bitwarden | Hilfezentrum Artikel

SICHERHEIT

Häufig gestellte Fragen (FAQ) zum Thema Sicherheit

Ansicht im Hilfezentrum:
https://bitwarden.com/help/security-faqs/

Häufig gestellte Fragen (FAQ) zum Thema Sicherheit

Dieser Artikel enthält häufig gestellte Fragen (FAQs) zum Thema Sicherheit.

A: Warum sollte ich Bitwarden mit meinen Passwörtern vertrauen?

A: Sie können uns aus einigen Gründen vertrauen:

1. Bitwarden ist **Open-Source** Software. Unser gesamter Quellcode ist auf GitHub gehostet und steht jedem zur Überprüfung frei zur Verfügung. Tausende von Softwareentwicklern folgen den Quellcode-Projekten von Bitwarden (und Sie sollten das auch tun!).

2. Bitwarden wird geprüft **von renommierten Drittanbieter-Sicherheitsfirmen** sowie unabhängigen Sicherheitsforschern.

3. Bitwarden **speichert Ihre Passwörter nicht**. Bitwarden speichert verschlüsselte Versionen Ihrer Passwörter die nur Sie entsperren können. Ihre sensiblen Informationen werden lokal auf Ihrem persönlichen Gerät verschlüsselt, bevor sie jemals an unsere Cloud-Server gesendet werden.

4. **Bitwarden hat einen Ruf.** Bitwarden wird von Millionen von Einzelpersonen und Unternehmen genutzt. Wenn wir etwas Fragwürdiges oder Riskantes tun würden, wären wir aus dem Geschäft!

Vertrauen Sie uns immer noch nicht? Du musst nicht. Open Source ist wunderschön. Sie können problemlos den gesamten Bitwarden-Stack selbst hosten. Sie kontrollieren Ihre Daten. Mehr dazu erfahren Sie hier.

F: Was passiert, wenn Bitwarden gehackt wird?

A: Bitwarden ergreift extreme Maßnahmen, um sicherzustellen, dass seine Websites, Anwendungen und Cloud-Server sicher sind. Bitwarden verwendet Microsoft Azure verwaltete Dienste, um die Serverinfrastruktur und Sicherheit zu verwalten, anstatt dies direkt zu tun.

Wenn Bitwarden aus irgendeinem Grund gehackt werden sollte und Ihre Daten kompromittiert wären, sind Ihre Informationen immer noch geschützt aufgrund von starker Verschlüsselung und einseitig gesalzenem Hashing, die auf Ihren Tresor-Daten und Ihrem Master-Passwort angewendet werden.

A: Kann Bitwarden meine Passwörter sehen?

A: Nein.

Ihre Daten werden vollständig verschlüsselt und/oder gehasht, bevor sie **Ihr** lokales Gerät verlassen, sodass niemand vom Bitwarden-Team jemals Ihre echten Daten sehen, lesen oder zurückentwickeln kann, um an sie zu gelangen. Bitwarden-Server speichern nur verschlüsselte und gehashte Daten. Für weitere Informationen darüber, wie Ihre Daten verschlüsselt werden, sehen Sie Verschlüsselung.

F: Wird mein Bitwarden Master-Passwort lokal gespeichert?

A: Nein.

Wir speichern das Master-Passwort nicht lokal oder im Speicher. Ihr Verschlüsselungsschlüssel (abgeleitet vom Master-Passwort) wird nur gespeichert, während die App entsperrt ist, was erforderlich ist, um Daten in Ihrem Tresor zu entschlüsseln. Wenn der Tresor gesperrt ist, werden diese Daten aus dem Speicher gelöscht.

Wir laden auch den Renderer-Prozess der Anwendung nach 10 Sekunden Inaktivität auf dem Sperrbildschirm neu, um sicherzustellen, dass alle verwalteten Speicheradressen, die noch nicht zur Sammlung von Müll gehören, gesperrt werden. Wir tun unser Bestes, um sicherzustellen, dass alle Daten, die möglicherweise im Speicher für die Funktion der Anwendung benötigt werden, nur so lange im Speicher gehalten werden, wie Sie es benötigen und dass der Speicher immer dann bereinigt wird, wenn die Anwendung gesperrt ist. Wir betrachten die verschlüsselten Daten der Anwendung als vollkommen sicher, während die Anwendung in einem gesperrten Zustand ist.

