bitwarden | Artikel Helpcentrum

BEVEILIGING

# Whitepaper Beveiliging Bitwarden

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

# Whitepaper Beveiliging Bitwarden

## Overzicht van het Bitwarden Beveiligings- en nalevingsprogramma

Met werk op afstand in opkomst en een internetgebruik dat hoger is dan ooit, is de vraag om tientallen (zo niet honderden) online accounts met logins en wachtwoorden aan te maken en te onderhouden enorm.

Beveiligingsexperts raden je aan om een verschillend, willekeurig gegenereerd wachtwoord te gebruiken voor elke account die je aanmaakt. Maar hoe beheer je al die wachtwoorden? En hoe zorg je voor een goede wachtwoordhygiëne binnen een organisatie?

Effectief wachtwoordbeheer is een zwaar onderbenutte bron in de onderneming. In het 2020 Under the Hoodie Report van Rapid7 wordt opgemerkt dat wachtwoordbeheer en secundaire controles zoals twee-factor authenticatie "ernstig tekortschieten, wat leidt tot 'gemakkelijke' compromissen". Het hergebruiken of delen van wachtwoorden op een onveilige manier maakt de onderneming kwetsbaar.

Om verandering te brengen in een organisatie, moeten beveiligings- en IT-teams werknemers informeren over best practices. Wat betreft wachtwoordbeheer is een van de eenvoudigste manieren om goede wachtwoordhygiëne aan te moedigen en te ondersteunen het inzetten van een oplossing voor wachtwoordbeheer op uw werkplek.

Bitwarden is de makkelijkste en veiligste manier om al je logins, wachtwoorden en andere gevoelige informatie op te slaan en ze eenvoudig te synchroniseren tussen al je apparaten.

Bitwarden biedt de tools om je wachtwoorden te maken, op te slaan en te delen met behoud van het hoogste beveiligingsniveau.

De oplossing, software, infrastructuur en beveiligingsprocessen van Bitwarden zijn vanaf de basis ontworpen met een meerlagige, defense-in-depth benadering. Het Bitwarden Security en Compliance Programma is gebaseerd op het ISO27001 Information Security Management System (ISMS). We hebben beleid opgesteld dat ons beveiligingsbeleid en onze beveiligingsprocessen regelt en werken ons beveiligingsprogramma voortdurend bij om te voldoen aan de toepasselijke wettelijke, branche- en regelgevingsvereisten voor services die we aan u leveren onder onze Servicevoorwaardenovereenkomst.

Bitwarden voldoet aan de industrienorm voor applicatiebeveiligingsrichtlijnen die een toegewijd beveiligingsteam omvatten en regelmatige controles van de applicatiebroncode en IT-infrastructuur omvatten om beveiligingskwetsbaarheden te detecteren, te valideren en te verhelpen.

Deze whitepaper geeft een overzicht van de beveiligingsprincipes van Bitwarden en bevat links naar aanvullende documenten die meer informatie geven over specifieke onderwerpen.

### Bitwarden Ve

### Bescherming

Bitwarden gebruik

**End-to-end versl** , salted hashing
en PBKDF2 SHA-25 lle versleuteling
gebeurt lokaal. Zie

**Zero knowledge e** l versleuteld met
uw individuele e-r en hebben er
geen toegang toe

**Note**

Bij de release van accountherstel medio 2021 is een nieuw RSA publiek/privaat sleutelpaar geïntroduceerd voor alle Organisaties. De privésleutel wordt verder versleuteld met de bestaande symmetrische sleutel van de organisatie voordat hij wordt opgeslagen. Het sleutelpaar wordt gegenereerd en versleuteld aan de clientside bij het aanmaken van een nieuwe organisatie of bij een bestaande organisatie:

- Navigatie naar het scherm Beheer → Personen.
- Updates voor alles op het scherm Instellingen→Mijn organisatie.
- Upgrades van het ene organisatietype naar het andere.

**Veilig delen van wachtwoorden:** Bitwarden maakt veilig delen en beheren van gevoelige gegevens met gebruikers binnen een hele organisatie mogelijk. Een combinatie van asymmetrische en symmetrische versleuteling beschermt gevoelige informatie als deze wordt gedeeld.

**Open source en broncode:**
De broncode voor alle Bitwarden softwareproducten wordt gehost op GitHub en we verwelkomen iedereen om de Bitwarden codebase te bekijken, te controleren en eraan bij te dragen. De broncode van Bitwarden wordt gecontroleerd door gerenommeerde externe beveiligingsbedrijven en onafhankelijke beveiligingsonderzoekers. Daarnaast roept het Bitwarden Vulnerability Disclosure Program de hulp in van de hackergemeenschap op HackerOne om Bitwarden veiliger te maken.

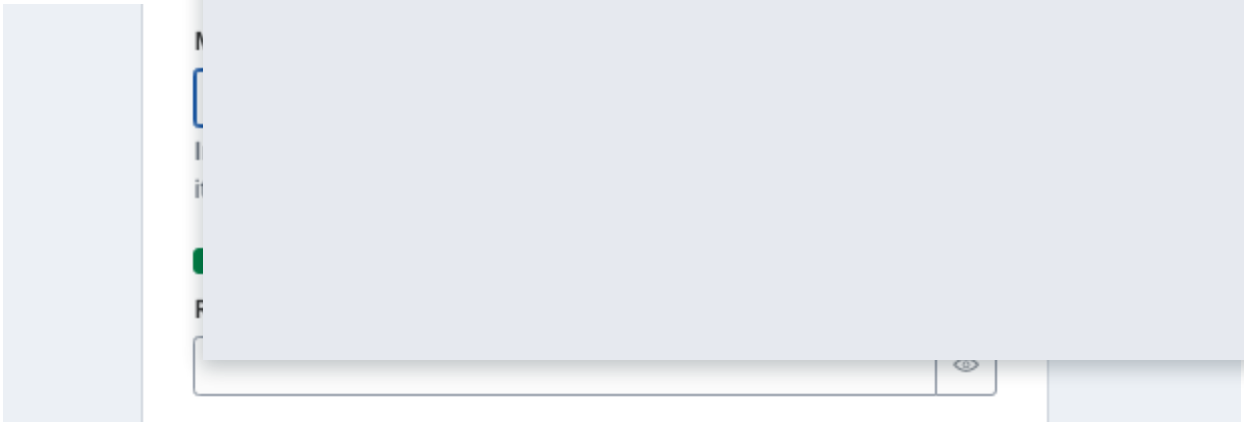
**Privacy door ontwerp:** Bitwarden slaat al je aanmeldingen op in een versleutelde kluis die synchroniseert op al je apparaten. Omdat de gegevens volledig versleuteld zijn voordat ze je apparaat verlaten, heb alleen jij toegang tot je gegevens. Zelfs het team van Bitwarden kan uw gegevens niet lezen (zelfs als we dat zouden willen). Je gegevens worden verzegeld met AES-CBC 256 bit encryptie, salted hashing en PBKDF2 SHA-256.

**Beveiligingsaudit en naleving:** Bitwarden is open source en gecontroleerd door derden en voldoet aan de AICPA SOC2 Type 2 / Privacy Shield-, GDPR- en CCPA-voorschriften.

