De zelf gehoste wachtwoordmanager van Bitwarden

Beheer bedrijfsgegevens en aangepast beveiligingsbeleid veilig op uw eigen server door de Bitwarden Password Manager zelf te hosten.

Bekijk de volledige interactieve weergave op
https://bitwarden.com/nl-nl/self-hosted-password-manager-on-premises/

bitwarden

Pas uw eigen beveiligingsmodel toe

Plaats uw Bitwarden-installatie achter een proxy, firewall en andere beveiligingen voor extra gegevensbeveiliging.

Back-ups en beschikbaarheid beheren

De containergebaseerde oplossingen van Docker of Kubernetes passen in uw bestaande strategie voor hoge beschikbaarheid en herstel, en binnen uw gevestigde procedures.

Aanpassen aan uw behoeften

Voldoe aan uw specifieke compliance-eisen en interne beleidsregels voor gegevensverblijven met flexibele omgevingsvariabelen voor veranderende behoeften.

De vertrouwde wachtwoordmanager voor thuis, op het werk en onderweg

Cross-platform toegankelijkheid & onbeperkte apparaten

Toegang tot kritieke gegevens in uw kluis vanaf elke locatie, browser en via een onbeperkt aantal apparaten

Bitwarden naadloos integreren

Sluit Bitwarden naadloos aan op uw bestaande technologiestack met flexibele integratieopties zoals SSO (Single Sign On) identity providers en directoryservices, waaronder SCIM.

Beveiligingsaudit & naleving

Open source, gecontroleerd door derden en in overeenstemming met GDPR-, Privacy Shield-, HIPAA- en CCPA-voorschriften

Directory-synchronisatie

Gebruik SCIM-ondersteuning of de Directory Connector om de provisioning van gebruikers en groepen te stroomlijnen en de synchronisatie met uw directoryservice te behouden

Kluis gezondheidsrapporten

Toegang tot inzichtelijke rapporten over zwakke en hergebruikte wachtwoorden en andere nuttige beveiligingsgegevens

Altijd ondersteuning

Customer Success agents zijn 24 uur per dag beschikbaar om u te ondersteunen

De voordelen van zelf gehoste wachtwoordmanagers

Echte gegevenssoevereiniteit

Of de zorgen nu komen van het bestuur of van je klanten, met self hosting is echte gegevenssoevereiniteit een realiteit.

Naleving van regelgeving

Als uw branche, service of product strenge eisen stelt aan de naleving van gegevens, dan is de zelfhostende Bitwarden Password Manager een goede keuze.

Aanpasbare beveiliging

Pas de beveiligingsinstellingen aan uw behoeften aan. Pas elk aspect van de beveiliging van uw organisatie aan, van zelf te hosten omgevingsvariabelen tot in-product beleidsregels.

Naadloze integratie

Ondersteunende installaties voor Windows, Linux, Docker of Kubernetes integreren met je bestaande IT-infrastructuur. De zelf gehoste Bitwarden server is compatibel met alle eindklanten, inclusief mobiele en desktop apps en browser extensies. In-product te integreren met uw Identity Provider, directoryservices en meer!

Klaar voor audits en naleving

Diepgaande eventlogs kunnen worden opgenomen door SIEM-tools via integraties of API's om gebruikersactiviteiten bij te houden en naleving van uw interne beleidsregels en externe voorschriften te garanderen. Auditresultaten van derden, SOC 2-rapporten en andere nalevingsinformatie voor de applicatie worden jaarlijks gepubliceerd en bijgewerkt.

Verkrijg toonaangevende beveiliging en volledige controle over uw gegevens

Maak uw online ervaring veiliger, sneller en leuker door Bitwarden Password Manager zelf te hosten.

FAQs

Meer self hosting FAQ's hier

- ### Wat zijn de voordelen van het gebruik van een zelf gehoste wachtwoordmanager?

  1. **Echte gegevenssoevereiniteit**: Een wachtwoordmanager zelf hosten geeft u volledige controle over uw gegevens. Je beheert je eigen server en zorgt ervoor dat gevoelige wachtwoorden en referenties worden opgeslagen op de infrastructuur die jij beheert.

