vitextra

WISSENSDATENBANKARTIKEL

Password Vault im Vergleich zu Browser-Kennwortmanagern und Enterprise-Kennwortmanagern: Was ist die richtige Wahl?

2026 © Vitextra SIA. Alle Rechte vorbehalten.

Haftungsausschluss

Für die Zwecke dieses Haftungsausschlusses:

- **Das Unternehmen** (in diesem Haftungsausschluss entweder als „das Unternehmen“, „wir“, „uns“ oder „unser“ bezeichnet) bezieht sich auf Vitextra SIA, LV-1009 Riga, Matīsa iela 61 – 25.
- **Dokument** verweist auf den Wissensdatenbank-Artikel.
- **Sie** sind die Person, die auf das Dokument zugreift, bzw. das Unternehmen oder eine andere juristische Person, in deren Namen eine solche Person auf das Dokument zugreift oder es nutzt.
- **Die Website** verweist auf Vitextra, zugänglich über https://vitextra.com

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen dienen nur der allgemeinen Information.

Das Unternehmen übernimmt keine Verantwortung für Fehler oder Auslassungen im Inhalt des Dokuments.

In keinem Fall haftet das Unternehmen für besondere, direkte, indirekte oder zufällige Schäden oder für Schäden jeglicher Art, die sich aus der Nutzung des Inhalts des Dokuments ergeben, unabhängig davon, ob es sich um eine Klage aufgrund von Vertrag, Fahrlässigkeit oder anderen Delikten handelt. Das Unternehmen behält sich das Recht vor, den Inhalt des Dokuments jederzeit und ohne vorherige Ankündigung zu ergänzen, zu streichen oder zu ändern.

Haftungsausschluss für Fehler und Auslassungen

Die in dem Dokument enthaltenen Informationen dienen lediglich als allgemeine Orientierungshilfe zu Fragen von Interesse. Daher können Fehler auftreten, auch wenn das Unternehmen alle Vorsichtsmaßnahmen ergreift, um sicherzustellen, dass der Inhalt des Dokuments aktuell und korrekt ist. Außerdem kann es angesichts der sich ändernden Gesetze, Regeln und Vorschriften zu Verzögerungen, Auslassungen oder Ungenauigkeiten bei den in diesem Dokument enthaltenen Informationen kommen.

Das Unternehmen haftet nicht für etwaige Fehler oder Auslassungen oder für die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben.

Haftungsausschluss für faire Nutzung

Das Unternehmen darf urheberrechtlich geschütztes Material verwenden, das der Urheberrechtsinhaber nicht ausdrücklich genehmigt hat. Das Unternehmen stellt dieses Material für Kritik, Kommentare, Berichterstattung, Schulung, Wissenschaft oder Forschung zur Verfügung.

Das Unternehmen ist der Ansicht, dass dies eine „faire Nutzung“ von urheberrechtlich geschütztem Material im Sinne von Abschnitt 107 des US-Urheberrechtsgesetzes darstellt.

Wenn Sie urheberrechtlich geschütztes Material aus dem Dokument für Ihre eigenen Zwecke verwenden möchten, die über eine angemessene Nutzung hinausgehen, müssen Sie die Erlaubnis des Urheberrechtsinhabers einholen.

„Benutzung auf eigene Gefahr“ Haftungsausschluss

Alle Informationen in diesem Dokument werden im Ist-Zustand zur Verfügung gestellt, ohne Garantie auf Vollständigkeit, Genauigkeit, Aktualität oder auf die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben, und ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, aber nicht beschränkt auf Garantien für Leistung, Marktgängigkeit und Eignung für einen bestimmten Zweck.

Das Unternehmen haftet weder Ihnen noch anderen gegenüber für Entscheidungen oder Handlungen, die im Vertrauen auf die Informationen des Dienstes getroffen wurden, noch für Folgeschäden, besondere oder ähnliche Schäden, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Kontaktieren Sie uns

Wenn Sie Fragen zu diesem Haftungsausschluss haben, können Sie uns per E-Mail kontaktieren: support@vitextra.com.

Inhaltsverzeichnis

Übersicht 4

Password Vault in Kürze 4

Vergleich auf einen Blick 5

Wann Password Vault gut passt 6

Wann ein Browser-Kennwortmanager gut passt 6

Wann ein Enterprise-Kennwortmanager gut passt 7

Die Werkzeuge nebeneinander verwenden 7

Fragen vor der Entscheidung 8

Übersicht

Organisationen, die möchten, dass Mitarbeiter keine Kennwörter mehr in Tabellen und Notizen aufbewahren, betrachten in der Regel drei Arten von Werkzeugen:

- **Browser-Kennwortmanager** – die in Webbrowser integrierte Kennwortspeicherung, die Anmeldedaten speichert, wenn sich der Benutzer bei Websites anmeldet.
- **Enterprise-Kennwortmanager** – spezialisierte Produkte, meist mit eigenem Dienst, Client-Apps und Browsererweiterungen, die für die organisationsweite Verwaltung von Anmeldedaten konzipiert sind.
- **Password Vault** – ein SharePoint-Framework-Webpart von Vitextra, das jedem Mitarbeiter einen schlanken persönlichen Tresor in Microsoft 365 (SharePoint Online und Microsoft Teams) bietet.

