

# Passwortverwaltung für Unternehmen

Als führender Passwort-Manager für Unternehmen, der auf einer vertrauenswürdigen Open-Source-Architektur basiert, stärkt Bitwarden die Sicherheit von Anmeldeinformationen und füllt automatisch alle Geräte, Plattformen und Browser aus, um die Produktivität der Mitarbeiter zu steigern.

Erhalten Sie die vollständige interaktive Ansicht bei <https://bitwarden.com/de-de/products/business/>

## Premium-Funktionen für alle Ihre Geschäftsnutzer

### Kontrollieren Sie die Sicherheit der Anmeldeinformationen

Etablieren Sie eine erste Verteidigungslinie bei der Arbeit gegen Cyber-Bedrohungen und Datenschutzverletzungen. Unternehmensberichterstattungstools und -richtlinien zentralisieren die Sicherheit und machen es den Mitarbeitern leicht, [sichere Passwörter und Passschlüssel zu verwalten](#).

### Nahtlose Integration

Verbinden Sie Bitwarden nahtlos mit Ihrem bestehenden Tech-Stack mit flexiblen Integrationsoptionen wie Single Sign On (SSO) - Identitätsanbietern und Verzeichnisdiensten einschließlich SCIM.

### Starke Passwörter sofort teilen

Teams generieren, verwalten und teilen sicher starke Benutzerkennwörter und andere sensible Daten von jedem Ort oder Gerät aus abteilungsübergreifend.

### Befähigen Sie Ihre Mitarbeiter zu Hause

Mit Bitwarden Password Manager für Unternehmen arbeiten Teammitglieder sicher von *überall* aus und profitieren von Gerätesynchronisierung, plattformübergreifender Unterstützung, Offline-Zugriff und über 50 unterstützten Sprachen.

---

## Zentralisierte Passwort-Speicherung

Verwalten und teilen Sie Geschäftspasswörter, Firmenkreditkarten und andere sensible Informationen sicher mit Ihrem Team in einem Ende-zu-Ende-verschlüsselten Tresor. Administratoren verwalten Benutzerzugriffs- und Authentifizierungsanforderungen einfach mit umfassenden Richtlinien und flexiblen Integrationen wie SSO.

---

## Beispiellose SSO-Integration

Schützen Sie alle Unternehmensanmeldungen mit Ihren Single Sign-On-Sicherheitsrichtlinien. Voll kompatibel mit SAML 2.0 und OIDC lässt sich Bitwarden schnell und einfach in Ihre bestehenden Lösungen integrieren. Administratoren können drei Möglichkeiten zur Verwendung von SSO wählen (vertrauenswürdige Geräte, Schlüsselanschluss, Master-Passwort).

---

## Automatisieren Sie die Bereitstellung von Benutzerkonten

Einfaches Onboarding und Verwalten Ihres gesamten Unternehmens über eine zentrale Admin-Konsole. Aktivieren Sie Unternehmensrichtlinien und stellen Sie Benutzer automatisch bereit, indem Sie Ihren vorhandenen Verzeichnisdienst nahtlos integrieren.

---

## Plattform-Funktionen und Vorteile

### Plattformübergreifende Zugänglichkeit & unbegrenzte Geräte

Greifen Sie auf kritische Daten in Ihrem Tresor von jedem Standort, Browser und über unbegrenzte Geräte zu

### Cloud-basierter oder selbst gehosteter Passwort-Manager

Schnell und effizient in der Cloud bereitstellen, oder selbst gehostet für Teams mit zusätzlichen IT- und Infrastruktur-Ressourcen

### Sicherheitsprüfung-und-compliance

Open Source, von Drittanbietern geprüft und konform mit den GDPR-, Privacy Shield-, HIPAA- und CCPA-Vorschriften

### Verzeichnis-Synchronisation

Nutzen Sie die SCIM-Unterstützung oder den Directory Connector, um die

### Tresor-Gesundheitsberichte

Greifen Sie auf aufschlussreiche Berichte zu, um schwache, wiederverwendete

### Immer-an-Unterstützung

Kundenerfolgsagenten stehen Ihnen rund um die Uhr zur Verfügung

Bereitstellung von Benutzern und Gruppen zu vereinfachen und die Synchronisation mit Ihrem Verzeichnisdienst aufrechtzuerhalten.

Passwörter und andere hilfreiche Sicherheitsmetriken aufzudecken

---

## Laufende Unterstützung und Schulung

Von Bereitstellungssupport bis hin zu Endbenutzerschulungen bietet Bitwarden robuste Dokumentation, Ressourcen und ein kompetentes Kundensupport-Team, das Sie und Ihr Unternehmen unterstützt.

