bitwarden | Artikel Helpcentrum

BEVEILIGING

Veelgestelde vragen over beveiliging

Weergeven in het Helpcentrum:
https://bitwarden.com/help/security-faqs/

Veelgestelde vragen over beveiliging

Dit artikel bevat veelgestelde vragen (FAQ's) over beveiliging.

V: Waarom zou ik mijn wachtwoorden aan Bitwarden toevertrouwen?

A: Je kunt ons om een paar redenen vertrouwen:

1. Bitwarden is **open source** software. Al onze broncode wordt gehost op GitHub en is voor iedereen vrij om te bekijken. Duizenden softwareontwikkelaars volgen de broncodeprojecten van Bitwarden (en dat zou u ook moeten doen!).

2. Bitwarden wordt gecontroleerd **door gerenommeerde externe beveiligingsbedrijven** en onafhankelijke beveiligingsonderzoekers.

3. Bitwarden slaat **uw wachtwoorden niet op**. Bitwarden slaat versleutelde versies van je wachtwoorden op die alleen jij kunt ontgrendelen. Je gevoelige informatie wordt lokaal versleuteld op je persoonlijke apparaat voordat het ooit naar onze cloudservers wordt verzonden.

4. **Bitwarden heeft een reputatie.** Bitwarden wordt gebruikt door miljoenen particulieren en bedrijven. Als we iets dubieus of riskant zouden doen, zouden we failliet zijn!

Vertrouw je ons nog steeds niet? Dat hoeft niet. Open source is prachtig. Je kunt de hele Bitwarden-stack gemakkelijk zelf hosten. U beheert uw gegevens. Lees hier meer.

V: Wat gebeurt er als Bitwarden wordt gehackt?

A: Bitwarden neemt extreme maatregelen om ervoor te zorgen dat haar websites, applicaties en cloudservers veilig zijn. Bitwarden maakt gebruik van Microsoft Azure managed services om de serverinfrastructuur en beveiliging te beheren, in plaats van dit zelf te doen.

Als Bitwarden om wat voor reden dan ook gehackt zou worden en uw gegevens bloot zouden komen te liggen, zijn uw gegevens nog steeds beschermd dankzij de sterke versleuteling en one-way salted hashing-maatregelen die zijn genomen op uw kluisgegevens en hoofdwachtwoord.

V: Kan Bitwarden mijn wachtwoorden zien?

A: Nee.

Uw gegevens zijn volledig versleuteld en/of gehasht voordat ze **uw** lokale apparaat verlaten, dus niemand van het Bitwarden-team kan ooit uw echte gegevens zien, lezen of reverse-engineeren. Bitwarden-servers slaan alleen versleutelde en gehashte gegevens op. Zie Versleuteling voor meer informatie over hoe je gegevens worden versleuteld.

V: Wordt mijn Bitwarden-hoofdwachtwoord lokaal opgeslagen?

A: Nee.

We bewaren het hoofdwachtwoord niet lokaal of in het geheugen. Je coderingssleutel (afgeleid van het hoofdwachtwoord) wordt alleen in het geheugen bewaard als de app ontgrendeld is, wat nodig is om gegevens in je kluis te ontsleutelen. Wanneer de kluis wordt vergrendeld, worden deze gegevens uit het geheugen gewist.

We herladen ook het renderer proces van de applicatie na 10 seconden van inactiviteit op het vergrendelscherm om er zeker van te zijn dat alle beheerde geheugenadressen die nog niet zijn afgehaald, worden gewist. We doen ons best om ervoor te zorgen dat alle gegevens die in het geheugen kunnen staan om de applicatie te laten werken, alleen in het geheugen blijven zolang je ze nodig hebt en dat het geheugen wordt opgeschoond wanneer de applicatie wordt vergrendeld. We beschouwen de versleutelde gegevens van de applicatie als volledig veilig zolang de applicatie zich in een vergrendelde toestand bevindt.

V: Wat moet ik doen als ik een nieuw apparaat dat inlogt op Bitwarden niet herken?

A: Als het IP-adres van een nieuw apparaat niet overeenkomt met bekende IP-adressen (thuisnetwerk, werknetwerk, mobiel netwerk, enzovoort), wijzig dan je hoofdwachtwoord en zorg ervoor dat tweestapsaanmelding is ingeschakeld voor je account. Je moet ook sessies deautoriseren op de pagina **Accountinstellingen** van je webkluis om uitloggen op alle apparaten te forceren. Als je denkt dat je kluisitems gecompromitteerd zijn, moet je je wachtwoorden wijzigen.

V: Waar voldoet Bitwarden aan? Welke certificaten heb je?

