bitwarden | Article du Centre d'Aide

SÉCURITÉ

FAQs de Sécurité

Afficher dans le centre d'aide:
https://bitwarden.com/help/security-faqs/

FAQs de Sécurité

Cet article contient des questions fréquemment posées (FAQ) concernant la sécurité.

Q: Pourquoi devrais-je faire confiance à Bitwarden avec mes mots de passe?

A: Vous pouvez nous faire confiance pour plusieurs raisons :

1. Bitwarden est un logiciel **open source**. Tout notre code source est hébergé sur GitHub et est gratuit pour quiconque souhaite le consulter. Des milliers de développeurs de logiciels suivent les projets de code source de Bitwarden (et vous devriez aussi !).

2. Bitwarden est audité **par des entreprises de sécurité tierce partie réputées** ainsi que par des chercheurs en sécurité indépendants.

3. Bitwarden **ne stocke pas vos mots de passe**. Bitwarden stocke des versions cryptées de vos mots de passe que seul vous pouvez déverrouiller. Vos informations sensibles sont cryptées localement sur votre appareil personnel avant d'être jamais envoyées à nos serveurs cloud.

4. **Bitwarden a une réputation.** Bitwarden est utilisé par des millions d'individus et d'entreprises. Si nous faisions quoi que ce soit de douteux ou de risqué, nous serions hors d'affaires !

Vous ne nous faites toujours pas confiance ? Tu n'es pas obligé. L'open source est magnifique. Vous pouvez facilement héberger vous-même toute la pile Bitwarden. Vous contrôlez votre donnée. En savoir plus ici.

Q: Que se passe-t-il si Bitwarden est piraté ?

A: Bitwarden prend des mesures extrêmes pour garantir que ses sites web, applications et serveurs cloud sont sécurisés. Bitwarden utilise les services gérés de Microsoft Azure pour gérer l'infrastructure et la sécurité des serveurs, plutôt que de le faire directement.

Si pour une raison quelconque Bitwarden était piraté et vos données étaient exposées, vos informations sont toujours protégées grâce à des mesures de cryptage fort et de hachage salé unidirectionnel prises sur les données de votre coffre et votre mot de passe principal.

Q: Bitwarden peut-il voir mes mots de passe?

A: Non.

Vos données sont entièrement cryptées et/ou hachées avant de quitter jamais **votre** appareil local, donc personne de l'équipe Bitwarden ne peut jamais voir, lire, ou inverser l'ingénierie pour accéder à vos vraies données. Les serveurs Bitwarden ne stockent que des données cryptées et hachées. Pour plus d'informations sur la façon dont vos données sont cryptées, voir Cryptage.

Q: Mon mot de passe principal Bitwarden est-il stocké localement ?

A: Non.

Nous ne conservons pas le mot de passe principal stocké localement ou en mémoire. Votre clé de chiffrement (dérivée du mot de passe principal) est conservée en mémoire uniquement lorsque l'application est déverrouillée, ce qui est nécessaire pour déchiffrer les données dans votre coffre. Lorsque le coffre est verrouillé, cette donnée est purgée de la mémoire.

Nous rechargeons également le processus de rendu de l'application après 10 secondes d'inactivité sur l'écran de verrouillage pour nous assurer que toutes les adresses mémoire gérées qui n'ont pas encore été collectées par le ramasse-miettes sont 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 les données cryptées de l'application sont totalement sûres lorsque l'application est dans un état verrouillé.

Q: Que dois-je faire si je ne reconnais pas un nouvel appareil se connectant à Bitwarden?

A: Si l'adresse IP d'un nouvel appareil ne correspond à aucune des adresses IP connues (réseau domestique, réseau de travail, réseau mobile, etc.), changez votre mot de passe principal et assurez-vous que la connexion en deux étapes est activée pour votre compte. Vous

devriez également révoquer les autorisations des sessions depuis la page des **paramètres du compte** de votre coffre web pour forcer la déconnexion sur tous les appareils. Si vous pensez que les éléments de votre coffre pourraient être compromis, vous devriez changer vos mots de passe.

Q: Avec quoi Bitwarden est-il conforme ? Quelles certifications avez-vous ?

A: Bitwarden est conforme aux politiques de sécurité suivantes :

- **RGPD.** Lisez plus ici.
- **CCPA.** Lisez plus ici.
- **HIPAA.** Lisez plus ici.
- **SOC 2 saisir 2.** Lisez plus ici.
- **SOC 3.** Lisez plus ici.