## Hoofdwachtwoord

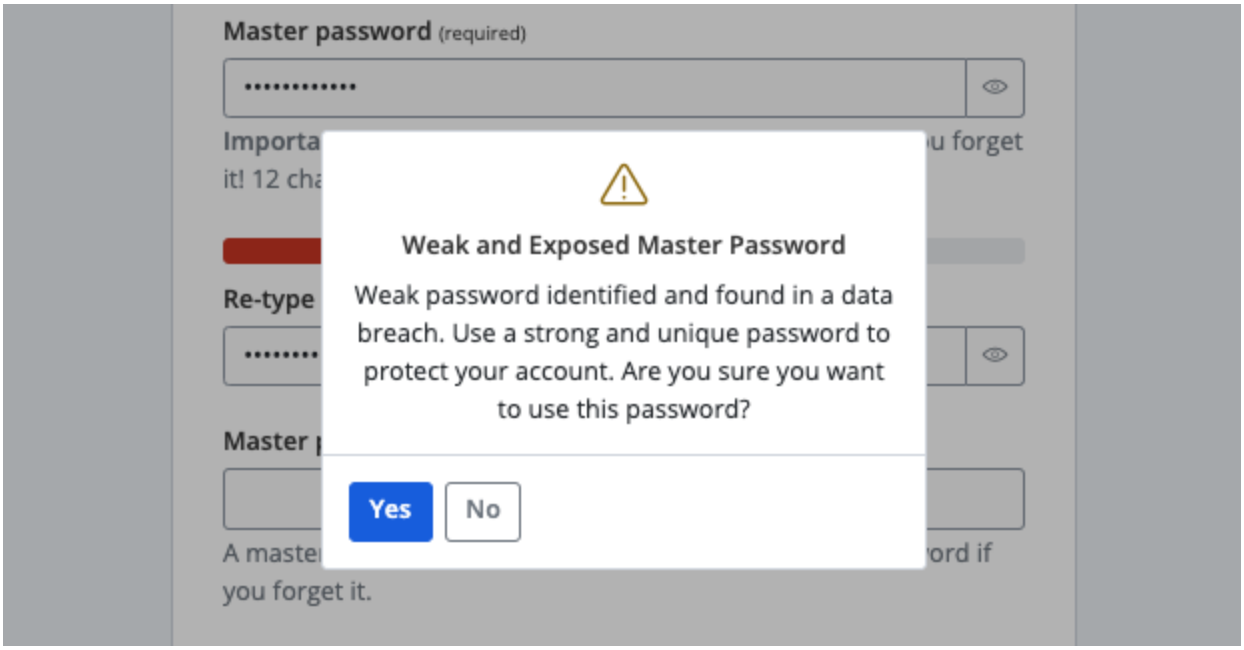
De bescherming van gebruikersgegevens in Bitwarden begint op het moment dat een gebruiker een account en een hoofdwachtwoord aanmaakt. We rad evat een wachtwoordsterkt eergeeft om een sterk hoofdwacht





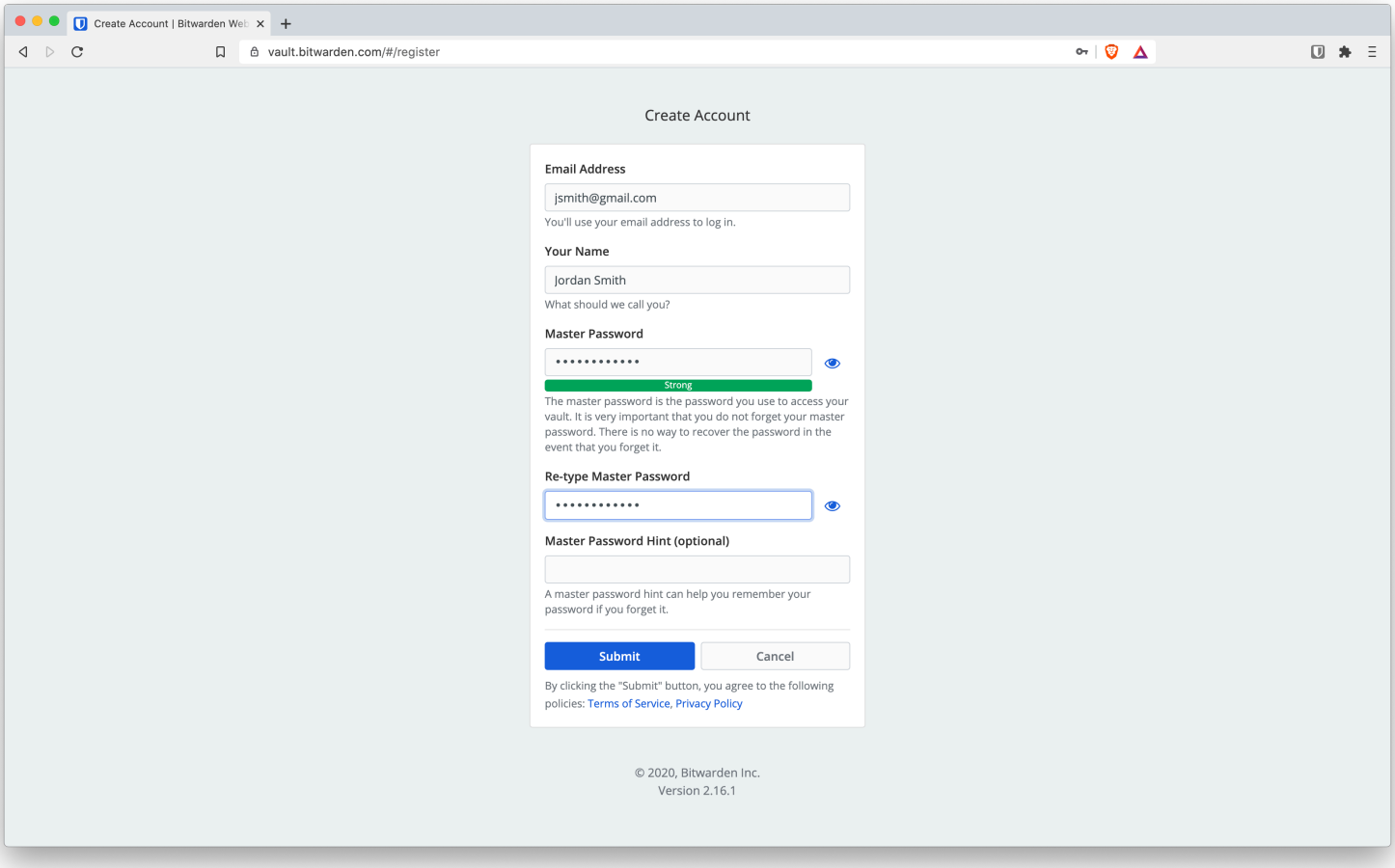
Maak een Bitwarden-account aan

Als u zich probeert aan te melden met een zwak wachtwoord, geeft Bitwarden een melding dat het gekozen hoofdwachtwoord zwak is. Wanneer u een Bitwarden-account aanmaakt, hebt u ook de optie om bekende datalekken te controleren voor het hoofdwachtwoord met behulp van HIBP.




Waarschuwing voor zwak hoofdwachtwoord

Het gebruik van een sterk hoofdwachtwoord is in uw eigen belang, omdat dit het token is dat u gebruikt om toegang te krijgen tot uw beveiligde kluis, waar uw gevoelige items worden opgeslagen. U bent zelf verantwoordelijk voor de beveiliging van uw account tijdens het gebruik van de Bitwarden-service. We bieden aanvullende maatregelen, zoals tweestapslogin, om u te helpen de beveiliging van uw account te handhaven, maar de inhoud van uw account en de beveiliging ervan bepaalt u zelf.




Kies een sterk hoofdwachtwoord

Lees meer: Vijf best practices voor wachtwoordbeheer en 3 tips van NIST om uw wachtwoorden veilig te houden

Handige hulpmiddelen: Bitwarden-wachtwoordsterkte-testprogramma en Bitwarden-wachtwoordgenerator

**Het is heel belang** geheugen en nooit via internet het vergeet.

Dit betekent ook le gegevens worden volledig v den neemt om u en uw gegevens t

Nadat u uw accou eutels die worden gebruikt om de ge



**Note**

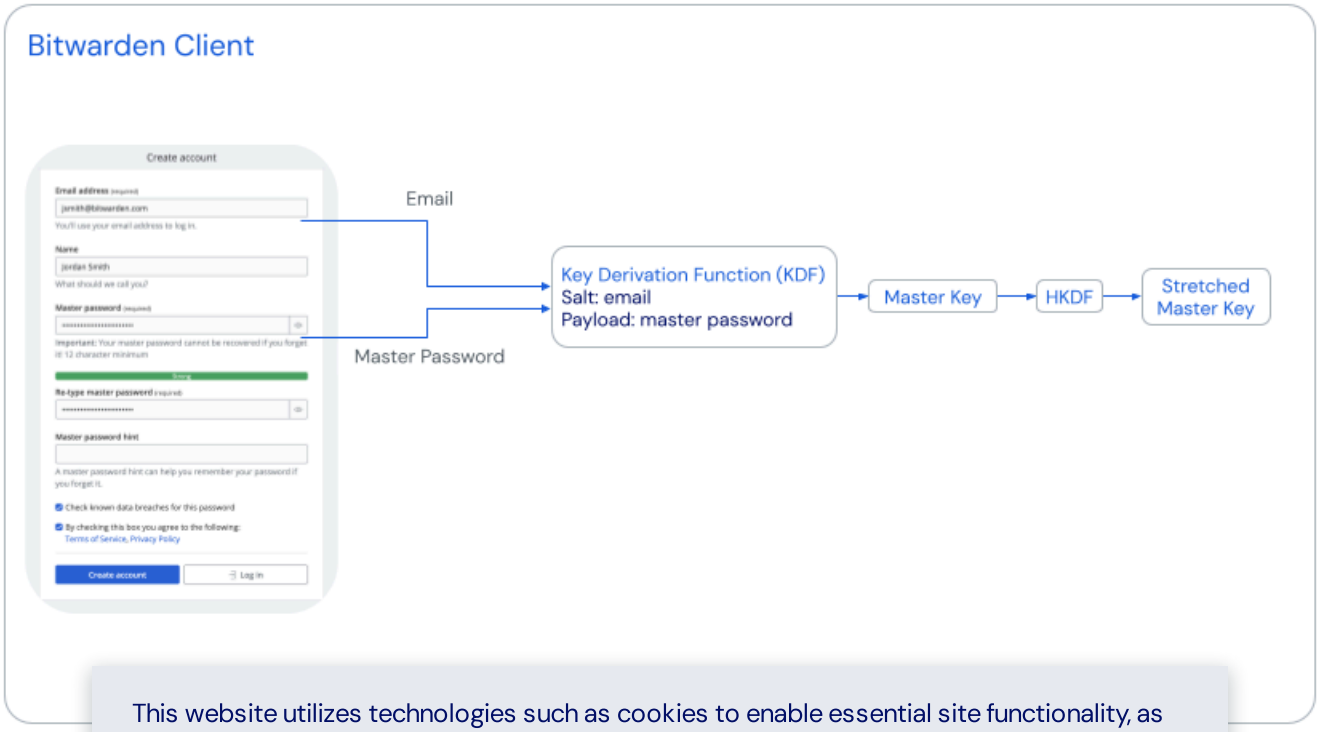
Medio 2021 int n organisaties de mogelijkhe ruikers kunnen resetten.

