

Suggestion des solutions de gestion de mots de passe

Date de publication 04-2024

TABLE DES MATIÈRES

À qui s'adresse ce document?	1
Aperçu	1
Enjeux.....	1
Hébergement local ou infonuagique.....	1
Solutions de type infonuagique	2
Avantages	2
Inconvénients	2
Solutions sur site « locale »	2
Avantages	2
Inconvénients	3
Sécurité d'une solution locale ou infonuagique	3
Solution infonuagique	4
Solution locale	4
Références	4
Méthodologie d'analyse / critères de sélection	5
Objectif	5
Fonctionnalités des solutions les plus connues.....	5
Consultation de plusieurs analyses.....	5
Vulnérabilités connues et corrigées	6
Facilité d'utilisation et d'administration	6
Disponibilité de la solution en français	6
Emplacement des données	7
Suggestion infonuagique n° 1 : Dashlane.....	7
Références	8
Suggestion infonuagique n° 2 : 1Password	9
Suggestion infonuagique n° 3 : Zoho Vault	11

TLP : VERT (DIFFUSION PERMISE)

Avantages	12
Inconvénients	13
Références	13
Suggestion locale n°1 : Bitwarden.....	13
Suggestion locale n° 2 : KeePassXC	15
Avantages	16
Inconvénients	16
Références	17
Suggestion locale n° 3 : Keeper Enterprise	17
Avantages	17
Inconvénients	18
Références	19
Récapitulatif	20
Références	21
Historique de vulnérabilités	21
Justifications du retrait de solutions	24
LastPass.....	24
NordPass.....	24
ManageEngine PasswordManager Pro.....	24
Révisions	25

À QUI S'ADRESSE CE DOCUMENT ?

Ce document s'adresse à tous les établissements d'enseignement qui envisagent de sécuriser les identifiants utilisés par ses utilisateurs (équipe informatique, personnel administratif ou enseignant) par le biais d'une solution de gestionnaire de mot de passe. L'information qui suit peut aussi être utile pour tout établissement qui n'envisageait pas l'utilisation d'un gestionnaire de mot de passe, mais qui pourrait y voir des avantages afin de sécuriser ses actifs et d'améliorer les bonnes habitudes de ses utilisateurs.

APERÇU

Ce guide présente quelques solutions de gestion des mots de passe qui ont été soumises par la communauté et choisies par l'équipe du Centre d'expertises en sécurité de l'information (CESI). Cependant, il est important de noter que même si la solution qui est actuellement utilisée dans votre environnement n'y figure pas qu'il n'est pas sous-entendu que cette dernière n'est pas adéquate ou sécuritaire.

Plusieurs solutions sur le marché offrent des fonctionnalités étendues et complètes en matière de gestion des accès utilisateurs et de voutes personnelles et partagées. Les solutions proposées par le CESI sont limitées afin de mieux aiguiller les organisations n'ayant pas encore de gestionnaire des mots de passe en place, mais elles auraient pu être plus nombreuses si nous avons inclus toutes les solutions qui remplissaient les critères qui en font un « bon » gestionnaire de mots de passe.

ENJEUX

Sans politique relative aux mots de passe, et sans solution corporative fournie en lien avec la gestion des accès, les utilisateurs se retournent souvent vers des stratégies de conservation de mots de passe comportant des risques pour l'organisation. Souvent, celles-ci ne répondent pas aux critères de sécurité requis afin d'assurer la confidentialité des accès. La fuite involontaire ou inconnue de ces accès pourrait rendre l'organisation à risque de plusieurs types d'attaques, causant la perte d'information, de temps, de réputation et de ressources financières.

HÉBERGEMENT LOCAL OU INFONUAGIQUE

Il existe plusieurs gestionnaires de mot de passe hébergés sur des infrastructures infonuagiques, et d'autres qui sont hébergés localement. Les deux présentent des avantages

TLP : VERT (DIFFUSION PERMISE)

et inconvénients pouvant influencer le choix de solution à mettre en place dans votre organisation. Il est donc important de prendre connaissance de ces différentes particularités afin de choisir la solution la plus appropriée pour votre établissement.

SOLUTIONS DE TYPE INFONUAGIQUE

AVANTAGES

- Le maintien et la sécurité de l'infrastructure sont la responsabilité du fournisseur;
- La disponibilité accrue du service;
- Les données ne sont pas sur place, ce qui restreint l'accès aux données lors d'une intrusion au réseau local de l'organisation;
- Aucune infrastructure interne supplémentaire n'est requise;
- Des fonctionnalités sont souvent disponibles ou intégrées pour la surveillance et la gestion de la sécurité;
- Les coûts sont prévisibles considérant qu'il s'agit d'une location de service;
- Le déploiement est généralement rapide;
- Le fournisseur assure la sauvegarde des données conformément au contrat de service;
- La majorité des solutions offrent un chiffrement double;
- Une solution mieux adaptée à la mobilité des usagers.

INCONVÉNIENTS

- Le contrôle de la solution infonuagique peut être limité selon le fournisseur;
- Les services sont inaccessibles si la connexion Internet est perdue;
- L'établissement d'une relation de confiance avec une organisation tiers est nécessaire;
- Une erreur de manipulation du fournisseur de service peut compromettre la sécurité de l'information;
- La visibilité publique attirant les acteurs malicieux à tester le périmètre pour des vulnérabilités;
- Le coût de maintien et d'utilisation peut devenir élevé à long terme, tout dépendant de la durée de vie de la solution.

SOLUTIONS SUR SITE « LOCALE »

AVANTAGES

- Une plus grande flexibilité de personnalisations et configuration;
- L'organisation conserve un contrôle et une visibilité sur le contenu;
- La possibilité d'ajouter plusieurs API d'automatisation afin d'aider avec la gestion de la sécurité et des événements de sécurité dans l'infrastructure et le réseau interne;

TLP : VERT (DIFFUSION PERMISE)

- La disponibilité de la solution n'est pas dépendante d'un signal Internet.

