bitwarden | Help Center Article

SÄKERHET

Bitwarden säkerhetsvitbok

View in the help center:
https://bitwarden.com/help/bitwarden-security-white-paper/

Bitwarden säkerhetsvitbok

Översikt

Alla är mer uppkopplade än någonsin

Internetanslutna enheter och tjänster är mer kritiska än någonsin i dagens samhälle. I takt med att fler och fler företag tillhandahåller innovativa mjukvaru-som-en-tjänst-produkter som förbättrar användarnas liv hemma och på jobbet, ökar antalet referenser och maskinhemligheter exponentiellt. Liksom hoten mot deras säkerhet.

Cybersäkerhetshot är höga, men praxis är låg

Hoten mot användar- och kunddata fortsätter att öka. Det är nästan varje vecka som ett intrång eller ransomware-attack kommer till nyheterna, och det är bara de incidenter som är tillräckligt stora för att publiceras. År 2023 rapporterade IBM att den genomsnittliga kostnaden för ett dataintrång i USA närmar sig 9,48 miljoner dollar, med hänsyn tagen till utredningskostnader, juridiska avgifter, alternativkostnad och förlust av kundernas förtroende.

Forskning från Verizon visar att kompromitterade referenser står för 86 % av dataintrången. Detta inkluderar användning av lösenord som har gissat, nätfiskat eller läckt i andra intrång.

Med sådana hot skulle man förvänta sig att företag beväpnade sina anställda med så mycket utbildning och verktyg som möjligt, men Bitwardens forskning visar att användare inte alltid följer bästa praxis, inklusive 90 % av de tillfrågade säger att de återanvände lösenord.

Säkerhetsexperter rekommenderar att användare har olika, slumpmässigt genererade lösenord för varje konto. Men hur hanterar man alla dessa lösenord? Och hur kan goda lösenordsvanor upprätthållas i en organisation?

Bitwarden hjälper till att säkra privatpersoner, företag och infrastrukturhemligheter

Bitwarden erbjuder en portfölj av säkerhetsprodukter för att hjälpa till att säkra alla, förhindra intrång och säkerställa produktivitet.

Bitwarden Password Manager ger användarna verktygen för att skapa, lagra och dela lösenord samtidigt som högsta säkerhetsnivå bibehålls. Det är det enklaste och säkraste sättet att lagra alla dina inloggningar, lösenord och annan känslig information samtidigt som du bekvämt håller dem synkroniserade mellan alla dina enheter.

Bitwarden Secrets Manager ger utvecklare, DevOps och IT-team möjlighet att lagra, dela och automatisera maskinhemligheter som autentiseringsnycklar, databaslösenord och API-nycklar. Den heltäckande krypterade hemlighetshanteringslösningen stöder säker distribution av infrastruktur och applikationskod utan risk för att avslöja kritiska maskinhemligheter.

Bitwarden Passwordless.dev tillhandahåller API:er och verktyg som behövs för utvecklare för att implementera FIDO2 WebAuthn-baserad autentisering med lösenord, nästa generations säker autentisering av autentiseringsuppgifter, för webbplatser och applikationer.

Upprätthålla säkerhet och efterlevnad

Bitwarden-lösningar, mjukvara, infrastruktur och säkerhetsprocesser har designats från grunden med en mångskiktad, djupgående försvarsmetod. Bitwardens program för säkerhet och efterlevnad är baserat på ISO27001 Information Security Management System (ISMS). Policyer har definierats som styr säkerhetspraxis och processer och uppdateras kontinuerligt för att överensstämma med tillämpliga juridiska, bransch- och regulatoriska krav för tjänster som tillhandahålls under användarvillkorsavtalet.

Bitwarden följer branschstandardiserade applikationssäkerhetsriktlinjer som inkluderar ett dedikerat säkerhetsingenjörsteam och inkluderar regelbundna granskningar av applikationskällkod och IT-infrastruktur för att upptäcka, validera och åtgärda eventuella säkerhetsbrister.

Den här vitboken ger en översikt över Bitwardens säkerhetsprinciper samt länkar till ytterligare dokument som ger mer detaljer inom specifika områden.

Bitwardens säkerhetsprinciper

Att skydda användardata med Bitwarden-produkter är ett partnerskap mellan Bitwarden-system och anställda, och användarna själva. Detta avsnitt kommer på hög nivå att täcka de viktigaste säkerhetsåtgärderna Bitwarden använder och verktygen Bitwarden gör tillgängliga för

användare för att skydda data som lagras i Bitwarden.

Viktiga säkerhetsåtgärder

Bitwarden använder följande viktiga säkerhetsåtgärder för att skydda data som lagras i Bitwarden:

End-to-end-kryptering: Lås dina lösenord och privat information med end-to-end AES-CBC 256-bitars kryptering med HMAC-autentisering, saltad hashing och nyckelhärledningsfunktioner som PBKDF2 SHA-256 eller Argon2id. Alla kryptografiska nycklar genereras och hanteras av klienten på dina enheter, och all kryptering sker lokalt. Se mer information här.

Noll kunskapskryptering: Bitwarden-teammedlemmar kan inte se dina lösenord. Dina data förblir krypterade från början med din individuella e-postadress och ditt huvudlösenord. Bitwarden lagrar aldrig och kan inte komma åt ditt huvudlösenord eller dina kryptografiska nycklar.

Säker lösenordsdelning: Bitwarden möjliggör säker delning och hantering av känslig data med användare över en hel organisation. En kombination av asymmetrisk och symmetrisk kryptering skyddar känslig information när den delas.

Öppen källkod och tillgänglig källkod: Källkoden för alla Bitwardens mjukvaruprodukter finns på GitHub och vi välkomnar alla att granska, granska och bidra till Bitwardens kodbas. Bitwardens källkod granskas av välrenommerade tredjeparts säkerhetsrevisionsbyråer såväl som oberoende säkerhetsforskare. Dessutom tar Bitwarden Vulnerability Disclosure Program hjälp av hackergemenskapen på HackerOne för att göra Bitwarden säkrare.

Integritet genom design: Bitwarden lagrar alla dina inloggningar i ett krypterat valv som synkroniseras över alla dina enheter. Eftersom den är helt krypterad innan den någonsin lämnar din enhet är det bara du som har tillgång till dina data. Inte ens teamet på Bitwarden kan läsa dina data (även om vi skulle vilja).

Säkerhetsrevision: Tredjeparts säkerhetsgranskningar och utvärderingar av applikationer och/eller plattformen utförs minst en gång per år.

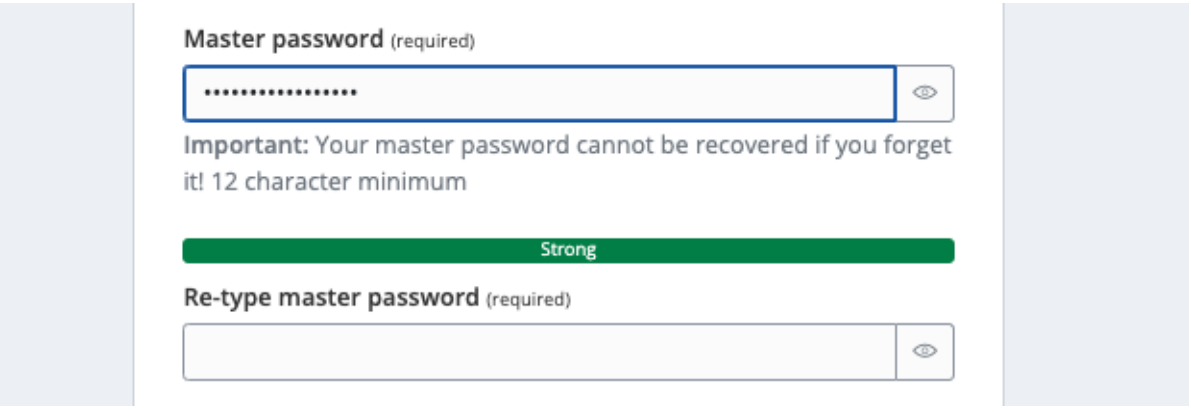
Efterlevnad: Bitwarden följer AICPA SOC2 Type 2 / Data Privacy Framework, GDPR och CCPA-bestämmelser.Läs mer.

Säkerhetsverktyg för användare

Följande verktyg tillhandahålls av Bitwarden och måste åtgärdas av enskilda användare och företag för att optimera kontoskyddet och undvika lockout:

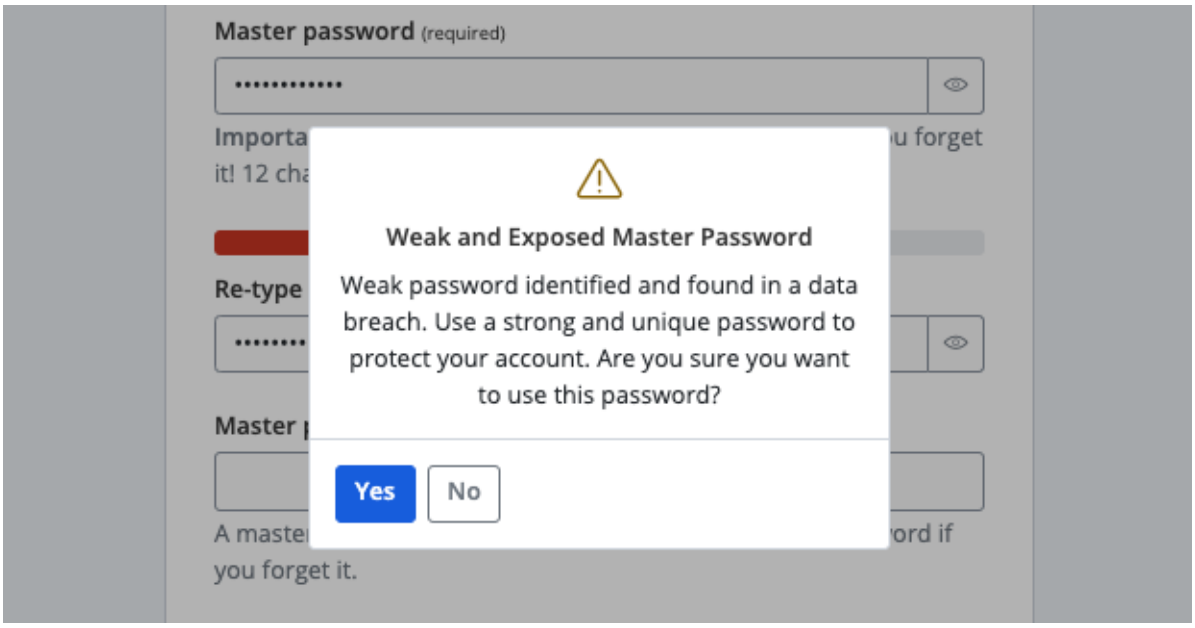
Huvudlösenord

Användardataskyddet i Bitwarden börjar i samma ögonblick som en användare skapar ett konto och ett huvudlösenord. Ett huvudlösenord är den token en användare använder för att komma åt sitt valv, där känslig data lagras. Användare bör skapa sina konton med ett starkt huvudlösenord och Bitwarden inkluderar en lösenordsstyrkemätare som en guide för att hjälpa användare att göra det:



Password strength meter

Användare varnas när de försöker registrera sig med ett svagt huvudlösenord och får även möjlighet att kontrollera kända dataintrång för huvudlösenordet med hjälp av en integration med Have I Been Pwned (HIBP):



Weak or exposed master password

Det är mycket viktigt att användare aldrig glömmer sina huvudlösenord. Huvudlösenord är:

- Raderad eller markerad för borttagning från minnet efter användning.
- Sänds aldrig över internet till Bitwarden-servrar.
- Kan inte ses, läsas eller reverse engineering av någon på Bitwarden.