## Overzicht van het hoofdwachtwoord-hashen, sleutelafleiden en coderingsproces

### Gebruikersaccount aanmaken

Wanneer het formulier Account aanmaken wordt verzonden, gebruikt Bitwarden de wachtwoordgebaseerde sleutelafleidingsfunctie 2 (PBKDF2) met 600.000 iteratierondes om het hoofdwachtwoord van de gebruiker te rekken met een salt van het e-mailadres van de gebruiker. De resulterende salted waarde is de 256 bit Master Key. De Master Key wordt bovendien uitgerekt tot 512 bits lang met behulp van de Extract-and-Expand Key Derivation Function (HKDF) op basis van HMAC. De Master Key en Stretched Master Key worden nooit opgeslagen op of verzonden naar Bitwarden-servers.

> **Note**
>
> In versie 2023.2.0 heeft Bitwarden Argon2id toegevoegd als alternatieve optie voor PBKDF2. Meer informatie.

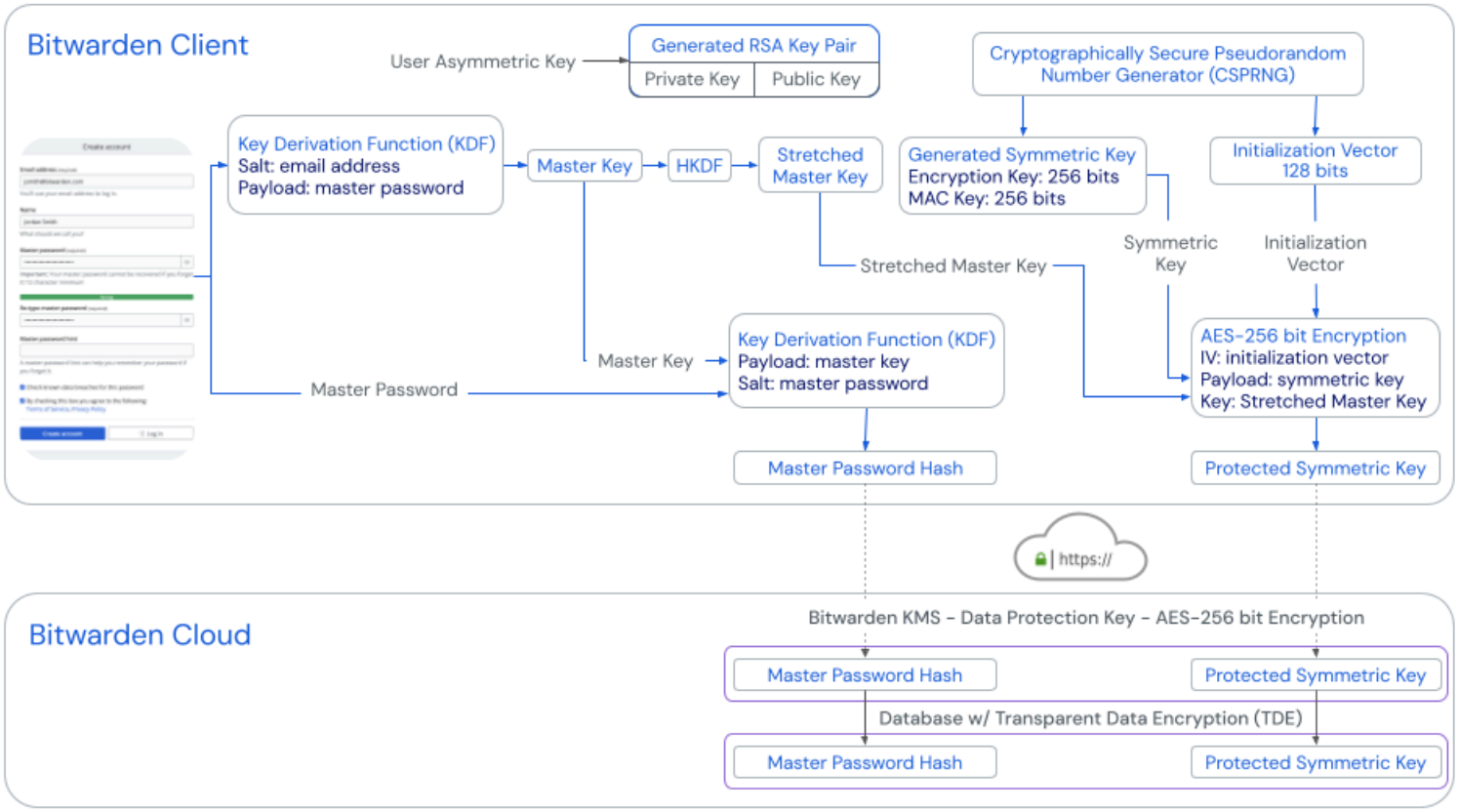





Daarnaast wordt e ige pseudo-
andom getalgene an de uitgerekte
hoofdsleutel en d ed Symmetric
Key is de hoofdsle ccount, en terug
wordt gestuurd na

Er wordt ook een a Het
Gegenereerde RSA sleutelpaar wordt gebruikt als en wanneer de gebruiker een Organisatie aanmaakt, die kan worden aangemaakt en gebruikt om gegevens te delen tussen gebruikers. Raadpleeg Gegevens delen tussen gebruikers voor meer informatie.

Er wordt ook een hash van het hoofdwachtwoord gegenereerd met PBKDF-SHA256 met een payload van de hoofdsleutel en een salt van het hoofdwachtwoord. De hash van het hoofdwachtwoord wordt naar de server gestuurd bij het aanmaken van de account en het aanmelden en wordt gebruikt om de gebruikersaccount te verifiëren. Eenmaal aangekomen op de server wordt het hoofdwachtwoord opnieuw gehasht met PBKDF2-SHA256 met een willekeurige salt en 600.000 iteraties. Hieronder staat een overzicht van het hashingproces van het wachtwoord, de sleutelafleiding en het versleutelingsproces.