A: Bitwarden voldoet aan de volgende beleidsregels:

- **GDPR.** Lees hier meer.
- **CCPA.** Lees hier meer.
- **HIPAA.** Lees hier meer.
- **SOC 2 Type 2.** Lees hier meer.
- **SOC 3.** Lees hier meer.

Ga voor meer informatie naar onze pagina over beveiliging en naleving.

V: Hoe voldoet Bitwarden aan de Europese compliance-eisen?

A: Bitwarden voldoet aan de GDPR en maakt gebruik van goedgekeurde mechanismen voor informatieoverdracht, waaronder EU-standaardcontractbepalingen (SCC's) krachtens Verordening (EU) 2016/679 van het Europees Parlement en de Raad, goedgekeurd bij Uitvoeringsbesluit (EU) 2021/914 van de Europese Commissie van 4 juni 2021, zoals momenteel uiteengezet op https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. Voor zakelijke en zakelijke klanten kan Bitwarden de Bitwarden Gegevensbeschermingsovereenkomst uitvoeren.

Bitwarden cloud servers worden momenteel gehost op Microsoft Azure binnen de Verenigde Staten en de Europese Unie. Vandaag de dag bedient Bitwarden miljoenen gebruikers, waaronder overheidsklanten en zakelijke klanten in heel Europa en de wereld, met deze infrastructuur.

Voor klanten die volledige controle willen over het verblijf van gegevens, kan Bitwarden ook privé worden gehost op uw eigen infrastructuur.

Alle kluisgegevens die zijn opgeslagen in Bitwarden, ongeacht of ze in de cloud of zelf gehost zijn, zijn end-to-end versleuteld en voor niemand toegankelijk behalve voor de Bitwarden-gebruiker. Met deze end-to-end, zero knowledge encryptiearchitectuur heeft zelfs Bitwarden geen toegang tot uw gegevens.

Ga voor een volledige lijst met Bitwarden certificeringen voor beveiliging en compliance naar https://bitwarden.com/compliance/.

V: Welke diensten, bibliotheken of identifiers van derden worden gebruikt in mijn Bitwarden-account?

A: In de mobiele apps wordt Firebase Cloud Messaging (vaak verward met een tracker) alleen gebruikt voor pushmeldingen met betrekking tot synchronisatie en voert het absoluut geen trackingfuncties uit. Microsoft Visual Studio App Center wordt gebruikt voor crashrapportage op een reeks mobiele apparaten. In de webkluis worden Stripe- en PayPal-scripts alleen op betaalpagina's gebruikt voor het verwerken van betalingen.

Voor degenen die liever alle communicatie van derden uitsluiten, zijn Firebase en Microsoft Visual Studio App Center volledig verwijderd uit de F-Droid build. Daarnaast zal het uitschakelen van pushmeldingen op een zelf gehoste Bitwarden-server het gebruik van de pushrelay-server uitschakelen.

De Bitwarden Android-applicatie bevat ook de mogelijkheid om crashrapportage uit te schakelen onder Instellingen.

Bitwarden neemt de veiligheid en privacy van gebruikers serieus. Bitwarden handhaaft veilige end-to-end-encryptie zonder enige kennis van uw encryptiesleutel. Als een bedrijf dat zich richt op open source, nodigen we iedereen uit om onze bibliotheekimplementaties op elk gewenst moment te bekijken op GitHub.

V: Hoe verplicht ik tweestapslogin voor mijn Bitwarden-organisatie?

A: Gebruik een bedrijfsbeleid, inbegrepen bij een Enterprise organisatieabonnement. U kunt ook Duo MFA integratie inschakelen om 2FA/MFA af te dwingen voor uw organisatie. Voor meer informatie, zie Tweevoudig inloggen via Duo.

V: Wat zijn de certificaatopties voor een zelf gehoste instantie van Bitwarden?

A: Zie Certificaatopties voor een volledige lijst en instructies.

V: Hoe vetrouwt Bitwarden codewijzigingen?

A: Vertrouwen in de veiligheid van onze systemen is van het grootste belang voor Bitwarden. Alle voorgestelde codewijzigingen worden beoordeeld door een of meer niet-auteur leden van het team voordat ze kunnen worden samengevoegd in een codebase. Alle code doorloopt meerdere test- en QA-omgevingen voordat deze in productie gaat. Bitwarden heeft een SOC2-rapport geïmplementeerd om onze interne procedures te controleren en valideren. Zoals vermeld in het rapport wordt ons team onderworpen aan strenge achtergrondcontroles en grondige sollicitatieprocessen. Omdat Bitwarden een open-sourceproduct is, is peer-review van onze code altijd welkom. Het team van Bitwarden doet er alles aan om het onze gebruikers naar de zin te maken en hun gegevens veilig te houden.