På grund av detta, och det faktum att dina data är helt krypterade och/eller hashade innan de någonsin lämnar din lokala enhet, **kommer** att glömma ett huvudlösenord resultera i att en användare blir utelåst från sitt konto såvida de inte har nödåtkomst eller aktiv kontoåterställning, som båda kommer att behandlas senare i detta dokument.

> **Tip**
> Users can change their master password from the Bitwarden web app. Learn how.

Alternativa inloggningsmetoder

Bitwarden-klienter erbjuder följande alternativa metoder för autentisering. Vissa av dessa metoder kan också användas för dekryptering vid inloggning:

- **Logga in med enhet**: Initiera en autentiseringsbegäran från en Bitwarden-klient och slutför autentiseringen genom att godkänna begäran på en enhet som du redan är inloggad på. Lär dig hur det fungerar.
- **Logga in med lösenord**: Använd en lösenordsnyckel för att logga in på en Bitwarden-klient och, om lösenordet är PRF-kompatibelt, använd det för att dekryptera dina valvdata. Lär dig hur det fungerar.
- **SSO med betrodda enheter**: SSO med betrodda enheter tillåter användare att autentisera med SSO och dekryptera sitt valv med en enhetslagrad krypteringsnyckel, vilket eliminerar behovet av att ange ett huvudlösenord. Lär dig hur det fungerar.

Tvåstegsinloggning

Tvåstegsinloggning (även kallad "tvåfaktorsautentisering" eller "2FA") är ett extra säkerhetslager för onlinekonton, designat för att skydda åtkomst till Bitwarden även om någon har huvudlösenordet. När tvåstegsinloggning är aktiv måste användarna slutföra ett sekundärt steg när de loggar in på Bitwarden, som att använda en FIDO2-säkerhetsnyckel eller en autentiseringsapp för att bekräfta inloggningsförsöket. Som en bästa praxis rekommenderar **Bitwarden alla användare att aktivera och använda tvåstegsinloggning**.

Bitwarden ger användarna en återställningskod som de kan använda för att stänga av tvåstegsinloggning i händelse av att en sekundär enhet tappas bort, till exempel om en YubiKey försvinner. **Användare bör hämta och spara sin återställningskod omedelbart efter att ha aktiverat funktionen**, eftersom Bitwarden-anställda och system inte har något sätt att avaktivera tvåstegsinloggning för användarnas räkning.

Lär dig mer om tillgängliga tvåstegsinloggningsmetoder, med flera metoder och vad du ska göra i händelse av att en sekundär enhet tappas bort.

Nödåtkomst

Premiumanvändare, inklusive medlemmar av betalda organisationer (familjer, team eller företag) kan utse betrodda nödkontakter som kan begära åtkomst till deras valv i nödfall. Betrodda nödkontakter kan tilldelas antingen visnings- eller övertagandeåtkomst till användarnas konton.

Nödåtkomst använder asymmetrisk kryptering för att tillåta användare att ge en betrodd nödkontakt behörighet att få åtkomst till valvdata i en miljö med noll kunskap:

> **Note**
>
> The following information references encryption key names and processes that are covered in the Hashing, key derivation, and encryption section. Consider reading that section first.

1. En Bitwarden-användare (bidragsgivaren) bjuder in en annan Bitwarden-användare att bli en betrodd nödkontakt (bidragstagaren). Inbjudan (giltig i endast fem dagar) anger en användaråtkomstnivå och inkluderar en begäran om bidragstagarens **RSA Public Key**.

2. Bidragstagaren meddelas om inbjudan via e-post och accepterar inbjudan att bli en betrodd nödkontakt. Vid godkännande lagras bidragstagarens **RSA Public Key** tillsammans med användarposten.

3. Grantor meddelas om inbjudan accepteras via e-post och bekräftar att bidragstagaren är sin betrodda nödkontakt. Vid bekräftelse krypteras bidragsgivarens symmetriska **användarnyckel med hjälp av** bidragstagarens offentliga **RSA-nyckel** och lagras tillsammans med inbjudan. Bidragstagaren meddelas om bekräftelse.

4. En nödsituation inträffar, vilket resulterar i att bidragsmottagaren behöver tillgång till bidragsgivarens valv. Bidragstagaren lämnar in en begäran om akutåtkomst.

5. Bidragsgivaren meddelas om begäran via e-post. Bidragsgivaren kan när som helst manuellt godkänna begäran, annars är begäran bunden av en bemyndigandespecifik väntetid. När begäran godkänns eller väntetiden löper ut, **levereras den** offentliga nyckel-krypterade användarens symmetriska nyckeln **till bidragsmottagaren för dekryptering med bidragstagarens privata** RSA-nyckel.

6. Beroende på den angivna användaråtkomstnivån kommer bidragstagaren antingen:
   - Skaffa visnings-/läsåtkomst till föremål i bidragsgivarens valv.
   - Bli ombedd att skapa ett nytt huvudlösenord för bidragsgivarens valv.

Kontoåterställning

Kontoåterställning tillåter utsedda administratörer för företagsorganisationer att återställa medlemskonton och återställa åtkomst i händelse av att en anställd glömmer sitt huvudlösenord. Företag kan också vilja använda kontoåterställning för att återta äganderätten till en medlems konto när ett anställningsförhållande upphör.

> **Note**
>
> The following information references encryption key names and processes that are covered in the Hashing, key derivation, and encryption section. Consider reading that section first.

När en organisationsmedlem registrerar sig för kontoåterställning kan användarens kontokrypteringsnyckel (aka **User Symmetric Key**) är krypterad med organisationens RSA Public Key. Resultatet lagras som **kontoåterställningsnyckel**.

När en återställningsåtgärd vidtas:

1. Organisationens **RSA Private Key** dekrypteras med **organisationens symmetriska nyckel**.
2. **Användarens kontoåterställningsnyckel dekrypteras med den dekrypterade privata RSA-nyckeln, vilket resulterar i den symmetriska användarnyckeln** (kallas "kontokrypteringsnyckel" i produkten).
3. Den symmetriska **användarnyckeln** krypteras med en ny **huvudnyckel** och en ny **huvudlösenords-hash** seedas från det nya huvudlösenordet, både den **huvudnyckel-krypterade användarsymmetriska nyckeln** och **huvudlösenords-hashen** ersätter redan existerande värden på serversidan.
4. **Användarens symmetriska användarnyckel** är krypterad med organisationens offentliga **RSA-nyckel och** ersätter den tidigare **kontoåterställningsnyckeln** med en ny.

Hashing, nyckelhärledning och kryptering

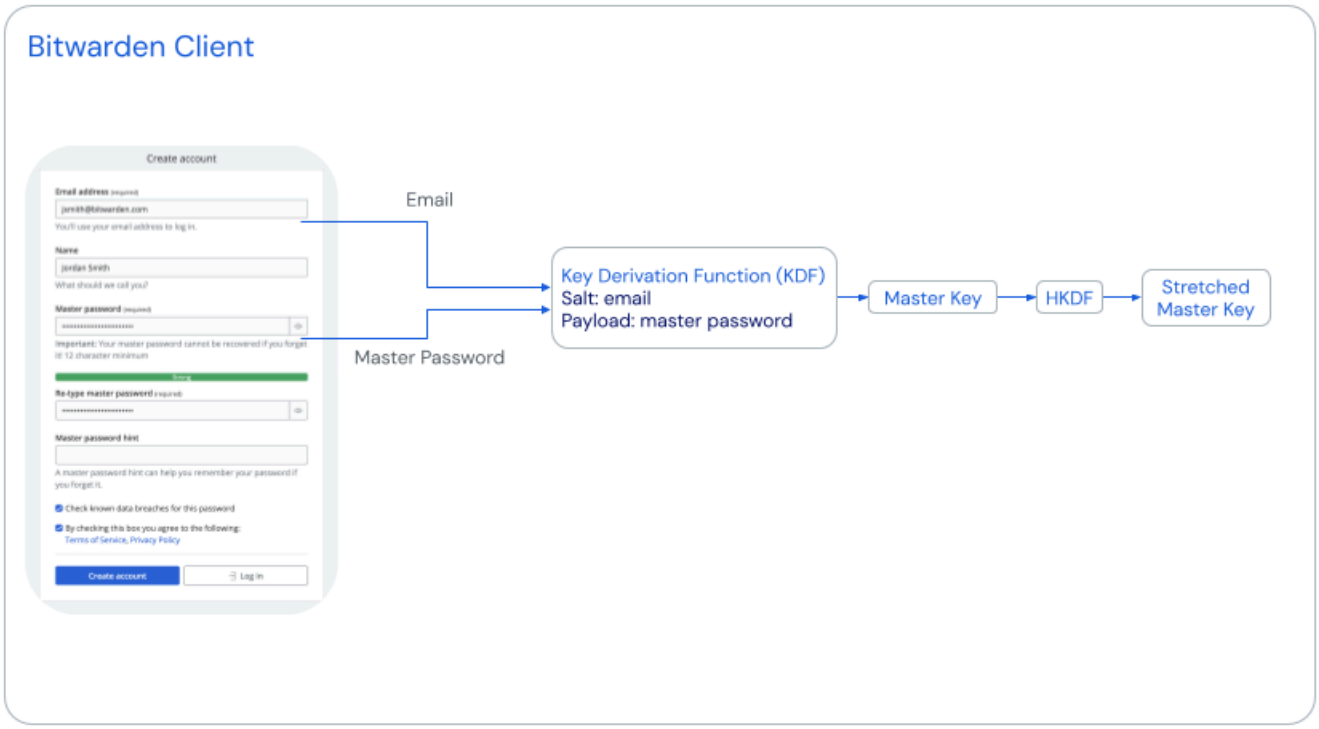
Det här avsnittet kommer att täcka de kryptografiska processer som implementeras när en användare skapar ett Bitwarden-konto och sedan loggar in för att komma åt sina data:

Skapa konto

När ett konto skapas använder Bitwarden lösenordsbaserad nyckelhärledningsfunktion 2 (PBKDF2) med 600 000 iterationsrundor för att sträcka ut användarens huvudlösenord med ett salt av användarens e-postadress.

> **Note**
>
> Though user accounts are initiated with PBKDF2, users may elect to change their key derivation function to Argon2id after the account has been created. Learn how to change the KDF algorithm.