Bitwarden wachtwoord hashing, sleutelafleiding en encryptie

### Inloggen gebruiker | Gebruikersauthenticatie | Toegang tot kluisgegevens gebruiker

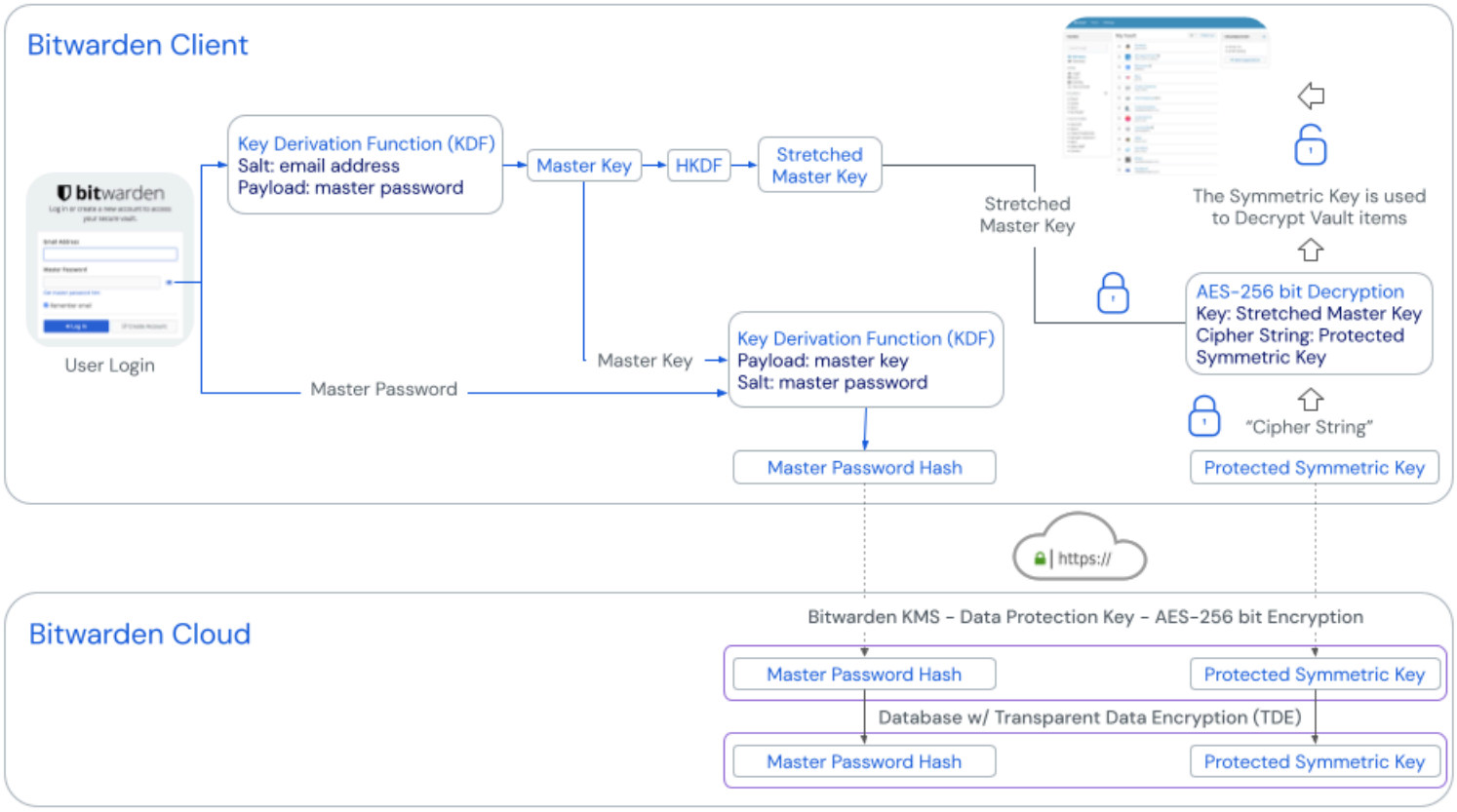
U moet eerst uw e

Vervolgens gebrui eratierondes om uw hoofdwachtwo er Key. Een hash van de hoofdsleut : om de gebruikersaccoun



> **Note**
>
> In versie 2023.

De Master Key wo ction (HKDF) op basis van HMAC. D e sleutel wordt gebruikt om kluisitems te decoderen. De ontcijfering gebeurt volledig op de Bitwarden Client omdat uw hoofdwachtwoord of opgerekte hoofdsleutel nooit wordt opgeslagen op of verzonden naar de Bitwarden-servers.




Een overzicht van gebruikersaanmeldingen

We bewaren het hoofdwachtwoord niet lokaal of in het geheugen van de Bitwarden Client. Je coderingssleutel (Symmetrische sleutel) wordt in het geheugen bewaard terwijl de app ontgrendeld is. Dit is nodig om gegevens in je kluis te ontsleutelen. Wanneer de kluis wordt vergrendeld, worden deze gegevens uit het geheugen gewist. Na een bepaalde periode van inactiviteit op het vergrendelscherm, herladen we de applicatieprocessen om ervoor te zorgen dat alle overgebleven beheerde geheugenadressen ook 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 applicatie als volledig veilig wanneer deze zich in een vergrendelde toestand bevindt.

**Extra bescherm**



Inloggen in twee s ount, ontworpen om ervoor te zorg rd zou ontdekken.

Als best practice unt. Wanneer tweestapslogin is woord). Standaard wordt je 2FA status opslaat, zodat je

Opmerking: Als je f je eerder "Onthoud mij" heb

Bitwarden ondersteunt inloggen in twee stappen met de volgende methoden:

**Gratis plannen**

- Een Authenticator-app gebruiken (bijvoorbeeld 2FAS, Ravio of Aegis)
- FIDO2 WebAuthn (elke FIDO2 WebAuthn gecertificeerde sleutel)
- E-mail

**Premium functies - inbegrepen als onderdeel van Familie-, Teams- en Enterprise-plannen**

- Duo Security met Duo Push, SMS, telefoongesprek en U2F-beveiligingssleutels
- YubiKey (elk apparaat uit de 4/5-serie of YubiKey NEO/NFC)

U kunt meerdere aanmeldingsmethoden in twee stappen inschakelen. Als u meerdere inlogmethodes in twee stappen hebt ingeschakeld, is de voorkeursvolgorde voor de standaardmethode die wordt weergegeven tijdens het inloggen als volgt: FIDO U2F > YubiKey > Duo > Authenticator app > E-mail. U kunt echter handmatig overschakelen naar elke methode en deze gebruiken tijdens het inloggen.

**Het is heel belangrijk dat u uw twee-staps inlogherstelcodes nooit kwijtraakt.** Bitwarden biedt een beveiligingsmodel voor accountbeveiliging waarbij gebruikers hun hoofdwachtwoord of twee-staps inlogcodes niet kunnen verliezen. Als u tweestapslogin hebt ingeschakeld op uw account en u verliest de toegang tot uw codes voor tweestapsloginherstel, dan kunt u niet inloggen op uw Bitwarden-account.

> **Note**
> Medio 2021 introduceerde Bitwarden accountherstel voor Enterprise-plannen. Met deze optie hebben gebruikers en organisaties de mogelijkheid om een nieuw beleid te implementeren waarmee beheerders en eigenaren wachtwoorden voor gebruikers kunnen resetten.

### Gebruikerswachtwoord wijzigen

Uw hoofdwachtwoord kan alleen worden gewijzigd via de webkluis. Voor specifieke stappen over hoe u uw gebruikerswachtwoord kunt wijzigen, raadpleegt u dit Bitwarden Help-artikel.

### De coderingssleutel van uw accounts roteren

Tijdens een wacht oteren van de coderingssleutel i s van uw Bitwarden Vault zi



> **Warning**
> Het draaien va Een sleutelrotatie lle **kluisgegevens**

### Gegevensbesch

Bitwarden neemt nooit naar de Bitwarden Cloud

Daarnaast gebruikt Bitwarden TLS/SSL om de communicatie tussen Bitwarden-clients en apparaten van gebruikers naar de Bitwarden Cloud te beveiligen. De TLS-implementatie van Bitwarden gebruikt 2048-bits X.509-certificaten voor serverauthenticatie en

sleuteluitwisseling en een sterke cipher suite voor bulkversleuteling. Onze servers zijn geconfigureerd om zwakke cijfers en protocollen te weigeren.

Bitwarden implementeert ook HTTP-beveiligingsheaders zoals HTTP Strict Transport Security (HSTS), waardoor alle verbindingen gedwongen worden TLS te gebruiken. Deze extra beschermingslaag met HSTS beperkt de risico's van downgrade-aanvallen en verkeerde configuratie.

### Gegevensbescherming in ruste

Bitwarden versleutelt en/of hasht uw gegevens altijd op uw lokale apparaat voordat ze naar de cloudservers worden verzonden voor synchronisatie. De Bitwarden-servers worden alleen gebruikt voor het opslaan en synchroniseren van versleutelde Vault-gegevens. Het is niet mogelijk om uw onversleutelde gegevens van de Bitwarden cloudservers te halen. Bitwarden gebruikt AES 256-bits encryptie en PBKDF-SHA256 om uw gegevens te beveiligen.

AES is een standaard in cryptografie en wordt gebruikt door de Amerikaanse overheid en andere overheidsinstellingen over de hele wereld voor het beschermen van topgeheime gegevens. Met de juiste implementatie en een sterke coderingssleutel (uw hoofdwachtwoord), wordt AES als onbreekbaar beschouwd.