INCONVÉNIENTS

- La responsabilité du maintien et de la sécurité est entièrement dans les mains de l'équipe TI;
- Toutes les mesures de sécurité internes doivent être mises en place pour protéger contre des attaques du type « menace interne »;
- La vulnérabilité aux attaques de rançongiciel;
- Un niveau élevé d'expertise et d'effort est demandé afin d'arriver à une sécurité élevée;
- Une erreur de manipulation peut compromettre la sécurité de l'information;
- Le coût d'acquisition direct et indirect peut être élevé;
- Le temps d'implantation est plus long;
- Les copies de sauvegarde sous la responsabilité de l'organisation.

SÉCURITÉ D'UNE SOLUTION LOCALE OU INFONUAGIQUE

En considérant les efforts nécessaires, les ressources requises et les contrôles de protection à mettre en place pour assurer la disponibilité, l'intégrité et la confidentialité d'une solution de gestion de mots de passe hébergée localement, le choix d'une solution infonuagique peut s'avérer plus adapté pour des organisations avec des moyens plus limités.

Bien qu'aucune solution ne puisse garantir une sécurité pleine et entière, la majorité des incidents récents affectant des solutions infonuagiques matures concerne généralement de mauvaises configurations ou utilisation sans atteinte aux données de la voute. Il est impératif de configurer des accès conditionnels et une authentification rehaussée sur ces plateformes.

Pour ce qui est des solutions hébergées dans une infrastructure locale, la sécurité repose sur la capacité et les connaissances de l'équipe responsable qui doit en assurer le maintien et l'évolutivité.

En résumé, il n'y a pas de différences significatives conceptuelles au niveau de la sécurité d'une solution locale maintenue à jour et la sécurité d'une solution infonuagique. Le choix entre une solution infonuagique ou une solution locale dépendra d'une multitude de facteurs qui seront propres à votre organisation :

- L'équipe dédiée à la sécurité;
- L'infrastructure locale avec capacité d'héberger la solution choisie;
- Le budget;

TLP : VERT (DIFFUSION PERMISE)

- Le délai de la mise en service de la solution;
- La charge de travail de l'équipe en sécurité;
- La criticité des mots de passe sauvegardés;
- Les obligations et contraintes gouvernementales.

Dans la situation où les mots de passe sauvegardés sont d'une importance critique au fonctionnement de l'organisation, il faut prendre des précautions afin de s'assurer que, dans l'éventualité d'une défaillance du système ou d'une cyberattaque, les mots de passe qui sont requis pour faire la récupération des systèmes sont accessibles. Il est possible de s'assurer que les mots de passe sont accessibles de plusieurs façons :

SOLUTION INFONUAGIQUE

La solution infonuagique assure que les mots de passe soient accessibles en tout temps, peu importe l'état de l'infrastructure et des systèmes locaux.

SOLUTION LOCALE

Nous pouvons réduire le risque de perte de disponibilité en nous assurant d'avoir une réplique prête à prendre la relève dans un autre centre de données. Certaines solutions supportent la haute disponibilité, assurant une continuité du service en cas de panne.

RÉFÉRENCES

<https://www.dnsstuff.com/cloud-vs-on-premise-security>

<https://www.techradar.com/news/cloud-vs-a-new-on-premises>

<https://securityescape.com/cloud-vs-on-premise-security/>

<https://www.xperience-group.com/cloud-vs-on-premise-software/>

https://www.itcentralstation.com/products/comparisons/cyberark-enterprise-password-vault_vs_hashicorp-vault

<https://docs.microsoft.com/en-us/azure/key-vault/>

<https://www.passwordmanager.com/best-enterprise-password-managers/>

<https://www.androidauthority.com/dashlane-vs-lastpass-1110550/>

<https://www.safetydetectives.com/best-password-managers/lastpass/>

TLP : VERT (DIFFUSION PERMISE)

<https://www.safetydetectives.com/best-password-managers/dashlane/>

<https://cybernews.com/best-password-managers/nordpass-vs-1password/>

<https://blog.1password.com/1password.com-is-now-available-in-multiple-languages/>

<https://www.manageengine.com/products/passwordmanagerpro/supported-languages.html>

MÉTHODOLOGIE D'ANALYSE / CRITÈRES DE SÉLECTION

Plusieurs facteurs ont été considérés afin de parvenir à suggérer des solutions de gestion de mot de passe. En prenant chacun de ces points en considération, deux solutions de type infonuagiques ont été retenues ainsi que deux solutions hébergées localement.

OBJECTIF

Le facteur le plus important pour chacune des solutions suggérées est celui de s'assurer qu'elle répond au besoin initial : sécuriser les mots de passe corporatifs des utilisateurs. Chacune des solutions analysées répondait à ce critère, mais seulement certaines d'entre elles permettaient aux utilisateurs d'avoir une voute qui sécurise leurs accès personnels. Les voutes personnelles permettent aux utilisateurs de garder de bonnes habitudes de conservation de mots de passe en dehors de l'organisation, réduisant ainsi les risques apportés par le recyclage de leurs mots de passe.

FONCTIONNALITÉS DES SOLUTIONS LES PLUS CONNUES

L'étendue des fonctionnalités additionnelles est assez grande lorsqu'on compare les différentes solutions. Celles-ci sont bénéfiques pour aider la gestion des utilisateurs, renforcer des politiques de sécurité, permettre l'intégration avec des fournisseurs d'identité corporative, la génération de rapports d'accès aux voutes partagées, et plusieurs autres. Ces outils s'ajoutent aux fonctionnalités de base des solutions de gestion de mots de passe, permettant un environnement plus sécuritaire pour les utilisateurs et l'organisation. C'est pourquoi il est important de les mentionner, et qu'il est intéressant d'en tenir compte.

