

Bitwarden Beveiliging en naleving

Bitwarden ziet een wereld voor zich waarin niemand wordt gehackt. Dit wordt weerspiegeld in een standvastig streven van Bitwarden naar veiligheid, privacy en naleving van internationale normen.

Bekijk de volledige interactieve weergave op <https://bitwarden.com/nl-nl/compliance/>

Bitwarden privacy en productbeveiliging

Door derden gecontroleerd

Externe experts beoordelen Bitwarden producten regelmatig, waardoor een sterke en betrouwbare beveiliging wordt gegarandeerd.

Nul-kennis, end-to-end encryptie

Beveiligd met sterke encryptie, heeft niemand toegang tot uw kluisgegevens, zelfs Bitwarden niet!

Voldoet aan privacy- en beveiligingsstandaarden

Laat Bitwarden producten snel goedkeuren door uw interne IT- en beveiligingsteams met compliance met de industrie.

Vertrouwen en transparantie aangedreven door open source

Dankzij de open source codebase kan de beveiliging van Bitwarden producten eenvoudig worden gecontroleerd door onafhankelijke beveiligingsonderzoekers, bekende beveiligingsbedrijven en de Bitwarden gemeenschap.

Vertrouwde open source-architectuur

De Bitwarden-codebase op GitHub wordt regelmatig beoordeeld en gecontroleerd door miljoenen beveiligingsenthousiastelingen en actieve leden van de Bitwarden-community.

Beoordeling van broncode

Bitwarden voert jaarlijks broncode-audits en penetratietests uit voor elke klant, inclusief web, browserextensie en desktop – naast de kernapplicatie en –bibliotheek.

Beoordeling van netwerkbeveiliging

Bitwarden voert jaarlijkse netwerkbeveiligingsbeoordelingen en penetratietests uit door gerenommeerde beveiligingsbedrijven.

HackerOne bug bounty

Onafhankelijke beveiligingsonderzoekers worden beloond voor het indienen van potentiële beveiligingsproblemen.

Uw gegevens veilig bewaren

Als uw wachtwoordbeheerder en leverancier van wachtwoordbeveiliging maakt Bitwarden gebruik van vertrouwde beveiligingsmaatregelen en versleutelingsmethoden om gebruikersgegevens te beschermen.

Nul-kennis, end-to-end encryptie

Bitwarden gebruikt end-to-end versleuteling voor alle kluisgegevens, die alleen door je hoofdwachtwoord kunnen worden ontsleuteld. Met een zero-knowledge architectuur heeft Bitwarden niet de mogelijkheid om versleutelde gegevens in uw kluis te lezen.

Multifactor encryptie

Multifactor-encryptie is een extra encryptielaag die je opgeslagen informatie beschermt. Dit maakt het praktisch onmogelijk voor een slechte speler om in te breken in je kluis, zelfs als ze toegang zouden krijgen tot je versleutelde kluisgegevens.

Opties voor zelf hosten

Kies ervoor om Bitwarden on-premises te implementeren en te beheren in uw eigen netwerk of infrastructuur met self-hosting opties. Met self-hosting hebben klanten meer gedetailleerde controle over hun opgeslagen informatie.

Naleving van beveiligingsvoorschriften

Bitwarden voldoet aan de beveiligingsstandaarden van de branche met SOC2- en SOC3-certificeringen en HIPAA-compliance.

SOC2 en SOC3

Systeem- en Organisatiecontroles (SOC) omvatten een reeks controlekaders die worden gebruikt om de beveiligingssystemen en het

HIPAA

Bitwarden voldoet aan de HIPAA-richtlijnen en wordt jaarlijks door derden gecontroleerd op naleving van de HIPAA-beveiligingsregel.

ISO 27001

Bitwarden is ISO 27001 gecertificeerd en voldoet aan de ISO 27001 controlesets rondom gegevensbeveiliging.

beveiligingsbeleid van een organisatie te valideren. Bitwarden is SOC2 Type II en SOC3 gecertificeerd.

SOC2-rapporten beschikbaar op aanvraag.

Naleving van privacy

Bitwarden geeft prioriteit aan het beschermen van de persoonlijke gegevens van gebruikers en het wereldwijd naleven van belangrijke privacystandaarden.

CCPA & CPRA

Bitwarden voldoet aan de California Consumer Privacy Act (CCPA) en de California Privacy Rights Act (CPRA).

GDPR

Bitwarden voldoet aan GDPR, de huidige EU-regels voor gegevensbescherming en de Standard Contractual Clauses (SCC's) van de EU.

Data Privacy Framework

Bitwarden voldoet aan de California Consumer Privacy Act (CCPA) en de California Privacy Rights Act (CPRA).

Voldoe aan uw beveiligingsnormen met Bitwarden

Bitwarden is meer dan een wachtwoordmanager; het is een fundamenteel hulpmiddel voor het bereiken en behouden van compliance met belangrijke beveiligingsstandaarden. Door middel van veilig delen, controlemogelijkheden, gecentraliseerd beheer en robuuste gegevensbescherming versterkt Bitwarden de cyberbeveiligingspositie van uw organisatie om te voldoen aan de compliance-eisen.

ISO 27001

ISO 27001, een internationale norm, legt de basis voor het creëren, onderhouden en ontwikkelen van beheersystemen voor informatiebeveiliging (ISMS), inclusief gegevensbeheer.

