RESOURCE CENTER

Enterprise-Referenzhandbuch zur Bitwarden-Authentifizierung

Erläuterung kritischer Funktionen rund um Bitwarden-Authentifizierung und SSO-Angebote

Get the full interactive view at https://bitwarden.com/de-de/resources/reference-guide-bitwarden-authentication/

bitwarden

Authentifizierungstyp	Was ist das?	Überlegungen zur Bereitstellung *Alle Optionen zur Bereitstellung der Authentifizierung stimmen mit dem Ende-zu-Ende-Verschlüsselungsmodell von Bitwarden überein*
SSO mit vertrauenswürdigen Geräten	Für ein passwortloses Erlebnis verwenden Mitarbeiter ihre SSO-Anmeldeinformationen, um sich in einem einzigen Schritt zu authentifizieren und zu entschlüsseln. Registrierte, vertrauenswürdige Geräte sind in der Lage, Tresore zu entschlüsseln und neue Geräte zu bestätigen und zu akzeptieren. Sobald ein Gerät vertrauenswürdig ist, braucht es keine Genehmigung mehr.	Wenn Sie diese Option auswählen, können sich Mitarbeiter anmelden und ihre Tresore entschlüsseln, ohne ein Passwort zu benötigen. Vertrauenswürdige Geräte werden registriert und können Anmeldungen bestätigen und das Vertrauen auf andere Geräte ausweiten. Bei der Kontoerstellung authentifiziert der SSO-Anbieter den Benutzer und registriert den Login-Client als erstes vertrauenswürdiges Gerät, sodass er den Tresor entschlüsseln kann. Zusätzliche vertrauenswürdige Geräte können mit Genehmigung der Bitwarden-Desktop-App, der mobilen App, der Web-App oder von einem Bitwarden-Administrator registriert werden. Jedes vertrauenswürdige Gerät verfügt über einen individuellen Geräteverschlüsselungsschlüssel, und Zero-Knowledge, End-to-End-Verschlüsselung und Sicherheit werden geräteübergreifend aufrechterhalten. Zusätzliche Ressourcen: Richten Sie SSO mit vertrauenswürdigen Geräten ein Enterprise passwortloses SSO bringt eine bessere Produktivität und Benutzeranmeldeerfahrung für Mitarbeiter
Mit SSO Zugangsdaten anmelden	Die Benutzerauthentifizierung wird von der Tresorentschlüsselung getrennt, indem der Identitätsanbieter Ihres Unternehmens genutzt wird, um Benutzer in ihrem Bitwarden-Tresor zu authentifizieren, und Master-Passwörter zur Entschlüsselung von Tresordaten verwendet werden.	Diese Option unterstützt Identitätsanbieter, die SAML 2.0- oder OpenID Connect-Standards verwenden. Die Auswahl dieser Option bedeutet, dass jedes Mal, wenn sich ein Mitarbeiter mit SSO bei Bitwarden anmeldet, er sein Master-Passwort verwenden muss, um seinen Tresor zu entschlüsseln und die kritischen

Authentifizierungstyp	Was ist das?	**Überlegungen zur Bereitstellung** *Alle Optionen zur Bereitstellung der Authentifizierung stimmen mit dem Ende-zu-Ende-Verschlüsselungsmodell von Bitwarden überein*
		Anmeldeinformationen und Geheimnisse Ihres Unternehmens zu schützen. Zusätzliche Ressourcen: Konfigurieren Sie Ihre Organisation mit Login mit SSO Einrichten der Anmeldung mit SSO
Anmeldung mit SSO und kundenverwalteter Verschlüsselung	Mitarbeiter verwenden ihre SSO-Anmeldeinformationen, um alles in einem einzigen Schritt zu authentifizieren und zu entschlüsseln. Diese Option verschiebt die Aufbewahrung der Benutzerhauptpasswörter auf Unternehmen, die vom Unternehmen die Bereitstellung eines Schlüsselkonnektors zum Speichern der Benutzerschlüssel verlangen.	Für Unternehmen mit weit verbreiteten SSO-Implementierungen und dem Wunsch, Authentifizierung und Entschlüsselung in eine lokale Lösung zu integrieren, bietet Bitwarden SSO mit kundenverwalteter Verschlüsselung an. In diesem Szenario verwalten Unternehmen einen Schlüsselkonnektor-Agenten. Dies erfordert eine Verbindung zu einer Datenbank, die verschlüsselte Benutzerschlüssel speichert, und ein RSA-Schlüsselpaar, um diese Schlüssel zu verschlüsseln und zu entschlüsseln. Dieser Ansatz unterhält eine Verschlüsselungsarchitektur ohne Wissen, da zu keinem Zeitpunkt Entschlüsselungsschlüssel über Bitwarden-Server laufen. Die Verwaltung kryptografischer Schlüssel ist unglaublich sensibel und wird nur für Unternehmen mit einem Team und einer Infrastruktur empfohlen, die bereits einen Schlüsselserver sicher bereitgestellt und verwaltet haben. SSO mit kundenverwalteter Verschlüsselung ist für Kunden verfügbar, die Bitwarden selbst hosten. Zusätzliche Ressourcen: Whitepaper: Wählen Sie die richtige SSO-Anmeldestrategie

Authentifizierungstyp	Was ist das?	**Überlegungen zur Bereitstellung** *Alle Optionen zur Bereitstellung der Authentifizierung stimmen mit dem Ende-zu-Ende-Verschlüsselungsmodell von Bitwarden überein* Hilfe-Artikel: Anmeldung mit SSO und Kundenverwaltung Verschlüsselung - Bereitstellung des Schlüsselanschlusses
Mit Bitwarden anmelden	Mitarbeiter verwenden ihre E-Mail-Adresse und ihr Master-Passwort, um sich anzumelden und ihren Bitwarden-Tresor zu entschlüsseln.	Für Unternehmen, die schnell loslegen möchten, ermöglicht die Anmeldung bei Bitwarden den Mitarbeitern, ihre eindeutige E-Mail-Adresse und ihr Master-Passwort zu verwenden, um auf ihren Tresor zuzugreifen. Es ist perfekt für Unternehmen, die die Authentifizierung noch nicht zentral verwalten oder einen Identitätsanbieter verwenden. Administratoren können Mitarbeiter manuell in Organisationen und freigegebene Sammlungen einladen oder den Bitwarden Directory Connector verwenden, um LDAP-Gruppen zu synchronisieren Zusätzliche Ressourcen: Fünf bewährte Verfahren für die Passwortverwaltung Erste Schritte mit Bitwarden

Authentifizierungstyp	Was ist das?	**Überlegungen zur Bereitstellung** *Alle Optionen zur Bereitstellung der Authentifizierung stimmen mit dem Ende-zu-Ende-Verschlüsselungsmodell von Bitwarden überein*
Mit Gerät anmelden	Mitarbeiter verwenden ihre E-Mail-Adresse, um sich anzumelden und dann die Anmeldung von einem zweiten, authentifizierten Gerät (mobile App oder Desktop-App) zu bestätigen, das den Tresor-Verschlüsselungsschlüssel bei der Genehmigung sicher freigibt.	Die Anmeldung mit Gerät steht allen Mitarbeitern zur Verfügung, nachdem sie sich mindestens einmal mit E-Mail und Master-Passwort auf dem Gerät angemeldet haben. Dies ermöglicht es den Mitarbeitern, sich nach der ersten Anmeldung in ihrer mobilen oder Desktop-App schnell wieder bei allen ihren Bitwarden-Clients anzumelden. Zusätzliche Ressourcen: Hilfe-Artikel: Login mit Gerät