

راهکاری مطمئن برای مدیریت رمزهای عبور سازمانی

Bitwarden راهکاری مطمئن و در عین حال ساده است که به افراد و کسب‌وکارها کمک می‌کند اطلاعات حساس خود را به راحتی و ایمن، روی هر دستگاهی مدیریت کنند.

Bitwarden: قابل اعتمادترین password manager برای افراد و سازمان‌ها

- ✓ **استفاده آسان:** تولید، ذخیره و پر کردن خودکار رمزهای عبور قوی برای تمام حساب‌ها – تنها با چند کلیک. قابلیت SSO این امکان را می‌دهد که تنها با یکبار وارد شدن، به تمام سرویس‌ها و برنامه‌های کاری دسترسی داشته باشید
- ✓ **مدیریت متمرکز:** اطلاعات حساس و رمزهای عبور کارکنان را در یک فضای امن و مرکزی نگهداری و مدیریت کنید. با ابزارهای پیشرفته Bitwarden، می‌توانید دسترسی‌ها را مشخص کرده، کاربران را مدیریت کنید و اطلاعات حساس را به صورت ایمن با دیگر اعضای تیم به اشتراک بگذارید.
- ✓ **امنیت مطمئن:** رمزگذاری سرتاسری با معماری Zero-Knowledge
Bitwarden از رمزگذاری سرتاسری و معماری Zero-Knowledge استفاده می‌کند، یعنی حتی خود سرویس‌دهنده هم به داده‌های شما دسترسی ندارد.

از کارمندان و کسب‌وکار خود محافظت کنید

- **امنیت بیشتر برای کارکنان**
ایمپنات حاصل کنید که تمام اعضای تیم (به‌ویژه هنگام استفاده از ابزارهایی خارج از سیستم SSO) از رمزهای عبور قوی، منحصربه‌فرد و به‌درستی مدیریت شده استفاده می‌کنند.
- **پیشگیری از آسیب‌های امنیتی پرهزینه**
۸۸٪ از نقض‌های امنیتی در برنامه‌های تحت وب به دلیل استفاده از رمزهای عبور ضعیف یا تکراری رخ می‌دهد. این موارد به‌طور میانگین تا ۹/۳ میلیون دلار هزینه دربر دارند. Bitwarden با تقویت مدیریت رمز عبور، از این آسیب‌ها پیشگیری می‌کند.
- **همکاری آسان، امن و ساخت‌یافته**
اعضای تیم می‌توانند به صورت ایمن اطلاعات ورود به حساب‌های سازمانی، کدهای یکبارمصرف (TOTP)، کارت‌های بانکی شرکت و سایر داده‌های حساس را با یکدیگر به اشتراک بگذارند. (بدون نیاز به ارسال رمز از طریق ایمیل یا پیام‌رسان‌ها)

تیم خود را توانمند کنید و ریسک‌ها را کاهش دهید

- **سفارشی‌سازی سیاست‌های امنیتی متناسب با نیاز سازمان**
با Bitwarden می‌توانید سیاست‌های امنیتی سازمان خود را به صورت دقیق تعریف و پیاده‌سازی کنید؛ این سیاست‌ها باعث ایجاد انسجام و استاندارد امنیتی در کل تیم می‌شوند.
- **شناسایی و اصلاح سریع آسیب‌پذیری‌های رمز عبور**
با استفاده از گزارش سلامت خزانه (Vault Health Reports) می‌توانید وضعیت امنیتی رمزهای عبور سازمان را بررسی کنید. این گزارش‌ها هشدارهایی درباره رمزهای افشا شده، تکراری، ضعیف یا در معرض خطر ارائه می‌دهند و به شما کمک می‌کنند به سرعت اقدامات اصلاحی انجام دهید.
- **اشتراک‌گذاری ایمن و مدیریت یکپارچه اطلاعات**
با استفاده از یک خزانه مرکزی در Bitwarden، می‌توانید اطلاعات حساس را به صورت ایمن و تنها با افراد مجاز به اشتراک بگذارید. این ساختار به شما امکان می‌دهد بر دسترسی‌ها نظارت داشته باشید، مالکیت داده‌ها را به درستی مدیریت کنید و همه اعضای تیم را به یک منبع اطلاعاتی دقیق و هماهنگ متصل کنید.

Bitwarden چشم‌اندازی دارد که در آن، امنیت دیجیتال آن قدر قوی است که هیچ‌کس هدف هکرها قرار نمی‌گیرد.



compliance badges

ویژگی‌های کلیدی و امکانات یکپارچه‌سازی پیشرفته Bitwarden

ورود امن با SSO

کاربران سازمانی می‌توانند با استفاده از پروتکل‌های استاندارد SAML ۲/۰ و OpenID Connect به اختصار (OIDC) احراز هویت شوند. Bitwarden از سرویس‌هایی مانند Okta، Google، Entra ID، Auth و دیگر ارائه‌دهندگان پشتیبانی می‌کند تا ورود سریع، امن و یکپارچه را تضمین نماید.

