UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

SUGGESTION DES SOLUTIONS

Gestion des mots de passe

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIERES

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.

MENTION : AVANT DE POURSUIVRE

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 du tout 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 voûtes 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 avions 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 de la perte d'information, de temps, de réputation et de ressources monétaires.

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 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 APIs d'automatisation afin d'aider avec la gestion de la sécurité et des événements de sécurité dans l'infrastructure et le réseau interne;
- 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 D'UNE SOLUTION 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 d'utilisation sans atteintes aux données de la voûte. 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;
- 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 / 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 soient 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/
- 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 voûte qui sécurise leurs accès personnels. Les voûtes 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 voûtes 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 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 vulnérabilités, l'analyse des différentes solutions a 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 voûtes 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 voûtes 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.

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 NO 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 voûte;
- 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;

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

Dashlane offre aussi un outil qui permet de changer automatiquement les mots de passe de plus de 380 sites différents. Il est possible, sur plusieurs pages pour lesquelles vous auriez enregistré des mots de passe, de faire un changement rapide du mot de passe en un seul clic selon des critères de complexité préétablis. Il y a aussi l'option de laisser Dashlane faire le changement des mots de passe de façon automatique. Donc, si jamais un de vos mots de passe se retrouve entre de mauvaises mains, Dashlane pourra vous avertir grâce à sa surveillance du « Dark Web », et vous suggérer de faire le changement rapidement par le biais de cet outil.

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) »		✓

Plan familial gratuit pour tous les membres de l'équipe[1]	✓

RÉFÉRENCES

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

SUGGESTION INFONUAGIQUE #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 voûtes.

Favorisant l'hébergement des voûtes sur Amazon Web services (AWS), 1Password offre à ses clients optant pour un forfait corporatif de choisir la région AWS [2] 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 voûte en mode hors-ligne.

[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.

[2] https://support.1password.com/regions/

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 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	✓	✓
Voûtes 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	✗	✓
Provisionnement avec Active Directory, Google Workspace, OneLogin, Rippling et JumpCloud	✗	✓
Rôles personnalisés pour concevoir et déléguer les responsabilités	✗	✓
Contrôles de sécurité personnalisés avec la protection avancée	✗	✓
Contrôle d'accès affiné pour chaque voûte	✗	✓
Journal d'activité pour le suivi des modifications apportées aux voûtes	✗	✓
Tableau de bord à l'échelle de l'entreprise pour la surveillance de la sécurité	✗	✓
Rapports d'activité Watchtower (Surveillance du Dark Web et réutilisation de mots de passe)	✗	✓
Compte familial gratuit pour tous les membres de l'équipe	✗	✓

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.

SUGGESTION LOCALE: BITWARDEN

Bitwarden est une solution Open Source licencé 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.

Bitwarden n'a peut-être pas des fonctionnalités aussi étendues et nombreuses que les compétiteurs 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 voûte 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 voûte 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	✓	✓

Fonctionnalités pour Entreprise	Teams	Enterprise
Authentification double facteur avancé	✓	✓
Rapports sur la santé de la voûte	✓	✓
Support prioritaire	✓	✓
Politiques d'entreprise	-	✓
Authentification SSO	-	✓
Réinitialisation du mot de passe maitre	-	✓
Rôles de gestion personnalisés	-	✓
Option d'hébergement sur place	-	✓

Bitwarden offre maintenant deux options gratuites infonuagiques pour sécuriser les mots de passe personnels. Bien que l'hébergement local de Bitwarden offre une voûte privée en même temps qu'une voûte partagée aux membres inscrits, il n'est pas impossible que ces derniers 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 voûte personnelle sans leur consentement, le risque d'avoir des mots de passe personnels qui ne sont pas entreposés dans une voûte sécurisée pose un danger réel et mesurable pour l'organisation, simplement due 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 voûte 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 voûte 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 #2: ManageEngine PasswordManager Pro

ManageEngine
PasswordManager Pro

ManageEngine PasswordManager Pro est une solution complète de contrôle, gestion et d'audits sur le cycle de vie complet de comptes avec privilèges et leurs accès. En un seul produit, il offre quatre solutions : Voûtes de mots de passe, gestion de comptes avec privilèges (P.A.M.), gestion d'accès à distance et gestion de session avec privilèges.

PasswordManager Pro chiffre (AES -256) et consolide tous vos comptes avec privilèges en une voûte centralisée, renforcée par des contrôles d'accès granulaires. Il mitige aussi les risques de sécurité en relation aux accès avec privilèges, et prévient des failles de sécurité et problèmes de conformité.

PasswordManager Pro est constitué de cinq rôles : administrateur, administrateur de mots de passe, administrateur avec privilèges, auditeur de mots de passe et utilisateur de mots de passe. Les licences limitent le nombre d'administrateurs. Il n'y a aucune limite d'utilisateurs et d'auditeurs de mots de passe.

