation

Le processus pour les utilisateurs suivants rejoignant une organisation est assez similaire, cependant certaines différences méritent d'être notées.

Tout d'abord, un membre établi de l'Organisation, spécifiquement quelqu'un avec l'autorisation d'intégrer d'autres utilisateurs, confirme l'utilisateur à l'Organisation. Ce membre établi, en vertu d'avoir déjà connecté à son compte et d'avoir traversé le processus de déchiffrement des Données de l'organisation décrit dans la section précédente, a accès à la clé symétrique déchiffrée de l'organisation.

Donc, lorsque le nouvel utilisateur est confirmé, le client du membre établi contacte les serveurs de Bitwarden, récupère la clé publique RSA du nouvel utilisateur, qui est stockée sur les serveurs de Bitwarden au moment de la création du compte, et crypte la clé symétrique de l'organisation déchiffrée avec celle-ci. Cela donne lieu à une nouvelle clé symétrique d'Organisation protégée qui est envoyée aux serveurs Bitwarden et stockée pour le nouveau membre.

Note

Chaque clé symétrique d'Organisation protégée est unique pour son utilisateur, mais chacune se déchiffrera en la même clé symétrique d'Organisation requise lorsqu'elle sera déchiffrée avec la clé privée RSA spécifique de son utilisateur.

Lorsque le nouvel utilisateur se connecte à son compte, l'application client utilise la clé privée RSA déchiffrée pour déchiffrer la nouvelle clé symétrique de l'organisation protégée, ce qui donne la clé symétrique de l'organisation. En utilisant la clé symétrique de l'organisation, les données du coffre appartenant à l'organisation sont déchiffrées localement.

Lire la suite : [Qu'est-ce que les organisations ?](#)

Contrôles d'accès et gestion des collections Bitwarden

Au fur et à mesure que l'utilisation de Bitwarden par votre organisation augmente, il est utile d'avoir des utilisateurs qui peuvent gérer les collections de manière indépendante, sans nécessiter un accès à tout ce qui se trouve dans le coffre de l'organisation.

La gestion des collections et des groupes est un moyen simple de séparer, d'accorder ou de limiter l'accès aux éléments du coffre dans Bitwarden, contrôlant ainsi la visibilité des ressources par l'utilisateur.

Une liste complète des rôles et du contrôle d'accès est documentée dans la section [Types d'Utilisateurs et Contrôle d'Accès](#) du Centre d'Aide Bitwarden.

Lire plus: [À propos des Collections](#)

Journaux d'événements

Les journaux d'événements contiennent des informations détaillées et horodatées sur les actions ou les modifications qui ont eu lieu au sein d'une organisation. Ces journaux sont utiles pour rechercher des modifications d'identifiants ou de configuration et très utiles pour les enquêtes de piste d'audit et les besoins de dépannage.

Des informations supplémentaires sur les [Journaux d'événements](#) sont documentées dans le Centre d'aide Bitwarden. Les journaux d'événements sont disponibles uniquement pour les plans Équipes et Business.

Pour recueillir plus de données, les plans avec accès à l'API peuvent utiliser l'API Bitwarden. Les réponses de l'API contiendront le type d'événement et les données pertinentes.

Intégration SIEM et Systèmes Externes

Pour les systèmes de gestion des informations et des événements de sécurité (SIEM) comme Splunk, lors de l'exportation des données de Bitwarden, une combinaison de données de l'API et du CLI peut être utilisée pour collecter des données.

Ce processus est décrit dans la note du centre d'aide sur les [Journaux d'événements d'organisation](#) sous [Intégrations de SIEM et de systèmes externes](#).

Protection du Compte et Éviter le Verrouillage

Aujourd'hui, pour les plans Basic, Premium, Familles et Équipes, Bitwarden offre une protection de compte avec un modèle de sécurité qui ne prend pas en charge les utilisateurs perdant leurs mots de passe ou les codes de récupération d'identifiant en deux étapes.

Bitwarden ne peut pas réinitialiser les mots de passe des utilisateurs ni désactiver l'identifiant en deux étapes s'il a été activé sur votre compte. Les propriétaires ou administrateurs de comptes Familles et Équipes ne peuvent pas réinitialiser les mots de passe des utilisateurs. Voir la section suivante pour plus de détails sur les plans de l'Entreprise.

Warning

Les utilisateurs qui perdent leur mot de passe principal, ou qui perdent leur code de récupération de connexion en deux étapes, devront supprimer leur compte et recommencer.