Pour plus d'informations, veuillez visiter notre page Sécurité et Conformité.

Q: Comment Bitwarden répond-il aux exigences de conformité européennes?

A: Bitwarden est conforme au RGPD et utilise des mécanismes de transfert d'informations approuvés, y compris les clauses contractuelles types (CCT) de l'UE conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil approuvé par la décision d'exécution (UE) 2021/914 de la Commission européenne du 4 juin 2021, tel que défini actuellement à l'adresse https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. Pour les clients commerciaux et d'entreprise, Bitwarden peut exécuter l'Accord de Protection des Données de Bitwarden.

Les serveurs cloud de Bitwarden sont actuellement hébergés sur Microsoft Azure aux États-Unis et dans l'Union européenne. Aujourd'hui, Bitwarden sert des millions d'utilisateurs, y compris des clients gouvernementaux et de l'entreprise à travers l'Europe et le monde, avec cette infrastructure.

Pour les clients qui ont besoin d'un contrôle total sur la résidence des données, Bitwarden peut alternativement être hébergé en privé sur votre propre infrastructure.

Toutes les données du coffre stockées dans Bitwarden, qu'elles soient sur le cloud ou auto-hébergées, sont cryptées de bout en bout et ne sont accessibles par personne sauf l'utilisateur de Bitwarden. Avec cette architecture de chiffrement de bout en bout, à connaissance zéro, même Bitwarden ne peut pas accéder à votre donnée.

Pour une liste complète des certifications de sécurité et de conformité de Bitwarden, veuillez visiter https://bitwarden.com/compliance/.

Q: Quels services, bibliothèques ou identifiants de tierce partie sont utilisés dans mon compte Bitwarden ?

A: Dans les applications mobiles, Firebase Cloud Messaging (souvent confondu avec un tracker) est utilisé uniquement pour les notifications push liées à la synchronisation et n'effectue absolument aucune fonction de suivi. Microsoft Visual Studio App Center est utilisé pour le rapport de plantage sur une gamme d'appareils mobiles. Dans le coffre web, les scripts Stripe et PayPal sont utilisés uniquement pour le traitement des paiements sur les pages de paiement.

Pour ceux qui préfèrent exclure toute communication de tiers, Firebase et Microsoft Visual Studio App Center sont complètement supprimés de la construction F-Droid. De plus, désactiver les notifications push sur un serveur Bitwarden auto-hébergé désactivera l'utilisation du serveur de relais de notification.

L'application Android Bitwarden comprend également la possibilité de désactiver le rapport de plantage dans les paramètres.

Bitwarden prend la sécurité et la confidentialité des utilisateurs au sérieux. Bitwarden maintient un chiffrement sécurisé de bout en bout avec zéro connaissance de votre clé de chiffrement. En tant qu'entreprise axée sur l'open source, nous invitons tout le monde à examiner

nos implémentations de bibliothèques à tout moment sur GitHub.

Q: Comment puis-je exiger une connexion en deux étapes pour mon organisation Bitwarden?

R : Utilisez une stratégie d'entreprise incluse dans un abonnement d'organisation Enterprise. Vous pouvez également activer l'intégration Duo MFA pour imposer 2FA/MFA à votre organisation. Pour plus d'informations, consultez Connexion en deux étapes via Duo.

Q: Quelles sont les options de certificat pour une instance auto-hébergée de Bitwarden?

A: Voir Options de Certificat pour une liste complète et des instructions.

Q: Comment Bitwarden vérifie-t-il les modifications de code ?

A: La confiance dans la sécurité de nos systèmes est d'une importance capitale pour Bitwarden. Toutes les modifications de code proposées sont examinées par un ou plusieurs membres non-auteurs de l'équipe avant qu'elles ne puissent être fusionnées dans une base de code. Tout le code passe par plusieurs tests et environnements de QA avant la production. Bitwarden a mis en œuvre un rapport SOC2 pour auditer et valider nos procédures internes. Comme mentionné dans le rapport, notre équipe est soumise à une vérification rigoureuse des antécédents et à des processus d'entretien approfondis. Bitwarden, étant un produit open-source, accueille également l'examen par les pairs de notre code à tout moment. L'équipe de Bitwarden s'efforce de faire tout ce que nous pouvons pour rendre nos utilisateurs à l'aise, et garder leurs données en sécurité.

Q : Combien de temps Bitwarden met-il en cache les informations de session ?