Si votre besoin est d'avoir une voûte sécuritaire pour entreposer vos mots de passe et de pouvoir faire du partage sélectif avec d'autres utilisateurs dans l'organisation, choisissez l'édition **standard.**

Fonctionnalités de l'édition Standard (2 administrateurs, mots de passe et utilisateurs illimités) 595 $ +
Voûte de mot de passe centralisée
Double cryptage – Au niveau applicatif et ensuite au niveau de la base de données
Authentification RADIUS
Importation de ressources par CVS/KeePass / Active Directory
Politiques de mots de passe
Partage de mots de passe
Audits et notifications instantanées
Gestion d'utilisateurs et de groupes d'utilisateurs
Authentification double factorielle
Applications mobiles/Extensions pour navigateurs
Restrictions par IP du portail Web

En plus des fonctionnalités de l'édition **Standard**, si vous désirez avoir des fonctionnalités de gestion de mots de passe, comme la synchronisation à distance de mots de passe, l'alertes et les notifications concernant vos mots de passe, la gestion de mots passe d'application à application, des rapports, de la haute disponibilité et autres, l'édition **Premium** serait un meilleur choix.

Fonctionnalités de l'édition Premium (5 administrateurs, mots de passe et utilisateurs illimités) 1395 $ +
Désactiver la réinitialisation des mots de passe pour comptes avec privilèges
Flux de contrôle pour l'accès aux mots de passe
Tableau de bord Administrateur (Rapports, Graphiques, flux en temps réel)
Notifications d'actions prises sur les mots de passe partagés
Réinitialisation de mots de passe à distance — Liste de plateformes supportées
Authentification double factorielle — Téléphone, Google Authenticator, YubiKey, RADIUS, Okta Verify, +
Haute disponibilité
Enregistrement des sessions privilégiées

L'édition **Entreprise** ajoute plusieurs fonctionnalités à celles de l'édition **Premium** qui permettent de faire la gestion des comptes avec privilèges (P.A.M.), et de faire la gestion du cycle de vie des clés SSH et des certificats SSL. Bien que ce ne sont pas des fonctionnalités requises pour avoir une voûte de mots de passe sécuritaire, elles peuvent ajouter une visibilité additionnelle pour des gestionnaires et administrateurs en faisant l'intégration à des solutions SIEM ou encore à des systèmes de billets tels que « ServiceDesk » ou JIRA.

Fonctionnalités de l'édition Entreprise (10 administrateurs, mots de passe et utilisateurs illimités) 3 995 $ +
Rotation de clés de cryptage
MS SQL Server comme base de données
API de gestion de mots de passe (XML RPC, SSH CLI)
Découverte de comptes avec privilèges
Synchronisation avec Active Directory
Synchronisation LDAP (Utilisateurs et Groupes)
Support SAML 2.0 — Okta, Azure AD, ADFS, OneLogin
Authentification double facteur - RADIUS
Gestion des identités fédérées

Fonctionnalités de l'édition Entreprise (10 administrateurs, mots de passe et utilisateurs illimités) 3 995 $ +
Personnalisation de rôles
API RESTful

RÉCAPITULATIF

	DASHLANE	1Password	bitwarden	ManageEngine PasswordManager Pro
Chiffrement	AES – 256bits	AES – 256bits	AES – 256bits	AES – 256bits
Zéro connaissance[3]	✓	✓	✓	✓
Disponible en français	✓	✓	✓	✓
MFA / 2FA	✓	✓	✓	✓
Voûtes personnelles	✓	✓	✓	✓
Voûtes partagées	✓	✓	✓	✓
Pays d'origine	É-U(New York)	Canada (ON)	É-U(Californie)	É-U(Californie)
Récupération de voûte	✓	✓	✓	✓
Surveillance "Dark Web"	✓	✓	✓	
Tableau de bord de sécurité	✓	✓	✓	✓

RÉFÉRENCES

Français – Récupération de voûte - Dashlane
Français – Récupération de voûte – 1Password
Anglais – Modifier la langue - Bitwarden
Anglais – Mot de passe maitre oublié - Bitwarden
Anglais – Réinitialiation de mot de passe maitre - Bitwarden
Anglais – Gestion des rôles et permissions – Password Manager Pro
Anglais – Notes de versions (Disponibilité du Français Version 9.8 build 9802) – Password Manager Pro

[3] Le principe de "Zéro connaissance" fait référence à un chiffrement local du contenu avant d'être envoyé vers le serveur de stockage (où il est chiffré à nouveau), assurant que le fabricant et l'organisation n'ont jamais connaissance du contenu déchiffré.

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 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 de truquer 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 entrainé 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 voûtes 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 voûte n'est envoyée par ces traqueurs. 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 voûtes et de les envoyer vers un serveur contrôlé par les attaquants. L'entreprise a suggéré aux utilisateurs de débuter 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 maitre.

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 mot de passe maitre 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 récupérer une sauvegarde des voûtes 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.

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, laissant même à un acteur malveillant obtenir une copie de la sauvegarde des voûtes 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 voûtes des utilisateurs à risque surviendrait à nouveau. Si votre établissement utilise Lastpass, il est recommandé de changer les mots de passe enregistrés dans les voûtes et de modifier le mot de passe maître du compte corporatif propriétaire des voûtes. 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.

RÉVISIONS

Date	Action	Auteur	Ver.
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
2022-02-14	Première version	Jean-François Blais CESI de l'UQ	1.0