Pour atténuer ces problèmes potentiels, Bitwarden recommande ce qui suit pour la protection du compte et l'évitement du verrouillage.

Mot de passe principal

Identifiez une méthode pour vous permettre de retenir et de pouvoir récupérer votre mot de passe principal si vous l'oubliez. Cela peut inclure l'écrire et le placer dans un coffre-fort, ou un endroit sûr.

Utilisez un indice pour le mot de passe principal

Si cela vous aide, utilisez l'indice du mot de passe principal fourni par Bitwarden lors de l'inscription. Ou configurez un indice à tout moment via les paramètres dans le coffre Web.

Gestion de l'organisation

Pour les organisations, ayez plusieurs administrateurs qui peuvent accéder et gérer l'organisation.

Code de récupération pour l'identifiant en deux étapes

Si vous choisissez ou si votre Organisation vous oblige à mettre en place une connexion en deux étapes, assurez-vous d'accéder et de conserver votre Code de récupération et de le stocker dans un endroit aussi sûr que votre mot de passe principal.

Récupération de compte dans les plans d'Entreprise

Au milieu de 2021, Bitwarden a introduit la [récupération de compte](#) pour les plans Entreprise. Avec cette option, les utilisateurs et les organisations ont la possibilité de mettre en œuvre une nouvelle politique de sécurité permettant aux administrateurs et aux propriétaires de réinitialiser les mots de passe des utilisateurs.

Sécurité de la plateforme cloud et de l'application web Bitwarden

Aperçu de l'architecture Bitwarden

Bitwarden traite et stocke toutes les données de manière sécurisée dans le cloud Microsoft Azure en utilisant des services qui sont gérés par l'équipe de Microsoft. Puisque Bitwarden n'utilise que les offres de service fournies par Azure, il n'y a aucune infrastructure de

serveur à gérer et à maintenir. Toutes les mises à jour de disponibilité, d'évolutivité et de sécurité, les correctifs et les garanties sont soutenus par Microsoft et leur infrastructure cloud.

Mises à jour de sécurité et correctifs

L'équipe chez Microsoft gère les correctifs OS à deux niveaux, les serveurs physiques et les machines virtuelles invitées (VMs) qui exécutent les ressources Azure App Service. Les deux sont mis à jour mensuellement, ce qui correspond au calendrier mensuel du [Patch Tuesday de Microsoft](#). Ces mises à jour sont appliquées automatiquement, d'une manière qui garantit le SLA de haute disponibilité des services Azure.

Lire la suite : [Application de correctifs dans Azure App Service](#) ou [SLA pour App Service](#)

Pour des informations détaillées sur la façon dont les mises à jour sont appliquées, [lisez ici](#)