CONSULTATION DE PLUSIEURS ANALYSES

Les gestionnaires de mots de passe sont le sujet d'analyses comparatives fréquentes. La présente analyse prend en considération l'évolution de plusieurs de ces comparatifs, conservant

TLP : VERT (DIFFUSION PERMISE)

les solutions les mieux réputées et recommandées. Certaines solutions se démarquaient en se retrouvant en haut de liste de façon consistante.

VULNÉRABILITÉS CONNUES ET CORRIGÉES

Chaque solution de gestion de mots de passe a été vulnérable à un moment ou à un autre depuis sa mise en service. Puisqu'aucune solution ne peut garantir un environnement évolutif sans vulnérabilité, l'analyse des différentes solutions à considérer d'autres facteurs plus stratégiques suivant la découverte d'une vulnérabilité : le temps de réponse des développeurs à distribuer et appliquer des correctifs, l'impact qu'ont eu les vulnérabilités, si elles ont été exploitées, et le niveau de communication de la compagnie auprès de ses clients dans l'éventualité d'un risque à leurs voutes protégées.

FACILITÉ D'UTILISATION ET D'ADMINISTRATION

Un aspect important qui permet l'acceptation et l'adoption d'une solution de gestion de mots de passe par les utilisateurs est sa facilité d'utilisation et d'administration. Les solutions proposées font partie de celles qui ont des fonctionnalités simples à mettre en place et simples à utiliser, avec une interface conviviale et des outils qui rendent les voutes partagées, corporatives et personnelles disponibles sur la majorité des appareils des utilisateurs.

DISPONIBILITÉ DE LA SOLUTION EN FRANÇAIS

Il était primordial dans les solutions choisies pour ce guide que les utilisateurs aient l'option de configurer la langue d'affichage du produit en français. Quoique certaines solutions n'offrent peut-être pas l'option permettant de configurer la langue initiale pour tous les utilisateurs de l'entreprise, ces derniers ont tout de même le choix de choisir le français comme langue d'affichage dans leurs options personnelles.

TLP : VERT (DIFFUSION PERMISE)

EMPLACEMENT DES DONNÉES

En concordance avec la nouvelle Loi 25 mise en place le 22 septembre 2022, les entreprises qui hébergent de l'information personnelle et sensible doivent le faire sur des centres de données où la juridiction offre la même protection et les mêmes contrôles qu'au Québec. C'est pourquoi même si parfois des solutions peuvent offrir des fonctionnalités étendues et intéressantes qu'elles ne figurent pas dans la liste des solutions choisies.

SUGGESTION INFONUAGIQUE N° 1 : DASHLANE



Il s'agit d'un joueur important dans le secteur de gestion de mots de passe depuis 2009. Sur plusieurs comparatifs de solutions de gestion de mots de passe, Dashlane se retrouve souvent en première place. Il est convivial à utiliser avec des fonctionnalités variées qui offre aux utilisateurs et aux administrateurs un environnement idéal pour conserver leurs accès en toute sécurité.

Dashlane assure la sécurité de plusieurs façons :

- Chiffrement AES 256 bits;
- Authentification à double facteur (avec options variées);
- Surveillance du « [Dark Web](#) » pour les accès ajoutés à la voute;
- Architecture « [zéro connaissance](#) » qui assure que même Dashlane ne peut pas consulter vos mots de passe;
- VPN « zéro log » qui sécurise vos comptes lorsque vous êtes sur un wifi public;
- Audits sur la sécurité de mots de passe.

Dashlane offre une grande quantité de fonctionnalités supplémentaires :

- Générateur de mots de passe;
- Plugiciels pour navigateurs;
- Dossiers d'équipe pour le partage d'accès;
- Connexions avec comptes fédérés;
- Rapports des accès aux ressources;
- Voutes personnelles et corporatives séparées;

TLP : VERT (DIFFUSION PERMISE)

- Option de récupération de comptes avec application mobile avec authentification biométrique;
- MSI pour déploiement facile par GPO/SCCM;
- Historique de mots de passe générés.

FONCTIONNALITÉS	TEAM	BUSINESS
Architecture zéro-connaissance	✓	✓
Remplissage automatique de formulaires et paiement	✓	✓
Partage sécurisé individuel et de groupe	✓	✓
Alertes de mots de passe compromis	✓	✓
Résultat sur la santé des mots de passe	✓	✓
Surveillance du « Dark Web »	✓	✓
Espaces personnels et corporatifs	✓	✓
Recouvrement zéro-connaissance de comptes	✓	✓
Authentification Biométrique ou avec une YubiKey	✓	✓
Authentification double facteur (2 FA)	✓	✓
VPN	✓	✓
Tableau de bord de sécurité	✓	✓
Réglages de politiques renforcées	✓	✓
Provisionnement SAML	✓	✓
Intégration avec « Active Directory »	✓	✓
« Single Sign-On (SSO) »	X	✓
Plan familial gratuit pour tous les membres de l'équipe¹	X	✓

RÉFÉRENCES

Anglais - <https://cybernews.com/best-password-managers/dashlane-review/>

¹ Le plan familial de Dashlane permet aux membres de l'équipe ayant un plan « Business » d'inviter jusqu'à cinq membres de la famille ou amis sans frais. Chaque compte du plan famille est indépendant et permet aux invités de gérer leur vie privée sur le Web avec simplicité et paix d'esprit.

SUGGESTION INFONUAGIQUE N^o 2 : 1PASSWORD

Mis en marché en 2006 par AgileBits, une entreprise ontarienne, 1Password a fait sa place grâce à son architecture de sécurité renforcée, ses fonctionnalités de gestion de mots de passe étendues et un historique impeccable sans compromission de voutes.