A: Excellente question ! La réponse dépend de l'information particulière et de l'application du client :

- Les sessions de coffre hors ligne expireront après 30 jours.
  - **Sauf** pour les applications client mobile, qui expireront au bout de 90 jours.
- Identification en deux étapes **Se souvenir de moi** les sélections expireront après 30 jours.
- Le cache de synchronisation du Connecteur de Répertoire sera effacé après 30 jours.
- Les invitations de l'organisation expireront après 5 jours. Les clients auto-hébergés peuvent configurer cela en utilisant une variable d'environnement.

Q: Comment puis-je valider la somme de contrôle d'une application Bitwarden ?

A: Tout d'abord, prenez le fichier yaml `le plus récent` pour la version pertinente (par exemple, `latest-linux.yml`) et le package de version correspondant (par exemple, `Bitwarden-1.33.0-amd64.deb`). Générez un hachage SHA512 du package de version téléchargé (par exemple, `sha512sum Bitwarden-1.33.0-amd64.deb`) et convertissez la valeur Hex générée en Base64. Comparez la valeur Base64 calculée à la valeur `sha512:` du fichier yaml pour valider.

Q: Comment puis-je faire une divulgation de sécurité ou un rapport à Bitwarden?

R : Bitwarden estime que travailler avec des chercheurs en sécurité du monde entier est crucial pour assurer la sécurité de nos utilisateurs. Si vous pensez avoir trouvé un problème de sécurité dans notre produit ou service, nous vous encourageons à soumettre un rapport via notre Programme HackerOne. Nous sommes ravis de travailler avec vous pour résoudre le problème rapidement. Apprenez-en davantage sur notre politique de divulgation .

Q: Pourquoi mon coffre web va-t-il à web-vault.pages.dev?

A: `web-vault.pages.dev` est un sous-domaine unique à Bitwarden qui est utilisé par Cloudflare Pages. Cette URL peut apparaître aux utilisateurs lorsque Cloudflare rencontre des problèmes de DNS. Vous devriez toujours être sur vos gardes contre les tentatives de hameçonnage en vérifiant l'URL avant d'entrer votre nom d'utilisateur et votre mot de passe principal, cependant `web-vault.pages.dev` devrait être considéré comme sûr pour se connecter.

Q: Comment puis-je protéger mon compte Bitwarden contre les attaques par force brute ?

A: Une attaque par force brute est lorsque un acteur malveillant parcourt une combinaison de mots de passe faibles et courts dans le but d'obtenir l'accès à votre compte. Bitwarden offre quelques moyens de vous protéger contre ces attaques potentielles :

- Ayez un long et unique mot de passe principal. Bitwarden exige un minimum de 12 caractères pour augmenter la sécurité du compte.
- Configurez 2FA sur tous les comptes Bitwarden pour ajouter une couche de sécurité supplémentaire.
- Bitwarden exigera une vérification CAPTCHA après 9 tentatives d'identifiant échouées depuis un appareil inconnu.

Questions concernant des applications spécifiques du client

Q: Quelles données Bitwarden utilise-t-il des applications client?

A: Bitwarden utilise des données administratives pour vous fournir le service Bitwarden. Comme indiqué par certains rapports de **Confidentialité des applications**, les utilisateurs fournissent les informations suivantes lors de la création de compte :

- Votre nom (facultatif).
- Votre adresse de courriel (utilisée pour la vérification du courriel, l'administration du compte et la communication entre vous et Bitwarden).

De plus, un GUID spécifique à l'appareil **généré par Bitwarden** (parfois appelé ID de l'appareil) est attribué à votre appareil. Ce GUID est utilisé pour vous alerter lorsqu'un nouvel appareil se connecte à votre coffre.

Q : Pouvez-vous expliquer la sécurité des applications Electron ?

A: Un article souvent partagé suggère un défaut avec les applications électroniques, cependant l'attaque référencée nécessite qu'un utilisateur ait une machine compromise, ce qui bien sûr permettrait à un attaquant malveillant de compromettre les données sur cette machine. Tant que vous n'avez aucune raison de croire que l'appareil que vous utilisez a été compromis, vos données sont en sécurité.

Q: Comment Bitwarden sécurise-t-il les extensions de navigateur?

A: Les extensions sont sûres à utiliser si elles sont correctement développées. En raison de la nature du fonctionnement des extensions de navigateur, il y a toujours une chance qu'un bug apparaisse. Nous prenons un soin et une prudence extrêmes lorsque nous développons nos extensions et add-ons, nous restons à l'affût de tout ce qui se passe dans l'industrie, et nous menons des audits de sécurité pour garder un œil sur tout.

