[MIS À JOUR] Analyse comparative des gestionnaires de mots de passe les plus populaires de 2020

Mis à jour le 2 avril 2020 : Nous avons ajouté Devolutions Password Hub et NordPass

Devolutions

LASTPASS - KEEPASS - 1PASSWORD - DASHLANE - PASSWORDSTATE - KEEPER - STICKY PASSWORD - DEVOLUTIONS PASSWORD HUB - ROBOFORM - NORDPASS

Il existe plusieurs solutions de gestion de mots de passe sur le marché, alors trouver la bonne qui répondra à tous vos besoins peut sembler aussi ardu que chercher une aiguille dans une botte de foin. Afin de vous aider à trouver celui qui est fait sur mesure pour vous, nous avons analysé et comparé les logiciels les plus populaires.

Un bon gestionnaire de mots de passe devrait vous aider à accomplir vos tâches quotidiennes en générant, en gérant et en stockant tous vos mots de passe à votre place. Il devrait être en mesure de générer des mots de passe sécuritaires rapidement et les enregistrer automatiquement dans une base de données chiffrée.

D'autres fonctionnalités à rechercher sont des évaluations de la sécurité, la génération de caractères aléatoires et la connexion automatique à vos sites Web préférés.

Maintenant, regardons de plus près les fonctionnalités des différentes applications de gestion de mots passe ci-dessous. Comme vous le savez déjà, il y a des logiciels de gestion de mots de passe qui sont conçus pour des entreprises et des équipes plus grandes comme Secret Server, AuthAnvil, Lieberman, Cyberark et ManageEngine. Cependant, nous avons opté pour les solutions les plus populaires selon nos RDMers : LastPass, KeePass, 1Password, Dashlane, Passwordstate, Keeper, Sticky Password, Devolutions Password Hub, RoboForm et NordPass.

LastPass

LASTPASS FAIT PARTIE DES GESTIONNAIRES DE MOTS DE PASSE LES PLUS CONNUS ET UTILISÉS.

ON AIME

FACILEMENT ACCESSIBLE : Non seulement il est possible d'utiliser LastPass sur macOS, Windows et Linux, mais il est également compatible avec les navigateurs Web Chrome, Firefox, Safari, Opéra, Microsoft Edge et même Internet Explorer. Vos informations de connexion sont automatiquement sauvegardées sur les serveurs de LastPass, et vous pouvez y accéder à partir de n'importe quel ordinateur ayant l'extension installée..

VERSION GRATUITE RICHE EN FONCTIONNALITÉS : La version gratuite de LastPass offre à peu près autant de fonctionnalités que la version payante, de la synchronisation entre un nombre illimité d'appareils (rarement présente dans une version gratuite) à un générateur de mots de passe, ainsi qu'un stockage sécuritaire et illimité de mots de passe pour un seul utilisateur. Il s'agit probablement du gestionnaire de mots de passe avec la meilleure offre gratuite.

CHANGEMENTS DE MOTS DE PASSE : LastPass conserve une base de données de comptes piratés sur le Web et vous alerte si l'un de vos comptes fait partie d'une brèche de sécurité. Une fois que vous avez reçu l'alerte, vous pouvez facilement changer votre mot de passe en un seul clic de souris.

ANALYSE DES MOTS DE PASSE : LastPass analyse vos mots de passe, indique quels mots de passe sont dupliqués ou faibles, puis vous aide à en créer des plus sécuritaires. Il s'agit d'une fonctionnalité importante qui vous permet de tester facilement la robustesse de vos mots de passe et qui vous permet alors de les renforcer.

ON AIME MOINS

SERVICE À LA CLIENTÈLE : LastPass pourrait améliorer son service à la clientèle en offrant l'assistance par téléphone ou par clavardage.

FUITE DE DONNÉES AU DOSSIER : Nous devons mentionner que LastPass a été piraté en 2015. En 2019, l'équipe d'analystes en sécurité informatique de Google a découvert une faille qui exposait le dernier mot de passe utilisé dans le navigateur Web. Cependant, LastPass a été prompt à réagir face à ces deux menaces.