Det resulterande saltade värdet är 256-bitars **huvudnyckeln**. **Huvudnyckeln** sträcks sedan igen till 512-bitar med användning av HMAC-baserad extrahera-och-expandera nyckelhärledningsfunktion (HKDF), vilket resulterar i den **utsträckta huvudnyckeln**. **Huvudnyckeln** och den **sträckta huvudnyckeln** lagras aldrig på eller överförs till Bitwarden-servrar:

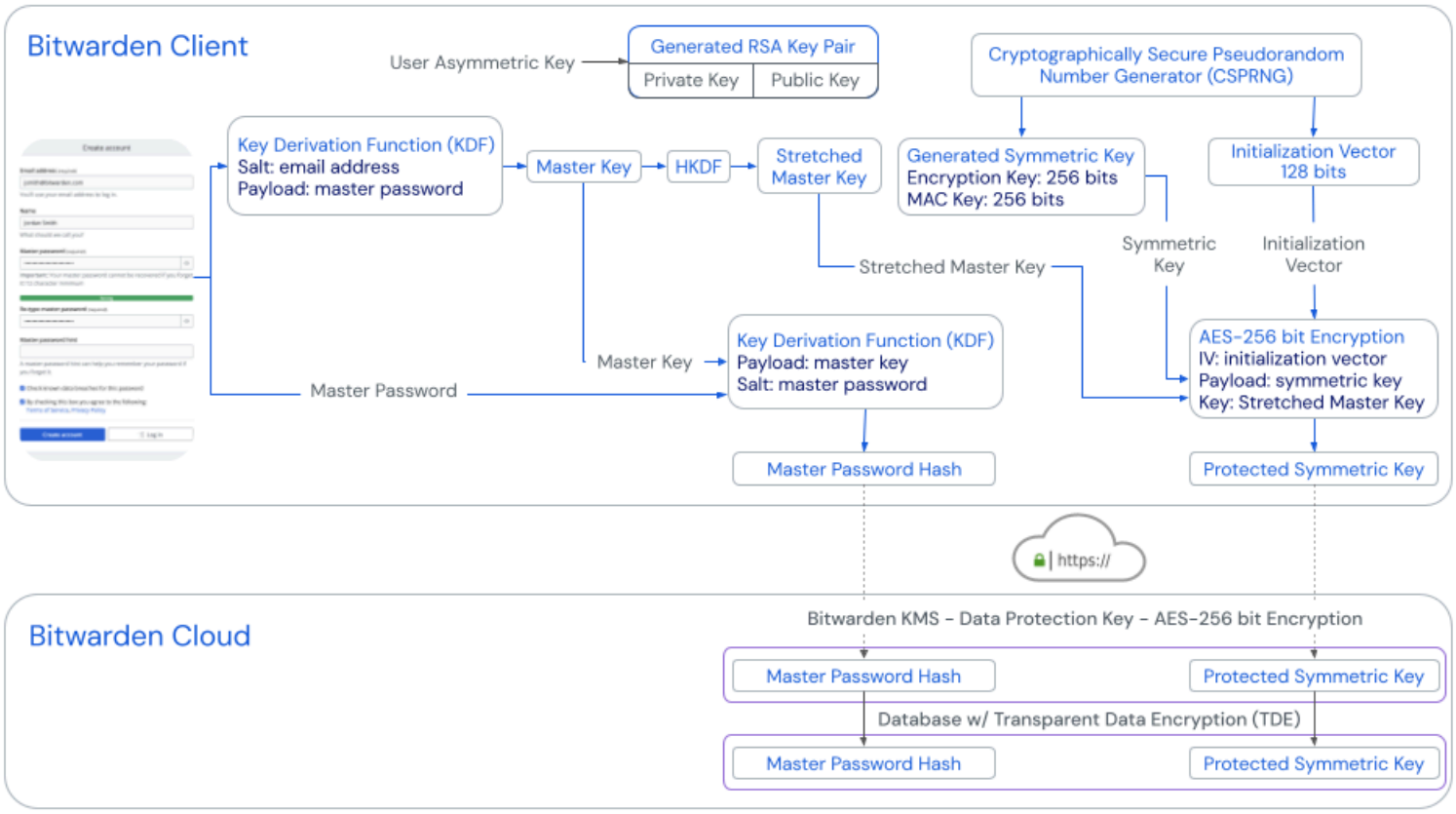


Password-based key derivation

Därefter **skapas en 512-bitars genererad symmetrisk nyckel och 128-bitars** initialiseringsvektor med hjälp av en kryptografiskt säker pseudoslumptalsgenerator (CSPRNG). Den **genererade symmetriska nyckeln** krypteras med AES-256-bitars kryptering med hjälp av **Stretched Master Key** och **initialiseringsvektor.** Resultatet kallas den **skyddade symmetriska nyckeln** och är huvudnyckeln som är kopplad till användaren. Den **skyddade symmetriska nyckeln** skickas till Bitwarden-servern när kontot skapas och skickas tillbaka till Bitwarden-klientapplikationer vid synkronisering.

Ett asymmetriskt nyckelpar skapas också när användaren registrerar sitt konto. Detta **genererade RSA-nyckelpar** används när användaren skapar en organisation och i processer som nödåtkomst som kan användas för att dela data mellan användare.

Slutligen genereras en **Master Password Hash** med hjälp av PBKDF-SHA256 med en nyttolast av **Master Key** och med en salt av huvudlösenordet. **Huvudlösenords-hash** skickas till Bitwarden-servern när kontot skapas och loggas in och används för att autentisera användarkontot. När det når servern hashas huvudlösenordet igen med PBKDF2-SHA256 med ett slumpmässigt salt och 600 000 iterationer:



Bitwarden password hashing, key derivation, and encryption

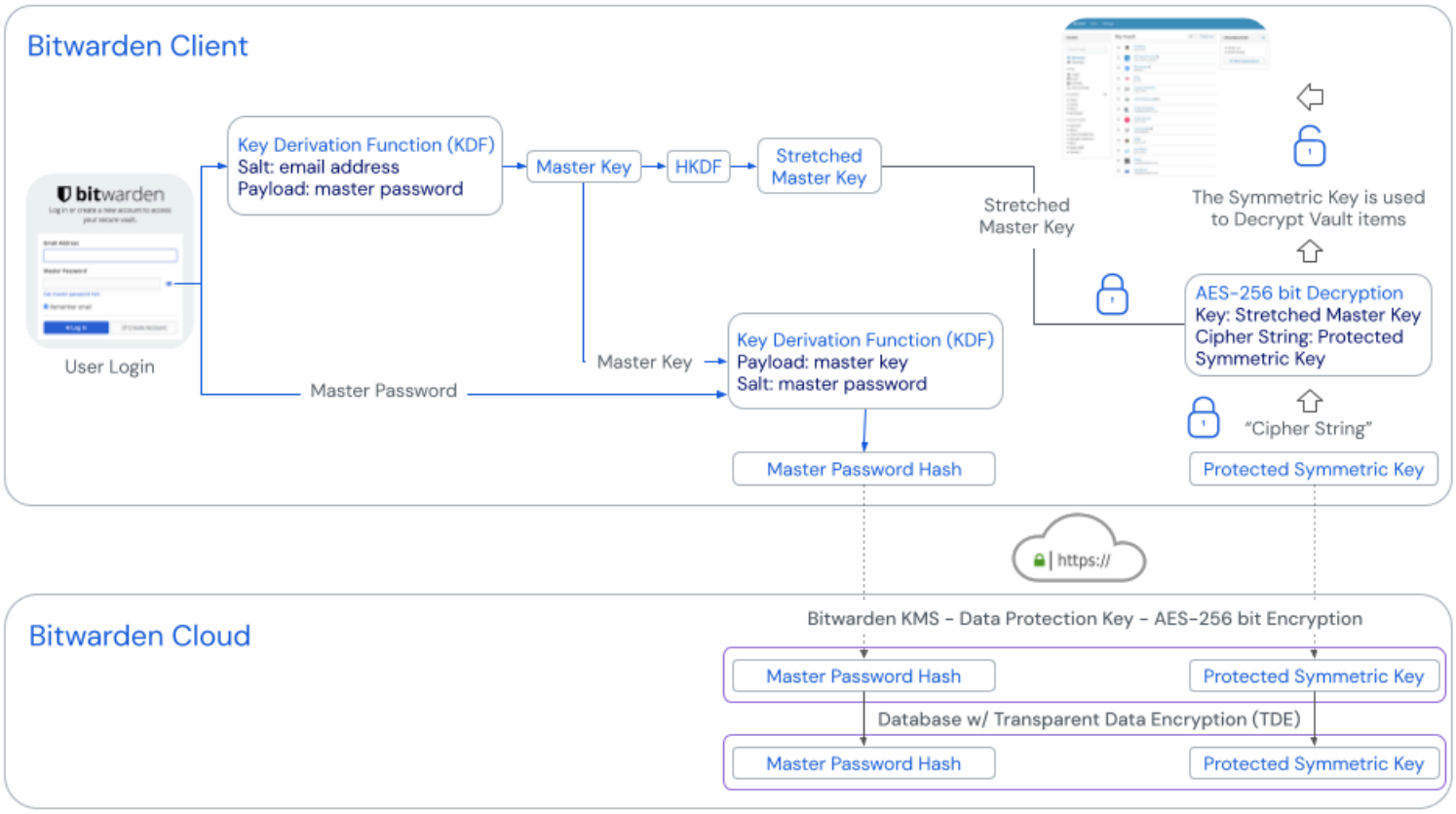
Autentisering och dekryptering

Användare måste ange en e-postadress och, vanligtvis, ett huvudlösenord för att logga in på ett Bitwarden-konto.

När de gör det använder Bitwarden lösenordsbaserad nyckelhärledningsfunktion 2 (PBKDF2) med en standard på 600 000 iterationsrundor för att sträcka ut huvudlösenordet med en salt av kontots e-postadress. Det resulterande saltade värdet är 256-bitars **huvudnyckeln**. En **huvudlösenordshash**, genererad med PBKDF-SHA256 med en nyttolast av **huvudnyckeln** och med ett salt av huvudlösenordet, skickas till servern för autentisering genom att jämföra hashen med den som lagras på serversidan.

> **ⓘ Note**
>
> Though user accounts are initiated with PBKDF2, users may elect to change their key derivation function to Argon2id after the account has been created. Learn how to change the KDF algorithm.

Samtidigt sträcks **huvudnyckeln** till 512-bitars längd med hjälp av HMAC-baserad extrahera-och-expandera nyckelderiveringsfunktion (HKDF), vilket resulterar i den **utsträckta huvudnyckeln**. Den **skyddade symmetriska nyckeln**, som lagras på serversidan och hämtas av klienten, dekrypteras med denna **utsträckta huvudnyckel**. Den resulterande **symmetriska nyckeln** används av klienten för att dekryptera valvdata. Denna dekryptering görs helt på Bitwarden-klienten. Huvudlösenord och **utsträckta huvudnycklar** lagras aldrig på eller överförs till Bitwarden-servrar:



An overview of user login

Bitwarden håller inte själva huvudlösenordet lagrat lokalt eller i minnet på Bitwarden-klienten. Din kontokrypteringsnyckel (**User Symmetric Key**) sparas i minnet medan appen är upplåst för att dekryptera valvdata.

När Bitwarden-klienten är låst rensas dina krypteringsnycklar och valvdata så aggressivt som möjligt från minnet. Efter en viss period av inaktivitet på låsskärmen laddar vi om applikationsprocesser eller utför andra rensningsåtgärder för att säkerställa att eventuellt överblivet hanterat minne också rensas eller förväntar oss att underliggande system rensar det minnet när det ligger utanför vår kontroll. Vi gör vårt bästa för att se till att all data som kan finnas i minnet för att applikationen ska fungera bara lagras i minnet så länge du behöver den och att minnet rensas upp på lämpligt sätt när applikationen är låst. Vi granskar regelbundet Bitwarden-applikationens minnestillstånd och justerar processer när det är möjligt för att rensa känsligt innehåll när det är låst.

Roterar kontokrypteringsnyckeln

Under en lösenordsändring har användare möjlighet att rotera (dvs. ändra) sin **symmetriska användarnyckel** (kallad "kontokrypteringsnyckel" i produkten). Att rotera den här nyckeln är en bra idé om användare tror att deras tidigare huvudlösenord har äventyrats eller att data som de har lagrat i Bitwarden har stulits från en av deras enheter.