A: Was mache ich, wenn ich ein neues Gerät, das sich bei Bitwarden anmeldet, nicht erkenne?

A: Wenn die IP-Adresse eines neuen Geräts keiner bekannten IP-Adressen (Heimnetzwerk, Arbeitsnetzwerk, Mobilfunknetzwerk usw.) entspricht, ändern Sie Ihr Master-Passwort und stellen Sie sicher, dass die Zwei-Schritt-Zugangsdaten für Ihr Konto aktiviert sind. Sie sollten auch Sitzungen von der Seite **Kontoeinstellungen** Ihres Web-Tresors deautorisieren, um die Abmeldung auf allen Geräten zu erzwingen. Wenn Sie denken, dass Ihre Tresor Einträge möglicherweise gefährdet sind, sollten Sie Ihre Passwörter ändern.

F: Mit was ist Bitwarden konform? Welche Zertifizierungen haben Sie?

A: Bitwarden entspricht den folgenden Richtlinien:

- **DSGVO.** Lesen Sie mehr hier.
- **CCPA.** Lesen Sie mehr hier.
- **HIPAA.** Lesen Sie mehr hier.
- **SOC 2 Typ 2.** Lesen Sie mehr hier.
- **SOC 3.** Lesen Sie mehr hier.

Für weitere Informationen besuchen Sie bitte unsere Sicherheits- und Compliance Seite.

F: Wie erfüllt Bitwarden die europäischen Compliance-Anforderungen?

A: Bitwarden ist DSGVO-konform und verwendet genehmigte Informationsübertragungsmechanismen, einschließlich EU-Standardvertragsklauseln (SCCs) gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, die durch die Durchführungsentscheidung der Europäischen Kommission (EU) 2021/914 vom 4. Juni 2021 genehmigt wurde, wie derzeit unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj festgelegt. Für Geschäfts- und Enterprise-Kunden kann Bitwarden die Bitwarden-Datenschutzvereinbarung ausführen.

Bitwarden-Cloud-Server werden derzeit auf Microsoft Azure innerhalb der Vereinigten Staaten und der Europäischen Union gehostet. Heute bedient Bitwarden Millionen von Nutzern, einschließlich Regierungs- und Enterprise-Kunden in ganz Europa und der Welt, mit dieser Infrastruktur.

Für Kunden, die volle Kontrolle über die Datenresidenz benötigen, kann Bitwarden alternativ auf Ihrer eigenen Infrastruktur privat gehostet werden.

Alle im Bitwarden Tresor gespeicherten Daten, unabhängig davon, ob sie in der Cloud oder selbst gehostet sind, sind durchgängig verschlüsselt und nur für den Bitwarden-Benutzer zugänglich. Mit dieser End-to-End-, Zero-Knowledge-Verschlüsselungsarchitektur kann selbst Bitwarden nicht auf Ihre Daten zugreifen.

Für eine vollständige Liste der Sicherheits- und Compliance-Zertifizierungen von Bitwarden besuchen Sie bitte https://bitwarden.com/compliance/.

A: Welche Drittanbieter-Dienste, Bibliotheken oder Kennungen werden in meinem Bitwarden-Konto verwendet?

A: In den mobilen Apps wird Firebase Cloud Messaging (oft fälschlicherweise für einen Tracker gehalten) nur für Push-Benachrichtigungen im Zusammenhang mit der Synchronisation verwendet und führt absolut keine Tracking-Funktionen aus. Microsoft Visual Studio App Center wird für die Berichterstattung über Abstürze auf einer Reihe von mobilen Geräten verwendet. Im Web-Tresor werden Stripe- und PayPal-Skripte nur auf Zahlungsseiten für die Zahlungsabwicklung verwendet.

Für diejenigen, die jegliche Kommunikation mit Drittanbietern ausschließen möchten, werden Firebase und Microsoft Visual Studio App Center vollständig aus dem F-Droid Build entfernt. Zusätzlich wird das Ausschalten von Push-Benachrichtigungen auf einem selbst gehosteten Bitwarden-Server die Verwendung des Push-Relay-Servers deaktivieren.

Die Bitwarden Android-Anwendung beinhaltet auch die Möglichkeit, das Absturz-Bericht erstatten unter Einstellungen zu deaktivieren.