---

## Bewährte Sicherheit und Transparenz im Passwort-Management

### Open-Source-Sicherheit

Vertrauen und Transparenz sind unerlässlich, wenn es um die Verwaltung von Geschäftspasswörtern geht. Als Open-Source-Passwort-Manager kann jede Codezeile in Bitwarden eingesehen werden. Bitwarden wurde entwickelt, um die höchsten Sicherheitsstandards und -anforderungen zu übertreffen, damit Sie sicher sein können, dass Ihre Daten geschützt sind und kritische Geschäftsfunktionen genau wie erwartet funktionieren.

### Passwort-Tresor mit Ende-zu-Ende-Verschlüsselung

Bitwarden verschlüsselt alle Ihre Daten mit einem Unternehmenspasswort-Tresor, bevor sie jemals Ihr Gerät verlassen, und nur Sie haben Zugang dazu. Selbst das Bitwarden-Team kann Ihre geschützten Daten nicht entsperren. Bitwarden versiegelt Ihre sensiblen Informationen mit End-to-End-AES-256-Bit-Verschlüsselung, gesalzenerem Hashing und PBKDF2 SHA-256 Authentifizierungsprozess.

### drittanbieter-geprüft

Neben der Open-Source-Codebasis von Bitwarden und dem Programm für unabhängige Sicherheitsforscher bieten seriöse Drittanbieter offizielle Sicherheitsbewertungen und Penetrationstests an. Bitwarden hat gründliche Sicherheitsaudits und kryptographische Analysen mit Sicherheitsexperten wie Cure53 abgeschlossen.

---

## Erfahren Sie mehr über die Verwaltung von Geschäftspasswörtern

### Warum benötigt Ihr Unternehmen ein Passwort-Verwaltungstool?

Fast 81 Prozent der Hackerangriffe auf Daten erfolgen durch gestohlene oder schwache Passwörter. Passwort-Manager generieren starke, eindeutige Passwörter, die Mitarbeiter sicher teilen.

Unternehmen, die eine [starke Cybersicherheitskultur etablieren](#), reduzieren ihre Risiken von Cyberbedrohungen erheblich. Passwort-Manager machen dies einfach, indem sie globale Richtlinien für die Passwortstärke festlegen, die Zwei-Faktor-Authentifizierung (2FA) erzwingen und detaillierte Ereignisprotokolle verwenden, um die Benutzeraktivität zu überwachen.

[Bitwarden-Pläne und -Preise entdecken >](#)

---

## Bester Enterprise-Passwort-Manager

Für acht Quartale in Folge platzierte sich Bitwarden auf Platz1 in der Kategorie Enterprise User Satisfaction des [G2 Enterprise Grid Report](#), der die besten Passwort-Manager für Unternehmen zählt.

## Häufig-gestellte-Fragen

- **Was ist ein Geschäfts-Passwort-Manager?**

Ein Business-Passwort-Manager ist eine Anwendung, die Passwörter und andere sichere Informationen in einem digitalen Tresor mit Verwaltungsfunktionen für Unternehmen generiert, verwaltet und speichert. Möchten Sie es in Aktion sehen? [Reservieren Sie einen Platz](#) bei einer wöchentlichen Live-Demo!

- **Warum einen passwort-manager für das geschäft verwenden?**

Passwort-Manager ermöglichen es Mitarbeitern, Passwörter sicher zu erstellen, zu verwalten und zu speichern. Dies reduziert das Risiko der häufigsten Cyberbedrohung: schwache, wiederverwendete oder kompromittierte Passwörter. Bitwarden [bringt Ihrem Unternehmen einen Mehrwert](#), indem es Risiken reduziert und die Produktivität erhöht!

- **Was ist der beste Passwort-Manager für ein kleines Unternehmen?**

G2 und Techradar haben Bitwarden als den [besten Passwort-Manager für kleine Unternehmen](#) eingestuft, da er Open Source ist und erweiterte Funktionen bietet, um die Sicherheit der Benutzer zu gewährleisten.

- **Sollte ein kleines Unternehmen einen Passwort-Manager verwenden?**

Laut einem kürzlichen [Cumulus Global Bericht](#) waren 43 % der kleinen und mittleren Unternehmen Ziel eines Cyberangriffs. Hacker betrachten oft SMB-Daten als ein leichtes Ziel, weil sie davon ausgehen, dass kleinere Unternehmen nicht die robuste Sicherheit oder den Schutz haben, den große Unternehmen sich leisten können.

- **Wie speichern unternehmen passwörter?**

Viele Unternehmen verwenden veraltete und unsichere Methoden zur Verwaltung von Passwörtern, wie gemeinsam genutzte Tabellenkalkulationen oder sogar schriftliche Notizen. Unternehmen, die sich vor Cyberangriffen schützen möchten, nutzen Ende-zu-Ende verschlüsselte Passwort-Manager, um eine sichere Speicherung und Weitergabe von Passwörtern zu gewährleisten.