> **⚠ Warning**
>
> Rotating the account's encryption key is a sensitive operation, which is why it is not a default option when changing a master password. A key rotation involves generating a new, random encryption key for the account and **re-encrypting all vault data** using this new key. See additional details in this article.

Variationer

Det här avsnittet kommer att täcka varianter av krypteringsprocesser när användare använder Logga in med enhet, Logga in med lösenord eller SSO med betrodda enheter.

Logga in med enheten

När inloggning med en enhet initieras:

1. Den initierande klienten skickar en begäran till Bitwarden-servern, som inkluderar kontots e-postadress, en unik **Auth-request Public Key**[a] och en åtkomstkod.
2. Registrerade enheter, det vill säga mobil- eller stationära appar som är inloggade och har en enhetsspecifik GUID lagrad på Bitwarden-servern, tillhandahålls begäran.
3. När begäran har godkänts, krypterar den godkännande klienten kontots **huvudnyckel** och **huvudlösenordshash** med hjälp **av den offentliga auktoriseringsnyckeln** som finns med i begäran.
4. Den godkännande klienten skickar sedan den **krypterade huvudnyckeln** och den **krypterade huvudlösenords-hash** till Bitwarden-servern och begäran markeras som uppfylld.
5. Den initierande klienten begär den **krypterade huvudnyckeln** och den **krypterade huvudlösenordshashen** från Bitwarden-servern.
6. Den initierande klienten **dekrypterar sedan huvudnyckeln och huvudlösenordshash lokalt med hjälp av den privata nyckeln för** autentiseringsbegäran.
7. Den initierande klienten använder sedan åtkomstkoden och uppfylld autentiseringsbegäran för att autentisera användaren med Bitwarden Identity-tjänsten.

[a] - **Auth-request Public and Private Keys** genereras unikt för varje lösenordslös inloggningsförfrågan och existerar bara så länge som begäran gör det. Begäranden löper ut och rensas från Bitwarden-servern var 15:e minut om de inte godkänns eller nekas.

Logga in med lösenord

Följande beskriver mekaniken för att logga in med lösenord när användarnas lösenord är inställda för kryptering. Användare kan välja att inte använda sina lösenord för kryptering istället.

När en lösenordsnyckel är registrerad för inloggning till Bitwarden:

1. Ett par **av** offentliga och privata nyckelnyckel genereras av autentiseringsverktyget via WebAuthn API. Detta nyckelpar, per definition, är det som utgör din lösenordsnyckel. Attestationsalternativ, som vilken krypteringsalgoritm som ska användas, och tillhandahålls av Bitwarden till autentiseringsenheten.
2. En **symmetrisk PRF-nyckel** genereras av autentiseringsenheten via WebAuthn API:s PRF-tillägg. Denna nyckel härrör från en **intern hemlighet** som är unik för din lösenordsnyckel och ett **salt** från Bitwarden.
3. Ett **PRF offentligt och privat nyckelpar** genereras av Bitwarden-klienten. Den offentliga PRF-nyckeln krypterar din symmetriska **användarnyckel (**kallad "kontokrypteringsnyckel" i produkten), som din klient kommer att ha tillgång till genom att vara inloggad och upplåst, och den resulterande **PRF-krypterade användarsymmetriska nyckeln** skickas till servern.
4. Den privata **PRF-nyckeln** krypteras med den symmetriska **PRF-nyckeln (**se steg 2) och den resulterande **PRF-krypterade privata nyckeln** skickas till servern.
5. Din klient skickar data till Bitwarden-servrar för att skapa en ny lösenordsnyckelpost för ditt konto. Om din lösenordsnyckel är registrerad med stöd för valvkryptering och dekryptering, inkluderar denna post:
   - Lösenordets namn

- Den offentliga lösenordsnyckeln
- PRF:s publika nyckel
- Den PRF-krypterade symmetriska användarnyckeln
- Den PRF-krypterade privata nyckeln

Din **privata lösenordsnyckel**, som krävs för att utföra autentisering, lämnar alltid klienten i ett krypterat format.

När en lösenordsnyckel används för att logga in och, specifikt, för att dekryptera dina valvdata:

1. Genom att använda WebAuthn API med publik nyckelkryptering, bekräftas och bekräftas din autentiseringsbegäran.
2. Din **PRF-krypterade symmetriska användarnyckel (**kallad "kontokrypteringsnyckel" i produkten) och **PRF-krypterade privata nyckel** skickas från servern till din klient.
3. Genom att använda samma **salt** som Bitwarden tillhandahåller och den **interna hemligheten** som är unik för din lösenordsnyckel, återskapas **PRF Symmetric Key** lokalt.
4. Den symmetriska **PRF-nyckeln** används för att dekryptera din **PRF-krypterade privata nyckel**, vilket resulterar i din privata **PRF-nyckel.**
5. Den **privata PRF-nyckeln** används för att dekryptera din **PRF-krypterade symmetriska användarnyckel**, vilket resulterar i din **symmetriska användarnyckel**. Detta används för att dekryptera dina valvdata.

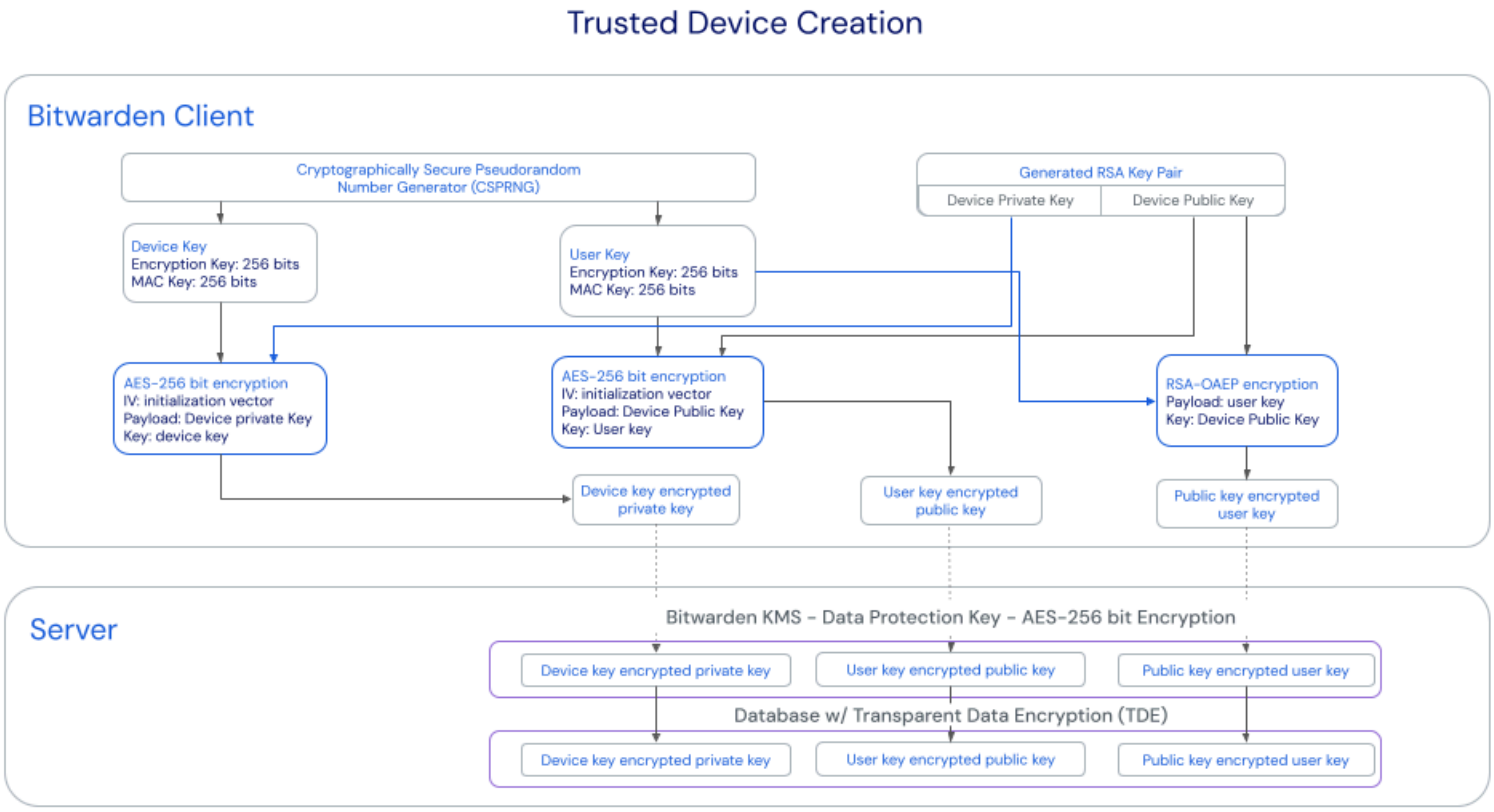
SSO med betrodda enheter

Följande avsnitt beskriver krypteringsprocesser och nyckelutbyten som sker under olika procedurer för betrodda enheter:

⇒Onboarding

När en ny användare går med i en organisation skapas en **kontoåterställningsnyckel** (läs mer) genom att kryptera deras kontokrypteringsnyckel med **organisationens offentliga nyckel**. Kontoåterställning krävs för att aktivera SSO med betrodda enheter.

Användaren tillfrågas sedan om de vill komma ihåg, eller lita på, enheten. När de väljer att göra det:



