Sécurité et conformité de Bitwarden

Bitwarden imagine un monde où personne n'est piraté. Cela se traduit par un engagement ferme de Bitwarden en faveur de la sécurité, de la protection de la vie privée et du respect des normes internationales.

Obtenez la vue interactive complète à
https://bitwarden.com/fr-fr/compliance/

bitwarden

Protection de la vie privée et sécurité des produits

Audit par un tiers

Des experts externes examinent régulièrement les produits Bitwarden, ce qui garantit une sécurité solide et fiable.

Cryptage de bout en bout à connaissance nulle

Sécurisé par un cryptage puissant, personne n'a accès à vos informations de coffre-fort, pas même Bitwarden !

Respect des normes en matière de protection de la vie privée et de sécurité

Faites approuver rapidement les produits Bitwarden par vos équipes informatiques et de sécurité internes en respectant les normes de l'industrie.

Confiance et transparence grâce à l'open source

Une base de code source ouverte permet à la sécurité des produits Bitwarden d'être facilement vérifiée par des chercheurs en sécurité indépendants, des entreprises de sécurité renommées et la communauté Bitwarden.

Une architecture open source fiable

La base de code Bitwarden sur GitHub est régulièrement examinée et vérifiée par des millions de passionnés de sécurité et de membres actifs de la communauté Bitwarden.

Évaluation du code source

Bitwarden réalise des audits annuels du code source et des tests de pénétration pour chaque client, y compris pour le web, les extensions de navigateur et les ordinateurs de bureau - en plus de l'application principale et de la bibliothèque.

Évaluation de la sécurité du réseau

Bitwarden procède chaque année à des évaluations de la sécurité du réseau et à des tests de pénétration par des sociétés de sécurité réputées.

HackerOne bug bounty

Les chercheurs indépendants en matière de sécurité sont récompensés lorsqu'ils signalent des problèmes de sécurité potentiels.

Préserver la sécurité de vos données

En tant que gestionnaire de mots de passe et fournisseur de sécurité, Bitwarden utilise des mesures de sécurité et des méthodes de cryptage fiables pour protéger les données des utilisateurs.

Cryptage de bout en bout à connaissance nulle

Bitwarden utilise un cryptage de bout en bout pour toutes les données du coffre-fort, que seul votre mot de passe principal peut décrypter. Avec une architecture à zéro connaissance, Bitwarden n'a pas la capacité de lire les données cryptées dans votre coffre-fort.

Cryptage multifactoriel

Le cryptage multifactoriel est une couche supplémentaire de cryptage qui protège vos informations stockées. Il est donc pratiquement impossible pour un acteur malveillant de pénétrer dans votre coffre-fort, même s'il parvenait à accéder à vos données cryptées.

Options d'auto-hébergement

Choisissez de déployer et de gérer Bitwarden sur place dans votre réseau privé ou votre infrastructure avec des options d'auto-hébergement. L'auto-hébergement permet aux clients de contrôler plus précisément les informations qu'ils stockent.

Conformité de sécurité

Bitwarden adhère aux normes de sécurité de l'industrie avec les certifications SOC2 et SOC3 et la conformité HIPAA.

SOC2 et SOC3

Les contrôles des systèmes et des organisations (SOC) comprennent un ensemble de cadres de contrôle utilisés pour valider les systèmes et les politiques de sécurité d'une organisation. Bitwarden est certifié SOC2 Type II et SOC3.

Rapports SOC2 disponibles sur demande.

HIPAA

Bitwarden est conforme à la loi HIPAA et fait l'objet d'audits annuels par des tiers pour s'assurer de la conformité à la règle de sécurité HIPAA.

ISO 27001

Bitwarden est certifié ISO 27001 et se conforme aux contrôles ISO 27001 relatifs à la sécurité des données.

Respect de la vie privée

Bitwarden accorde la priorité à la protection des données personnelles des utilisateurs et au respect des principales normes de protection de la vie privée dans le monde entier.

CCPA ET CPRA

Bitwarden est conforme à la loi californienne sur la protection des consommateurs (CCPA) et à la loi californienne sur les droits à la vie privée (CPRA).

RGPD

Bitwarden se conforme au GDPR, aux règles actuelles de l'UE en matière de protection des données et aux clauses contractuelles types (CCN) de l'UE.

Data Privacy Framework

Bitwarden est conforme à la loi californienne sur la protection des consommateurs (CCPA) et à la loi californienne sur les droits à la vie privée (CPRA).

Respectez les normes de conformité en matière de sécurité avec Bitwarden

Bitwarden est plus qu'un gestionnaire de mots de passe ; c'est un outil fondamental pour atteindre et maintenir la conformité de l'industrie avec les normes de sécurité clés. Grâce au partage sécurisé, aux capacités de surveillance, à la gestion centralisée et à la protection robuste des données, Bitwarden renforce la position de votre organisation en matière de cybersécurité afin de répondre aux besoins de conformité.

ISO 27001

La norme internationale ISO 27001 pose les bases de la création, du maintien et du développement des systèmes de gestion de la sécurité de l'information (SGSI), y compris la gestion des données.

SOC 2

Les rapports Service Organization Control 2 (SOC 2) sont souvent demandés par les clients et les partenaires commerciaux des fournisseurs de solutions externalisées. Les entreprises qui souhaitent se conformer à la norme SOC 2 peuvent s'appuyer sur un gestionnaire de mots de passe conforme à la norme SOC 2 pour répondre aux exigences.

NERC

La North American Electric Reliability Corporation (NERC) est un organisme de réglementation international à but non lucratif qui a pour mission d'établir des normes de conformité permettant de réduire les risques pour le réseau électrique et les systèmes d'alimentation desservant des centaines de millions de personnes aux États-Unis, au Canada et dans une partie du Mexique.