Bitwarden nimmt die Sicherheit und Privatsphäre der Benutzer ernst. Bitwarden verwendet sichere End-to-End-Verschlüsselung, ohne Kenntnis Ihres Verschlüsselungsschlüssels. Als ein auf Open Source fokussiertes Unternehmen laden wir jeden ein, unsere Bibliotheksimplementierungen jederzeit auf GitHub zu überprüfen.

F: Wie kann ich eine zweistufige Anmeldung für meine Bitwarden Organisation verlangen?

A: Verwenden Sie eine Enterprise-Richtlinie, die in einem Enterprise-Organisation-Abonnement enthalten ist. Sie können auch die Duo MFA-Integration aktivieren, um 2FA/MFA für Ihre Organisation durchzusetzen. Für weitere Informationen, siehe Zwei-Schritt-Zugangsdaten über Duo.

A: Was sind die Zertifikatsoptionen für eine selbst gehostete Instanz von Bitwarden?

A: Siehe Zertifikatsoptionen für eine vollständige Liste und Anweisungen.

F: Wie prüft Bitwarden Code-Änderungen?

A: Das Vertrauen in die Sicherheit unserer Systeme ist für Bitwarden von größter Bedeutung. Alle vorgeschlagenen Code-Änderungen werden von einem oder mehreren nicht-autor Mitgliedern des Teams überprüft, bevor sie in irgendeine Codebasis eingefügt werden können. Alle Codes durchlaufen mehrere Test- und QA-Umgebungen, bevor sie in Produktion gehen. Bitwarden hat einen SOC2-Bericht implementiert, um unsere internen Verfahren zu prüfen und zu validieren. Wie im Bericht erwähnt, unterliegt unser Team einer strengen Überprüfung des Hintergrunds und gründlichen Interviewprozessen. Bitwarden, als Open-Source-Produkt, begrüßt auch jederzeit Peer-Reviews unseres Codes. Das Team bei Bitwarden bemüht sich, alles zu tun, um unsere Benutzer zufrieden zu stellen und ihre Daten sicher zu halten.

F: Wie lange speichert Bitwarden Sitzungsinformationen im Cache?

A: Tolle Frage! Die Antwort hängt von der speziellen Information und der Client-Anwendung ab:

- Offline-Tresor-Sitzungen laufen nach 30 Tagen ab.
  - **Mit Ausnahme** mobiler Client-Anwendungen, die nach 90 Tagen ablaufen.
- Anmeldung in zwei Schritten. Die Auswahl **„Angemeldet bleiben** “ läuft nach 30 Tagen ab.
- Der Directory Connector Synchronisation Cache wird nach 30 Tagen gelöscht.
- Einladungen der Organisation laufen nach 5 Tagen ab. Selbst gehostete Kunden können dies über eine Umgebungsvariable konfigurieren.

F: Wie validiere ich die Prüfsumme einer Bitwarden-App?

A: Zuerst, holen Sie die `neueste` yaml-Datei für die relevante Version (zum Beispiel, `latest-linux.yml`) und das entsprechende Release-Paket (zum Beispiel, `Bitwarden-1.33.0-amd64.deb`). Generieren Sie einen SHA512-Hash des heruntergeladenen Release-Pakets (zum Beispiel, `sha512sum Bitwarden-1.33.0-amd64.deb`) und konvertieren Sie den generierten Hex-Wert in Base64. Vergleichen Sie den berechneten Base64-Wert mit dem `sha512:` Wert aus der yaml-Datei zur Validierung.

F: Wie kann ich eine Sicherheitsmeldung oder einen Bericht an Bitwarden senden?

A : Bitwarden ist davon überzeugt, dass die Zusammenarbeit mit Sicherheitsforschern auf der ganzen Welt für die Sicherheit unserer Benutzer von entscheidender Bedeutung ist. Wenn Sie glauben, dass Sie ein Sicherheitsproblem in unserem Produkt oder Dienst gefunden haben, ermutigen wir Sie, bitte einen Bericht über unser HackerOne Programm einzureichen. Wir freuen uns darauf, mit Ihnen zusammen das Problem schnellstmöglich zu lösen. Erfahren Sie mehr über unsere Offenlegungsrichtlinie .

F: Warum geht mein Web-Tresor zu web-vault.pages.dev?