Favorisant l'hébergement des voutes sur Amazon Web services (AWS), 1Password offre à ses clients optant pour un forfait corporatif de choisir la région AWS² où leur contenu sera hébergé, assurant ainsi aux clients canadiens que leur contenu se trouvera au Canada. Si un compte corporatif désire changer de région, 1Password offre une stratégie afin de migrer vers une autre région.

1Password assure la sécurité de plusieurs façons :

- Chiffrement AES 256 bits;
- Authentification à double facteur (avec options variées);
- Surveillance du « Dark Web » avec l'outil Watchtower;
- Rapport de sécurité des mots de passe (complexité, réutilisation, etc.);
- Authentification double facteur (2FA);
- Conformité de sécurité : GDPR, SOC2.

Contrairement à plusieurs solutions, 1Password offre une application native pour les systèmes d'exploitation Windows, Linux et Mac. En plus des plugiciels compatibles avec la majorité des navigateurs, l'application native permet l'utilisation d'une voute en mode hors-ligne.

1Password permet aux utilisateurs d'identifier certains sites comme étant « sécuritaires pour voyager ». Lorsqu'un utilisateur active le mode « voyage », tous les sites qui ne sont pas identifiés « sécuritaires pour voyager » sont retirés de l'appareil, assurant une sécurité supplémentaire dans l'éventualité que l'appareil soit perdu ou volé.

Pour les organisations, 1Password offre trois plans différents : le plan Teams, Business ou Entreprise. Le plan Entreprise est identique au plan Business, à la différence que l'organisation

² <https://support.1password.com/regions/>

TLP : VERT (DIFFUSION PERMISE)

aura un gestionnaire de compte dédié, une formation de l'installation sur mesure, et accès à un ingénieur pour la mise en service.

FONCTIONNALITÉS	TEAMS	BUSINESS
Nombre d'utilisateurs	10	Illimité
Applications pour Mac, Windows, Linux, iOS, Android et Web	✓	✓
Voutes partagées illimitées	✓	✓
Stockage de secrets illimité	✓	✓
Coffre-fort chiffré pour chaque utilisateur	✓	✓
Stockage de document, par utilisateur	1GB	5GB
Administration des autorisations	✓	✓
Authentification double facteur (2FA)	✓	✓
Assistance par courriel 24h/7j	✓	✓
Comptes invités pour un partage limité	5	20
Groupes personnalisés pour organiser les équipes	X	✓
Provisionnement avec Active Directory, Google Workspace, OneLogin, Rippling et JumpCloud	X	✓
Rôles personnalisés pour concevoir et déléguer les responsabilités	X	✓
Contrôles de sécurité personnalisés avec la protection avancée	X	✓
Contrôle d'accès affiné pour chaque voute	X	✓
Journal d'activité pour le suivi des modifications apportées aux voutes	X	✓
Tableau de bord à l'échelle de l'entreprise pour la surveillance de la sécurité	X	✓
Rapports d'activité Watchtower (Surveillance du Dark Web et réutilisation de mots de passe)	X	✓
Compte familial gratuit pour tous les membres de l'équipe	X	✓

Il est aussi important de mentionner que, malgré la documentation en ligne qui n'est pas disponible en français, 1Password offre sa solution dans plusieurs langues variées, dont le français. Les utilisateurs peuvent, lorsqu'ils le désirent, modifier la langue d'affichage en accédant à leurs réglages personnels.

TLP : VERT (DIFFUSION PERMISE)

SUGGESTION INFONUAGIQUE N° 3 : ZOH Vault



Zoho Vault est une application sécurisée de gestion de mots de passe en ligne destinée aux particuliers et aux entreprises, à laquelle on peut accéder à partir de n'importe quel appareil, où que l'on se trouve dans le monde.

Avec Zoho Vault, vous pouvez :

- Sauvegarder un nombre illimité de mots de passe, de documents et d'autres informations sensibles;
- Générer et sauvegarder des mots de passe forts et uniques pour chacun de vos comptes;
- Synchroniser les mots de passe sur un nombre illimité d'appareils;
- Suivre les scores de sécurité de tous vos mots de passe;
- Ajouter l'authentification multifactorielle à votre application;
- Télécharger des applications mobiles natives et des extensions pour les navigateurs les plus courants;
- Remplir automatiquement les mots de passe sur différents sites Web et applications.

Des fonctionnalités sur mesure pour les entreprises.

Zoho Vault offre également des fonctions de gestion fine des mots de passe pour protéger les informations d'identification sensibles des entreprises. Les équipes et les entreprises peuvent utiliser Vault pour :

- Ajouter des utilisateurs et les organiser en groupes en fonction de leurs équipes;
- Partager en toute sécurité des mots de passe et des dossiers avec des individus, des groupes et des collaborateurs tiers (p. ex., pigistes, travailleurs temporaires);
- Contrôler les scores de sécurité des mots de passe de chaque employé de l'organisation;
- Utiliser des contrôles administratifs puissants pour personnaliser et restreindre l'accès des utilisateurs;

TLP : VERT (DIFFUSION PERMISE)

- Obtenir des journaux d'audit en temps réel sur chaque action effectuée par les utilisateurs;
- Consulter des rapports détaillés sur les actions des utilisateurs et la gestion des mots de passe;
- Activer l'authentification sans mot de passe pour les applications dans le nuage avec l'authentification unique (SSO);
- Étendre l'accès d'urgence aux mots de passe professionnels à un petit nombre d'employés de confiance;
- Configurer des alertes de sécurité personnalisées pour les administrateurs et les superadministrateurs.

Zoho Vault est-il sûr?