V: Hoe lang slaat Bitwarden sessiegegevens op?

A: Geweldige vraag! Het antwoord hangt af van de specifieke informatie en de toepassing van de klant:

- Offline kluissessies verlopen na 30 dagen.
  - **Behalve** voor mobiele clienttoepassingen, die na 90 dagen verlopen.
- Twee-staps login **Onthoud mij** selecties verlopen na 30 dagen.
- De synchronisatiecache van Directory Connector wordt na 30 dagen gewist.
- Uitnodigingen voor organisaties verlopen na 5 dagen. Zelf gehoste klanten kunnen dit configureren met behulp van een omgevingsvariabele.

V: Hoe valideer ik de checksum van een Bitwarden-app?

A: Pak eerst het `nieuwste` yaml-bestand voor de betreffende release (bijvoorbeeld `latest-linux.yml`) en het bijbehorende release-pakket (bijvoorbeeld `Bitwarden-1.33.0-amd64.deb`). Genereer een SHA512 hash van het gedownloade release-pakket (bijvoorbeeld `sha512sum Bitwarden-1.33.0-amd64.deb`) en converteer de gegenereerde Hex-waarde naar Base64. Vergelijk de berekende Base64-waarde met de `sha512:` waarde uit het yaml-bestand om te valideren.

V: Hoe maak ik een beveiligingsmelding of -rapport aan Bitwarden?

A: Bitwarden gelooft dat samenwerking met beveiligingsonderzoekers over de hele wereld cruciaal is om onze gebruikers veilig te houden. Als u denkt dat u een beveiligingsprobleem in ons product of onze service hebt gevonden, moedigen we u aan om een rapport in te dienen via ons HackerOne-programma. We werken graag met je samen om het probleem snel op te lossen. Lees meer over ons openbaarmakingsbeleid.

V: Waarom gaat mijn webvault naar web-vault.pages.dev?

A: `web-vault.pages.dev` is een subdomein dat uniek is voor Bitwarden en dat wordt gebruikt door Cloudflare Pages. Deze URL kan verschijnen voor gebruikers wanneer Cloudflare problemen heeft met DNS. Je moet altijd op je hoede zijn voor phishingpogingen door de URL te controleren voordat je je gebruikersnaam en hoofdwachtwoord invoert, maar `web-vault.pages.dev` zou als veilig moeten worden beschouwd om op in te loggen.

V: Hoe kan ik mijn Bitwarden-account beschermen tegen brute-force-aanvallen?

A: Bij een brute-forceaanval doorloopt een kwaadwillende een combinatie van zwakke en korte wachtwoorden in een poging om toegang te krijgen tot je account. Bitwarden biedt een aantal manieren om jezelf te beschermen tegen deze potentiële aanvallen:

- Zorg voor een lang en uniek hoofdwachtwoord. Bitwarden vereist een minimum van 12 tekens om de veiligheid van het account te verhogen.
- Stel 2FA in op alle Bitwarden-accounts om een extra beveiligingslaag toe te voegen.
- Bitwarden vraagt om CAPTCHA-verificatie na 9 mislukte inlogpogingen vanaf een onbekend apparaat.

Vragen over specifieke apps voor klanten

V: Welke gegevens gebruikt Bitwarden van klantapplicaties?

A: Bitwarden gebruikt administratieve gegevens om de Bitwarden-service aan u te kunnen leveren. Zoals aangegeven in sommige **App Privacy** rapporten, verstrekken gebruikers de volgende informatie bij het aanmaken van een account:

- Je naam (optioneel).
- Uw e-mailadres (gebruikt voor e-mailverificatie, accountadministratie en communicatie tussen u en Bitwarden).

Daarnaast wordt een **door Bitwarden gegenereerde** apparaatspecifieke GUID (ook wel apparaat-ID genoemd) toegewezen aan uw apparaat. Deze GUID wordt gebruikt om je te waarschuwen wanneer een nieuw apparaat zich aanmeldt bij je kluis.

V: Kunt u de beveiliging van elektron-apps uitleggen?

A: Een vaak gedeeld artikel suggereert een fout in elektron-apps, maar de aanval waarnaar wordt verwezen vereist dat een gebruiker een gecompromitteerde machine heeft, wat een kwaadwillende aanvaller natuurlijk in staat zou stellen om gegevens op die machine te compromitteren. Zolang je geen reden hebt om aan te nemen dat het apparaat dat je gebruikt gecompromitteerd is, zijn je gegevens veilig.

