

Bitwarden säkerhet och efterlevnad

Bitwarden föreställer sig en värld där ingen blir hackad. Detta återspeglas i ett ständaktigt Bitwardens engagemang för säkerhet, integritet och efterlevnad av internationella standarder.

Get the full interactive view at
<https://bitwarden.com/sv-se/compliance/>

Bitwarden integritet och produktsäkerhet

Tredje part granskad

Externa experter granskar regelbundet Bitwarden-produkter, vilket säkerställer stark och pålitlig säkerhet.

Noll-kunskap, end-to-end-kryptering

Säkrad med stark kryptering, ingen har tillgång till din valvinformation, inte ens Bitwarden!

Överensstämmer med integritets- och säkerhetsstandarder

Få Bitwarden-produkter snabbt godkända av dina interna IT- och säkerhetsteam med branschefterlevnad.

Förtroende och transparens som drivs av öppen källkod

En kodbas med öppen källkod gör att säkerheten för Bitwarden-produkter enkelt kan granskas av oberoende säkerhetsforskare, kända säkerhetsföretag och Bitwarden-gemenskapen.

Pålitlig arkitektur med öppen källkod

Bitwarden-kodbasen på GitHub granskas och granskas regelbundet av miljontals säkerhetsentusiaster och aktiva Bitwarden-gemenskapsmedlemmar.

Källkodsbedömning

Bitwarden genomför årliga källkodsrevisioner och penetrationstester för varje klient inklusive webb, webbläsartillägg och skrivbord – förutom kärnapplikationen och biblioteket.

Nätverkssäkerhetsbedömning

Bitwarden genomför årliga nätverkssäkerhetsbedömningar och penetrationstester av välrenommerade säkerhetsföretag.

HackerOne bug bounty

Oberoende säkerhetsforskare belönas för att de skickar in potentiella säkerhetsfrågor.

Håller din data säker

Som din lösenordshanterare och leverantör av autentiseringssäkerhet använder Bitwarden pålitliga säkerhetsåtgärder och krypteringsmetoder för att skydda användardata.

Noll-kunskap, end-to-end-kryptering

Bitwarden använder end-to-end-kryptering för all valvdata, som endast ditt huvudlösenord kan dekryptera. Med en noll-kunskapsarkitektur har Bitwarden inte möjlighet att läsa någon krypterad data i ditt valv.

Multifaktorkryptering

Multifaktorkryptering är ett extra lager av kryptering som skyddar din lagrade information. Detta gör det praktiskt taget omöjligt för en dålig skådespelare att bryta sig in i ditt valv, även om de kunde få tillgång till dina krypterade valvdata.

Alternativ för självhotell

Välj att distribuera och hantera Bitwarden lokalt i ditt privata nätverk eller infrastruktur med alternativ för självvärd. Self-hosting tillåter kunder att ha mer detaljerad kontroll över sin lagrade information.

Säkerhetsefterlevnad

Bitwarden följer industrisäkerhetsstandarder med en ISO 27001-certifiering, SOC2- och SOC3-certifieringar och HIPAA-efterlevnad.

SOC2 och SOC3

System- och organisationskontroller (SOC) omfattar en uppsättning kontrollramverk som används för att validera en organisations

HIPAA

Bitwarden är HIPAA-kompatibel och genomgår årliga tredjepartsrevisioner för efterlevnad av HIPAA-säkerhetsregler.

ISO 27001

Bitwarden är ISO 27001-certifierad och i enlighet med ISO 27001 kontrolluppsättningar kring datasäkerhet.

säkerhetssystem och policyer. Bitwarden är SOC2 Type II och SOC3 certifierad.

SOC2-rapporter tillgängliga på begäran.

Sekretessefterlevnad

Bitwarden prioriterar att skydda användarnas personliga data och säkerställa efterlevnad av viktiga integritetsstandarder över hela världen.

CCPA & CPRA

Bitwarden är kompatibel med California Consumer Privacy Act (CCPA) och California Privacy Rights Act (CPRA).

GDPR

Bitwarden följer GDPR, gällande EU-dataskyddsregler och EU Standard Contractual Clauses (SCCs).

Datasekretessram

Bitwarden följer Data Privacy Framework (DPF), tidigare kallat Privacy Shield, som definierar säker överföring av personuppgifter.

Uppfyll dina säkerhetsstandarder med Bitwarden

Bitwarden är mer än en lösenordshanterare; det är ett grundläggande verktyg för att uppnå och upprätthålla branschens överensstämmelse med viktiga säkerhetsstandarder. Genom säker delning, övervakningsmöjligheter, centraliserad hantering och robust dataskydd stärker Bitwarden din organisations cybersäkerhetsställning för att möta efterlevnadsbehov.

ISO 27001

ISO 27001, en internationell standard, lägger grunden för att skapa, underhålla och utveckla ledningssystem för informationssäkerhet (ISMS), inklusive datahantering.

SOC 2

Service Organization Control 2 (SOC 2)–rapporter efterfrågas ofta av kunder och affärspartners från outsourceade lösningsleverantörer. Företag som söker SOC 2-kompatibilitet kan utnyttja en SOC 2-kompatibel lösenordshanterare för att uppfylla kraven.

NERC

North American Electric Reliability Corporation (NERC) är ett icke-vinstdrivande internationellt tillsynsorgan som är dedikerat till att fastställa efterlevnadsstandarder som hjälper till att minska riskerna för elnätet och kraftsystemen som betjänar hundratals miljoner människor i USA, Kanada och delar av Mexiko.

NIS2

NIS2 är en uppsättning krav för att säkra nätverk och informationssystem i hela EU. Direktivet ger företag som identifierats som operatörer av väsentliga tjänster mandat att genomföra lämpliga åtgärder för att förbättra cybersäkerheten och uppfylla rättsliga skyldigheter.

