Der selbst gehostete Passwort-Manager von Bitwarden

Verwalten Sie geschäftliche Anmeldeinformationen und benutzerdefinierte Sicherheitsrichtlinien sicher auf Ihrem eigenen Server, indem Sie den Bitwarden Password Manager selbst hosten.

Erhalten Sie die vollständige interaktive Ansicht bei https://bitwarden.com/de-de/self-hosted-password-manager-on-premises/

bitwarden

Wenden Sie Ihr eigenes Sicherheitsmodell an

Platzieren Sie Ihre Bitwarden-Installation hinter einem Proxy, einer Firewall und anderen Sicherheitsvorkehrungen für zusätzliche Datensicherheit.

Kontrolle von Backups und Verfügbarkeit

Die containerbasierten Lösungen von Docker oder Kubernetes passen in Ihre bestehende Hochverfügbarkeits- und Wiederherstellungsstrategie und in Ihre etablierten Verfahren.

Passen Sie es an Ihre Bedürfnisse an

Erfüllen Sie Ihre spezifischen Compliance-Anforderungen und internen Datenaufenthaltsrichtlinien mit flexiblen Umgebungsvariablen für sich ändernde Anforderungen.

Der vertrauenswürdige Passwort-Manager zu Hause, bei der Arbeit und unterwegs

Plattformübergreifende Zugänglichkeit & unbegrenzte Geräte

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

Bitwarden nahtlos integrieren

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

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

Tresor-Gesundheitsberichte

Greifen Sie auf aufschlussreiche Berichte zu, um schwache, wiederverwendete Passwörter und andere hilfreiche Sicherheitsmetriken aufzudecken

Immer-an-Unterstützung

Kundenerfolgsagenten stehen Ihnen rund um die Uhr zur Verfügung

Die Vorteile von selbst gehosteten Passwort-Managern

Echte Datenhoheit

Ob die Bedenken vom Vorstand oder von Ihren Kunden kommen, mit Self-Hosting ist echte Datenhoheit Realität.

Einhaltung gesetzlicher Vorschriften

Wenn für Ihre Branche, Ihren Service oder Ihr Produkt strenge Anforderungen an die Datenkonformität gelten, aktiviert der selbst hostende Bitwarden Password Manager ein großes Compliance-Kästchen.

Anpassbare Sicherheit

Passen Sie die Sicherheitseinstellungen an Ihre Bedürfnisse an. Passen Sie jeden Aspekt der Sicherheit Ihres Unternehmens an, von Self-Host-Umgebungsvariablen bis hin zu produktinternen Richtlinien.

Nahtlose Integration

Unterstützung von Installationen für Windows, Linux, Docker oder Kubernetes, Integration in Ihre vorhandene IT-Infrastruktur. Der selbst gehostete Bitwarden-Server ist mit allen Endclients kompatibel, einschließlich mobiler und Desktop-Apps und Browsererweiterungen. Integrieren Sie produktintern mit Ihrem Identity Provider, Verzeichnisdiensten und mehr!

Audit- und Compliance-fähig

Detaillierte Ereignisprotokolle können von SIEM-Tools über Integrationen oder APIs aufgenommen werden, um die Benutzeraktivität zu verfolgen und die Einhaltung Ihrer internen Richtlinien und externen Vorschriften sicherzustellen. Auditergebnisse von Drittanbietern, SOC 2-Berichte und andere Compliance-Informationen für die Anwendung werden jährlich veröffentlicht und aktualisiert.

Gewinnen Sie branchenführende Sicherheit und vollständige Kontrolle über Ihre Daten

Machen Sie Ihre Online-Erfahrung sicherer, schneller und angenehmer, indem Sie Bitwarden Password Manager selbst hosten.

Häufig gestellte Fragen

Weitere häufig gestellte Fragen zum Selbsthosting findest du hier

- **Welche Vorteile bietet die Verwendung eines selbst gehosteten Passwort-Managers?**

  1. **Echte Datenhoheit**: Das Self-Hosting eines Passwort-Managers gibt Ihnen die vollständige Kontrolle über Ihre Daten. Sie verwalten Ihren eigenen Server und stellen sicher, dass vertrauliche Passwörter und Anmeldeinformationen in der von Ihnen kontrollierten Infrastruktur gespeichert werden.

  2. **Erhöhte Sicherheit**: Mit einer selbst gehosteten Lösung können Sie Ihr eigenes Sicherheitsmodell anwenden. Platzieren Sie Ihre Passwortverwaltungsinstallation für zusätzlichen Schutz hinter Proxys und Firewalls.

  3. **Anpassung**: Selbst gehostete Passwort-Manager bieten oft flexible Umgebungsvariablen, mit denen Sie das Setup an Ihre spezifischen Anforderungen und Compliance-Anforderungen anpassen können.

