Bitwarden Sicherheit und Compliance

Bitwarden stellt sich eine Welt vor, in der niemand gehackt wird. Dies spiegelt sich in einem unerschütterlichen Engagement von Bitwarden für Sicherheit, Datenschutz und die Einhaltung internationaler Standards wider.

Get the full interactive view at
https://bitwarden.com/de-de/compliance/

bitwarden

Bitwarden Datenschutz und Produktsicherheit

Von Dritten geprüft

Externe Experten überprüfen regelmäßig Bitwarden-Produkte, um eine starke und vertrauenswürdige Sicherheit zu gewährleisten.

Zero-Knowledge, Ende-zu-Ende-Verschlüsselung

Durch eine starke Verschlüsselung hat niemand Zugriff auf Ihre Tresorinformationen, nicht einmal Bitwarden!

Einhaltung der Datenschutz- und Sicherheitsstandards

Lassen Sie Bitwarden-Produkte schnell von Ihren internen IT- und Sicherheitsteams mit Branchen-Compliance genehmigen.

Vertrauen und Transparenz auf Open-Source-Basis

Eine Open-Source-Codebasis ermöglicht eine einfache Überprüfung der Sicherheit von Bitwarden-Produkten durch unabhängige Sicherheitsforscher, namhafte Sicherheitsfirmen und die Bitwarden-Community.

Vertrauenswürdige Open-Source-Architektur

Die Bitwarden-Codebasis auf GitHub wird regelmäßig von Millionen von Sicherheitsbegeisterten und aktiven Bitwarden-Community-Mitgliedern überprüft und auditiert.

Quellcode-Bewertung

Bitwarden führt jährliche Quellcode-Audits und Penetrationstests für jeden Client durch, einschließlich Web, Browsererweiterung und Desktop — zusätzlich zur Kernanwendung und -bibliothek.

Bewertung der netzwerk-sicherheit

Bitwarden führt jährliche Netzwerksicherheitsbewertungen und Penetrationstests durch renommierte Sicherheitsfirmen durch.

HackerOne Bug Bounty

Unabhängige Sicherheitsforscher werden für die Einreichung potenzieller Sicherheitsprobleme belohnt.

Schützen Sie Ihre Daten

Als Ihr Passwort-Manager und Anmeldedaten-Sicherheitsanbieter verwendet Bitwarden vertrauenswürdige Sicherheitsmaßnahmen und Verschlüsselungsmethoden, um Benutzerdaten zu schützen.

Zero-Knowledge, Ende-zu-Ende-Verschlüsselung

Bitwarden verwendet eine Ende-zu-Ende-Verschlüsselung für alle Vault-Daten, die nur Ihr Master-Passwort entschlüsseln kann. Mit einer Zero-Knowledge-Architektur ist Bitwarden nicht in der Lage, verschlüsselte Daten in Ihrem Tresor zu lesen.

Multifaktor-Verschlüsselung

Die Multifaktor-Verschlüsselung ist eine zusätzliche Verschlüsselungsebene, die Ihre gespeicherten Informationen schützt. Dies macht es für einen bösen Akteur praktisch unmöglich, in Ihren Tresor einzubrechen, selbst wenn er Zugriff auf Ihre verschlüsselten Tresordaten erhalten konnte.

Optionen für Selfhosting

Entscheiden Sie sich für die Bereitstellung und Verwaltung von Bitwarden vor Ort in Ihrem privaten Netzwerk oder Ihrer Infrastruktur mit Self-Hosting-Optionen. Self-Hosting ermöglicht Kunden eine detailliertere Kontrolle über ihre gespeicherten Informationen.

Einhaltung der Sicherheitsvorschriften

Bitwarden hält sich an die Sicherheitsstandards der Branche mit SOC2- und SOC3-Zertifizierungen und HIPAA-Compliance.

SOC2 und SOC3

System- und Organisationskontrollen (SOC) umfassen eine Reihe von Kontrollrahmen, die zur Validierung der Sicherheitssysteme und -richtlinien einer Organisation verwendet werden. Bitwarden ist SOC2 Typ II und SOC3 zertifiziert.

SOC2-Berichte auf Anfrage erhältlich.

HIPAA

Bitwarden ist HIPAA-konform und wird jährlichen Audits durch Dritte zur Einhaltung der HIPAA-Sicherheitsregeln unterzogen.

ISO 27001

Bitwarden ist ISO 27001 zertifiziert und in Übereinstimmung mit ISO 27001 Kontrollsets rund um die Datensicherheit.