PBKDF-SHA256 wordt gebruikt om de coderingssleutel af te leiden van je hoofdwachtwoord. Vervolgens wordt deze sleutel gezouten en gehasht voor verificatie met de Bitwarden-servers. De standaard iteratietelling die wordt gebruikt met PBKDF2 is 600.001 iteraties op de client (deze iteratietelling aan de clientkant is instelbaar via je accountinstellingen), en dan nog eens 100.000 iteraties als het wordt opgeslagen op onze servers (standaard in totaal 700.001 iteraties).

> **Note**
>
> In versie 2023.2.0 heeft Bitwarden Argon2id toegevoegd als alternatieve optie voor PBKDF2. Meer informatie.

Sommige versleutelde gegevens, zoals de beschermde symmetrische sleutel van een gebruiker en de hash van het hoofdwachtwoord, worden ook transparant versleuteld in rust door de applicatie, wat betekent dat ze worden versleuteld en weer ontsleuteld als ze in en uit de Bitwarden-database stromen.

Bitwarden maakt daarnaast gebruik van Azure transparante data-encryptie (TDE) om te beschermen tegen de dreiging van kwaadwillige offline activiteit door het uitvoeren van real-time encryptie en decryptie van de database, bijbehorende back-ups en transactielogbestanden in rust.

Meer informatie: H ruikt



### Inloggen met v

Naast het hoofdw proces maakt gebruik van een g lie sleutelmateriaal v leutelen van gegevens die zijn to-end, zero knowledge-encry

Wanneer een wac

1. De authentica uw passkey.
2. Een **PRF symmetrische sleutel** wordt gegenereerd door de authenticator via de PRF-extensie van de WebAuthn API. Deze sleutel is afgeleid van een **intern geheim** dat uniek is voor uw passkey en een **zout** dat door Bitwarden wordt geleverd.

3. Een **PRF publiek en privésleutelpaar** wordt gegenereerd door de Bitwarden-client. De openbare PRF-sleutel versleutelt uw **accountcoderingssleutel**, waartoe uw client toegang heeft omdat hij is aangemeld en ontgrendeld, en de resulterende **PRF-gecodeerde accountcoderingssleutel** wordt naar de server gestuurd.

4. De **PRF-privésleutel** wordt versleuteld met de **PRF-symmetrische sleutel** (zie stap 2) en de resulterende **PRF-gecodeerde privésleutel** wordt naar de server gestuurd.

5. Uw cliënt stuurt gegevens naar de Bitwarden-servers om een nieuwe credential record voor uw account aan te maken. Als je passkey geregistreerd is met ondersteuning voor kluisversleuteling en -ontsleuteling, dan bevat deze record:
   - De naam van de passkey
   - De openbare sleutel van de passkey
   - De openbare PRF-sleutel
   - De PRF-gecodeerde coderingssleutel voor de account
   - De PRF-gecodeerde privésleutel

De privésleutel van je passkey, die nodig is voor authenticatie, verlaat de client alleen versleuteld.

Wanneer een wachtwoord wordt gebruikt om in te loggen en, specifiek, om je kluisgegevens te ontsleutelen:

1. Met behulp van WebAuthn API openbare sleutelcryptografie wordt uw authenticatieverzoek bevestigd.

2. Je **PRF-gecodeerde accountcoderingssleutel** en **PRF-gecodeerde privésleutel** worden van de server naar je client gestuurd.

3. Met dezelfde **salt** die Bitwarden heeft verstrekt en het **interne geheim** dat uniek is voor uw passkey, wordt de **symmetrische PRF-sleutel** lokaal opnieuw gemaakt.

4. De **PRF-symmetrische sleutel** wordt gebruikt om uw **PRF-gecodeerde privésleutel** te decoderen, wat resulteert in uw **PRF-privésleutel**.

5. De **PRF-privésleutel** wordt gebruikt om uw **PRF-gecodeerde accountcoderingssleutel** te decoderen, wat resulteert in uw **accountcoder**



### Hoe kluisitems

Alle informatie (Lo hermd met end-to-end versleuteli her-object wordt genoemd. C worden door uw beschermde sym gebeurt volledig op de Bitwarden C n naar de Bitwarden-server

### Kluis gezondhe

Alle betaalde plar es.

Voor individuele kluizen hebben individuen toegang tot het volgende:

- Blootgestelde wachtwoorden Rapport
- Hergebruikte wachtwoorden Rapport
- Rapport over zwakke wachtwoorden
- Rapport onbeveiligde websites
- Inactief 2FA-verslag
- Rapport gegevensinbraak

Voor zakelijke gebruikers is er een vergelijkbare set rapporten voor Organization Vault-items.

Lees meer:Vault Health rapporten

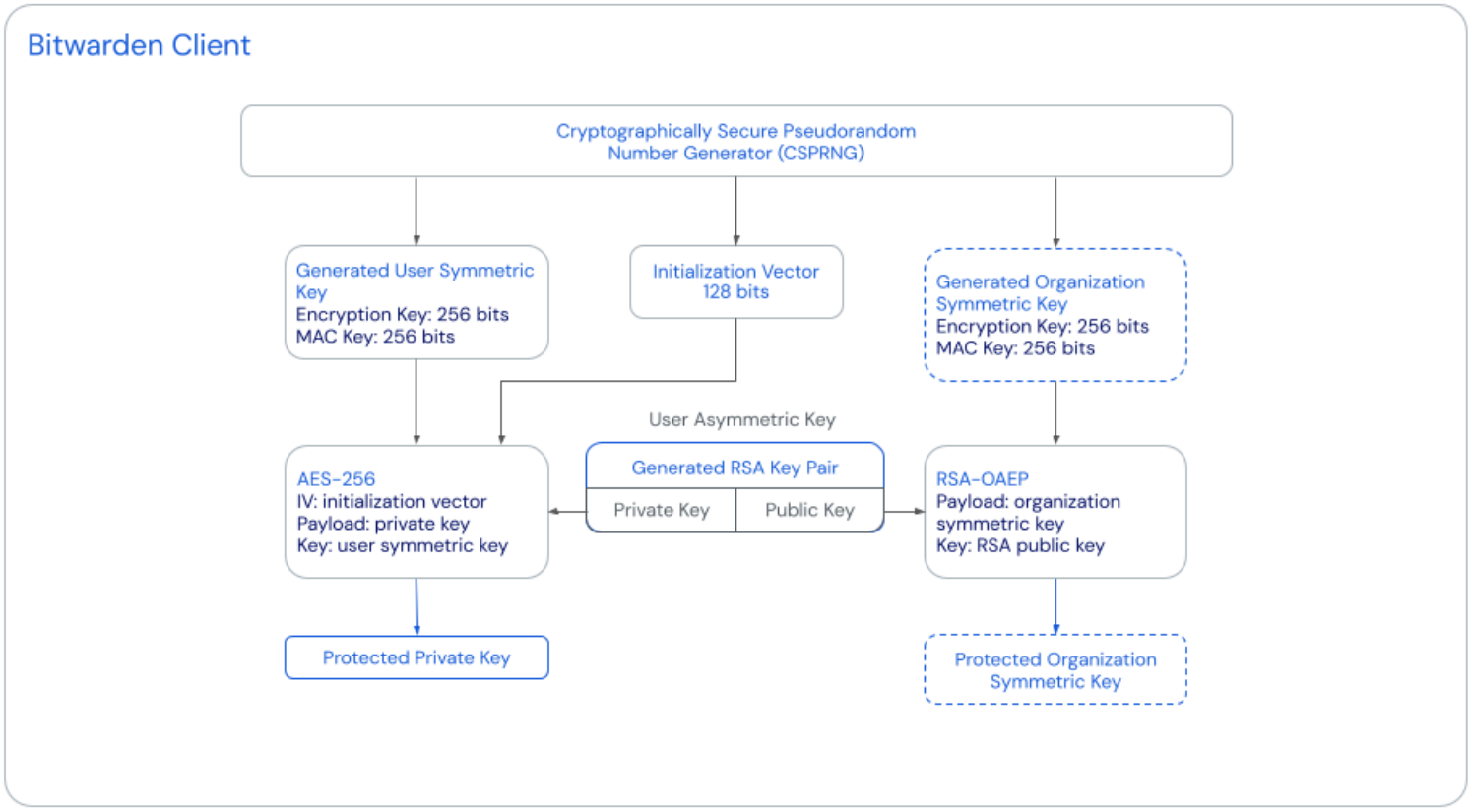
Zie Gebeurtenislogboeken voor meer informatie over Bitwarden-gebeurtenislogboeken en externe rapportage.

### Wachtwoorden en andere geheimen importeren in Bitwarden

U kunt uw gegevens van meer dan 40 verschillende diensten, waaronder alle populaire wachtwoordbeheerprogramma's, eenvoudig importeren naar Bitwarden. De volledige lijst van ondersteunde toepassingen en aanvullende informatie, waaronder stappen voor het oplossen van problemen bij het importeren van uw gegevens in Bitwarden, zijn gedocumenteerd in het Bitwarden Helpcentrum.