Create a trusted device

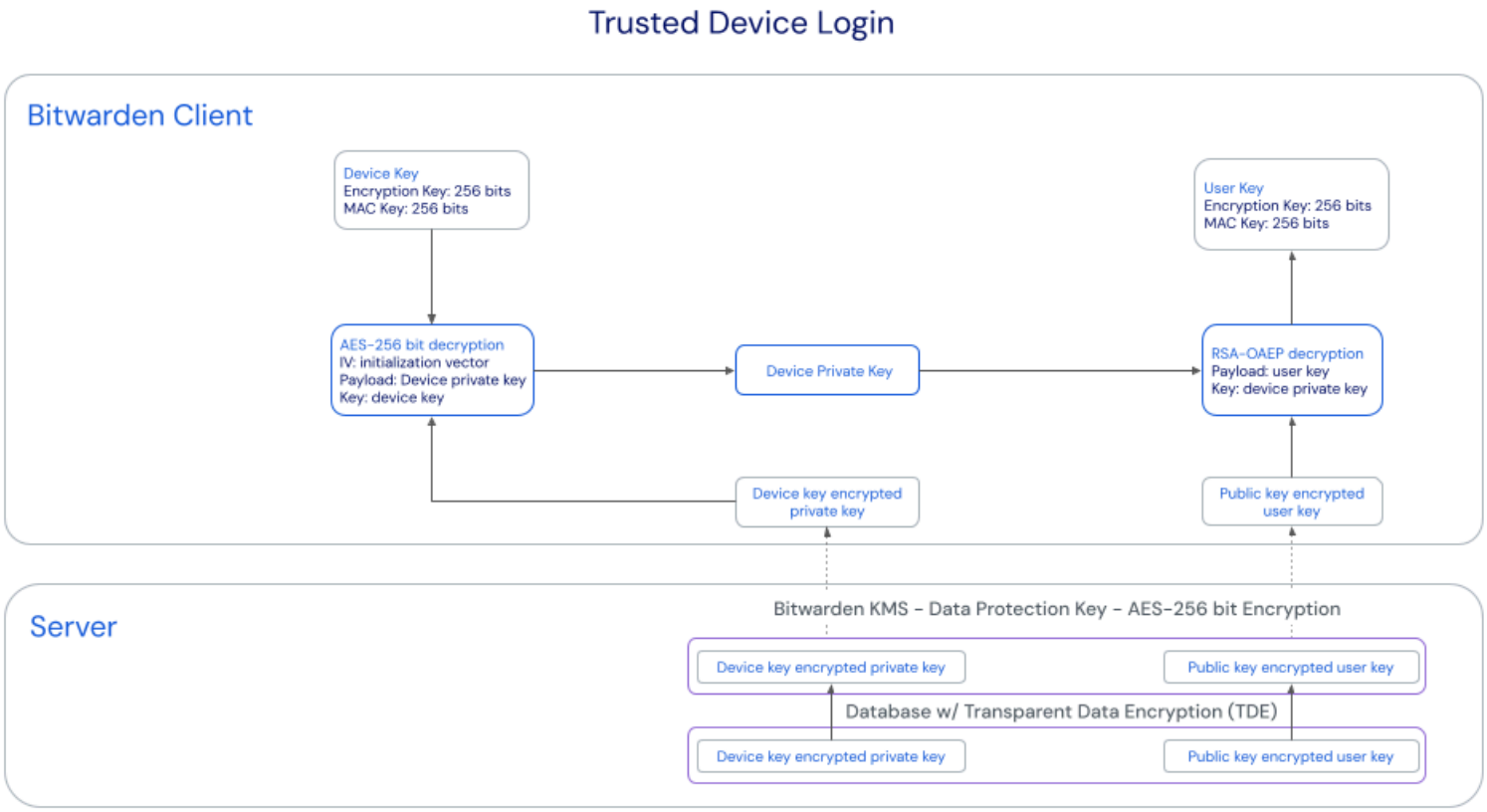
1. En ny **enhetsnyckel** genereras av klienten. Denna nyckel lämnar aldrig klienten.
2. Ett nytt RSA-nyckelpar, kallat **Device Private Key** och **Device Public Key**, genereras av klienten.
3. Användarens kontokrypteringsnyckel krypteras med den okrypterade **enhetens publika nyckel** och det resulterande värdet skickas till servern som den **offentliga nyckelkrypterade användarnyckeln**.
4. Den offentliga **enhetens nyckel** krypteras med **användarens kontokrypteringsnyckel och det resulterande värdet skickas till servern som den användarnyckelkrypterade publika nyckeln**.
5. **Enhetens privata nyckel** krypteras med den första **enhetsnyckeln** och det resulterande värdet skickas till servern som den **enhetsnyckelkrypterade privata nyckeln**.

Den **offentliga nyckel-krypterade användarnyckeln** och **enhetsnyckel-krypterade privata nyckel** kommer, avgörande, att skickas från server till klient när en inloggning initieras.

Den **användarnyckel-krypterade publika nyckeln** kommer att användas om användaren behöver rotera sin kontokrypteringsnyckel.

⇒Loggar in

När en användare autentiserar med SSO på en redan betrodd enhet:



Use a trusted device

1. Användarens **Public Key-Encrypted User Key**, som är en krypterad version av kontokrypteringsnyckeln som används för att dekryptera valvdata, skickas från servern till klienten.

2. Användarens **Device Key-Encrypted Private Key**, vars okrypterade version krävs för att dekryptera den **Public Key-Encrypted User Key**, skickas från servern till klienten.

3. Klienten dekrypterar den **enhetsnyckel-krypterade privata nyckeln** med hjälp av **enhetsnyckeln**, som aldrig lämnar klienten.

4. Den nu okrypterade **enhetens privata nyckel** används för att dekryptera den **offentliga nyckel-krypterade användarnyckeln**, vilket resulterar i användarens kontokrypteringsnyckel.

5. Användarens kontokrypteringsnyckel dekrypterar valvdata.

⇒Godkännande

När en användare autentiserar med SSO och väljer att dekryptera sitt valv med en opålitlig enhet (dvs. en **Device Symmetric Key finns** inte på den enheten), måste de välja en metod för att godkänna enheten och eventuellt lita på den för framtida användning utan ytterligare godkännande. Vad som händer härnäst beror på det valda alternativet:

- **Godkänn från en annan enhet**:

  1. Processen som dokumenteras här utlöses, vilket resulterar i att klienten har erhållit och dekrypterat kontokrypteringsnyckeln.

  2. Användaren kan nu dekryptera sina valvdata med den dekrypterade kontokrypteringsnyckeln. Om de har valt att lita på enheten etableras förtroende med klienten enligt beskrivningen på **fliken** Onboarding.

- **Begär administratörsgodkännande**:
  1. Den initierande klienten POSTAR en begäran, som inkluderar kontots e-postadress, en unik offentlig nyckel för autentiseringsbegäran[a] och en åtkomstkod, till en tabell för autentiseringsbegäran i Bitwarden-databasen.
  2. Administratörer kan godkänna eller neka begäran på sidan Enhetsgodkännanden.
  3. När begäran godkänns av en administratör, krypterar den godkännande klienten användarens kontokrypteringsnyckel med hjälp av den **offentliga autentiseringsnyckeln** som finns med i begäran.
  4. Den godkännande klienten PUTAR sedan den krypterade kontokrypteringsnyckeln till posten för autentiseringsbegäran och markerar begäran som uppfylld.
  5. Den initierande klienten HÅR den krypterade kontokrypteringsnyckeln **och dekrypterar** den lokalt med den privata nyckeln för autentiseringsbegäran.
  6. Genom att använda den dekrypterade kontokrypteringsnyckeln etableras förtroende med klienten enligt beskrivningen på **fliken** Onboarding.

[a] – **Offentliga** och **privata autentiseringsnycklar** genereras unikt för varje lösenordslös inloggningsförfrågan och existerar bara så länge som begäran gör det. Ej godkända förfrågningar upphör att gälla efter 1 vecka.

- **Godkänn med huvudlösenord**:
  1. Användarnas kontokrypteringsnyckel hämtas och dekrypteras enligt dokumentationen i avsnittet Autentisering och dekryptering av säkerhetsdokumentet.
  2. Genom att använda den dekrypterade kontokrypteringsnyckeln etableras förtroende med klienten enligt beskrivningen på **fliken** Onboarding.

⇒Nyckelrotation

> **ⓘ Note**
>
> Only users who have a master password can rotate their account encryption key. Learn more.

När en användare roterar sin kontokrypteringsnyckel, under den normala rotationsprocessen:

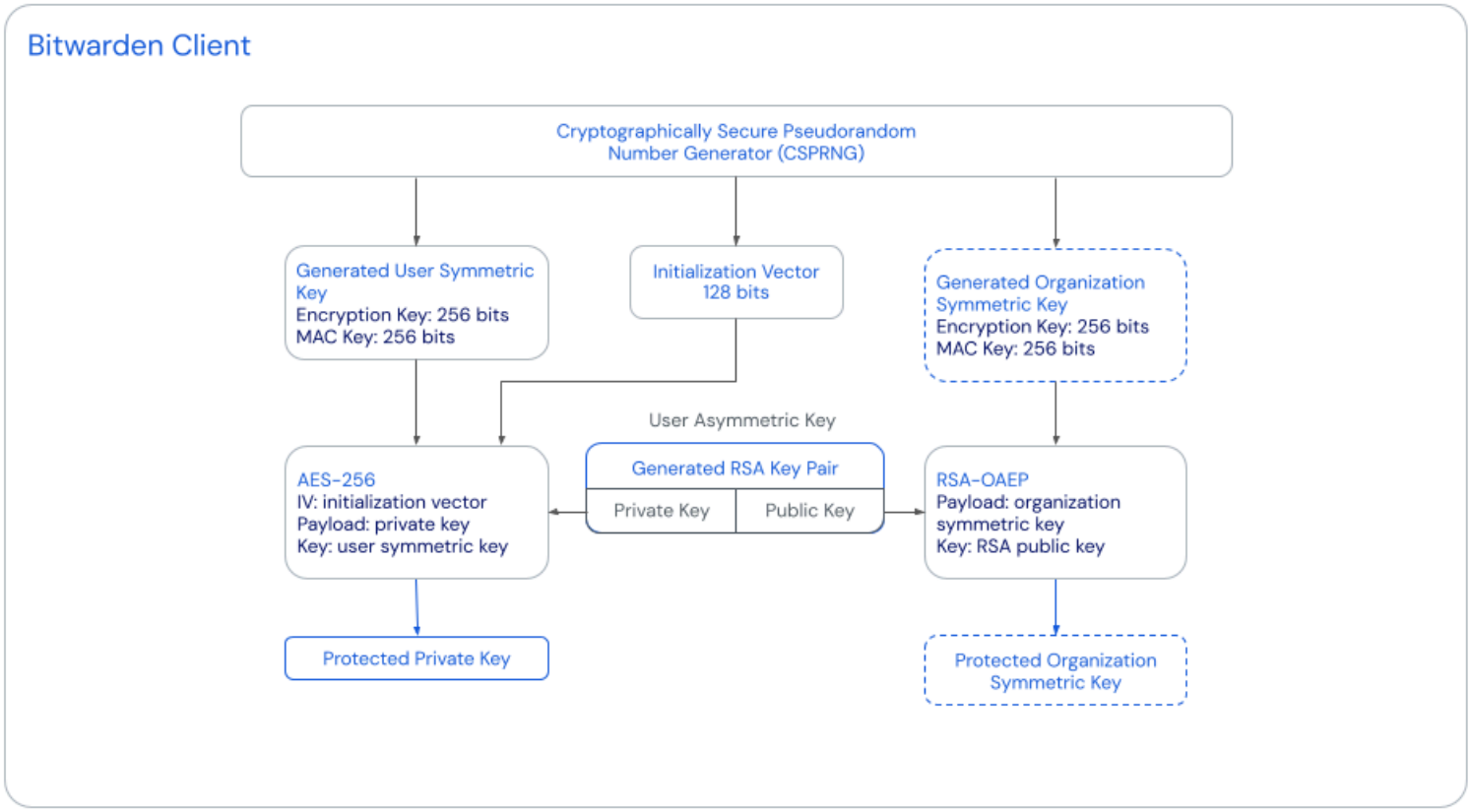
1. Den **användarnyckelkrypterade publika nyckeln** skickas från servern till klienten och dekrypteras sedan med den gamla kontokrypteringsnyckeln (aka **Användarnyckel), vilket** resulterar i **enhetens publika nyckel**.
2. Användarens nya kontokrypteringsnyckel krypteras med den okrypterade **enhetens publika nyckel** och det resulterande värdet skickas till servern som den nya **offentliga nyckelkrypterade användarnyckeln**.
3. Den offentliga **enhetens nyckel** krypteras med **användarens nya kontokrypteringsnyckel och det resulterande värdet skickas till servern som den nya användarnyckelkrypterade publika nyckeln**.
4. Betrodda enhetskrypteringsnycklar för alla andra enheter som finns kvar på serverlagring rensas för användaren. Detta lämnar endast de tre nödvändiga nycklarna (**public Key-Encrypted User Key**, **User Key-Encrypted Public Key** och **Device Key-Encrypted Private Key** som inte ändrades av denna process) för den enstaka enheten kvar på servern.

Alla nu opålitliga klienter måste återupprätta förtroendet genom en av metoderna som beskrivs på **fliken** Godkännande.

Dela data mellan användare

Samarbete är en av de ledande fördelarna med att använda en lösenordshanterare. För att möjliggöra delning måste du först skapa en organisation. En Bitwarden-organisation är en enhet som kopplar samman användare som vill dela objekt. En organisation kan vara en familj, ett team, ett företag eller någon annan typ av grupp som vill dela data.