Datenschutz-Compliance

Bitwarden legt Wert darauf, die personenbezogenen Daten der Benutzer zu schützen und die Einhaltung der wichtigsten Datenschutzstandards auf der ganzen Welt sicherzustellen.

CCPA & CPRA

Bitwarden ist konform mit dem California Consumer Privacy Act (CCPA) und dem California Privacy Rights Act (CPRA).

GDPR

Bitwarden hält die DSGVO, die aktuellen EU-Datenschutzvorschriften und die EU-Standardvertragsklauseln (SCCs) ein.

Data Privacy Framework

Bitwarden ist konform mit dem California Consumer Privacy Act (CCPA) und dem California Privacy Rights Act (CPRA).

Erfüllen Sie Ihre Sicherheits-Compliance-Standards mit Bitwarden

Bitwarden ist mehr als ein Passwort-Manager; es ist ein grundlegendes Werkzeug, um die Einhaltung der wichtigsten Sicherheitsstandards in der Branche zu erreichen und aufrechtzuerhalten. Durch sichere Freigabe, Überwachungsfunktionen, zentrales Management und robusten Datenschutz stärkt Bitwarden die Cybersicherheit Ihres Unternehmens, um Compliance-Anforderungen zu erfüllen.

ISO 27001

ISO 27001, eine internationale Norm, legt die Grundlage für die Erstellung, Wartung und Entwicklung von Informationssicherheitsmanagementsystemen (ISMS), einschließlich Datenmanagement.

SOC 2

Service Organization Control 2 (SOC 2) -Berichte werden häufig von Kunden und Geschäftspartnern von ausgelagerten Lösungsanbietern angefordert. Unternehmen, die die Einhaltung von SOC 2 anstreben, können einen SOC 2-konformen Passwort-Manager nutzen, um die Anforderungen zu erfüllen.

NERC

Die North American Electric Reliability Corporation (NERC) ist eine gemeinnützige internationale Regulierungsbehörde, die sich der Festlegung von Compliance-Standards widmet, die dazu beitragen, die Risiken für das Stromnetz und die Stromnetze von Hunderten von

NIS2

NIS2 ist eine Reihe von Anforderungen für die Sicherung von Netzwerk- und Informationssystemen in der gesamten EU. Die Richtlinie verpflichtet Unternehmen, die als Betreiber wesentlicher Dienste identifiziert wurden, geeignete Maßnahmen zur Verbesserung

Millionen Menschen in den Vereinigten Staaten, Kanada und einem Teil von Mexiko zu reduzieren.

NIST Cybersicherheitsrahmenwerk

Das National Institute of Standards and Technology (NIST) bietet Unternehmen Leitlinien und bewährte Verfahren, um Unternehmen, gemeinnützige Organisationen und andere private Institutionen bei der Verbesserung des Risikomanagements für Cybersicherheit zu unterstützen.

Reifegradmodell der Passwortverwaltung

Dieses Framework hilft Unternehmen, ihren Reifegrad des Passwort-Managers — basierend auf ihrem aktuellen Betrieb — zu verstehen und zu ermitteln, welche Schritte erforderlich sind, um ihre Sicherheit zu stärken und ihre bestehende Klassifizierung zu verbessern.

der Cybersicherheit zu ergreifen und den gesetzlichen Verpflichtungen nachzukommen.

SOX

Die Einhaltung des Sarbanes-Oxley Act (SOX) beinhaltet die Einhaltung einer Reihe von Sicherheitsanforderungen, die die Integrität der Finanzberichterstattung gewährleisten sollen.

Häufig gestellte Fragen

- **Kann das Bitwarden-Team meine Passwörter sehen?**

  Nr.

  Ihre Daten werden vollständig verschlüsselt und/oder gehasht, bevor **Sie Ihr** lokales Gerät verlassen, sodass niemand aus dem Bitwarden-Team jemals Ihre echten Daten sehen, lesen oder zurückentwickeln kann. Bitwarden-Server speichern nur verschlüsselte und gehashte Daten. Weitere Informationen darüber, wie Ihre Daten verschlüsselt werden, finden Sie unter Verschlüsselung.

  Mehr erfahren >

- **Wie halten Sie die Cloud-Server sicher?**

  Bitwarden ergreift extreme Maßnahmen, um die Sicherheit seiner Websites, Anwendungen und Cloud-Server zu gewährleisten. Bitwarden verwendet Microsoft Azure Managed Services, um Serverinfrastruktur und Sicherheit zu verwalten, anstatt dies direkt zu tun.