Als u uw sites exporteert vanuit de LastPass.com Web Vault, raadpleeg dan de specifieke informatie in deze Help-notitie Importeer uw gegevens vanuit LastPass.

### Gegevens delen tussen gebruikers




Bescherming en uitwisseling van organisatiesleutels

Samenwerking is een van de belangrijkste voordelen van het gebruik van een wachtwoordmanager. Om delen mogelijk te maken, moet je eerst een Organisatie aanmaken. Een Bitwarden Organisatie is een entiteit die gebruikers met elkaar verbindt die items willen delen. Een organisatie kan een familie, team, bedrijf of een ander soort groep zijn die gegevens wil delen.

Een individuele gebruikersaccount kan veel verschillende Organisaties aanmaken en/of er deel van uitmaken, zodat je je items vanuit één account kunt beheren.

U kunt een nieuwe atie vragen u een uitnodiging te stu



### Wanneer je een

Wanneer je een O tografisch Veilige Pseudo-Random gegevens die eigendom zijn var een veilige toegang nodig. De

Zodra de symmet tel van de organisatie te ver gegenereerd voor elke gebruiker bij al al bestaan voordat de Organ

> **Note**
>
> De RSA-privésleutel, waarvan het gebruik hieronder wordt beschreven, wordt versleuteld opgeslagen met de coderingssleutel van de gebruikersaccount, dus gebruikers moeten volledig ingelogd zijn om er toegang toe te krijgen.

De resulterende waarde van deze bewerking wordt de symmetrische sleutel van de beveiligde organisatie genoemd en wordt naar Bitwarden-servers gestuurd.

Wanneer de organisator of een ander organisatielid inlogt op zijn account, gebruikt de clientapplicatie de ontcijferde RSA privésleutel om de beschermde symmetrische sleutel van de organisatie te ontcijferen, wat resulteert in de symmetrische sleutel van de organisatie. Met behulp van de symmetrische sleutel van de organisatie worden kluisgegevens die eigendom zijn van de organisatie lokaal gedecodeerd.

### Wanneer gebruikers lid worden van een organisatie

Het proces voor opeenvolgende gebruikers die lid worden van een organisatie is vrij gelijkaardig, maar er zijn enkele verschillen die het vermelden waard zijn.

Eerst bevestigt een gevestigd lid van de Organisatie, in het bijzonder iemand met toestemming om andere gebruikers aan te melden, de gebruiker aan de Organisatie. Dit gevestigde lid heeft toegang tot de ontsleutelde symmetrische sleutel van de Organisatie, omdat hij al is ingelogd op zijn account en het ontsleutelingsproces van de Organisatiegegevens, zoals beschreven in de vorige paragraaf, heeft doorlopen.

Dus wanneer de nieuwe gebruiker is bevestigd, gaat de client van het gevestigde lid naar de Bitwarden-servers, haalt de openbare RSA-sleutel van de nieuwe gebruiker op, die is opgeslagen op de Bitwarden-servers op het moment dat het account werd aangemaakt, en versleutelt de ontsleutelde symmetrische sleutel van de organisatie ermee. Dit resulteert in een nieuwe beschermde symmetrische sleutel van de organisatie die naar de Bitwarden-servers wordt gestuurd en wordt opgeslagen voor het nieuwe lid.

> **Note**
>
> Elke beschermde symmetrische sleutel van de organisatie is uniek voor de gebruiker, maar elke sleutel zal ontsleutelen naar dezelfde vereiste symmetrische sleutel van de organisatie als deze ontsleuteld wordt met de RSA privésleutel van de specifieke gebruiker.

Wanneer de nieuw ésleutel om de nieuwe beveiligde n de organisatie. Met behulp van d e lokaal gedecodeerd.

Lees meer: Wat zij

### Toegangscontr

Naarmate het geb dig collecties kunnen beheren, z

Het beheren van V eiden, toe te kennen of te bepe



Een volledige lijst van rollen en toegangscontrole is gedocumenteerd in de sectie Gebruikerstypen en toegangscontrole van het Bitwarden Helpcentrum.

Lees meer: Over collecties

### Gebeurtenislogboeken

Gebeurtenislogboeken bevatten gedetailleerde informatie met tijdstempels over welke acties of wijzigingen er hebben plaatsgevonden binnen een organisatie. Deze logs zijn handig bij het onderzoeken van wijzigingen in credentials of configuratie en zeer nuttig voor audit trail onderzoek en het oplossen van problemen.

Aanvullende informatie over gebeurtenislogboeken is gedocumenteerd in het Bitwarden Helpcentrum. Gebeurtenislogboeken zijn alleen beschikbaar voor Teams en Business-plannen.

Om meer gegevens te verzamelen, kunnen plannen met API-toegang de Bitwarden API gebruiken. API-reacties bevatten het type gebeurtenis en relevante gegevens.

### SIEM-integratie en externe systemen

Voor SIEM-systemen (Security Information and Event Management) zoals Splunk kan bij het exporteren van gegevens uit Bitwarden een combinatie van gegevens uit de API en CLI worden gebruikt om gegevens te verzamelen.

Dit proces wordt beschreven in de opmerking in het Helpcentrum over **logboeken van organisatiegebeurtenissen** onder SIEM en integraties met externe systemen.

## Accountbeveiliging en uitsluiting voorkomen

Vandaag de dag biedt Bitwarden voor Basis-, Premium-, Familie- en Teams-abonnementen accountbeveiliging met een beveiligingsmodel dat gebruikers niet ondersteunt bij het verliezen van hun wachtwoorden of twee-staps inlogherstelcodes.

Bitwarden kan gebruikerswachtwoorden niet resetten en Bitwarden kan inloggen in twee stappen niet uitschakelen als dit is ingeschakeld op uw account. Eigenaars of beheerders van familie- en teamaccounts kunnen gebruikerswachtwoorden niet resetten. Zie de volgende sectie voor meer informatie over Enterprise-plannen.

> ⚠ **Warning**
>
> Gebruikers die hun hoofdwachtwoord kwijtraken of hun inlogcode in twee stappen kwijtraken, moeten hun account verwijderen en opnieuw beginnen.

Om deze potentië ng te voorkomen.

**Hoofdwachtwoor**
Zoek een manier c opschrijft en op een veilige plek b

**Gebruik een hoof**
Als dat handig is, moment een hint in via de Instelling

**Organisatiemana**
Heb voor Organisa

**Tweestaps inlogh**
Als uw organisatie ervoor kiest of eist dat u in twee stappen inlogt, zorg er dan voor dat u uw herstelcode opent en bewaart en bewaar deze op een even veilige plaats als uw hoofdwachtwoord.

### Accountherstel in Enterprise-plannen

Medio 2021 introduceerde Bitwarden accountherstel voor Enterprise-plannen. Met deze optie hebben gebruikers en organisaties de mogelijkheid om een nieuw beleid te implementeren waarmee Beheerders en Eigenaren wachtwoorden voor gebruikers kunnen resetten.