Bitwarden Architectural Overview

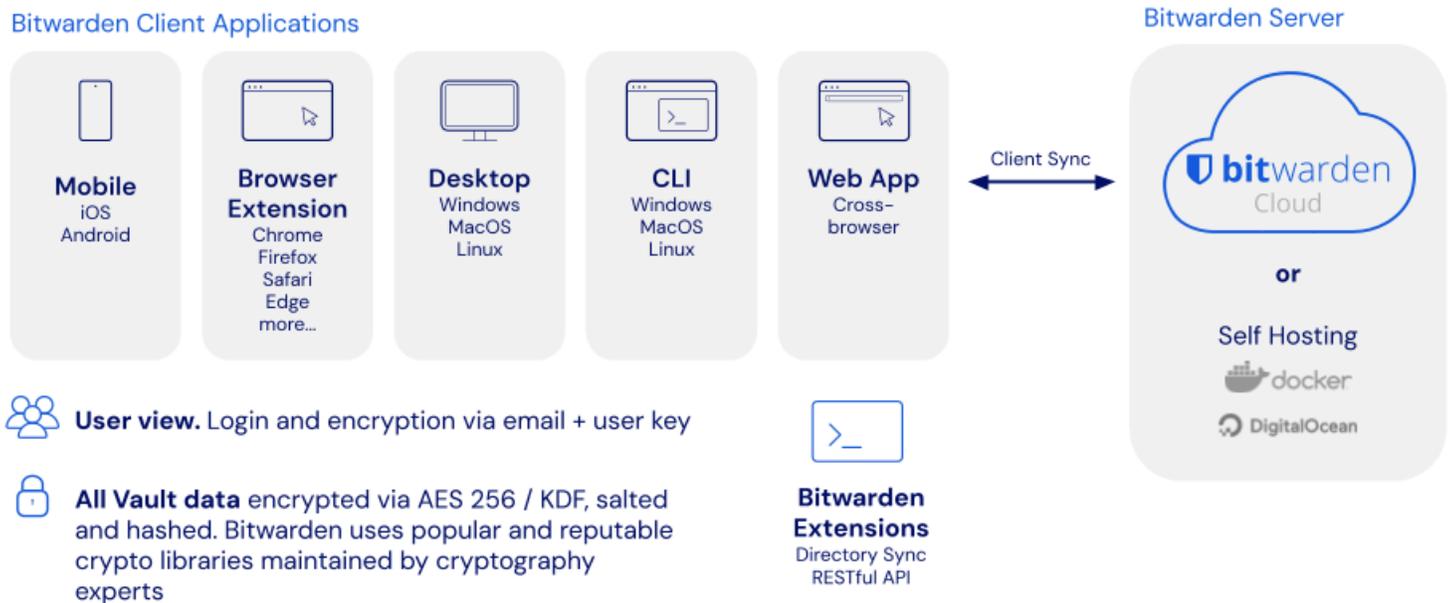


Figure : Un aperçu de l'architecture de Bitwarden

Contrôles d'accès Bitwarden

Les employés de Bitwarden ont une formation et une expertise significatives pour le type de données, de systèmes et d'actifs d'information qu'ils conçoivent, architectent, mettent en œuvre, gèrent, soutiennent et avec lesquels ils interagissent.

Bitwarden suit un processus d'intégration établi pour garantir que le niveau d'accès approprié est attribué et maintenu. Bitwarden a établi des niveaux d'accès qui sont appropriés pour chaque rôle. Toutes les demandes, y compris les demandes de modification d'accès, doivent être examinées et approuvées par le gestionnaire. Bitwarden suit une politique de moindre privilège qui accorde aux employés le niveau minimum d'accès requis pour accomplir leurs tâches. Bitwarden suit un processus de départ établi par le biais des Ressources Humaines de Bitwarden qui révoque tous les droits d'accès lors de la résiliation.

Cycle de vie du logiciel et gestion des changements

Bitwarden évalue les modifications apportées à la plateforme, aux applications et à l'infrastructure de production pour minimiser les risques et ces modifications sont mises en œuvre conformément aux procédures opérationnelles standard chez Bitwarden.

Les éléments de la demande de changement sont planifiés en fonction de la feuille de route et soumis à l'ingénierie à ce stade. L'ingénierie examinera et évaluera leur capacité et évaluera le niveau d'effort pour chaque élément de demande de changement. Après examen et évaluation, ils formuleront sur quoi ils vont travailler pour une sortie spécifique. Le CTO fournit les détails de la version à travers les canaux de communication et les réunions de gestion et le cycle de vie du développement commence pour cette version.

Processus de développement, de publication, de test et d'approbation de haut niveau :

- Développer, construire et itérer en utilisant des demandes d'extraction sur GitHub
- Amenez les fonctionnalités à un point où elles sont testables
- L'ingénierie effectue des tests fonctionnels de la fonctionnalité et/ou du produit pendant qu'ils sont en cours de développement et de construction.
- Le test unitaire de construction est automatisé dans le cadre des pipelines d'Intégration Continue (CI) de Bitwarden
- Certains tests sont également effectués par l'équipe du succès client.
- Le Directeur de l'Ingénierie aide à la revue et aide à formaliser le processus, y compris les mises à jour de la documentation.
- Le CTO donne l'approbation finale Go / No-Go

Participation à la réunion : Pour garantir une revue réussie, l'approbation, la mise en œuvre et la clôture des demandes de changement, chaque membre du personnel central des opérations et des services informatiques devrait être représenté lors de la réunion pour examiner et discuter de la demande de changement.

Le déploiement d'urgence / les correctifs reçoivent une priorité accrue, et l'examen et l'approbation du changement sont reçus d'un gestionnaire ou d'un directeur avant que le changement ne soit effectué et est par la suite examiné, communiqué et clôturé lors de la prochaine réunion de changement prévue. Cela se produit normalement lors d'une interruption de service, lorsque le système est en panne ou dans une situation urgente de prévention de panne.