  Mehr erfahren >

- **Wird Bitwarden auditiert?**

  Bitwarden führt regelmäßig umfassende Sicherheitsaudits von Drittanbietern mit namhaften Sicherheitsfirmen durch. Diese jährlichen Audits umfassen Quellcodebewertungen und Penetrationstests für Bitwarden-IPs, Server und Webanwendungen.

  Mehr erfahren >

- **Was passiert, wenn Bitwarden gehackt wird?**

  Wenn Bitwarden aus irgendeinem Grund gehackt werden sollte und Ihre Daten offengelegt wurden, sind Ihre Daten aufgrund der starken Verschlüsselung und der einseitigen Hashing-Maßnahmen für Ihre Tresordaten und Ihr Master-Passwort immer noch geschützt.

  Mehr erfahren >

- **Wo werden meine Daten in der Cloud gespeichert?**

  Bitwarden verarbeitet und speichert alle Vault-Daten sicher in der Microsoft Azure Cloud in den USA oder der EU mithilfe von Diensten, die vom Team bei Microsoft verwaltet werden. Da Bitwarden ausschließlich von Azure bereitgestellte Serviceangebote nutzt, ist keine Server-Infrastruktur zu verwalten und zu warten. Alle Betriebszeiten, Skalierbarkeit, Sicherheitsupdates und Garantien werden von Microsoft und seiner Cloud-Infrastruktur unterstützt. Weitere Informationen finden Sie in der Dokumentation zu Microsoft Azure-Compliance-Angeboten.

  Mehr erfahren >

- **Warum sollte ich Bitwarden meine Passwörter anvertrauen?**

  Sie können uns aus mehreren Gründen vertrauen:

  1. Bitwarden ist **Open-Source-Software**. Unser gesamter Quellcode wird auf GitHub gehostet und kann von jedem kostenlos überprüft werden. Tausende von Softwareentwicklern folgen Bitwardens Quellcode-Projekten (und das sollten Sie auch!).

  2. Bitwarden wird **von seriösen externen Sicherheitsfirmen** sowie unabhängigen Sicherheitsforschern **geprüft**.

  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 guten Ruf.** Bitwarden wird von Millionen von Einzelpersonen und Unternehmen genutzt. Wenn wir etwas Fragwürdiges oder Riskantes getan hätten, wären wir aus dem Geschäft!

  Du vertraust uns immer noch nicht? Das musst du nicht. Open Source ist schön. Sie können ganz einfach den gesamten Bitwarden-Stack selbst hosten. Sie haben die Kontrolle über Ihre Daten.

  Mehr erfahren >

- **Verwendet Bitwarden einen gesalzenen Hash für mein Passwort?**

  PBKDF2 SHA-256 wird verwendet, um den Verschlüsselungsschlüssel von Ihrem Master-Passwort abzuleiten, aber Sie können Argon2 als Alternative wählen. Bitwarden salzt und hasht Ihr Master-Passwort mit Ihrer E-Mail-Adresse **lokal**, bevor es an unsere Server übertragen wird. Sobald ein Bitwarden-Server das gehashte Passwort erhält, wird es erneut mit einem kryptographisch sicheren Zufallswert gesalzen, erneut gehasht und in unserer Datenbank gespeichert.

  Mehr erfahren >

- **Wie werden meine Daten sicher auf Bitwarden-Servern übertragen und gespeichert?**

  Bitwarden verschlüsselt und/oder hasht Ihre Daten **immer** auf Ihrem lokalen Gerät, bevor etwas zur Speicherung an Cloud-Server gesendet wird. **Bitwarden-Server werden nur zur Speicherung verschlüsselter Daten verwendet.** Weitere Informationen finden Sie unter Speicher.

  Mehr erfahren >

- **Welche Verschlüsselung wird verwendet?**

  Bitwarden verwendet AES-CBC 256-Bit-Verschlüsselung für Ihre Vault-Daten und PBKDF2 SHA-256 oder Argon2, um Ihren Verschlüsselungsschlüssel abzuleiten.

  Mehr erfahren >

- **Welche Informationen werden verschlüsselt?**

  Alle Vault-Daten werden von Bitwarden verschlüsselt, bevor sie irgendwo gespeichert werden. Weitere Informationen finden Sie unter Verschlüsselung.

  Mehr erfahren >

- **Wo werden meine Daten auf meinem Computer/Gerät gespeichert?**

  Daten, die auf Ihrem Computer/Gerät gespeichert sind, werden verschlüsselt und erst entschlüsselt, wenn Sie Ihren Tresor entsperren. Entschlüsselte Daten werden nur **im Speicher** gespeichert und **niemals in einen dauerhaften Speicher geschrieben**.

  Mehr erfahren >