NIST Cybersecurity Framework

National Institute of Standards and Technology (NIST) tillhandahåller vägledning och bästa praxis för organisationer att följa, för att hjälpa företag, ideella organisationer och andra privata institutioner att förbättra riskhanteringen för cybersäkerhet.

SOX

Sarbanes-Oxley Act (SOX) efterlevnad innebär att följa en uppsättning säkerhetskrav som är utformade för att säkerställa integriteten i den finansiella rapporteringen.

Lösenordshantering Mognadsmodell

Detta ramverk hjälper organisationer att förstå deras mognadsnivå för lösenordshanteraren – baserat på deras nuvarande verksamhet – och identifiera vilka steg som är nödvändiga för att stärka deras säkerhet och förbättra deras befintliga klassificering.

Vanliga frågor

- Kan Bitwarden-teamet se mina lösenord?

Inga.

Din data är helt krypterad och/eller hashad innan den någonsin lämnar **din** lokala enhet, så ingen från Bitwarden-teamet kan någonsin se, läsa eller bakåtkonstruera för att komma till din riktiga data. Bitwarden-serverar lagrar endast krypterad och hashad data. För mer information om hur dina data krypteras, se [Kryptering](#).

[Läs mer >](#)

- Hur håller du molnservrarna säkra?

Bitwarden vidtar extrema åtgärder för att säkerställa att dess webbplatser, applikationer och molnservrar är säkra. Bitwarden använder Microsoft Azure-hanterade tjänster för att hantera serverinfrastruktur och säkerhet, snarare än att göra det direkt.

[Läs mer >](#)

- Är Bitwarden granskad?

Bitwarden genomför regelbundet omfattande säkerhetsrevisioner från tredje part med kända säkerhetsföretag. Dessa årliga revisioner inkluderar källkodsbedömningar och penetrationstester över Bitwarden IP:er, servrar och webbapplikationer.

[Läs mer >](#)

- Vad händer om Bitwarden blir hackad?

Om Bitwarden av någon anledning skulle bli hackad och din data avslöjades, är din information fortfarande skyddad på grund av [stark kryptering och envägssaltade](#) hashåtgärder som vidtagits på dina valvdata och huvudlösenord.

[Läs mer >](#)

- Var lagras min data i molnet?

Bitwarden bearbetar och lagrar all valvdata säkert i [Microsoft Azure Cloud](#) i [USA](#) eller [EU](#) med hjälp av tjänster som hanteras av teamet på Microsoft. Eftersom Bitwarden endast använder tjänsteerbjudanden från Azure, finns det ingen serverinfrastruktur att hantera och underhålla. All drifttid, skalbarhet, säkerhetsuppdateringar och garantier backas upp av Microsoft och deras molninfrastruktur. Läs dokumentationen för [Microsoft Azure Compliance Offerings](#) för mer information.

[Läs mer >](#)

- Varför ska jag lita på Bitwarden med mina lösenord?

Du kan lita på oss av flera anledningar:

1. Bitwarden är programvara **med öppen källkod**. All vår källkod finns på [GitHub](#) och är gratis för alla att granska. Tusentals mjukvaruutvecklare följer Bitwardens källkodsprojekt (och det borde du också!).
2. Bitwarden **granskas av välrenommerade tredjepartssäkerhetsföretag** såväl som oberoende säkerhetsforskare.
3. Bitwarden lagrar **inte dina lösenord**. Bitwarden lagrar krypterade versioner av dina lösenord **som bara du kan låsa upp**. Din känsliga information krypteras lokalt på din personliga enhet innan den någonsin skickas till våra molnservrar.
4. **Bitwarden har ett rykte**. Bitwarden används av miljontals individer och företag. Om vi gjorde något tveksamt eller riskabelt, skulle vi gå i konkurs!

Litar du fortfarande inte på oss? Du behöver inte. Öppen källkod är vackert. Du kan enkelt vara värd för hela Bitwarden-stacken själv. Du kontrollerar din data.

[Läs mer >](#)

- Använder Bitwarden en saltad hash för mitt lösenord?

PBKDF2 SHA-256 används för att härleda krypteringsnyckeln från ditt huvudlösenord, men du kan välja [Argon2](#) som ett alternativ. Bitwarden **salta** och **hashar** ditt huvudlösenord med din e-postadress **lokalt** innan överföring till våra servrar. När en Bitwarden-server får det hashade lösenordet, saltas det igen med ett kryptografiskt säkert slumpmässigt värde, hashas igen och lagras i vår databas.

[Läs mer >](#)

- Hur överförs och lagras mina data säkert på Bitwarden-servrar?

Bitwarden krypterar och/eller hashar **alltid** dina data på din lokala enhet innan något skickas till molnservrar för lagring. **Bitwarden-servrar används endast för att lagra krypterad data**. För mer information, se [Lagring](#).

[Läs mer >](#)

- Vilken kryptering används?

Bitwarden använder [AES-CBC](#) 256-bitars kryptering för dina valvdata och [PBKDF2](#) SHA-256 eller [Argon2](#) för att härleda din krypteringsnyckel.

[Läs mer >](#)

- Vilken information är krypterad?

All valvdata krypteras av Bitwarden innan den lagras någonstans. För att lära dig hur, se [Kryptering](#).

[Läs mer >](#)

- Var finns min data lagrad på min dator/enhet?

Data som lagras på din dator/enhet är krypterad och dekrypteras först när du låser upp ditt valv. Dekrypterad data lagras endast i **minnet** och skrivs **aldrig till beständig lagring**.

[Läs mer >](#)