- Zoho Vault utilise un mécanisme d'hébergement à l'épreuve des hôtes, une technique sûre et éprouvée pour héberger des données sensibles sous forme cryptée et s'assurer que seuls les clients peuvent accéder à leurs données et les gérer à l'aide de leur mot de passe principal unique.
- Toutes les données de l'utilisateur sont chiffrées et déchiffrées (AES-256) dans le navigateur à l'aide de ce mot de passe principal, et seules les données chiffrées sont stockées dans les serveurs de Zoho.
- Le mot de passe principal de l'utilisateur n'est jamais stocké par Vault, ce qui empêche même les employés de Zoho d'accéder à vos données. Toutes les connexions aux serveurs utilisent le cryptage TLS (TLS 1.2/1.3) avec des algorithmes de chiffrement puissants.
- Zoho est également conforme aux normes SOC II, GDPR et HIPAA, ce qui en fait un excellent choix pour les entreprises.

AVANTAGES

- Chiffrement AES-256, authentification à deux facteurs (2FA), surveillance des accès, et options de sécurité avancées pour les entreprises.
- Stockage de mots de passe, gestion des identités et des accès (GIA), partage sécurisé de fichiers, et surveillance du « Dark Web » (disponible dans les plans payants).
- Fonctionne avec divers navigateurs Web, appareils mobiles et applications Zoho.
- Version gratuite disponible avec des fonctionnalités limitées, et versions payantes pour répondre aux besoins des utilisateurs individuels et des équipes.

TLP : VERT (DIFFUSION PERMISE)

- Interface utilisateur simple et facile à utiliser pour une gestion efficace des mots de passe.

INCONVÉNIENTS

- Absence de surveillance du « Dark Web » dans la version gratuite : Fonctionnalité importante pour la sécurité des comptes, qui est uniquement accessible dans les plans payants.
- Assistance en ligne et par courriel disponible, mais pas de clavardage en direct ni de support téléphonique.
- Comparé à certains concurrents, Zoho Vault ne propose pas encore de fonctionnalités avancées comme le partage de mot de passe à usage unique ou la reconnaissance biométrique.
- Des utilisateurs ont rapporté des problèmes de synchronisation entre les appareils, bien que cela semble rare.
- Version gratuite disponible avec des fonctionnalités limitées, et versions payantes pour répondre aux besoins des utilisateurs individuels et des équipes.
- Interface utilisateur simple et facile à utiliser pour une gestion efficace des mots de passe.

RÉFÉRENCES

<https://www.zoho.com/fr/vault/>

<https://cybernews.com/best-password-managers/zoho-vault-review/>

SUGGESTION LOCALE N°1 : BITWARDEN



Bitwarden est une solution « open source » accréditée sous la norme GNU GLPv3 et GNU AGPLv3. Offrant une version limitée complètement gratuite, Bitwarden est une des solutions de gestion de mots de passe les mieux réputées pour de l'hébergement sur site.

TLP : VERT (DIFFUSION PERMISE)

Bitwarden n'a peut-être pas des fonctionnalités aussi étendues et nombreuses que les concurrents infonuagiques, mais elle en contient tout de même une quantité intéressante qui sert à renforcer la sécurité du contenu qui y sera enregistré et qui en fait une solution de voute de mots de passe excellente :

- Cryptage zéro connaissance (tout le contenu est crypté avant d'être enregistré);
- Transparence du code source;
- Politiques d'entreprise sur les requis de complexité de mots de passe;
- Conformité de sécurité : Privacy shield, HIPAA, GDPR, CCPA, SOC2, SOC3;
- Encryption AES 256 bits;
- Générateur de mots de passe sécurisé;
- Authentification double facteur avec options avancées;
- Exportation sécurisée de la voute personnelle.

L'organisation peut se procurer une licence **Entreprise** afin d'accéder aux fonctionnalités avancées de Bitwarden. Celles-ci s'ajoutent aux fonctionnalités de base de Bitwarden et des fonctionnalités du plan Teams.

FONCTIONNALITÉS POUR ENTREPRISE	TEAMS	ENTERPRISE
Toutes les fonctionnalités de base de Bitwarden	✓	✓
Utilisateurs illimités	✓	✓
Partage illimité par collection	✓	✓
Accès par API	✓	✓
Synchronisation de répertoire d'utilisateurs	✓	✓
Rapports d'audit et d'événements	✓	✓
Groupes d'utilisateurs	✓	✓
Authentification double facteur avancé	✓	✓
Rapports sur la santé de la voute	✓	✓
Support prioritaire	✓	✓
Politiques d'entreprise	X	✓
Authentification SSO	X	✓
Réinitialisation du mot de passe maître	X	✓
Rôles de gestion personnalisés	X	✓
Option d'hébergement sur place	X	✓

Bitwarden offre maintenant deux options gratuites infonuagiques pour sécuriser les mots de passe personnels. Bien que l'hébergement local de Bitwarden offre une voute privée en même temps qu'une voute partagée aux membres inscrits, il n'est pas impossible que ces derniers

TLP : VERT (DIFFUSION PERMISE)

hésitent à conserver leurs accès personnels dans une solution hébergée et contrôlée par l'établissement. Que ce soit par crainte de perte d'accès en cas de changement à leur carrière, ou la crainte qu'une des ressources qui gèrent la solution puisse consulter leur voute personnelle sans leur consentement, le risque d'avoir des mots de passe personnels qui ne sont pas entreposés dans une voute sécurisée pose un danger réel et mesurable pour l'organisation. Le tout est simplement dû aux habitudes connues des utilisateurs à faire du recyclage de mots de passe entre leurs accès personnels et leurs accès corporatifs. Si leurs accès personnels sont à risque, il est probable que certains de leurs accès corporatifs le soient aussi.