A: `web-vault.pages.dev` ist eine einzigartige Subdomain von Bitwarden, die von Cloudflare Pages verwendet wird. Diese URL kann Benutzern angezeigt werden, wenn Cloudflare DNS-Probleme hat. Sie sollten immer auf der Hut vor Phishing-Versuchen sein, indem Sie die URL überprüfen, bevor Sie Ihren Benutzernamen und Ihr Master-Passwort eingeben. Allerdings sollte `web-vault.pages.dev` als sicher zum Anmelden betrachtet werden.

F: Wie kann ich mein Bitwarden-Konto vor Brute-Force-Angriffen schützen?

A: Ein Brute-Force-Angriff ist, wenn ein bösartiger Akteur eine Kombination aus schwachen und kurzen Passwörtern durchläuft, in dem Versuch, Zugang zu Ihrem Konto zu erhalten. Bitwarden bietet einige Möglichkeiten, wie Sie sich vor diesen potenziellen Angriffen schützen können:

- Haben Sie ein langes und einzigartiges Master-Passwort. Bitwarden erfordert ein Minimum von 12 Zeichen, um die Sicherheit des Kontos zu erhöhen.
- Richten Sie 2FA auf allen Bitwarden Konten ein, um eine zusätzliche Sicherheitsebene hinzuzufügen.
- Bitwarden wird nach 9 fehlgeschlagenen Zugangsdaten Versuchen von einem unbekannten Gerät eine CAPTCHA-Verifizierung verlangen.

Fragen zu spezifischen Client-Apps

A: Welche Daten verwendet Bitwarden von Client-Anwendungen?

A: Bitwarden verwendet administrative Daten, um Ihnen den Bitwarden-Dienst zur Verfügung zu stellen. Wie in einigen **App-Datenschutz** Berichten angegeben, geben Benutzer bei der Erstellung eines Kontos die folgenden Informationen an:

- Ihr Name (optional).
- Ihre E-Mail-Adresse (wird für die E-Mail-Verifizierung, Konto-Verwaltung und Kommunikation zwischen Ihnen und Bitwarden verwendet).

Zusätzlich wird Ihrem Gerät eine spezifische GUID (manchmal als Geräte-ID bezeichnet), die von **Bitwarden generiert** wurde, zugewiesen. Diese GUID wird verwendet, um Sie zu benachrichtigen, wenn ein neues Gerät sich in Ihren Tresor einloggt.

F: Können Sie die Sicherheit von Electron-Apps erklären?

A: Ein häufig geteilter Artikel deutet auf einen Fehler in Electron-Apps hin, jedoch erfordert der referenzierte Angriff, dass ein Benutzer über eine kompromittierte Maschine verfügt, was natürlich einem bösartigen Angreifer erlauben würde, Daten auf dieser Maschine zu kompromittieren. Solange Sie keinen Grund haben zu glauben, dass das Gerät, das Sie verwenden, kompromittiert wurde, sind Ihre Daten sicher.

A: Wie sichert Bitwarden Browser-Erweiterungen?

A: Erweiterungen sind sicher zu verwenden, wenn sie richtig entwickelt wurden. Aufgrund der Art und Weise, wie Browser-Erweiterungen funktionieren, besteht immer die Möglichkeit, dass ein Fehler auftritt. Wir gehen äußerst sorgfältig und vorsichtig vor, wenn wir unsere Erweiterungen und Add-Ons entwickeln, wir halten unsere Augen und Ohren offen für alles, was in der Branche vor sich geht, und wir führen Sicherheitsaudits durch, um viele Augen auf alles zu haben.

A: Wofür bittet die Browser-Erweiterung um Berechtigung?

A: Bei der Installation wird die Browser-Erweiterung um Berechtigung bitten, auf Ihre Zwischenablage zuzugreifen, um die Funktion zum geplanten Löschen der Zwischenablage zu nutzen (zugänglich im **Optionen**-Menü).

Wenn diese **optionale Funktion** aktiviert ist, wird die Zwischenablage alle Bitwarden-Einträge, die erstellt oder in einem konfigurierbaren Intervall ausgefüllt wurden, löschen. Der Zugriff auf die Zwischenablage ermöglicht es Bitwarden, dies zu tun, ohne einen nicht mit der

Bitwarden-Anwendung verknüpften Eintrag aus der Zwischenablage zu entfernen, indem der zuletzt kopierte Eintrag mit dem zuletzt aus Ihrem Tresor kopierten Eintrag verglichen wird. Bitte beachten Sie, diese Funktion ist **standardmäßig ausgeschaltet**.