Contrôle des Systèmes de Production

Bitwarden maintient des livres de procédures documentés pour tous les systèmes de production, qui couvrent les processus de déploiement, de mise à jour et de dépannage. Des alertes étendues sont mises en place pour notifier et escalader en cas de problèmes.

Configurations de Base

Bitwarden traite et stocke toutes les données de manière sécurisée dans le cloud Microsoft Azure en utilisant des services qui sont gérés par l'équipe de Microsoft. Puisque Bitwarden n'utilise que les offres de service fournies par Azure, il n'y a aucune infrastructure de serveur à gérer et à maintenir. Toutes les mises à jour et garanties de disponibilité, d'évolutivité et de sécurité sont soutenues par Microsoft et leur infrastructure cloud.

Les configurations de service Azure sont utilisées par Bitwarden pour garantir que les applications sont configurées et déployées de manière répétable et cohérente.

Procédures de Gestion des Clés de Plateforme Bitwarden

Les clés et autres secrets utilisés par la plateforme Bitwarden elle-même, incluent les identifiants pour les comptes des fournisseurs de cloud Bitwarden. Toutes ces clés sont générées, stockées de manière sécurisée et régénérées au besoin, conformément aux pratiques standard de l'industrie. Bitwarden utilise un coffre interne Bitwarden pour le stockage sécurisé et la sauvegarde de clés sensibles ou

d'autres secrets utilisés par la plateforme Bitwarden. Le contrôle d'accès au coffre Bitwarden utilise les [Types d'Utilisateurs et le Contrôle d'Accès](#).

Types de Données et Rétention des Données

Bitwarden traite deux types de données utilisateur pour fournir le service Bitwarden : (i) Donnée de Coffre et (ii) Donnée Administrative.

(i) Donnée de Coffre

Les Données du coffre comprennent toutes les informations stockées dans les comptes du service Bitwarden et peuvent inclure des informations personnelles. Si nous hébergeons le service Bitwarden pour vous, nous hébergerons les Données du Coffre. Les données du coffre sont cryptées à l'aide de clés cryptographiques sécurisées sous votre contrôle. Bitwarden ne peut pas accéder aux Données du Coffre.

Conservation des Données de Coffre : Vous pouvez ajouter, modifier et supprimer les Données de Coffre à tout moment.

(ii) Donnée Administrative

Bitwarden obtient des informations personnelles en lien avec la création de votre compte, l'utilisation du service Bitwarden et le support, ainsi que les paiements pour le service Bitwarden tels que les noms, les adresses de courriel, le téléphone et d'autres informations de contact pour les utilisateurs du service Bitwarden et le nombre d'éléments dans votre compte de service Bitwarden ("Donnée Administrative"). Bitwarden utilise les Données Administratives pour vous fournir le service Bitwarden. Nous conservons les Données Administratives aussi longtemps que vous êtes un client de Bitwarden et comme requis par la loi. Si vous mettez fin à votre relation avec Bitwarden, nous supprimerons vos informations personnelles conformément à nos politiques de sécurité de rétention de Donnée.

Lorsque vous utilisez le Site ou communiquez avec nous (par exemple, via courriel), vous fournirez et Bitwarden recueillera certaines informations personnelles telles que :

- Nom
- Nom de l'entreprise et adresse
- Numéro de téléphone professionnel
- Adresse électronique
- Adresse IP et autres identifiants en ligne
- Tout témoignage de client que vous nous avez donné la permission de partager.
- Les informations que vous fournissez aux zones interactives du site, telles que les formulaires remplissables ou les zones de texte, la formation, les webinaires ou l'inscription à des événements.
- Informations sur l'appareil que vous utilisez, comprenant le modèle de matériel, le système d'exploitation et sa version, les identifiants uniques de l'appareil, les informations réseau, l'adresse IP et/ou les informations du service Bitwarden lors de l'interaction avec le site.
- Si vous interagissez avec la communauté Bitwarden ou la formation, ou si vous vous êtes inscrit à un examen ou à un événement, nous pouvons collecter des informations biographiques et le contenu que vous partagez.
- Informations recueillies via des cookies, des balises pixel, des journaux, ou d'autres technologies similaires.

Veuillez vous référer à la [Politique de confidentialité de Bitwarden](#) pour plus d'informations.