La première option gratuite offerte par Bitwarden se nomme **Compte de base gratuit**. Celle-ci offre toutes les fonctionnalités de base de Bitwarden, permettant la gestion de la voute personnelle de n'importe quel endroit, appareil et type d'appareil. <https://vault.bitwarden.com/#/register>

La deuxième option gratuite se nomme **Organisation de 2 personnes gratuite**. Celle-ci offre toutes les fonctionnalités de base de Bitwarden, permettant la gestion de la voute personnelle de n'importe quel endroit, appareil et type d'appareil, en plus de permettre le partage de mots de passe entre deux personnes de l'organisation. <https://vault.bitwarden.com/#/register>

Lecture : <https://bitwarden.com/blog/the-importance-of-the-personal-vault-for-business-users/>

SUGGESTION LOCALE N° 2 : KEEPASSXC



KeePassXC est un gestionnaire de mots de passe « open source » et gratuit pour Windows, macOS et Linux. Il est généralement considéré comme une solution sécurisée pour stocker vos mots de passe.

KeePassXC s'adresse aux personnes et aux entreprises ayant des exigences extrêmement élevées en matière de gestion sécurisée des données personnelles.

AVANTAGES

- Disponible sur plusieurs plateformes (Cross-platform) telles que Windows, macOS et Linux.
- Plus sécurisé que de nombreux produits basés sur le nuage.

INCONVÉNIENTS

- Interface obsolète.
- Pas de synchronisation de mot de passe intégrée.

Voici les principales fonctionnalités de KeePassXC :

- Stockage de nombreux types d'informations, telles que les noms d'utilisateur, les mots de passe, les URL, les pièces jointes et les notes, dans un fichier crypté hors ligne qui peut être stocké n'importe où, y compris dans les solutions de nuage privé et public.
- Vous pouvez organiser vos mots de passe dans des groupes et des dossiers.
- KeePassXC peut générer des mots de passe forts et uniques pour tous vos comptes.
- Vous pouvez facilement rechercher et filtrer vos mots de passe.
- KeePassXC est un logiciel « open source », ce qui signifie que le code est auditable par tous.
- Interface utilisateur intuitive et facile à utiliser.

KeePassXC propose également un certain nombre d'autres fonctionnalités avancées, telles que :

- Ajouter des extensions pour ajouter des fonctionnalités supplémentaires.
- Synchroniser votre base de données de mots de passe entre plusieurs appareils.
- Importer et exporter vos mots de passe vers et depuis d'autres gestionnaires de mots de passe, dans plusieurs formats de fichiers.

Au terme de Sécurité :

- KeePassXC utilise le cryptage AES-256, l'un des algorithmes de cryptage les plus sécurisés disponibles.
- Vos mots de passe sont stockés dans un fichier de base de données crypté, protégé par un mot de passe principal (Master key).
- KeePassXC prend en charge plusieurs options de sécurité supplémentaires, telles que le hachage de mot de passe PBKDF2 et les clés de fichier.
- Le code de KeePassXC est régulièrement audité par des experts en sécurité.

TLP : VERT (DIFFUSION PERMISE)

En plus des fonctionnalités citées ci-dessus, KeePassXC offre également :

- Plusieurs options de verrouillage pour la base de données, y compris le verrouillage automatique après une période d'inactivité.
- Protection contre les attaques par force brute.

RÉFÉRENCES

<https://keepassxc.org/docs/>

<https://keepassxc.org/#project>

<https://www.techradar.com/reviews/keepassxc>

SUGGESTION LOCALE N° 3 : KEEPER ENTERPRISE



Keeper Enterprise est une solution de gestion de mots de passe complète et sécurisée qui peut répondre aux besoins des entreprises de toutes tailles.

Keeper la version entreprise offre des fonctionnalités avancées pour les entreprises. Il est idéal pour les organisations qui ont besoin d'un contrôle strict sur les mots de passe et les accès, et qui doivent respecter des normes de sécurité et de confidentialité strictes.

Cependant, il est important de noter que le coût de Keeper Enterprise peut être élevé pour les petites entreprises et que la configuration et la gestion peuvent être complexes.

AVANTAGES

- Fonctionnalités avancées de sécurité et de gestion des utilisateurs incluant l'authentification unique (SSO), gestion des groupes et des autorisations, rapports d'activité détaillés, surveillance des accès suspects, etc.
- Contrôle et administration centralisés permettent aux administrateurs de gérer les utilisateurs, les groupes et les mots de passe de manière centralisée.
- Conforme aux normes de sécurité et de confidentialité, notamment RGPD et SOC 2.
- Intégration possible avec d'autres outils, tels que les annuaires d'utilisateurs, les services infonuagiques et les outils de sécurité.

TLP : VERT (DIFFUSION PERMISE)

- Accès à un soutien technique prioritaire et dédié pour les entreprises.

INCONVÉNIENTS

- Les versions Enterprise de Keeper sont généralement plus coûteuses que les versions pour les particuliers.
- La configuration et la gestion de Keeper Enterprise peuvent être complexes pour les entreprises de grande taille.
- Absence de certaines fonctionnalités présentes dans d'autres gestionnaires de mots de passe d'entreprise, comme la prise en charge des clés de sécurité physiques³.

Voici les principales fonctionnalités de Keeper Enterprise :

- Keeper peut stocker vos mots de passe, noms d'utilisateur et autres informations de connexion de manière sécurisée.
- Vous pouvez partager des mots de passe avec d'autres utilisateurs de Keeper Enterprise de manière sécurisée.
- Keeper peut générer des mots de passe forts et uniques pour tous vos comptes.
- Keeper prend en charge plusieurs méthodes de 2 FA pour ajouter une couche de sécurité supplémentaire à votre compte.
- Keeper peut générer des rapports d'audit pour vous aider à suivre l'activité de votre compte.