Det här avsnittet kommer att täcka de kryptografiska processer som implementeras för att säkerställa en säker, end-to-end, noll kunskapskrypteringsmetod för att dela data samt de ytterligare säkerhetsåtgärder som implementeras för att säkerställa kontroll av dina data:



Organization key protection and exchange

När du skapar en organisation

När du skapar en organisation används en Cryptographically Secure Pseudorandom Number Generator (CSPRNG) för att generera **organisationens symmetriska nyckel**. Den här nyckeln är vad som används för att kryptera valvdata som ägs av organisationen, därför kräver delning av data med organisationsmedlemmar säker åtkomst till **organisationens symmetriska nyckel**. Den oskyddade **organisationens symmetriska nyckeln** lagras aldrig på Bitwarden-servrar.

Så snart **organisationens symmetriska nyckel** har skapats används RSA-OAEP för att kryptera den med organisationsskaparens **offentliga RSA-nyckel**.

> **Note**
>
> A **RSA Key Pair** is generated for every user upon account creation, regardless of whether they are an organization member or not, so this key will already exist prior to organization creation. The **RSA Private Key**, the use for which is described below, is stored encrypted with the user's **User Symmetric Key**, so users must be fully logged in to gain access to it.

Det resulterande värdet av denna operation kallas den **skyddade organisationens symmetriska nyckel** och skickas till Bitwarden-servrar.

När organisationsskaparen, eller någon organisationsmedlem, loggar in på sitt konto, använder klientapplikationen den dekrypterade **RSA-privata nyckeln** för att dekryptera den **skyddade organisationens symmetriska nyckel**, vilket resulterar i den **symmetriska organisationsnyckeln**. Med hjälp av detta dekrypteras organisationsägda valvdata lokalt.

När användare går med i en organisation

Processen för efterföljande användare att gå med i en organisation är ganska lik, men vissa skillnader är värda att notera.

Först bekräftar en etablerad medlem i organisationen, särskilt någon med behörighet att ta med andra användare, användaren till organisationen. Denna etablerade medlem har, i kraft av att ha redan loggat in på sitt konto och gått igenom organisationens datadekrypteringsprocess som beskrivs i föregående avsnitt, tillgång till den dekrypterade **organisationssymmetriska nyckeln**.

Så när den nya användaren har bekräftats, når den etablerade medlemmens klient ut till Bitwardens servrar, hämtar den nya användarens **RSA Public Key**, som lagras på Bitwarden-servrar vid tidpunkten för kontoskapandet, och krypterar den dekrypterade **organisationens symmetriska nyckeln** med den. Detta resulterar i en ny symmetrisk nyckel **för** skyddad organisation som skickas till Bitwardens servrar och lagras för den nya medlemmen.

> **ⓘ Note**
>
> Each **Protected Organization Symmetric Key** is unique to its user, but each will decrypt to the same required **Organization Symmetric Key** when decrypted with its specific user's **RSA Private Key**.

När den nya användaren loggar in på sitt konto använder klientapplikationen den dekrypterade privata **RSA-nyckeln** för att dekryptera den nya symmetriska nyckeln för **den** skyddade organisationen, vilket resulterar i den råa **organisationssymmetriska nyckeln**. Med hjälp av detta dekrypteras organisationsägda valvdata lokalt.

Ytterligare säkerhetsåtgärder

Åtkomstkontroller, behörigheter och roller

Bitwarden-organisationer använder samlingar, projekt och grupper för att logiskt gruppera valvdata och användare:

- **Samlingar och projekt**: Organisera dina valvdata logiskt i diskreta enheter för att säkerställa att medlemmar får tillgång till alla och bara de resurser de behöver.
- **Grupper**: Organisera dina medlemmar logiskt i diskreta enheter för att säkerställa att alla får tillgång till allt och bara det de behöver.
- **Medlemsroller**: Tilldela roller till medlemmar för att ge dem tillgång till lämplig nivå av verktyg inom ramen för din organisation.
- **Behörigheter**: Ange vilka åtgärder dina medlemmar får vidta med valvdata som de har fått åtkomst till.

Händelseloggar

Händelseloggar innehåller tidsstämplad, detaljerad information om vilka åtgärder eller förändringar som har inträffat inom en organisation. Dessa loggar är användbara för att undersöka ändringar i autentiseringsuppgifter eller konfiguration och är mycket användbara för granskningsspår och felsökningsändamål. Händelseloggar är tillgängliga för Teams och Enterprise-organisationer för både Password Manager och Secrets Manager. Läs mer om händelseloggar.

Team och företagsorganisationer kan också använda Bitwardens offentliga API för att samla in mer data för sina händelseloggar.

SIEM-integrationer

Flera integrationer av säkerhetsinformation och händelsehantering (SIEM) är tillgängliga för Bitwarden:

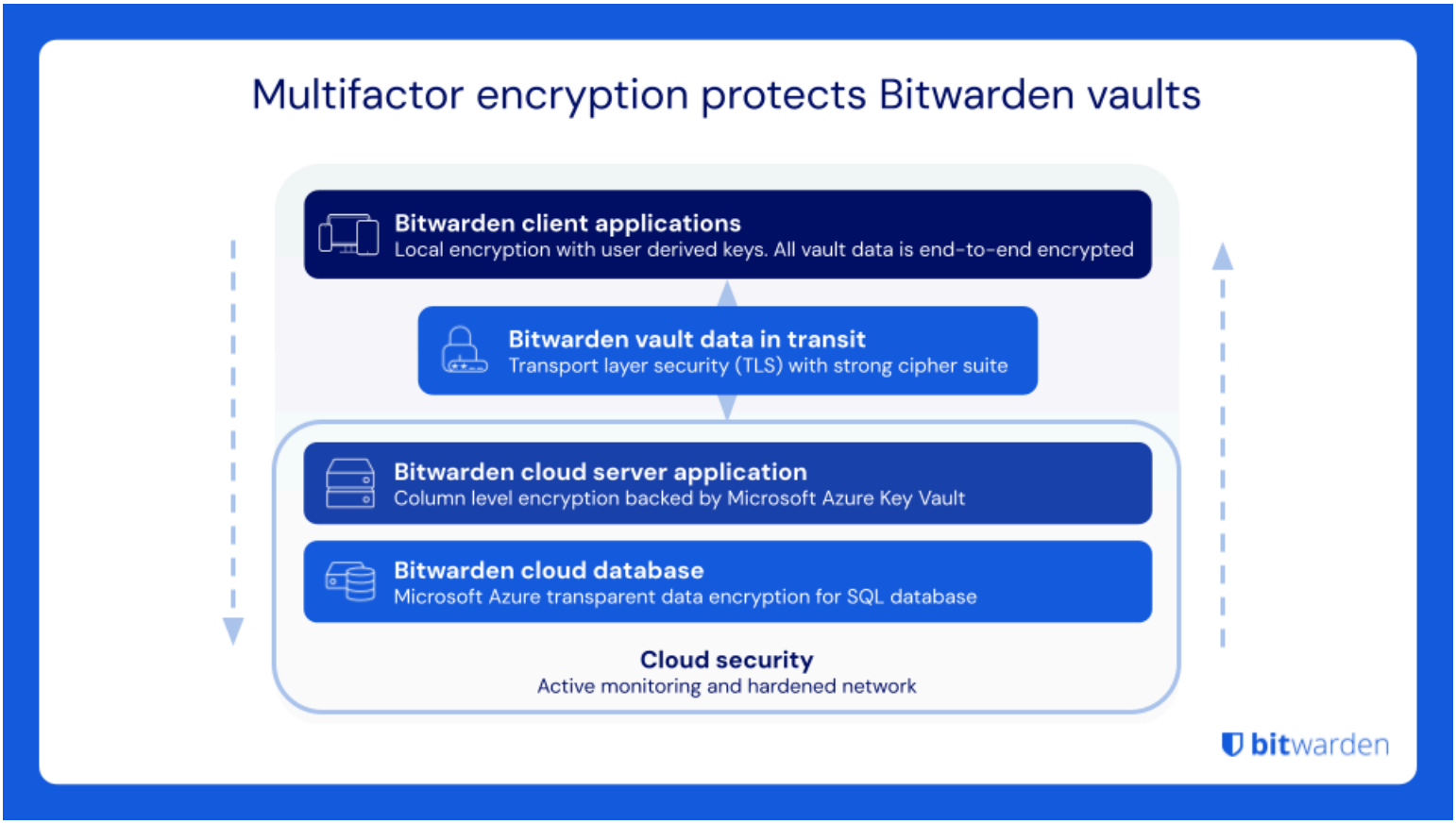
- Splunk

- Panter
- Elastisk

För andra SIEM-system kan en kombination av data från API och CLI användas för att samla in data. Denna process beskrivs här.

Dataskydd

Detta avsnitt kommer att täcka de åtgärder som vidtagits för att säkerställa att data förblir säkra:



Multifactor encryption

Hur valvdata krypteras

Alla valvdata (inloggningar, kort, identiteter, anteckningar och hemligheter) är skyddade med end-to-end-kryptering. Data som du väljer att lagra i Bitwarden lagras först som ett objekt som kallas chiffer. Chiffer krypteras lokalt när ett valvobjekt skapas, redigeras eller importeras med en unik, slumpmässig, 64-byte **chiffernyckel**. Varje **chiffernyckel** krypteras med antingen den **symmetriska användarnyckeln** eller den symmetriska organisationsnyckeln**, beroende på om objektet är individuellt eller** organisatoriskt ägt, innan det skickas till Bitwardens servrar. Dessa krypteringsoperationer utförs helt på Bitwarden-klientapplikationen.

När en användare loggar in på Bitwarden får klienten åtkomst till sin symmetriska **användarnyckel** genom att dekryptera sin **skyddade symmetriska nyckel** med den **utsträckta huvudnyckeln**. Om de är medlem i en organisation får kunden tillgång till **organisationens symmetriska nyckel** genom sin privata **RSA-nyckel.** Med en av dessa nycklar dekrypteras **chiffernycklar** lokalt och det resulterande värdet används för att dekryptera data för enskilda eller organisationers valv.

När en användare roterar sin kontokrypteringsnyckel, här kallad **användarens symmetriska nyckel**, krypteras varje befintlig **krypteringsnyckel** med den nya **symmetriska användarnyckeln**.

> **Note**
>
> In the case of attachments, the **Cipher Key** is used to encrypt the attachment's metadata, specifically the file name and size. The **Cipher Key** is also used to encrypt the **Attachment Key**, which in turn is used to encrypt the attachment data itself.

Vault hälsorapporter

Arkivhälsorapporter kan användas för att utvärdera säkerheten för data som lagras i Bitwarden Password Manager. Rapporter, till exempel rapporterna Återanvända lösenord och svaga lösenord, körs lokalt på Bitwarden-klientapplikationen. Detta gör att kränkande föremål kan identifieras utan att Bitwarden någonsin har tillgång till okrypterade versioner av denna data. Läs mer om de tillgängliga hälsorapporterna för valv.

Dataskydd under transport

Bitwarden använder TLS/SSL för att säkra kommunikation mellan Bitwarden-klienter och användarenheter till Bitwarden-molnet. Bitwardens TLS-implementering använder X.509-certifikat för serverautentisering och nyckelutbyte och en stark chiffersvit för bulkkryptering. Bitwarden-servrar är konfigurerade att avvisa svaga chiffer och protokoll.