همگام‌سازی دایرکتوری

با پشتیبانی از پروتکل‌های استاندارد مانند SCIM و LDAP، فرآیند تأمین و مدیریت کاربران را ساده و خودکار کنید. Bitwarden به راحتی با ارائه‌دهندگانی مانند Okta، OneLogin، JumpCloud و Microsoft Entra ID (Azure AD) و دیگر سیستم‌های مدیریت هویت ادغام می‌شود.

مناسب برای توسعه‌دهندگان (Developer-friendly)

با استفاده از API‌های قدرتمند، رابط خط فرمان (CLI) و اسکریپت‌نویسی، Bitwarden به شما اجازه می‌دهد تا با ابزارهای دلخواه خود یکپارچه شوید و فرآیندها را خودکار کنید. این قابلیت‌ها، توسعه و مدیریت رمزها را برای تیم‌های فنی ساده‌تر، سریع‌تر و امن‌تر می‌سازد.

عامل کلید SSH (SSH Key Agent)

Bitwarden کلیدهای SSH شما را به صورت امن رمزگذاری و ذخیره می‌کند، تا بتوانید بدون نیاز به افشای کلیدها، عملیات امضای کامیت‌های Git و احراز هویت روی سرورها را به‌سادگی انجام دهید.

پشتیبانی جهانی ۷/۲۴

تیم متخصص ما در تمام ساعات شبانه‌روز و هفت روز هفته آماده پشتیبانی از شماست - از راه‌اندازی اولیه و استقرار گرفته تا آموزش کاربران نهایی و رفع مشکلات فنی.

استقرار خودکار روی دستگاه‌های کاربران

Bitwarden به شما امکان می‌دهد افزونه‌های مرورگر را به‌صورت خودکار و متمرکز روی دستگاه‌های کاربران، از طریق پلتفرم‌های مدیریت نقطه پایانی (Endpoint Management)، نصب و پیکربندی کنید.

مدیریت متمرکز کاربران

Bitwarden به شما اجازه می‌دهد با استفاده از سیستم ارائه‌دهنده هویت (Identity Provider)، احراز هویت کاربران سازمان را به‌صورت متمرکز و ایمن مدیریت کنید. این فرآیند از طریق پروتکل‌های استاندارد مانند SAML ۲/۰ و OpenID Connect انجام می‌شود.

سازگار با همه دستگاه‌ها و سیستم‌عامل‌ها

Bitwarden روی همه دستگاه‌ها و سیستم‌عامل‌ها قابل استفاده است - از موبایل و دسکتاپ تا مرورگر و نسخه تحت وب. پشتیبانی از بیش از ۵۰ زبان، تجربه‌ای روان و سازگار برای کاربران در هر نقطه از جهان را فراهم می‌کند.

لاگ رویدادها و سازگاری با SIEM

Bitwarden ثبت کامل رویدادهای قابل حسابرسی (Audit Logs) را فراهم می‌کند. این داده‌ها را می‌توان برای بازرسی دستی یا یکپارچه‌سازی با سامانه‌های مدیریت اطلاعات و رخدادهای امنیتی (SIEM) مانند Splunk، Microsoft Sentinel، Elastic، Panther، RapidV و سایر ابزارهای امنیتی تحلیل و بررسی مورد استفاده قرار داد.

گزارش‌های سلامت خزانه (Vault Health Reports)

با گزارش‌های Vault health، وضعیت امنیت رمزهای عبور ذخیره شده را بررسی کنید؛ از جمله رمزهای عبور ضعیف، تکراری یا افشا شده، و اطلاعات مهم امنیتی دیگر که به بهبود محافظت شما کمک می‌کند.

میزبانی اختصاصی سازمانی (Self-Hosting)

Bitwarden به شما این امکان را می‌دهد تا راهکار را روی زیرساخت داخلی یا ابر خصوصی سازمان خود مستقر کنید، تا کنترل کامل داده‌ها و امنیت مطابق با سیاست‌های داخلی در اختیار شما باشد.

امکانات تکمیلی Bitwarden برای توسعه امن

Bitwarden قابلیت‌های تکمیلی پیشرفته‌ای را ارائه می‌دهد؛ از جمله Secrets Manager برای مدیریت امن اطلاعات حساس توسعه (مانند API Keys و Token ها) و Passwordless.dev برای پیاده‌سازی ورود بدون رمز عبور با استفاده از Passkey.