Diese Werkzeuge lösen unterschiedliche Probleme. Dieser Artikel beschreibt die allgemeinen Merkmale jeder Kategorie, damit Sie entscheiden können, welche zu einem bestimmten Bedarf passt. Einzelne Produkte innerhalb einer Kategorie unterscheiden sich; prüfen Sie daher die Besonderheiten jedes in Frage kommenden Produkts anhand Ihrer eigenen Anforderungen.

Password Vault in Kürze

Password Vault speichert die Einträge jedes Benutzers verschlüsselt in einer Datei im eigenen OneDrive dieses Benutzers und zeigt sie in einem Webpart auf einer SharePoint-Seite oder in Teams an. Der Zugriff innerhalb des Webparts ist durch eine 4-stellige PIN geschützt, aus der der Verschlüsselungsschlüssel abgeleitet wird; solange der Tresor gesperrt ist, werden keine Einträge angezeigt, und nach 5 Minuten ohne Interaktion wird er automatisch gesperrt. Da eine PIN nur 4 Ziffern hat, bleibt die Zugriffssteuerung für OneDrive die erste Schutzebene für die Datei. Enthalten sind ein Kennwortgenerator, eine Stärkeanzeige, Ordner, Tags, Favoriten und eine Suche. Details finden Sie in KB10437. Password Vault. Lösungsübersicht.

Ebenso wichtig ist, was es **nicht** tut:

- kein automatisches Ausfüllen von Anmeldeformularen und keine Browsererweiterung – Anmeldedaten werden mit **In Zwischenablage kopieren** kopiert;
- kein Teilen von Einträgen und keine Teamtresore;
- keine Verwaltungskonsole und keine Wiederherstellung einer vergessenen PIN – nach 5 falschen PINs bleibt nur das Zurücksetzen des Tresors, wodurch alle Einträge gelöscht werden;
- kein Export und kein Import.

Vergleich auf einen Blick

Die Spalte Password Vault beschreibt das Produkt; die beiden anderen Spalten beschreiben, was für die Kategorie typisch ist.

Aspekt	**Password Vault**	**Browser-Kennwortmanager (typisch)**	**Enterprise-Kennwortmanager (typisch)**
Zweck	Persönliche Anmeldedaten eines Mitarbeiters, innerhalb von Microsoft 365	Persönlicher Komfort beim Surfen	Organisationsweite Verwaltung von Anmeldedaten
Wo die Daten liegen	Verschlüsselte Datei im eigenen OneDrive des Benutzers	Im Browserprofil, oft über das Konto des Browserherstellers synchronisiert	Im eigenen Dienst des Produkts oder in einer von der Organisation betriebenen Infrastruktur
Zugriff	SharePoint-Seite oder Microsoft Teams, mit dem Geschäftskonto und einer 4-stelligen PIN	Der Browser, in dem das Profil angemeldet ist	Client-Apps, Browsererweiterungen und Webzugriff des Produkts
Automatisches Ausfüllen von Anmeldeformularen	Nein	Ja	Meist ja
Teilen mit Kollegen	Nein	Im beruflichen Kontext eingeschränkt oder nicht vorhanden	Meist ja, mit gemeinsamen Ordnern oder Tresoren
Verwaltung, Richtlinien, Überwachung	Nein; nur Bereitstellung und die Graph-	Abhängig von den Verwaltungsoptionen des Browsers	Meist umfangreich

Aspekt	**Password Vault**	**Browser-Kennwortmanager (typisch)**	**Enterprise-Kennwortmanager (typisch)**
	Berechtigung		
Wiederherstellung bei Zugriffsverlust	Keine; Zurücksetzen löscht den Tresor	Abhängig vom Browserkonto	Bietet meist Wiederherstellungsoptionen für Administratoren oder Benutzer
Bereitstellung	Ein SPFx-Paket und eine Graph-Berechtigung; keine zusätzliche Client-Software	Bereits im Browser vorhanden	Ein separates Produkt, das ausgerollt, konfiguriert und pro Benutzer lizenziert werden muss
Typisches Kostenmodell	Lizenz pro Mandant	Im Browser enthalten	Meist Abonnement pro Benutzer