Bitwarden implementerar även HTTP-säkerhetsrubriker som HTTP Strict Transport Security (HSTS), som kommer att tvinga alla anslutningar att använda TLS. Detta extra skyddslager med HSTS minskar riskerna för nedgraderingsattacker och felkonfiguration.

Dataskydd i vila

Bitwarden krypterar och/eller hashar alltid din data på din lokala enhet innan den skickas till molnservrarna för synkronisering. Bitwarden-servrar används endast för att lagra och synkronisera krypterad valvdata. Det är inte möjligt att få dina okrypterade data från Bitwardens molnservrar. Specifikt använder Bitwarden AES 256-bitars kryptering samt PBKDF2 SHA-256 eller Argon2id för att säkra dina data. Nyckelord, när de lagras i valvet, genereras med hjälp av ES256-algoritmen.

AES är en standard inom kryptografi och används av den amerikanska regeringen och andra statliga myndigheter runt om i världen för att skydda topphemlig data. Med korrekt implementering och en stark krypteringsnyckel (dvs ditt huvudlösenord) anses AES vara okrossbar.

PBKDF2 SHA-256 eller Argon2id används för att härleda krypteringsnyckeln från ditt huvudlösenord. Sedan saltas och hashas denna nyckel för autentisering med Bitwarden-servrarna. Standard iterationsantal som används med PBKDF2 är 600 000 iterationer på klienten (detta iterationsantal på klientsidan kan konfigureras från dina kontoinställningar).

> **Note**
>
> Though user accounts are initiated with PBKDF2, users may elect to change their key derivation function to Argon2id after the account has been created. Learn how to change the KDF algorithm.

Molndatabasen Bitwarden lagrar ditt krypterade valv och är värd inom den säkra Microsoft Azure-molninfrastrukturen. Den är konfigurerad med en kryptering-at-vila-teknik från Azure som kallas Transparent Data Encryption (TDE). TDE utför realtidskryptering och dekryptering av hela Bitwardens molndatabas, tillhörande säkerhetskopieringsdata och transaktionsloggfiler när de inte är i bruk. Azure hanterar krypteringsnycklarna för TDE, som endast auktoriserade Bitwarden-serverkomponenter kan komma åt. Läs mer om Azures Transparent Data Encryption här.

Dessutom utför Bitwarden-serverapplikationer sin egen kryptering av känsliga databaskolumner relaterade till ditt användarkonto. Huvudlösenordshaschar och skyddade användarnycklar krypteras i farten när de rör sig in och ut ur Bitwardens molndatabas. Dessa krypteringsoperationer på kolumnnivå utförs med nycklar som Bitwarden hanterar i en strikt kontrollerad nyckelhanteringstjänst (KMS).

Läs mer: Hur end-to-end-kryptering banar väg för noll kunskap och vilken kryptering som används

Datatyper och datalagring

Bitwarden behandlar två typer av användardata för att leverera Bitwarden-tjänsten: (i) Valvdata och (ii) Administrativ data.

(i) Valvdata

Valvdata inkluderar all information som lagras på konton till Bitwarden-tjänsten och kan inkludera personlig information. Om vi är värd för Bitwarden-tjänsten för dig kommer vi att vara värd för Vault Data. Valvdata krypteras med säkra kryptografiska nycklar under din kontroll. Bitwarden kan inte komma åt Vault Data.

Datalagring av valvdata: Du kan lägga till, ändra och ta bort valvdata när som helst.

(ii) Administrativa data

Bitwarden erhåller personlig information i samband med ditt kontoskapande, användning av Bitwarden-tjänsten och support, och betalningar för Bitwarden-tjänsten såsom namn, e-postadress, telefon och annan kontaktinformation för användare av Bitwarden-tjänsten och antalet objekt på ditt Bitwarden-tjänstkonto ("Administrativa data"). Bitwarden använder administrativa data för att tillhandahålla Bitwarden-tjänsten till dig. Vi behåller administrativa uppgifter så länge du är kund hos Bitwarden och enligt lag. Om du avslutar din relation med Bitwarden kommer vi att radera din personliga information i enlighet med vår datalagringspolicy.

När du använder webbplatsen eller kommunicerar med oss (t.ex. via e-post) kommer du att tillhandahålla, och Bitwarden kommer att samla in viss personlig information såsom:

- Namn
- Företagsnamn och adress
- Företagstelefonnummer
- E-postadress
- IP-adress och andra onlineidentifierare
- Alla kundrekommendationer som du har gett oss samtycke till att dela.
- Information som du tillhandahåller till webbplatsens interaktiva områden, såsom ifyllbara formulär eller textrutor, utbildning, webbseminarier eller evenemangsregistrering.
- Information om enheten du använder, innefattande hårdvarumodell, operativsystem och version, unika enhetsidentifierare, nätverksinformation, IP-adress och/eller Bitwarden-tjänstinformation när du interagerar med webbplatsen.
- Om du interagerar med Bitwarden-gemenskapen eller utbildningen, eller registrerade dig för ett prov eller evenemang, kan vi samla in biografisk information och innehållet som du delar.
- Information som samlas in via cookies, pixeltaggar, loggar eller annan liknande teknik.

Se Bitwardens sekretesspolicy för ytterligare information.

Molnplattform och webbapplikationssäkerhet

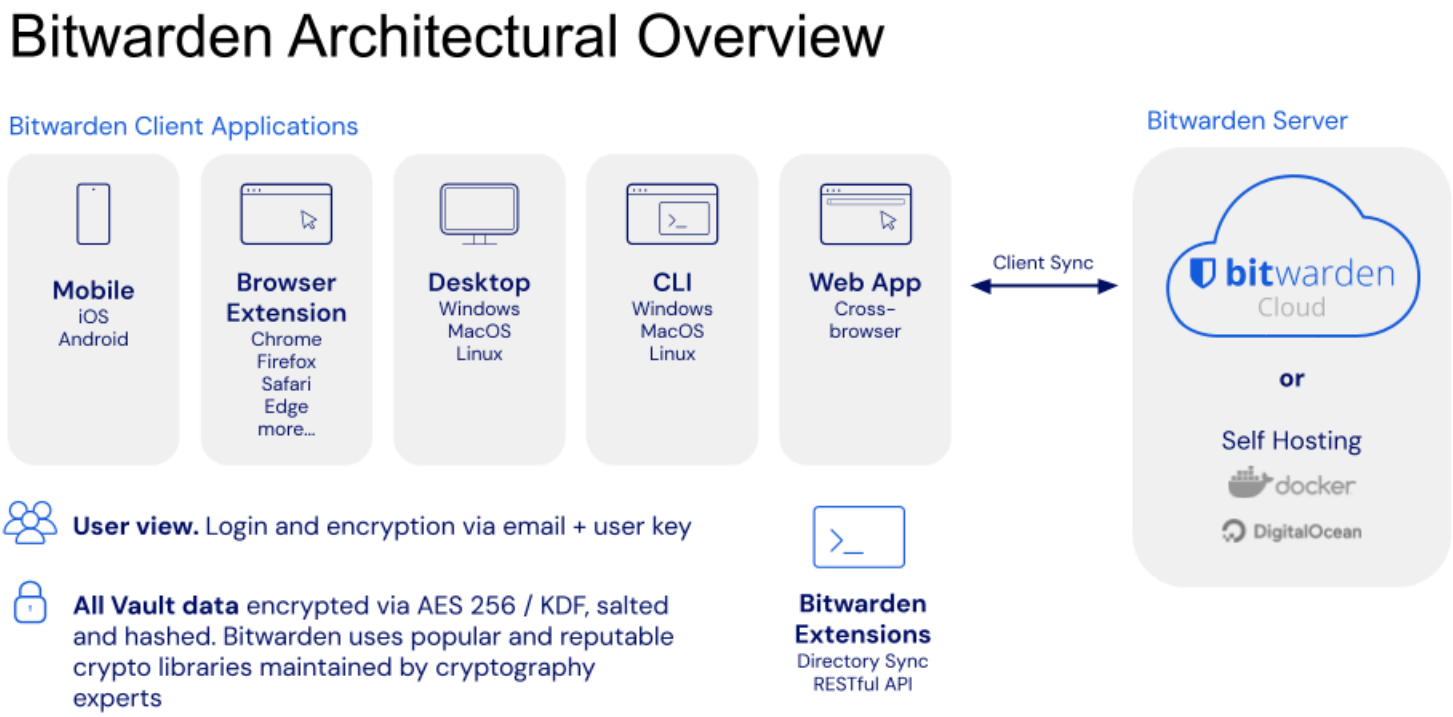
Arkitektur översikt

Bitwarden bearbetar och lagrar all data säkert i Microsoft Azure-molnet med hjälp av tjänster som hanteras av teamet på Microsoft, inklusive Azure Kubernetes Services (AKS).

Azure Kubernetes Services är en hanterad Kubernetes-tjänst som tillhandahålls av Microsoft som minskar komplexiteten i att distribuera och hantera Kubernetes-kluster. Microsoft hanterar kontrollplanet fullt ut. Kontrollplanet innehåller alla komponenter och tjänster som används för

att driva och underhålla Bitwarden Kubernetes-klustren. Microsoft och AKS-teamet distribuerar, driver och är ansvariga för AKS-tjänstens tillgänglighet och funktionalitet. Teamet på Bitwarden hanterar:

- Åtkomsthanteringen av AKS-tjänsten
- Patchningen och uppdateringen för att tillämpa säkerhetskorrigeringarna för Node OS, uppgraderingar av nodbildsversioner och Kubernetes-versionen (klusteruppgraderingar)
- Behållarsäkerheten för docker-bilderna och körande containrar i AKS
- Nätverkssäkerheten för noderna



Bitwarden architectural overview

Säkerhetsuppdateringar och patchning

Azure Kubernetes Services (AKS)

Microsoft tillhandahåller patchar, nya nodbilder och nya Kubernetes-versioner för sin AKS-tjänst. Teamet på Bitwarden hanterar och övervakar AKS-miljön och följer uppgraderingsrekommendationerna från Microsoft och sårbarhetsrapporter för att säkerställa att säkerhetskorrigeringar för Node OS, uppgraderingar av nodavbildningar och Kubernetes-versionen (klusteruppgraderingar) tillämpas. Dessutom tillämpar Bitwarden-teamet uppdateringar och patchar för att upprätthålla behållarsäkerheten för docker-avbildarna och körande behållare i AKS.

Styrning av produktionssystem

Bitwarden upprätthåller dokumenterade runbooks för alla produktionssystem som täcker distributions-, uppdaterings- och felsökningsprocesser. Omfattande varningar ställs in för att meddela och eskalera vid problem.

Baslinjekonfigurationer

Bitwarden bearbetar och lagrar all data säkert i Microsoft Azure-molnet med hjälp av tjänster som hanteras av teamet hos Microsoft, inklusive Azure Kubernetes Service (AKS).

Azure Kubernetes Services (AKS)

Säkerhetsbaslinjekonfigurationer upprättas och övervakas med hjälp av Cloud Security Posture Management och Vulnerability Management-tjänster.

HTTP-säkerhetsrubriker

Bitwarden använder HTTP-säkerhetsrubriker som en ytterligare skyddsnivå för Bitwardens webbapplikation och kommunikation. Till exempel kommer HTTP Strict Transport Security (HSTS) att tvinga alla anslutningar att använda TLS, vilket minskar riskerna för nedgraderingsattacker och felkonfiguration. Innehållssäkerhetspolicyrubriker ger ytterligare skydd mot injektionsattacker, såsom cross-site scripting (XSS). Dessutom implementerar Bitwarden X-Frame-Options: SAMEORIGIN för att försvara sig mot clickjacking.