En plus de ces fonctionnalités, Keeper Enterprise propose également un certain nombre d'autres fonctionnalités avancées, telles que :

- S'intégrer à votre solution SSO (Single Sign-On) pour une expérience utilisateur transparente.
- Permet de contrôler les personnes qui ont accès à vos applications et données.
- Permet de stocker des fichiers sensibles de manière sécurisée.

Au terme de sécurité :

- Keeper utilise le cryptage AES-256, l'un des algorithmes de cryptage les plus sécurisés disponibles.
- Keeper prend en charge plusieurs méthodes de 2 FA, ce qui ajoute une couche de sécurité supplémentaire à votre compte.

³ La prise en charge des clés de sécurité physiques est une fonctionnalité de sécurité supplémentaire offerte par certains gestionnaires de mots de passe. Elle permet d'utiliser une clé de sécurité physique, comme une clé USB ou un YubiKey, pour authentifier votre compte et accéder à vos mots de passe.

TLP : VERT (DIFFUSION PERMISE)







- Keeper utilise des techniques de protection contre les attaques par force brute pour empêcher les pirates informatiques de deviner votre mot de passe principal.
- Keeper a obtenu plusieurs certifications de sécurité, notamment ISO/IEC 27001 et SOC 2.

RÉFÉRENCES

<https://docs.keeper.io/enterprise-guide>

<https://www.keepersecurity.com/remote-enterprise-password-manager.html>

TLP : VERT (DIFFUSION PERMISE)
RÉCAPITULATIF

	 DASHLANE	 1Password	 KeePassXC	 bitwarden	 KEEPER®	 Z O H O
Chiffrement	AES – 256 bits	AES – 256 bits	AES – 256 bits	AES – 256 bits	AES – 256 bits	AES – 256 bits
Zéro connaissance	✓	✓	✓	✓	✓	✓
Disponible en français	✓	✓	✓	✓	✓	✓
MFA / 2FA	✓	✓	✓ (via des plugins et extensions)	✓	✓	✓
Voutes personnelles	✓	✓	✓	✓	✓	✓
Voutes partagées	✓	✓	✓ (Via des plugins et extensions)	✓	✓	✓
Pays d'origine	É.-U. (New York)	Canada (ON)	Open-source	É.-U. (Californie)	É.-U. (Chicago)	É.-U. (Californie)
Récupération de voute	✓	✓	✓ (Possible avec fichier de secours ou clé de récupération)	✓	✓	✓
Surveillance « Dark Web »	✓	✓		✓		
Tableau de bord de sécurité	✓	✓		✓	✓	✓

TLP : VERT (DIFFUSION PERMISE)

RÉFÉRENCES

Français – [Récupération de voute - Dashlane](#)

Français – [Récupération de voute – 1Password](#)

Anglais – [Modifier la langue - Bitwarden](#)

Anglais – [Mot de passe maitre oublié - Bitwarden](#)

Anglais – [Réinitialiation de mot de passe maitre - Bitwarden](#)

Anglais – [Authentification à deux facteurs https://keepassxc.org/docs/](https://keepassxc.org/docs/)

Anglais – [Base de données cryptés AES-256 - https://www.techradar.com/reviews/keepassxc](https://www.techradar.com/reviews/keepassxc)

HISTORIQUE DE VULNÉRABILITÉS

2014

- **LastPass, My1Login, NeedMyPassword, PasswordBox, et RoboForm** : des chercheurs de l'Université de la Californie Berkeley ont découvert [un nombre de vulnérabilités](#) dans plusieurs gestionnaires de mots de passe. Dans quatre des cinq gestionnaires de mots de passe étudiés, un acteur malveillant peut apprendre les accès utilisateurs pour des sites arbitraires.

2015

- **LastPass** : une intrusion dans les serveurs de la compagnie [a été détectée](#). Quoique les informations cryptées des utilisateurs n'aient pas été volées, les cybercriminels ont réussi à voler les adresses courriel de comptes Lastpass, des rappels de mots de passe, le salage serveur par utilisateur et le hachage d'authentification des utilisateurs.

2016

- **LastPass** : une faille critique jour zéro permettant à un acteur malveillant de complètement compromettre un compte a été découverte. Cette faille repose sur une prémisse qu'un cybercriminel parvient à attirer un utilisateur vers un site compromis par le biais d'une

TLP : VERT (DIFFUSION PERMISE)

attaque de type hameçonnage. LastPass a corrigé la faille en moins de 24 heures et a publié un état de situation [sur son blogue](#).

- Plusieurs vulnérabilités ont été rapportées par des pirates éthiques et des experts en sécurité. Parmi les gestionnaires de mots de passe affectés sont **LastPass**, **Dashlane**, **1Password** et **Keeper**. Dans la majorité des cas, un acteur malveillant devait tout de même utiliser de l'hameçonnage afin d'amener les utilisateurs à révéler certaines informations.

2017

- **LastPass** a rapporté une vulnérabilité sérieuse dans ses extensions pour navigateurs et a demandé à ses clients de s'abstenir de les utiliser. La situation a été résolue en moins de 24 heures. **Keeper** et **OneLogin** ont aussi eu des problèmes qui n'ont entraîné aucune fuite de données.

2019

- De sérieuses vulnérabilités ont été trouvées dans le code de **Dashlane**, **LastPass**, **1Password**, et **KeePass**. Ceci s'appliquait aux utilisateurs de Windows 10 et seulement si le bon logiciel malveillant était installé. Une fois de plus, les utilisateurs n'ont souffert d'aucune perte.

2020

- [Des chercheurs de l'Université de York](#) ont découvert que les applications Android de **RoboForm** et **Dashlane** sont susceptibles à des attaques de types « Brute force » sur les NIP des applications. Cette faille permet des tentatives illimitées pour entrer le NIP maître qui permet ultimement de déverrouiller les voutes de mots de passe.
- Ils ont aussi découvert [quatre nouvelles vulnérabilités](#) incluant une faille qui touche les applications Android de **1Password** et **LastPass** qui les rend susceptibles à des attaques d'hameçonnage. La vulnérabilité est causée par leur utilisation de faibles critères d'identification de mots de passe qui devraient être suggérés pour le remplissage automatique.