Journalisation, Surveillance, et Notification d'Alerte

Bitwarden maintient des livres de procédures documentés pour tous les systèmes de production qui couvrent les processus de déploiement, de mise à jour et de dépannage. Des alertes étendues sont mises en place pour notifier et escalader en cas de problèmes. Une combinaison de surveillance manuelle et automatisée de l'infrastructure Cloud de Bitwarden offre une vue complète et détaillée de la santé du système ainsi que des alertes proactives sur les zones de préoccupation. Les problèmes sont rapidement identifiés afin que notre équipe d'infrastructure puisse répondre efficacement et atténuer les problèmes avec un minimum de perturbations.

Continuité des Affaires / Récupération après Sinistre

Bitwarden utilise toute une gamme de pratiques de récupération après sinistre et de continuité des activités de Microsoft Azure qui sont intégrées dans le Cloud Bitwarden. Cela comprend la haute disponibilité et les services de sauvegarde pour nos niveaux d'application et de base de données.

Prévention et Réponse aux Menaces

Bitwarden effectue des évaluations de vulnérabilité sur une base régulière. Nous utilisons des outils de tierce partie et des services externes, y compris : OWASP ZAP, [Mozilla Observatory](#), OpenVAS, et d'autres sont utilisés pour effectuer des évaluations internes.

Bitwarden utilise Cloudflare afin de fournir un WAF à la périphérie, une meilleure protection DDoS, distribué disponibilité et mise en cache. Bitwarden utilise également des proxies au sein de Cloudflare pour une meilleure sécurité réseau et performance de ses services et sites.

Bitwarden est un logiciel open source. Tout notre code source est hébergé sur GitHub et est gratuit pour quiconque souhaite le consulter. Le code source de Bitwarden est audité par des entreprises d'audit de sécurité tierce partie réputées ainsi que par des chercheurs indépendants en sécurité. De plus, le [Programme de Divulgaration de Vulnérabilités Bitwarden](#) recrute l'aide de la communauté de hackers chez HackerOne pour rendre Bitwarden plus sûr.

Auditabilité et Conformité

Le programme de sécurité et de conformité Bitwarden est basé sur le système de gestion de la sécurité de l'information (ISMS) ISO27001. Nous avons défini des politiques qui régissent nos politiques de sécurité et nos processus et nous mettons constamment à jour notre programme de sécurité pour qu'il soit conforme aux exigences légales, industrielles et réglementaires applicables aux services que nous vous fournissons en vertu de notre [Contrat de Conditions de Service](#).

Bitwarden se conforme aux directives de sécurité des applications standard de l'industrie qui comprennent une équipe d'ingénierie de sécurité dédiée et incluent des revues régulières du code source de l'application et de l'infrastructure informatique pour détecter, valider et remédier à toute vulnérabilité de sécurité.

Examens de Sécurité Externes

Les revues et évaluations de sécurité par une tierce partie des applications et/ou de la plateforme sont effectuées au minimum une fois par an.

Certifications

Les certifications de Bitwarden comprennent :

- SOC2 Type II (renouvelé annuellement)
- SOC3 (renouvelé annuellement)

Selon l'AICPA, l'utilisation du rapport SOC 2 de type II est restreinte. Pour les demandes de rapport SOC 2, veuillez [nous contacter](#).

Lire la suite : [Bitwarden obtient la certification SOC2](#)

Le rapport SOC 3 fournit un résumé du rapport SOC 2 qui peut être distribué publiquement. Selon l'AICPA, le SOC 3 est le rapport SOC pour les organisations de services sur les critères de services de confiance pour une utilisation générale.

Bitwarden fait une copie de notre rapport SOC 3 [disponible ici](#).

Ces certifications SOC représentent un aspect de notre engagement à protéger la sécurité et la confidentialité de nos clients, et à respecter des normes rigoureuses. Bitwarden effectue également une cadence régulière d'audits sur la sécurité de notre réseau et l'intégrité du code.

Lire plus: [L'audit de sécurité Bitwarden 2020 est terminé et Bitwarden termine l'audit de sécurité de tierce partie](#)

En-têtes de sécurité HTTP

Bitwarden utilise les en-têtes de sécurité HTTP comme un niveau supplémentaire de protection pour l'application web Bitwarden et les communications. Par exemple, la Sécurité de Transport Strict HTTP (HSTS) forcera toutes les connexions à utiliser TLS, ce qui atténue les risques d'attaques de déclassé et de mauvaise configuration. Les en-têtes de politiques de sécurité de contenu offrent une protection supplémentaire contre les attaques par injection, telles que le scriptage intersites (XSS). De plus, Bitwarden met en œuvre X-Frame-Options: SAMEORIGIN pour se défendre contre le détournement de clics.