  2. **Verbeterde beveiliging**: Met een zelfgehoste oplossing kunt u uw eigen beveiligingsmodel toepassen. Plaats uw wachtwoordbeheerinstallatie achter proxy's en firewalls voor extra bescherming.

  3. **Aanpassing**: Self-hosted wachtwoordmanagers bieden vaak flexibele omgevingsvariabelen, zodat u de setup kunt aanpassen aan uw specifieke behoeften en compliance-eisen.

  4. **Voordelen van open source**: Vertrouwen en transparantie zijn essentieel bij het kiezen van een wachtwoordmanager om zelf te hosten. Omdat Bitwarden een open source wachtwoordmanager is, zijn de beveiligingsmaatregelen zelfcontroleerbaar en wordt elke regel code regelmatig geïnspecteerd door duizenden beveiligingsexperts en enthousiastelingen wereldwijd.

  5. **Naleving van regelgeving**: Self-hosting kan helpen om te voldoen aan de strenge vereisten voor gegevensnaleving in verschillende sectoren, omdat je volledige controle hebt over de verblijfplaats van en toegang tot gegevens.

  6. **Integratie met bestaande systemen**: Self-hosted oplossingen ondersteunen vaak naadloze integratie met uw huidige IT-infrastructuur, inclusief directoryservices en identiteitsproviders.

  7. **Gereedheid voor audits**: Krijg toegang tot gedetailleerde eventlogs voor het bijhouden van gebruikersactiviteiten, wat cruciaal kan zijn voor interne audits en het handhaven van compliance.

- ### Op welke platforms kan ik hosten?

  Bitwarden clients zijn cross-platform en de server kan worden ingezet in Docker containers op Windows, Linux of in Kubernetes met behulp van een Helm chart.

  Docker Desktop op Windows kan een licentie vereisen, afhankelijk van of je bedrijf voldoet aan de Docker-vereisten voor licenties, maar Docker op Linux is gratis.

  Je kunt meer lezen over Docker en containertechnologieën op de Docker-website.

- Hoe zet ik Bitwarden in op AWS, Azure, GCP of VMware vCenter?

  Bitwarden heeft uitgebreide handleidingen voor het implementeren van Docker-installaties in de helpdocumentatie. Instructies voor installatie op AWS EKS, OpenShift en Azure AKS met Helm zijn ook beschikbaar. Hieronder staan aanbevolen bronnen om je op weg te helpen:

  - Docker inzetgidsen
  - Helm inzetgidsen
  - Hoe zelf een Bitwarden-organisatie te hosten

- Hoe stel ik een open source wachtwoordmanager in op mijn eigen server?

  Het instellen van een open source wachtwoordmanager op uw eigen server omvat meestal de volgende stappen

  1. **Bereid je server voor**: Zorg ervoor dat je een server of virtuele machine klaar hebt staan. Dit kan hardware op locatie zijn of een server in de cloud.
  2. **Selecteer een installatiemethode**: Veel zelf gehoste wachtwoordmanagers bieden meerdere installatieopties. De meest voorkomende zijn:
     - Docker-containers
     - Kubernetes-implementaties
  3. **Installatie**: Bekijk de gedetailleerde Bitwarden self-host documentatie voor verschillende implementatietypes.
  4. **Configuratie**: Omgevingsvariabelen instellen en instellingen aanpassen om te voldoen aan uw beveiligingsvereisten en organisatorische behoeften.
  5. **Gebruikersbeheer**: Beheerdersaccounts instellen en toegangsrechten voor gebruikers configureren.
  6. **Client instellen**: Installeer browser-extensies, desktop apps en mobiele apps voor je gebruikers en zorg ervoor dat ze geconfigureerd zijn om verbinding te maken met je zelf gehoste server.
  7. **Testen**: Test de installatie grondig, inclusief functies zoals de wachtwoordgenerator, veilig delen en verificatie met meerdere factoren.
  8. **Onderhoudsplan**: Stel procedures op voor regelmatige back-ups, updates en beveiligingsaudits om uw zelf gehoste wachtwoordmanager veilig en up-to-date te houden.

  Onthoud dat, hoewel zelf hosten veel voordelen biedt, het ook voortdurend onderhoud en beveiligingswaakzaamheid vereist. Zorg ervoor dat je de middelen en expertise hebt om een zelfgehoste oplossing effectief te beheren.