A: Welche Berechtigungen fordert die mobile App an?

A: Die Bitwarden Android- und iOS-Apps können während der Nutzung der App um die folgenden Berechtigungen bitten:

Berechtigung	Grund
Bitwarden erlauben, Bilder aufzunehmen und Videos zu drehen?	Um QR-Codes für die zweistufige Zugangsdaten oder Bitwarden Authentifizierung zu scannen.
Bitwarden den Zugriff auf Fotos und Medien auf Ihrem Gerät erlauben?	Um Anhänge oder Sends aus einer auf Ihrem Gerät gespeicherten Datei zu erstellen.

Zusätzliche grundlegende Berechtigungen, die von Bitwarden benötigt werden, sind im Google Play Store aufgelistet.

F: Warum benötigt die Browser-Erweiterung die nativeMessaging-Berechtigung?

A: Version 1.48.0 der Browsererweiterung ermöglicht die biometrische Entsperrung für Browsererweiterungen .

Diese Berechtigung, auch bekannt als `nativeMessaging`, ist sicher zu akzeptieren und ermöglicht es der Browser-Erweiterung, mit der Bitwarden-Desktop-App zu kommunizieren, was erforderlich ist, um das Entsperren mit Biometrie zu ermöglichen.

Beachten Sie, dass Sie bei der Aktualisierung Ihres Browsers auf diese Version möglicherweise aufgefordert werden, eine neue Berechtigung namens "Kommunikation mit kooperierenden nativen Anwendungen" (in Chromium-basierten Browsern) oder "Nachrichtenaustausch mit Programmen außer Firefox" zu akzeptieren. Wenn Sie diese Berechtigung nicht akzeptieren, bleibt die Erweiterung deaktiviert.

F: Ist Bitwarden FIPS-konform?

A: Bitwarden verwendet FIPS 140-konforme Bibliotheken und Kryptographie, und die meisten FIPS 140-Installationen von Bitwarden nutzen die Option der selbst gehosteten Lösung, um Bewertungen (zum Beispiel Cyber Maturity Model Certification) zu erleichtern. Die Bitwarden-Plattform hat bis jetzt keine FIPS-Zertifizierungen durchgeführt. Anfragen sind willkommen über die Kontaktieren Sie uns Seite.

F: Kann ich den Zugriff auf Bitwarden auf bestimmte Geräte beschränken?

A: Durch die Verwendung von selbst gehostet, können Sie benutzerdefinierte Firewall- und NGINX-Konfigurationen sowie VPN/VLAN-Zugriffskontrollen verwenden, um die Gerätetypen und/oder Netzwerkschichtzugriffe für Ihre Bitwarden-Instanz zu bestimmen. Sie können auch andere Werkzeuge wie Geräte-Level-Zertifikate verwenden, um den spezifischen Gerätezugriff auf die Bitwarden-Instanz zu steuern.

F: Hat Bitwarden eine tragbare Anwendung?

A: Ja! Die Bitwarden Desktop-App ist als tragbare `.exe` verfügbar, die hier heruntergeladen werden kann. Die portable App eignet sich gut für **immer-offline** Umgebungen oder Szenarien, in denen eine automatische Aktualisierung der App nicht gewünscht ist. Die tragbare App **wird sich nicht selbst aktualisieren**.

F: Werden die Optionen für den Seitenzugriff die Bitwarden-Browser-Erweiterung beeinträchtigen?

A: Die Zugriffseinstellungen für die Bitwarden Browser Erweiterung müssen auf **Auf allen Seiten** oder auf **Auf bestimmten Seiten** mit dem Bitwarden-Server, der zur Liste hinzugefügt wurde, eingestellt sein, damit die Browser Erweiterung ordnungsgemäß funktioniert. Der Zugriff

auf die Einstellungsseite auf **Beim Klicken** beschränkt die Fähigkeit von Bitwarden, Daten vom Bitwarden-Server abzurufen, was grundsätzlich erforderlich ist, um Anmeldeinformationen zu speichern oder eine Aktualisierung durchzuführen.