## Bitwarden Cloud Platform en beveiliging van webapplicaties

### Overzicht Bitwarden-architectuur

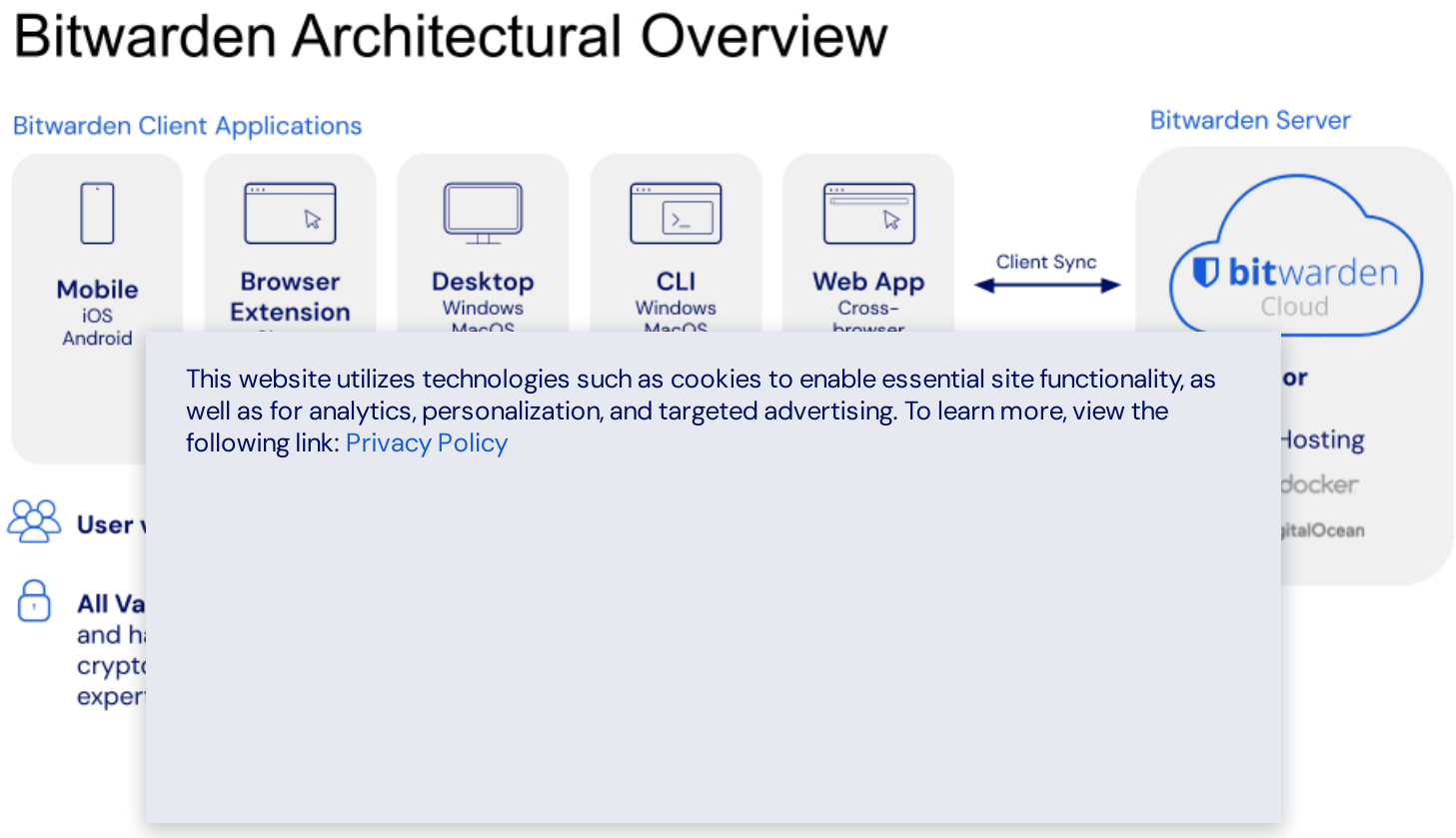
Bitwarden verwerkt en slaat alle gegevens veilig op in de Microsoft Azure-cloud met behulp van diensten die worden beheerd door het team van Microsoft. Omdat Bitwarden alleen gebruik maakt van diensten die worden aangeboden door Azure, hoeft er geen serverinfrastructuur te worden beheerd en onderhouden. Alle uptime, schaalbaarheid en beveiligingsupdates, patches en garanties worden ondersteund door Microsoft en hun cloudinfrastructuur.

### Beveiligingsupdates en patches

Het team van Microsoft beheert OS patching op twee niveaus, de fysieke servers en de virtuele gastmachines (VM's) waarop de Azure App Service resources draaien. Beide worden maandelijks bijgewerkt, wat overeenkomt met het maandelijkse Patch Tuesday-schema van Microsoft. Deze updates worden automatisch toegepast, op een manier die de SLA met hoge beschikbaarheid van Azure services garandeert.

Lees meer: Patching in Azure App Service of SLA voor App Service

Voor gedetailleerde informatie over hoe updates worden toegepast, lees hier



### Bitwarden Toegangscontrole

De medewerkers van Bitwarden beschikken over aanzienlijke training en expertise voor het type gegevens, systemen en informatie-assets dat ze ontwerpen, ontwerpen, implementeren, beheren, ondersteunen en waarmee ze omgaan.

Bitwarden volgt een vastgesteld on-boardingproces om ervoor te zorgen dat het juiste toegangsniveau wordt toegewezen en gehandhaafd. Bitwarden heeft toegangsniveaus ingesteld die geschikt zijn voor elke rol. Alle verzoeken, inclusief alle verzoeken om toegang te wijzigen, moeten worden beoordeeld en goedgekeurd door de manager. Bitwarden hanteert een 'least-privilege'-beleid dat medewerkers het minimale toegangsniveau geeft dat nodig is om hun taken uit te voeren. Bitwarden volgt een vastgesteld off-boarding proces via Bitwarden Human Resources dat alle toegangsrechten intrekt bij beëindiging.

### Software Levenscyclus en Wijzigingsbeheer

Bitwarden evalueert wijzigingen aan platform, applicaties en productie-infrastructuur om risico's te minimaliseren en dergelijke wijzigingen worden geïmplementeerd volgens de standaard operationele procedures bij Bitwarden.

Change Request-items worden gepland op basis van de roadmap en op dit punt ingediend bij engineering. Engineering bekijkt en evalueert hun capaciteit en beoordeelt het inspanningsniveau voor elk item van het wijzigingsverzoek. Na beoordeling en evaluatie formuleren ze waar ze aan gaan werken voor een specifieke release. De CTO verstrekt details over de release via communicatiekanalen en managementvergaderingen en de ontwikkelingslevenscyclus begint voor die release.

Ontwikkelings-, release-, test- en goedkeuringsproces op hoog niveau:

- Ontwikkelen, bouwen en itereren met behulp van pull requests in GitHub
- Kenmerken op een punt krijgen waarop ze testbaar zijn
- Engineering voert functionele tests uit van de functie en/of het product tijdens het ontwikkelen en bouwen
- Het bouwen van eenheidstesten is geautomatiseerd als onderdeel van Bitwarden Continuous Integration (CI) pipelines
- Sommige tests worden ook uitgevoerd door het Klanten succesteam
- De directeur Engineering helpt bij de beoordeling en bij het formaliseren van het proces, inclusief het bijwerken van documentatie
- CTO geeft definitieve goedkeuring voor Go / No-Go



Aanwezigheid ver geïmplementeerd
en afgesloten, mo ijzigingsverzoek
te beoordelen en

Emergency Deplo ing wordt
ontvangen van ee ommuniceerd en
afgesloten tijdens ysteemuitval of
in een urgente situ

### Besturing van p

Bitwarden onderh
probleemoplossir te escaleren.

**Basisconfiguraties**

Bitwarden verwerkt en slaat alle gegevens veilig op in de Microsoft Azure-cloud 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 en beveiligingsupdates en -garanties worden ondersteund door Microsoft en hun cloudinfrastructuur.

Azure Service Configurations worden door Bitwarden gebruikt om ervoor te zorgen dat applicaties op een herhaalbare en consistente manier worden geconfigureerd en ingezet.

### Bitwarden Platform Sleutelbeheer Procedures

Sleutels en andere geheimen die door het Bitwarden-platform zelf worden gebruikt, zijn onder andere referenties voor de Bitwarden-accounts bij cloudproviders. Al deze sleutels worden gegenereerd, veilig opgeslagen en indien nodig geroteerd, in overeenstemming met de industrienormen. Bitwarden gebruikt een interne Bitwarden kluis voor veilige opslag en back-up van gevoelige sleutels of andere geheimen die worden gebruikt door het Bitwarden platform. Toegangscontrole tot de Bitwarden-kluis maakt gebruik van gebruikerstypes en toegangscontrole.

### Gegevenstypen en gegevensopslag

Bitwarden verwerkt twee soorten gebruikersgegevens om de Bitwarden Service te leveren: (i) kluisgegevens en (ii) administratieve gegevens.

(i) Kluisgegevens

Kluisgegevens omvatten alle informatie die is opgeslagen in accounts bij de Bitwarden Service en kunnen persoonlijke gegevens bevatten. Als wij de Bitwarden Service voor u hosten, hosten wij Kluisgegevens. Vault Data wordt versleuteld met behulp van veilige cryptografische sleutels onder uw beheer. Bitwarden heeft geen toegang tot kluisgegevens.

Bewaren van Vault-gegevens: U kunt op elk gewenst moment Vault Data toevoegen, wijzigen en verwijderen.

(ii) Administratieve gegevens

Bitwarden verkrijgt persoonlijke gegevens in verband met het aanmaken van uw account, het gebruik van de Bitwarden Service en ondersteuning, en betalingen voor de Bitwarden Service, zoals namen, e-mailadressen, telefoon- en andere contactgegevens van gebruikers van de Bitwarden Service en het aantal items in uw Bitwarden Service-account ("Administratieve gegevens"). Bitwarden gebruikt Administratieve Gegevens om de Bitwarden Service aan u te kunnen leveren. We bewaren Administratieve Gegevens zolang u klant bent van Bitwarden en zoals wettelijk vereist. Als u uw relatie met Bitwarden beëindigt, verwijderen we uw persoonlijke gegevens in overeenstemming met ons beleid voor het bewaren van gegevens.