Nyckelhanteringsprocedurer

Nycklar och andra hemligheter som används av själva Bitwarden-plattformen, inklusive autentiseringsuppgifter för Bitwardens molnleverantörskonton, genereras, lagras säkert och roteras efter behov i enlighet med branschstandardpraxis. Bitwarden använder interna Bitwarden-valv för säker lagring och säkerhetskopiering av känsliga nycklar eller andra hemligheter som används av Bitwarden-plattformen. Åtkomst till dessa valv hanteras noggrant med åtkomstkontroller, behörigheter och roller.

Loggning, övervakning och varningsmeddelande

Bitwarden upprätthåller dokumenterade runbooks för alla produktionssystem som täcker distributions-, uppdaterings- och felsökningsprocesser. Omfattande varningar ställs in för att meddela och eskalera vid problem. En kombination av manuell och automatiserad övervakning av Bitwardens molninfrastruktur ger en heltäckande och detaljerad bild av systemets hälsa samt proaktiva varningar om problemområden. Problem uppstår snabbt så att Bitwardens infrastrukturteam effektivt kan svara och mildra problem med minimala störningar.

Hotförebyggande och bemötande

Bitwarden utför kontinuerlig säkerhetsövervakning av våra nätverk, tillgångar, data och tjänster med hjälp av tjänster och verktyg inklusive men inte begränsat till Security Information Event Management (SIEM), etablerat Security Operations Center (SOC), Vulnerability Management, Data Loss Prevention (DLP) och Endpoint Detection and Response (EDR). Bitwarden upprätthåller en policy och plan för säkerhetsincidentrespons som är utformad för att minimera den övergripande effekten av cyberincidenter och inkluderar följande som en del av Incident Response Lifecycle:

- Förberedelser och planering
- Detektion och analys
- Inneslutning
- Utrotning
- Återhämtning
- Aktiviteter efter incidenten

Bitwarden använder Content Delivery Network-tjänster (CDN) för att tillhandahålla webbapplikationsbrandväggar (WAF) vid kanten, bättre DDoS-skydd, distribuerad tillgänglighet och cachning. Bitwarden använder också proxyservrar inom CDN-leverantören för bättre nätverkssäkerhet och prestanda för sina tjänster och webbplatser.

Kodbedömningar

Bitwarden är programvara med öppen källkod. All vår källkod finns på GitHub och är gratis för alla att granska. Bitwardens källkod granskas av välrenommerade tredjeparts säkerhetsrevisionsbyråer såväl som oberoende säkerhetsforskare. Dessutom tar Bitwarden Vulnerability Disclosure Program hjälp av hackergemenskapen på HackerOne för att göra Bitwarden säkrare.

Affärskontinuitet och katastrofåterställning

Bitwarden använder ett komplett utbud av katastrofåterställning och affärskontinuitetsmetoder från Microsoft Azure som är inbyggda i Bitwarden-molnet. Detta inkluderar hög tillgänglighet och backuptjänster för våra applikations- och databasnivåer.

Programvarans livscykel och förändringshantering

Bitwarden utvärderar förändringar av plattform, applikationer och produktionsinfrastruktur för att minimera risker och sådana förändringar implementeras enligt de vanliga driftsprocedurerna hos Bitwarden.

Ändringsförfrågningar planeras baserat på färdplanen och skickas till teknik. Engineering kommer att granska och utvärdera sin kapacitet och bedöma ansträngningsnivån för varje ändringsbegäran. Efter granskning och utvärdering kommer produkt- och ingenjörsteamen att formulera vad de ska arbeta med för en specifik release. CTO tillhandahåller detaljer om releasen genom kommunikationskanaler och ledningsmöten när utvecklingslivscykeln börjar för den releasen.

På en hög nivå inkluderar utvecklings-, release-, test- och godkännandeprocessen:

- Utveckla, bygg och iterera med hjälp av pull-förfrågningar i GitHub.
- Få funktioner till en punkt där de är testbara.
- Engineering utför funktionstestning av funktionen och/eller produkten medan de utvecklas och bygger.
- Enhetstestning och statisk applikationssäkerhetstestning (SAST) automatiseras som en del av Bitwarden Continuous Integration (CI) pipelines.
- Vissa tester utförs också av Customer Success-teamet.
- Ingenjörsledningen hjälper till med granskning och hjälper till att formalisera processen, inklusive dokumentationsuppdateringar.
- CTO ger slutgiltigt Go/No-Go-godkännande

Mötesnärvaro: För att säkerställa framgångsrik granskning, implementering av godkännande och stängning av ändringsförfrågningar, bör varje kärnverksamhet och IT-tjänstpersonal vara representerad under mötet för att granska och diskutera ändringsbegäran.

Nödimplementering och snabbkorrigeringar får eskalerad prioritet, och granskning och godkännande av ändringen erhålls från en chef eller direktör innan ändringen görs och granskas, kommuniceras och avslutas under nästa planerade ändringsmöte. Detta är normalt i ett serviceavbrott, ett system nere eller i en akut situation för att förebygga avbrott.

Reviderbarhet och efterlevnad

Bitwardens program för säkerhet och efterlevnad är baserat på ISO-27001 Information Security Management System (ISMS). Bitwardens personal har definierat policyer som styr säkerhet och processer, och uppdaterar kontinuerligt säkerhetsprogrammet för att överensstämma med tillämpliga juridiska, bransch- och regulatoriska krav för tjänster som tillhandahålls till dig under vårt användarvillkor.

Bitwarden följer branschstandardiserade applikationssäkerhetsriktlinjer som inkluderar ett dedikerat säkerhetsingenjörsteam och inkluderar regelbundna granskningar av applikationskällkod och IT-infrastruktur för att upptäcka, validera och åtgärda eventuella säkerhetsbrister.

Externa säkerhetsgranskningar

Tredjeparts säkerhetsgranskningar och utvärderingar av applikationer och/eller plattformen utförs minst en gång per år.

Certifieringar

Bitwarden-certifieringar inkluderar:

- SOC2 Typ II (förnyas årligen)
- SOC3 (förnyas årligen)
- ISO 27001

Enligt AICPA är användningen av Systems and Organization Controls (SOC), SOC 2 Type II-rapporten begränsad. Kontakta oss för SOC 2-rapportförfrågningar.

Läs mer: Bitwarden uppnår SOC2-certifiering

SOC 3-rapporten ger en sammanfattning av SOC 2-rapporten och distribueras offentligt. Enligt AICPA är SOC 3 SOC för serviceorganisationer att rapportera om kriterier för förtroendetjänster för allmänt bruk. Bitwarden gör en kopia av SOC 3-rapporten tillgänglig här och sammanfattningen visar vårt engagemang för säkerhets- och integritetsstandarder.

Dessa SOC-certifieringar representerar en aspekt av Bitwardens engagemang för att skydda kundernas säkerhet och integritet och överensstämmelse med rigorösa standarder. Bitwarden utför också en regelbunden kadens av granskningar av vår nätverkssäkerhet och kodintegritet.

Läs mer: Bitwarden 2020 säkerhetsrevision är klar och Bitwarden slutför tredjeparts säkerhetsrevision

Anställdas åtkomstkontroller

Bitwarden-anställda har betydande utbildning och expertis för den typ av data, system och informationstillgångar som de designar, bygger, implementerar, hanterar, stödjer och interagerar med.

Bitwarden följer en etablerad ombordstigningsprocess för att säkerställa att lämplig åtkomstnivå tilldelas och upprätthålls. Bitwarden har etablerat åtkomstnivåer som är lämpliga för varje roll. Alla förfrågningar, inklusive alla begäranden om åtkomständring, måste granskas och godkännas av chefen. Bitwarden följer en policy för minst privilegier som ger anställda den lägsta nivån av åtkomst som krävs för att utföra sina uppgifter. Bitwarden följer en etablerad off-boardingprocess genom Bitwarden Human Resources som återkallar alla åtkomsträttigheter vid en anställds uppsägning.

Översikt över hotmodell och attackytaanalys

Bitwarden följer ett riskbaserat tillvägagångssätt för att designa säkra tjänster och system som inkluderar hotmodellering och attackytaanalys för att identifiera hot och utveckla begränsning av dem. Risk- och hotmodelleringsanalysen sträcker sig till alla delar av Bitwarden-plattformen inklusive kärnan Bitwarden molnserverapplikation och Bitwarden-klienter som mobil, skrivbord, webbapplikation, webbläsare och/eller kommandoradsgränssnitt.

Bitwarden-klienter

Användare interagerar främst med Bitwarden genom klientapplikationer som mobil, stationär, webbapplikation, webbläsare och/eller kommandoradsgränssnitt. Säkerheten för dessa enheter, arbetsstationer och webbläsare är avgörande eftersom om en eller flera av dessa enheter äventyras kan en angripare kunna installera skadlig programvara som en keylogger som skulle fånga all information som skrivs in på dessa enheter inklusive alla dina lösenord och hemligheter. Du, som slutanvändare och/eller enhetsägare, är ansvarig för att se till att dina enheter är säkrade och skyddade från obehörig åtkomst.

HTTPS TLS och webbläsare kryptering ände-till-ände-kryptering

Bitwarden-webbklienten körs i din webbläsare. Äktheten och integriteten för Bitwarden-webbklienten beror på integriteten hos HTTPS TLS-anslutningen som den levereras med. En angripare som kan manipulera trafiken som levererar webbklienten kan leverera en skadlig klient till användaren.

Webbläsaresattacker är ett av de mest populära sätten för angripare och cyberbrottslingar att injicera skadlig programvara eller orsaka skada. Attackvektorer på webbläsaren kan inkludera:

- En del av **social ingenjörskonst, som nätfiske,** för att lura och övertala offret att vidta alla åtgärder som äventyrar säkerheten för deras användarhemligheter och konto.
- **Webbläsarattacker och webbläsartillägg/tilläggsutnyttjande**: Ett skadligt tillägg utformat för att kunna fånga användarhemligheter när de skrivs på tangentbordet.
- **Attacker på webbapplikationer via webbläsaren:** Clickjacking, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).

Bitwarden använder HTTP-säkerhetsrubriker som en ytterligare skyddsnivå för Bitwardens webbapplikation och kommunikation.

Slutsats

Den här översikten av Bitwardens säkerhets- och efterlevnadsprogram erbjuds för din granskning. Bitwardens lösning, mjukvara, infrastruktur och säkerhetsprocesser har designats från grunden med en flerskikts, försvarsdjupgående strategi.

Bitwardens program för säkerhet och efterlevnad är baserat på ISO-27001 Information Security Management System (ISMS). Bitwardens personal har definierat policyer som styr säkerhet och processer, och uppdaterar kontinuerligt säkerhetsprogrammet för att överensstämma med tillämpliga juridiska, bransch- och regulatoriska krav för tjänster som tillhandahålls till dig under vårt användarvillkor.

Kontakta oss om du har några frågor.

Ändringslogg för dokument

Publiceringsdatum	Sammanfattning av ändringar
11 mars 2024	Lade till ISO 27001-certifiering.
11 december 2024	Justerat språk kring minneshantering.
2 augusti 2024	Omstrukturerade dokumentet för enklare navigering, förbättrad informationsarkitektur och mer konsekvent stil
25 juli 2024	Lade till information relaterad till chiffernycklar för kryptering av valvobjekt
23 mars 2024	Lade till nya beskrivningar och diagram i avsnittet **Dela data mellan användare**
12 januari 2024	Lade till information relaterad till Logga in med lösenord