Wann Password Vault gut passt

- Mitarbeiter brauchen einen Ort für **ihre eigenen** beruflichen Anmeldedaten – Lieferantenportale, Partner-Extranets, Testsysteme, Gerätekonsolen –, und die Organisation möchte, dass dieser Ort innerhalb von Microsoft 365 liegt statt in persönlichen Werkzeugen oder Dateien.
- Die Organisation bevorzugt, dass die Daten **im eigenen Mandanten** (im OneDrive jedes Benutzers) bleiben und nicht bei einem zusätzlichen Drittanbieterdienst.
- Ein einfaches Werkzeug, das auf einer SharePoint-Seite und in Teams ohne Installation von Erweiterungen oder Client-Software funktioniert, ist wichtiger als automatisches Ausfüllen.
- Die Anmeldedaten werden nicht geteilt, und ihr Verlust bei einer vergessenen PIN ist akzeptabel, weil sie im Quellsystem wiederhergestellt werden können (zum Beispiel über die „Kennwort vergessen“-Funktion des jeweiligen Dienstes).

Wann ein Browser-Kennwortmanager gut passt

- Der Hauptbedarf ist Komfort: Kennwörter für Websites beim Surfen speichern und

automatisch ausfüllen.
- Benutzer arbeiten hauptsächlich in einem Browser, und die Richtlinie der Organisation erlaubt es, berufliche Anmeldedaten darin zu speichern.

Bedenken Sie, dass ein Browser-Kennwortmanager Anmeldedaten im Browserprofil speichert. Was verfügbar ist, hängt daher vom Browser und dem Konto ab, mit dem der Benutzer angemeldet ist, sowie davon, wie die Organisation Browser verwaltet.

Wann ein Enterprise-Kennwortmanager gut passt

- Anmeldedaten müssen in Teams **geteilt** werden, zum Beispiel Dienstkonten oder freigegebene Postfächer.
- Die Organisation benötigt zentrale **Richtlinien, Überwachungsprotokolle, Zugriffsüberprüfungen und Wiederherstellungsverfahren**.
- **Hochprivilegierte** Administratorkonten müssen verwaltet werden – oft in Kombination mit Privileged Access Management.
- Automatisches Ausfüllen über Browser, Desktop- und mobile Apps hinweg ist erforderlich.

Diese Funktionen bedeuten ein separates Produkt, das bereitgestellt, konfiguriert, geschult und lizenziert werden muss – meist pro Benutzer.

Warnung

Password Vault ist für persönliche Anmeldedaten gedacht. Es ist kein Ersatz für eine Lösung, die gemeinsam genutzte oder hochprivilegierte Konten verwaltet. Befolgen Sie für solche Konten die Sicherheitsrichtlinie Ihrer Organisation.

Die Werkzeuge nebeneinander verwenden

Die Kategorien schließen sich nicht gegenseitig aus. Eine Organisation kann einen Enterprise-Kennwortmanager für die IT und gemeinsam genutzte Konten betreiben und Password Vault allen Mitarbeitern als einfachen persönlichen Ort für die übrigen beruflichen Anmeldedaten anbieten – oder die Speicherung im Browser für Websites mit geringem Risiko erlauben. Entscheidend ist eine klare Richtlinie, die festlegt, welche Art von Anmeldedaten wohin gehört.

Hinweis

Password Vault hat weder Import noch Export; Einträge in den Tresor zu übernehmen oder aus ihm herauszuholen bedeutet daher, sie einzeln hinzuzufügen. Treffen Sie die Wahl, bevor Mitarbeiter beginnen, ihre Tresore zu füllen.

Fragen vor der Entscheidung

1 Müssen Anmeldedaten geteilt werden, oder sind sie streng persönlich?
2 Ist das automatische Ausfüllen von Anmeldeformularen erforderlich?
3 Wo dürfen die verschlüsselten Daten gespeichert werden – in Ihrem Microsoft 365-Mandanten, im Konto eines Browserherstellers oder in einem Drittanbieterdienst?
4 Benötigen Sie administrative Wiederherstellung, Richtlinien und Überwachung?
5 Was können Sie bereitstellen: ein SPFx-Webpart oder Client-Software und Erweiterungen auf jedem Gerät?
6 Was passiert mit den Anmeldedaten, wenn ein Benutzer den Zugriff verliert – können sie im Quellsystem wiederhergestellt werden?

Tipp

Wie Password Vault Daten schützt und wer darauf zugreifen kann, lesen Sie in KB10452. Wie Password Vault Ihre Daten schützt: Verschlüsselung, PIN und Speicherung und KB10456. Wer Ihre Kennwörter in Password Vault sehen kann. Zum Ausprobieren siehe KB10438. So fügen Sie das Password Vault-Webpart einer Seite hinzu und erstellen Ihren Tresor.