  4. **Open-Source-Vorteile**: Vertrauen und Transparenz sind unerlässlich, wenn es darum geht, welchen Passwort-Manager Sie selbst hosten möchten. Da Bitwarden ein Open-Source-Passwort-Manager ist, sind die Sicherheitsmaßnahmen selbstverifizierbar und jede Codezeile wird regelmäßig von Tausenden von Sicherheitsexperten und Enthusiasten weltweit überprüft.

  5. **Einhaltung gesetzlicher Vorschriften**: Self-Hosting kann dazu beitragen, die strengen Anforderungen an die Datenkonformität in verschiedenen Branchen zu erfüllen, da du die volle Kontrolle über die Datenspeicherung und den Datenzugriff hast.

  6. **Integration in bestehende Systeme**: Selbst gehostete Lösungen unterstützen oft eine nahtlose Integration in Ihre aktuelle IT-Infrastruktur, einschließlich Verzeichnisdiensten und Identitätsanbietern.

  7. **Auditbereitschaft**: Erhalten Sie Zugriff auf detaillierte Ereignisprotokolle für die Verfolgung der Benutzeraktivitäten, die für interne Audits und die Einhaltung der Compliance entscheidend sein können.

- **Auf welchen Plattformen kann ich Gastgeber sein?**

  Bitwarden-Clients sind plattformübergreifend und der Server kann in Docker-Containern unter Windows, Linux oder in Kubernetes mithilfe eines Helm-Diagramms bereitgestellt werden.

  Docker Desktop unter Windows erfordert möglicherweise eine Lizenz, je nachdem, ob Ihr Unternehmen die Lizenzanforderungen von Docker erfüllt. Docker unter Linux ist jedoch kostenlos.

  Weitere Informationen zu Docker und Containertechnologien finden Sie auf der Docker-Website.

- ### Wie stelle ich Bitwarden auf AWS, Azure, GCP oder VMware vCenter bereit?

  Bitwarden verfügt über ausführliche Anleitungen zum Bereitstellen von Docker-Installationen in der Hilfedokumentation. Anweisungen zur Installation auf AWS EKS, OpenShift und Azure AKS mit Helm sind ebenfalls verfügbar. Nachfolgend finden Sie empfohlene Ressourcen, die Ihnen den Einstieg erleichtern:

  - Docker-Bereitstellungsleitfäden
  - Helm-Einsatzleitfäden
  - Wie man eine Bitwarden-Organisation selbst hostet

- ### Wie richte ich einen Open-Source-Passwort-Manager auf meinem eigenen Server ein?

  Das Einrichten eines Open-Source-Passwort-Managers auf Ihrem eigenen Server beinhaltet in der Regel diese Schritte

  1. **Bereiten Sie Ihren Server** vor: Stellen Sie sicher, dass Sie einen Server oder eine virtuelle Maschine bereit haben. Dies kann lokale Hardware oder ein Cloud-basierter Server sein.
  2. **Bereitstellungsmethode auswählen**: Viele selbst gehostete Passwort-Manager bieten mehrere Installationsoptionen an. Häufige sind:
     - Docker-Container
     - Kubernetes-Bereitstellungen
  3. **Installation**: Erkunden Sie die detaillierte Bitwarden Self-Host-Dokumentation für verschiedene Bereitstellungstypen.
  4. **Konfiguration**: Richten Sie Umgebungsvariablen ein und passen Sie die Einstellungen an Ihre Sicherheitsanforderungen und organisatorischen Anforderungen an.
  5. **Benutzerverwaltung**: Richten Sie Administratorkonten ein und konfigurieren Sie Benutzerzugriffsrechte.
  6. **Client-Setup**: Installieren Sie Browsererweiterungen, Desktop-Apps und mobile Apps für Ihre Benutzer und stellen Sie sicher, dass sie so konfiguriert sind, dass sie eine Verbindung zu Ihrem selbst gehosteten Server herstellen.
  7. **Testen: Testen** Sie die Installation gründlich, einschließlich Funktionen wie dem Passwortgenerator, der sicheren Freigabe und der Multi-Faktor-Authentifizierung.
  8. **Wartungsplan**: Richten Sie Verfahren für regelmäßige Backups, Updates und Sicherheitsaudits ein, um Ihren selbst gehosteten Passwort-Manager sicher und auf dem neuesten Stand zu halten.

  Denken Sie daran, dass Self-Hosting zwar viele Vorteile bietet, aber auch eine kontinuierliche Wartung und Sicherheitsüberwachung erfordert. Stellen Sie sicher, dass Sie über die Ressourcen und das Fachwissen verfügen, um eine selbst gehostete Lösung effektiv zu verwalten.