Wanneer u de Site vens, die Bitwarden verzam



- Naam
- Bedrijfsnaam e
- Zakelijk telefoo
- E-mailadres
- IP-adres en ar
- Elke klantgetu
- Informatie die u verstrekt aan de Interactieve gedeelten van de site, zoals invulbare formulieren of tekstvakken, training, webinars of registratie voor evenementen.

- Informatie over het apparaat dat u gebruikt, waaronder het hardwaremodel, besturingssysteem en versie, unieke apparaat-id's, netwerkinformatie, IP-adres en/of Bitwarden Service-informatie bij interactie met de site.
- Als u interactie hebt met de Bitwarden-community of -training, of u hebt ingeschreven voor een examen of evenement, kunnen we biografische gegevens verzamelen en de inhoud die u deelt.
- Informatie verzameld via cookies, pixeltags, logs of andere soortgelijke technologieën.

Raadpleeg het privacybeleid van Bitwarden voor meer informatie.

### Registratie, bewaking en waarschuwingsmeldingen

Bitwarden onderhoudt gedocumenteerde runbooks voor alle productiesystemen voor de implementatie, updates en het oplossen van problemen. Er zijn uitgebreide waarschuwingen ingesteld om problemen te melden en te escaleren. Een combinatie van handmatige en geautomatiseerde bewaking van de Bitwarden Cloud-infrastructuur biedt een uitgebreid en gedetailleerd overzicht van de gezondheid van het systeem en proactieve waarschuwingen voor probleemgebieden. Problemen komen snel aan het licht zodat ons infrastructuurteam effectief kan reageren en problemen met minimale onderbreking kan verhelpen.

### Bedrijfscontinuïteit / noodherstel

Bitwarden maakt gebruik van een volledig scala aan rampherstel- en bedrijfscontinuïteitspraktijken van Microsoft Azure die zijn ingebouwd in de Bitwarden Cloud. Dit omvat hoge beschikbaarheid en back-upservices voor onze applicatie- en databaselagen.

### Bedreigingspreventie en reactie

Bitwarden voert regelmatig kwetsbaarhedenanalyses uit. We maken gebruik van tools van derden en externe services, waaronder: OWASP ZAP, Mozilla Observatory, OpenVAS en anderen worden gebruikt om interne beoordelingen uit te voeren.

Bitwarden gebruikt Cloudflare om een WAF aan de rand, betere DDoS-bescherming, gedistribueerde beschikbaarheid en caching. Bitwarden gebruikt ook proxy's binnen Cloudflare voor betere netwerkbeveiliging en prestaties van haar diensten en sites.

Bitwarden is open source software. Al onze broncode wordt gehost op GitHub en is voor iedereen vrij om te bekijken. De broncode van Bitwarden wordt gecontroleerd door gerenommeerde externe beveiligingsbedrijven en onafhankelijke beveiligingsonderzoekers. Daarnaast roept het Bitwarden Vulnerability Disclosure Program de hulp in van de hackergemeenschap op HackerOne om Bitwarden veiliger te maken.

### Controleerbaar



Het Bitwarden Sec ystem (ISMS). We hebben beleid op rogramma voortdurend bij or aan u leveren onder onze Servic

Bitwarden voldoet atten en regelmatige contr tecteren, te valideren en te ve

**Externe veiligheic**

Beveiligingsbeoor jaar uitgevoerd.

**Certificeringen**

Bitwarden certificeringen zijn onder andere:

- SOC2 Type II (jaarlijks vernieuwd)
- SOC3 (jaarlijks vernieuwd)

Volgens de AICPA is het gebruik van het SOC 2 Type II-rapport beperkt. Neem voor vragen over SOC 2-rapporten contact met ons op.

Lees meer: Bitwarden behaalt SOC2-certificering

Het SOC 3-rapport geeft een samenvatting van het SOC 2-rapport dat publiekelijk kan worden verspreid. Volgens de AICPA is SOC 3 de SOC voor serviceorganisaties die rapporteren over criteria voor trustdiensten voor algemeen gebruik.
Bitwarden stelt hier een kopie van ons SOC 3-rapport beschikbaar.

Deze SOC-certificeringen vormen één facet van ons streven om de veiligheid en privacy van klanten te waarborgen en te voldoen aan strenge normen. Bitwarden voert ook regelmatig audits uit op onze netwerkbeveiliging en code-integriteit.

Lees meer: Bitwarden 2020 beveiligingsaudit is afgerond en Bitwarden rondt beveiligingsaudit derde partij af

### HTTP-beveiligingsheaders

Bitwarden maakt gebruik van HTTP-beveiligingsheaders als een extra beschermingsniveau voor de Bitwarden-webtoepassing en -communicatie. HTTP Strict Transport Security (HSTS) dwingt bijvoorbeeld alle verbindingen om TLS te gebruiken, wat de risico's van downgrade-aanvallen en verkeerde configuratie vermindert. Content Security Policy-headers bieden verdere bescherming tegen injectieaanvallen, zoals cross-site scripting (XSS). Daarnaast implementeert Bitwarden X-Frame-Options: SAMEORIGIN om clickjacking tegen te gaan.

## Overzicht van het bedreigingsmodel en analyse van het aanvalsoppervlak

Bitwarden volgt een risicogebaseerde aanpak voor het ontwerpen van veilige diensten en systemen, waaronder bedreigingsmodellering en analyse van het aanvalsoppervlak om bedreigingen te identificeren en er maatregelen tegen te ontwikkelen. De analyse van risico- en dreigingsmodellen strekt zich uit tot alle gebieden van het Bitwarden-platform, inclusief de kernapplicatie Bitwarden Cloud Server en de Bitwarden-clients zoals mobiel, desktop, webapplicatie, browser en/of opdrachtregelinterfaces.

### Bitwarden Klanten

Gebruikers communiceren voornamelijk met Bitwarden via onze clientapplicaties, zoals mobiel, desktop, webapplicaties, browsers en/of opdrachtregelinterfaces. De beveiliging van deze apparaten, werkstations en webbrowsers is cruciaal, want als een of meer van deze apparaten in geva op deze apparaten wordt nt er verantwoordelijk v



### HTTPS TLS en w

De Bitwarden Web nkelijk van de integriteit van de dat de webclient aflevert, kan een k

Webbrowseraanv en of schade toe te brengen. Aanva

- Een element v e ondernemen die de veilighe
- **Webbrowseraanvallen en Browseruitbreidingen / invoegtoepassingen:** Een kwaadaardige extensie die is ontworpen om

gebruikersgeheimen vast te leggen terwijl ze op het toetsenbord worden getypt.

- **Aanvallen op webtoepassingen via de browser:** Clickjacking, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).

Bitwarden maakt gebruik van HTTP-beveiligingsheaders als een extra beschermingsniveau voor de Bitwarden-webtoepassing en -communicatie.

### Codebeoordelingen

Bitwarden is een open source wachtwoordmanager. Al onze broncode wordt gehost en is openbaar beschikbaar op GitHub. De broncode van Bitwarden is en wordt jaarlijks gecontroleerd door gerenommeerde externe beveiligingsbedrijven en onafhankelijke beveiligingsonderzoekers. Daarnaast roept het Bitwarden Vulnerability Disclosure Program de hulp in van de hackergemeenschap op HackerOne om Bitwarden veiliger te maken.

Lees meer:

- Bitwarden Beveiliging FAQ's
- Bitwarden Bedreigingspreventie en -respons
- Bitwarden Beveiligings- en nalevingsbeoordelingen, reviews, kwetsbaarheidsscans, pentests

## Conclusie

Dit overzicht van het Bitwarden Security en Compliance programma wordt u ter beoordeling aangeboden. De oplossing, software, infrastructuur en beveiligingsprocessen van Bitwarden zijn vanaf de basis ontworpen met een meerlagige, defense-in-depth benadering.

Het Bitwarden Security en Compliance Programma is gebaseerd op het ISO27001 Information Security Management System (ISMS). We hebben beleid opgesteld dat ons beveiligingsbeleid en onze beveiligingsprocessen regelt en werken ons beveiligingsprogramma voortdurend bij om te voldoen aan de toepasselijke wettelijke, branche- en regelgevingsvereisten voor services die we aan u leveren onder onze Servicevoorwaardenovereenkomst.

Neem contact met ons op als je vragen hebt.