SOC 2

Service Organization Control 2 (SOC 2) rapporten worden vaak gevraagd door klanten en zakenpartners van leveranciers van uitbestede oplossingen. Bedrijven die SOC 2-compliant willen zijn, kunnen een SOC 2-compliant wachtwoordbeheerder gebruiken om aan de vereisten te voldoen.

NERC

De North American Electric Reliability Corporation (NERC) is een internationale regelgevende instantie zonder winstoogmerk die zich toelegt op het opstellen van nalevingsnormen die de risico's voor het elektriciteitsnet en de elektriciteitssystemen die honderden miljoenen mensen in de Verenigde Staten, Canada en een deel van Mexico van stroom voorzien, helpen verminderen.

NIS2

NIS2 is een reeks vereisten voor de beveiliging van netwerk- en informatiesystemen in de hele EU. De richtlijn verplicht bedrijven die zijn aangemerkt als exploitanten van essentiële diensten om passende maatregelen te nemen om de cyberbeveiliging te verbeteren en te voldoen aan wettelijke verplichtingen.

NIST Cyberveiligheidskader

Het National Institute of Standards and Technology (NIST) biedt richtlijnen en best practices voor organisaties om bedrijven, non-profits en andere particuliere instellingen te helpen het risicobeheer voor cyberbeveiliging te verbeteren.

SOX

Naleving van de Sarbanes-Oxley Act (SOX) houdt in dat je je houdt aan een reeks beveiligingsvereisten die zijn ontworpen om de integriteit van de financiële verslaglegging te waarborgen.

Wachtwoordbeheer volwassenheidsmodel

Dit raamwerk helpt organisaties inzicht te krijgen in het volwassenheidsniveau van hun wachtwoordmanager – gebaseerd op hun huidige activiteiten – en vast te stellen welke stappen

nodig zijn om hun beveiliging te versterken en hun bestaande classificatie te verbeteren.

FAQs

- Kan het Bitwarden-team mijn wachtwoorden zien?

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.

[Lees meer >](#)

- Hoe houdt u de cloudservers veilig?

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.

[Lees meer >](#)

- Wordt Bitwarden gecontroleerd?

Bitwarden voert regelmatig uitgebreide beveiligingsaudits uit bij gerenommeerde beveiligingsbedrijven. Deze jaarlijkse audits omvatten broncodebeoordelingen en penetratietests voor Bitwarden IP's, servers en webapplicaties.

[Lees meer >](#)

- Wat gebeurt er als Bitwarden wordt gehackt?

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.

[Lees meer >](#)

- Waar worden mijn gegevens in de cloud opgeslagen?

Bitwarden verwerkt en slaat alle kluisgegevens veilig op in de [Microsoft Azure Cloud](#) in de [VS of de EU](#) met behulp van diensten die worden beheerd door het team van Microsoft. Omdat Bitwarden alleen gebruik maakt van diensten die worden aangeboden door Azure, hoeft er geen serverinfrastructuur te worden beheerd en onderhouden. Alle uptime, schaalbaarheid, beveiligingsupdates en garanties worden ondersteund door Microsoft en hun cloudinfrastructuur. Raadpleeg de documentatie over [het Microsoft Azure Compliance-aanbod](#) voor meer informatie.

[Lees meer >](#)

- **Waarom zou ik mijn wachtwoorden aan Bitwarden toevertrouwen?**

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 meer >](#)

- **Gebruikt Bitwarden een salted hash voor mijn wachtwoord?**

PBKDF2 SHA-256 wordt gebruikt om de coderingssleutel van je hoofdwachtwoord af te leiden, maar je kunt ook [Argon2](#) als alternatief kiezen. Bitwarden [verzilt en hashed](#) uw hoofdwachtwoord met uw e-mailadres **lokaal**, voordat het naar onze servers wordt verzonden. Zodra een Bitwarden-server het gehashte wachtwoord ontvangt, wordt het opnieuw gezouten met een cryptografisch veilige willekeurige waarde, opnieuw gehasht en opgeslagen in onze database.

[Lees meer >](#)

- **Hoe worden mijn gegevens veilig verzonden en opgeslagen op Bitwarden-servers?**

Bitwarden versleutelt en/of hasht uw gegevens **altijd** op uw lokale apparaat voordat iets naar cloudservers wordt verzonden voor opslag. **Bitwarden-servers worden alleen gebruikt voor het opslaan van versleutelde gegevens**. Zie [Opslag](#) voor meer informatie.

[Lees meer >](#)

- **Welke versleuteling wordt gebruikt?**

Bitwarden gebruikt [AES-CBC](#) 256-bits encryptie voor uw kluisgegevens en [PBKDF2](#) SHA-256 of [Argon2](#) om uw encryptiesleutel af te leiden.

[Lees meer >](#)

- **Welke informatie is gecodeerd?**

Alle kluisgegevens worden versleuteld door Bitwarden voordat ze ergens worden opgeslagen. Zie [Encryptie](#) om te leren hoe.

[Lees meer >](#)

- **Waar worden mijn gegevens opgeslagen op mijn computer/apparaat?**

Gegevens die zijn opgeslagen op je computer/apparaat worden versleuteld en alleen ontsleuteld wanneer je je kluis ontgrendelt. Ontcijferde gegevens worden alleen **in het geheugen** opgeslagen en worden **nooit naar permanente opslag geschreven**.

[Lees meer >](#)