Q: Pour quoi l'extension du navigateur demande-t-elle une autorisation ?

A: Lors de l'installation, l'extension du navigateur demandera l'autorisation d'accéder à votre presse-papiers afin d'utiliser la fonction de nettoyage programmé du presse-papiers (accessible dans le menu **Options**).

Lorsque cette **fonctionnalité optionnelle** est activée, le nettoyage du presse-papiers effacera toutes les entrées Bitwarden effectuées par ou remplies sur un intervalle configurable. L'accès au presse-papiers permet à Bitwarden de faire cela sans supprimer un élément du presse-papiers non associé à l'application Bitwarden en vérifiant le dernier élément copié par rapport au dernier élément copié de votre coffre. Veuillez noter, cette fonctionnalité est **désactivée par défaut**.

Q: Quelles autorisations d'application sont demandées par l'application mobile?

A: Les applications Bitwarden Android et iOS peuvent demander les autorisations suivantes pendant que vous utilisez l'application :

Permission	Raison
Autoriser Bitwarden à prendre des photos et à enregistrer des vidéos ?	Pour scanner les codes QR pour l'identifiant en deux étapes ou l'authentification Bitwarden.
Autoriser Bitwarden à accéder aux photos et aux médias sur votre appareil ?	Pour créer des pièces jointes ou des Sends à partir d'un fichier enregistré sur votre appareil.

Les autorisations de base supplémentaires requises par Bitwarden sont répertoriées dans le Google Play Store.

Q: Pourquoi l'extension du navigateur a-t-elle besoin de l'autorisation nativeMessaging?

A: La version 1.48.0 de l'extension du navigateur permet le déverrouillage biométrique pour les extensions de navigateur.

Cette autorisation, également connue sous le nom de `nativeMessaging`, est sûre à accepter et permet à l'extension du navigateur de communiquer avec l'application de bureau Bitwarden, ce qui est nécessaire pour activer le déverrouillage avec la biométrie.

Notez que lorsque votre navigateur se met à jour vers cette version, on peut vous demander d'accepter une nouvelle autorisation appelée "communiquer avec des applications natives coopératives" (dans les navigateurs basés sur Chromium), ou "échanger des messages avec des programmes autres que Firefox". Si vous n'acceptez pas cette autorisation, l'extension restera désactivée.

Q: Bitwarden est-il conforme à FIPS ?

A: Bitwarden utilise des bibliothèques et de la cryptographie conformes à FIPS 140, et la plupart des installations FIPS 140 de Bitwarden tirent parti de l'option auto-hébergée pour faciliter les évaluations (par exemple, la certification du modèle de maturité cybernétique). La plateforme Bitwarden n'a effectué aucune certification FIPS à ce jour. Les demandes de renseignements sont les bienvenues via la page contactez-nous.

Q: Puis-je restreindre l'accès à Bitwarden à certains appareils ?

A: En utilisant l'auto-hébergement, vous pouvez utiliser des configurations de pare-feu personnalisées et NGINX ainsi que le contrôle d'accès VPN/VLAN pour déterminer les types d'appareils et/ou l'accès à la couche réseau pour votre instance Bitwarden. Vous pouvez également utiliser d'autres outils tels que des certificats au niveau de l'appareil pour contrôler l'accès spécifique de l'appareil à l'instance Bitwarden.

Q: Bitwarden a-t-il une application portable ?

A: Oui! L'application de bureau Bitwarden est disponible pour Windows sous forme d'un `.exe` portable qui peut être téléchargé ici. L'application portable convient bien aux environnements ou scénarios **toujours hors ligne** où la mise à jour automatique de l'application n'est pas souhaitée. L'application portable **ne se mettra pas à jour elle-même**.

Q: Les options d'accès au site interféreront-elles avec l'extension Bitwarden du navigateur?

A: Les paramètres d'accès au site pour l'extension de navigateur Bitwarden doivent être réglés sur **Sur tous les sites**, ou sur **Sur des sites spécifiques** avec le serveur Bitwarden ajouté à la liste, pour que l'extension de navigateur fonctionne correctement. Définir l'accès au site sur **Au clic** limitera la capacité de Bitwarden à récupérer des données du serveur Bitwarden, ce qui est fondamentalement nécessaire pour enregistrer ou mettre à jour les identifiants.