NIS2

NIS2 est un ensemble d'exigences visant à sécuriser les réseaux et les systèmes d'information dans l'UE. La directive impose aux entreprises considérées comme des opérateurs de services essentiels de mettre en œuvre des mesures appropriées pour renforcer la cybersécurité et se conformer aux obligations légales.

Cadre de Cybersecurité du NIST

Le National Institute of Standards and Technology (NIST) fournit des conseils et des bonnes pratiques aux organisations, afin d'aider les entreprises, les organisations à but non lucratif et les autres institutions du secteur privé à améliorer la gestion des risques liés à la cybersécurité.

Modèle de maturité de la gestion des mots de passe

Ce cadre aide les organisations à comprendre le niveau de maturité de leur gestionnaire de mots de passe - sur la base de leurs opérations actuelles - et à identifier les étapes nécessaires pour renforcer leur sécurité et améliorer leur classification existante.

SOX

La conformité à la loi Sarbanes-Oxley (SOX) implique le respect d'un ensemble d'exigences de sécurité conçues pour garantir l'intégrité des rapports financiers.

FAQ

- **L'équipe Bitwarden peut-elle voir mes mots de passe ?**

  Non.

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

  En savoir plus >

- **Comment assurez-vous la sécurité des serveurs en nuage ?**

  Bitwarden prend des mesures extrêmes pour s'assurer que ses sites web, ses applications et ses serveurs en nuage 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.

  En savoir plus >

- **Bitwarden fait-il l'objet d'un audit ?**

  Bitwarden effectue régulièrement des audits de sécurité complets avec des sociétés de sécurité renommées. Ces audits annuels comprennent des évaluations du code source et des tests de pénétration sur les IP, les serveurs et les applications web de Bitwarden.

  En savoir plus >

- **Que se passe-t-il si Bitwarden est piraté ?**

  Si, pour une raison quelconque, Bitwarden devait être piraté et que vos données étaient exposées, vos informations seraient toujours protégées grâce à un cryptage fort et à des mesures de hachage salé à sens unique prises sur les données de votre coffre-fort et votre mot de passe principal.

  En savoir plus >

- Où mes données sont-elles stockées dans le nuage ?

  Bitwarden traite et stocke toutes les données du coffre-fort en toute sécurité dans le nuage Microsoft Azure aux États-Unis ou dans l'UE, en utilisant des services gérés par l'équipe de Microsoft. Comme Bitwarden n'utilise que des offres de service fournies par Azure, il n'y a pas d'infrastructure de serveur à gérer et à entretenir. La disponibilité, l'évolutivité, les mises à jour de sécurité et les garanties sont soutenues par Microsoft et son infrastructure en nuage. Consultez la documentation Microsoft Azure Compliance Offerings pour plus de détails.

  En savoir plus >

- Pourquoi devrais-je confier mes mots de passe à Bitwarden ?

  Vous pouvez nous faire confiance pour plusieurs raisons :

  1. Bitwarden est un logiciel **libre**. L'ensemble de notre code source est hébergé sur GitHub et peut être consulté gratuitement par tous. Des milliers de développeurs de logiciels suivent les projets de code source de Bitwarden (et vous devriez le faire aussi !).

  2. Bitwarden est **contrôlé par des sociétés de sécurité tierces 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 vous seul pouvez déverrouiller. Vos informations sensibles sont cryptées localement sur votre appareil personnel avant d'être envoyées sur nos serveurs en nuage.

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

  Vous ne nous faites toujours pas confiance ? Vous n'êtes pas obligé de le faire. L'open source, c'est magnifique. Vous pouvez facilement héberger vous-même l'ensemble de la pile Bitwarden. Vous contrôlez vos données.

  En savoir plus >

- Bitwarden utilise-t-il un hachage salé pour mon mot de passe ?

  PBKDF2 SHA-256 est utilisé pour dériver la clé de cryptage à partir de votre mot de passe principal, mais vous pouvez également choisir Argon2. Bitwarden s'occupe de saler et de hacher votre mot de passe principal avec votre adresse e-mail **localement**, avant de le transmettre à nos serveurs. Lorsqu'un serveur Bitwarden reçoit le mot de passe haché, il est à nouveau salé à l'aide d'une valeur aléatoire cryptographiquement sécurisée, à nouveau haché et stocké dans notre base de données.

  En savoir plus >

- Comment mes données sont-elles transmises et stockées en toute sécurité sur les serveurs de Bitwarden ?

  Bitwarden crypte et/ou hachure **toujours** vos données sur votre appareil local avant qu'elles ne soient envoyées vers des serveurs en nuage pour y être stockées. **Les serveurs de Bitwarden ne sont utilisés que pour stocker des données cryptées.** Pour plus d'informations, voir Stockage.

  En savoir plus >

- Quel est le cryptage utilisé ?

  Bitwarden utilise le cryptage AES-CBC 256 bits pour les données de votre coffre-fort, et PBKDF2 SHA-256 ou Argon2 pour dériver votre clé de cryptage.

  En savoir plus >

- **Quelles sont les informations cryptées ?**

  Toutes les données du coffre-fort sont cryptées par Bitwarden avant d'être stockées où que ce soit. Pour en savoir plus, voir Cryptage.

  En savoir plus >

- **Où mes données sont-elles stockées sur mon ordinateur/appareil ?**

  Les données stockées sur votre ordinateur/appareil sont cryptées et ne sont décryptées que lorsque vous déverrouillez votre chambre forte. Les données décryptées sont stockées **en mémoire** uniquement et ne sont **jamais écrites sur un support persistant**.

  En savoir plus >