2021

- Sept traqueurs ont été trouvés dans l'application Android de **LastPass**. LastPass assure les utilisateurs qu'aucune information d'utilisateur ou de voute n'est envoyée par ces traqueurs.

TLP : VERT (DIFFUSION PERMISE)

Dans les réglages de l'application Android, il est possible de désactiver l'option qui active les traqueurs.

- **PasswordState** a signalé qu'[une mise à jour malicieuse](#) a été téléchargée par plus de 29 000 utilisateurs, permettant à des acteurs malicieux d'extraire les voutes et de les envoyer vers un serveur contrôlé par les attaquants. L'entreprise a suggéré aux utilisateurs de commencer une campagne de changement de mots de passe, mais [a laissé les utilisateurs dans l'ombre](#) avec les détails de ce qui a causé l'attaque de la chaîne logistique.
- **Lastpass** a signalé qu'une attaque « bourrage d'identifiants (Credential Stuffing) » a été lancée sur le compte de plusieurs de ses utilisateurs. Lastpass confirme qu'aucune information n'a été compromise, mais suggère tout de même aux utilisateurs ayant reçu des notifications courriel de modifier leur mot de passe maître.

2022

- **Lastpass** a signalé à ses utilisateurs qu'ils ont détectés de l'activité suspecte sur leur environnement de développement. Ils ont trouvé assez rapidement qu'une entité tierce est parvenue à obtenir une partie du code source de l'environnement de développement par le biais d'un compte de développeur compromis. Ils assurent, cependant, qu'aucune voute ni aucun mot de passe maître n'est compromis.
- **Lastpass** a signalé à ses utilisateurs qu'ils ont détectés de l'activité suspecte sur un des services de stockage tiers. À la suite d'une enquête, ils ont déterminé qu'un individu, exploitant de l'information obtenue dans l'incident précédent, a obtenu l'accès à certaines informations des clients de Lastpass.
- **Lastpass** a ajouté qu'un acteur malveillant aurait récupéré une sauvegarde des voutes chiffrées des utilisateurs. Un risque majeur s'impose à tous les utilisateurs ayant choisi un mot de passe maître ne correspondant pas aux critères minimaux de complexité suggérés par Lastpass.

2023

- **ManageEngine** a été impliqué dans une attaque de sécurité en janvier 2023 impliquant des pirates informatiques exploitant des failles dans les produits **ManageEngine** sur site. Selon un avis de sécurité officiel, la vulnérabilité était due à une dépendance tierce obsolète appelée Apache Santuario. Cela a affecté un certain nombre de logiciels ManageEngine, notamment Password Manager Pro.

TLP : VERT (DIFFUSION PERMISE)

- **ManageEngine** peut aujourd'hui être considérée comme une solution de gestion des mots de passe sûre, il est important de prendre en compte le facteur de risque associé à l'incident récent. Ceci est particulièrement crucial compte tenu de la grande quantité de données de mots de passe potentiellement affectées.

JUSTIFICATIONS DU RETRAIT DE SOLUTIONS**LASTPASS**

Le retrait de LastPass a été effectué à la suite d'une publication faite par la compagnie en août 2022 à la suite d'une détection de compromission dans leur environnement de développement. Cette compromission a laissé place à des incidents plus graves encore, permettant à un acteur malveillant d'obtenir une copie de la sauvegarde des voutes des utilisateurs. À la suite d'un incident de ce type, Lastpass a été retiré de nos recommandations, ne pouvant savoir si les acteurs malveillants ont réussi à obtenir de la persistance sur les systèmes ou si un incident mettant les voutes des utilisateurs à risque surviendrait à nouveau. Si votre établissement utilise Lastpass, il est recommandé de changer les mots de passe enregistrés dans les voutes et de modifier le mot de passe maître du compte corporatif propriétaire des voutes. Activer le MFA sur toutes les plateformes ayant des accès enregistrés dans Lastpass, lorsque possible.

NORDPASS

Le retrait de NordPass des solutions proposées a été fait suivant la découverte que la compagnie était localisée au Panama. Considérant que le Panama n'a pas de loi obligatoire sur la rétention de l'information et n'est pas dans l'obligation de conserver des journaux d'activités ni de les partager avec les gouvernements, et considérant que, malgré les fonctionnalités de la solution qui sont excellentes, le produit demeure jeune sur le marché, le CESI a choisi de le retirer de ses suggestions en faveur d'un produit plus mature.

MANAGEENGINE PASSWORDMANAGER PRO

Compte tenu de la gravité de l'attaque de 2023 et du risque associé à la vulnérabilité découverte, liés à une dépendance tierce obsolète appelée Apache Santuario, il est recommandé de retirer ManageEngine PasswordManager Pro de la liste des gestionnaires de mots de passe.

TLP : **VERT** (DIFFUSION PERMISE)

RÉVISIONS

Date	Action	Auteur	Version
2024-03-24	Retrait de ManageEngine PasswordManager Pro Ajouter de KeePassXC, Keeper Enterprise et Zoho Vault aux recommandations	Kamel Chraïti CESI de l'UQ	1.3
2023-01-05	Retrait de NordPass des recommandations Ajout d'un tableau récapitulatif Ajout de 1Password aux recommandations	Jean-François Blais CESI de l'UQ	1.2
2022-10-27	Révision annuelle Retrait de LastPass des recommandations Considération de la solution NordPass	Jean-François Blais CESI de l'UQ	1.1
2022-03-11	Version initiale	Jean-François Blais CESI de l'UQ	1.0

Date de révision : 2024-04-15