V: Hoe beveiligt Bitwarden browserextensies?

A: Extensies zijn veilig om te gebruiken als ze correct zijn ontwikkeld. Door de aard van de werking van browserextensies is er altijd een kans op een bug. We gaan uiterst zorgvuldig en voorzichtig te werk bij het ontwikkelen van onze extensies en add-ons, we houden onze ogen en oren open voor alles wat er gaande is in de branche en we voeren beveiligingsaudits uit om alles goed in de gaten te houden.

V: Waar vraagt de browserextensie toestemming voor?

A: Bij de installatie vraagt de browserextensie toestemming om toegang te krijgen tot je klembord om de geplande functie voor het wissen van het klembord te kunnen gebruiken (te vinden in het menu **Opties**).

Als deze **optionele functie** is ingeschakeld, wist het klembord alle Bitwarden-items die zijn gemaakt door of gevuld met een instelbaar interval. Met toegang tot het klembord kan Bitwarden dit doen zonder een klemborditem te verwijderen dat niet is gekoppeld aan de Bitwarden-toepassing door het laatst gekopieerde item te vergelijken met het laatst gekopieerde item uit uw kluis. Let op, deze functie is **standaard uitgeschakeld**.

V: Om welke app-toestemmingen vraagt de mobiele app?

A: Bitwarden Android- en iOS-apps kunnen tijdens het gebruik van de app om de volgende toestemmingen vragen:

Toestemming	Reden
Bitwarden toestaan foto's en video's te maken?	QR-codes scannen voor authenticatie in twee stappen of Bitwarden.
Bitwarden toegang geven tot foto's en media op uw apparaat?	Om bijlagen te maken of te verzenden vanuit een bestand dat op uw apparaat is opgeslagen.

Aanvullende basismachtigingen die nodig zijn voor Bitwarden staan vermeld in de Google Play-winkel.

V: Waarom heeft de browserextensie toestemming nodig voor nativeMessaging?

A: Versie 1.48.0 van de browserextensie maakt biometrische ontgrendeling voor browserextensies mogelijk.

Deze toestemming, ook wel bekend als `nativeMessaging`, is veilig om te accepteren en zorgt ervoor dat de browserextensie kan communiceren met de Bitwarden desktop app, die nodig is om ontgrendeling met biometrie mogelijk te maken.

Merk op dat wanneer uw browser naar deze versie wordt bijgewerkt, u mogelijk wordt gevraagd een nieuwe toestemming te accepteren genaamd "communiceren met samenwerkende native applicaties" (in Chromium-gebaseerde browsers), of "berichten uitwisselen met andere programma's dan Firefox". Als je deze toestemming niet aanvaardt, blijft de extensie uitgeschakeld.

V: Is Bitwarden FIPS-compliant?

A: Bitwarden gebruikt FIPS 140-conforme bibliotheken en cryptografie, en de meeste FIPS 140-installaties van Bitwarden maken gebruik van de self-hostingoptie om evaluaties (bijvoorbeeld Cyber Maturity Model Certification) eenvoudiger te maken. Het Bitwarden platform heeft op dit moment nog geen FIPS certificeringen uitgevoerd. Vragen zijn welkom via de contactpagina.

V: Kan ik de toegang tot Bitwarden beperken tot bepaalde apparaten?

A: Bij self-hosting kunt u aangepaste firewall- en NGINX-configuraties gebruiken, evenals VPN/VLAN-toegangsbeheer om de apparaattypen en/of netwerklaagtoegang voor uw Bitwarden-instantie te bepalen. U kunt ook andere hulpmiddelen gebruiken, zoals certificaten op apparaatniveau, om de toegang van specifieke apparaten tot de Bitwarden-instantie te regelen.

V: Heeft Bitwarden een draagbare applicatie?

A: Ja! De Bitwarden desktop app is beschikbaar voor Windows als een portable `.exe` die je hier kunt downloaden. De draagbare app is zeer geschikt voor omgevingen **die altijd offline zijn** of scenario's waarin het automatisch bijwerken van de app niet gewenst is. De draagbare app **werkt zichzelf niet bij**.

V: Kan de Bitwarden-browserextensie de toegang tot de site blokkeren?

A: Om de browserextensie goed te laten werken, moeten de site-toegangsinstellingen voor de Bitwarden-browserextensie worden ingesteld op **Op alle sites**, of op **Op specifieke sites** met de Bitwarden-server toegevoegd aan de lijst. Door site-toegang in te stellen op **Aanklikken** wordt de mogelijkheid van Bitwarden om gegevens op te halen van de Bitwarden-server beperkt, wat in principe nodig is om referenties op te slaan of bij te werken.