Aperçu du Modèle de Menace et de l'Analyse de la Surface d'Attaque

Bitwarden suit une approche basée sur le risque pour concevoir des services et des systèmes sécurisés qui incluent la modélisation des menaces et l'analyse de la surface d'attaque pour identifier les menaces et développer des mesures d'atténuation à leur encontre. L'analyse de modélisation des risques et des menaces s'étend à tous les domaines de la plateforme Bitwarden, y compris l'application principale du serveur Cloud Bitwarden et les clients Bitwarden tels que Mobile, Bureau, Application Web, Navigateur et/ou Interfaces en ligne de commande.

Clients Bitwarden

Les utilisateurs interagissent principalement avec Bitwarden via nos applications client telles que Mobile, Bureau, Application Web, Navigateur et/ou Interfaces en ligne de commande. La sécurité de ces appareils, postes de travail et navigateurs web est essentielle car si un ou plusieurs de ces appareils sont compromis, un attaquant pourrait être en mesure d'installer des logiciels malveillants tels qu'un enregistreur de frappe qui capturerait toutes les informations entrées sur ces appareils, y compris tous vos mots de passe et secrets. Vous, en tant qu'utilisateur final et/ou propriétaire de l'appareil, êtes responsable de garantir que vos appareils sont sécurisés et protégés contre l'accès non autorisé.

HTTPS TLS et Cryptographie de Navigateur Web avec Chiffrement de Bout en Bout

Le client Web Bitwarden fonctionne dans votre navigateur web. L'authenticité et l'intégrité du client Web Bitwarden dépendent de l'intégrité de la connexion HTTPS TLS par laquelle il est livré. Un attaquant capable de manipuler le trafic qui livre le client web pourrait livrer un client malveillant à l'utilisateur.

Les attaques de navigateur Web sont l'une des méthodes les plus populaires pour les attaquants et les cybercriminels d'injecter des logiciels malveillants ou d'infliger des dommages. Les vecteurs d'attaque sur le navigateur web pourraient inclure :

- Un élément de **l'Ingénierie Sociale, comme le Phishing**, pour tromper et persuader la victime de prendre une action qui compromet la sécurité de leurs secrets d'utilisateur et de leur compte.
- **Attaques de navigateur web et exploits d'extension / add-on de navigateur** : Une extension malveillante conçue pour pouvoir saisir les secrets de l'utilisateur lorsqu'ils sont tapés sur le clavier.
- **Attaques contre les applications Web via le navigateur** : détournement de clics, cross-site scripting (XSS), cross-site request forgery (CSRF).

Bitwarden utilise les [en-têtes de sécurité HTTP](#) comme niveau de protection supplémentaire pour l'application web Bitwarden et les communications.

Évaluations de code

Bitwarden est un gestionnaire de mots de passe open source. Tout notre code source est hébergé et disponible publiquement sur [GitHub](#) pour examen. Le code source de Bitwarden a été et continue d'être audité annuellement par des cabinets d'audit de sécurité de tierce partie réputés ainsi que par des chercheurs indépendants en sécurité. De plus, le Programme de Divulcation de Vulnérabilités de Bitwarden fait appel à l'aide de la communauté de hackers chez HackerOne pour rendre Bitwarden plus sûr.

Lire plus:

- [FAQs sur la sécurité de Bitwarden](#)
- [Prévention et Réponse aux Menaces Bitwarden](#)
- [Évaluations de sécurité et de conformité Bitwarden, revues, scans de vulnérabilité, PenTesting](#)

Conclusion

Cette vue d'ensemble du programme de sécurité et de conformité Bitwarden est proposée pour votre examen. La solution, le logiciel, l'infrastructure et les processus de sécurité de Bitwarden ont été conçus dès le départ avec une approche de défense en profondeur à plusieurs niveaux.

Le programme de sécurité et de conformité Bitwarden est basé sur le système de gestion de la sécurité de l'information (ISMS) ISO27001. Nous avons défini des politiques qui régissent nos politiques de sécurité et nos processus et nous mettons constamment à jour notre programme de sécurité pour qu'il soit conforme aux exigences légales, industrielles et réglementaires applicables aux services que nous vous fournissons en vertu de notre [Contrat de Conditions de Service](#).

Si vous avez des questions, veuillez [nous contacter](#).