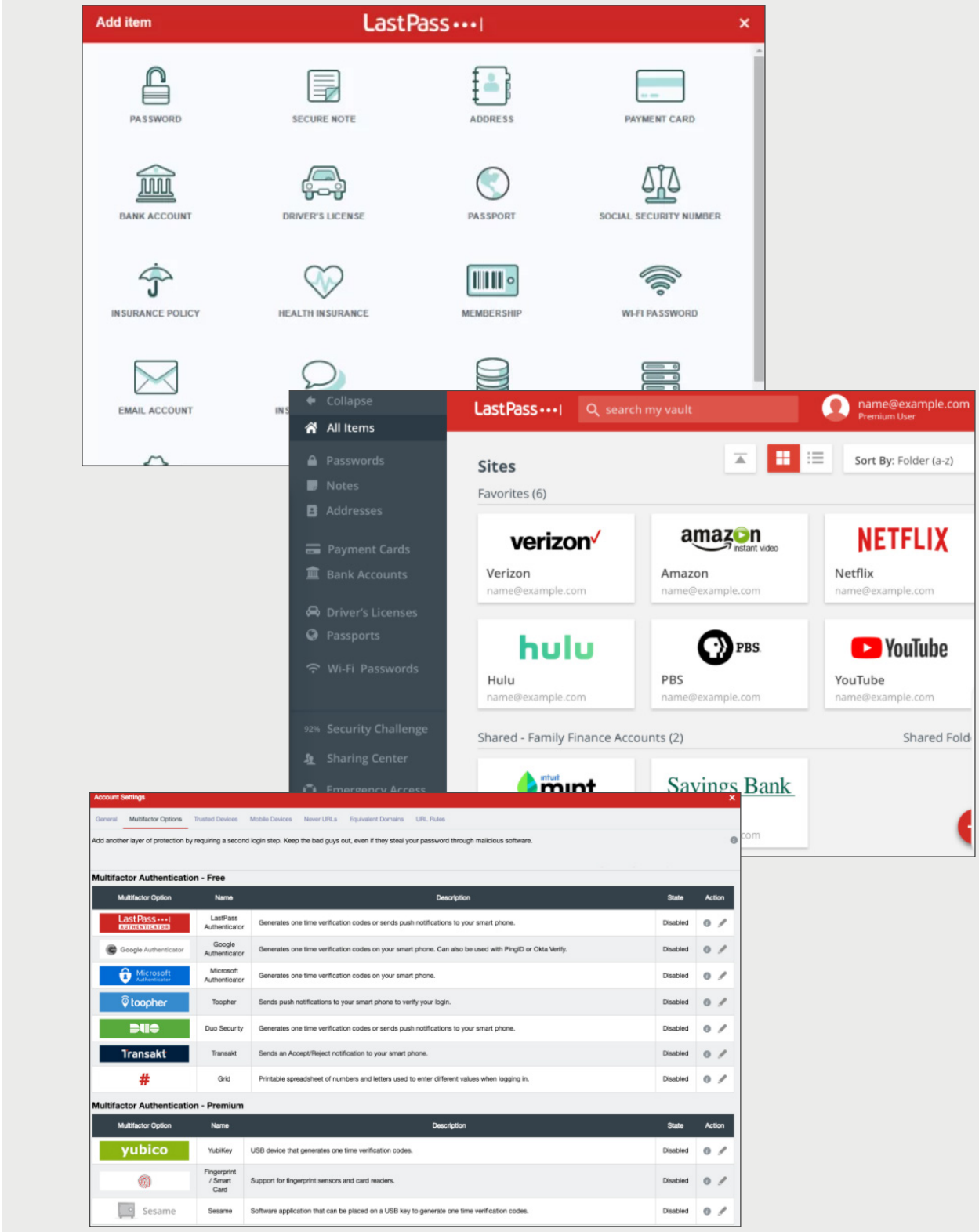
CLIENTÈLE CIBLE

LastPass s'adresse aux gens qui souhaitent ne pas se casser la tête pour stocker leurs mots de passe dans un endroit sécurisé. Même la version gratuite offre plusieurs fonctionnalités avancées qui plairont à la plupart des utilisateurs expérimentés.

LastPass est celui qui prend en charge le plus de téléphones mobiles, avec des applications pour Android, iOS, Windows et Blackberry. Grâce à son intégration impeccable dans les navigateurs Web et ses applications mobiles parfaites, LastPass aide à réconcilier les utilisateurs avec la gestion de mots de passe.

LastPass offre une version gratuite, LastPass Free, qui inclut toutes les fonctionnalités de base, dont la synchronisation entre divers appareils pour un utilisateur.

Pour avoir accès à toutes les fonctionnalités, dont l'accès en cas d'urgence et le partage avec plusieurs personnes, il vous coûtera 3,00$/mois pour un utilisateur, et 4,00$/mois pour 6 utilisateurs. La licence Team convient parfaitement aux petites entreprises de 50 utilisateurs ou moins, et coûte 4,00$/utilisateur/mois. La licence Enterprise s'adresse aux entreprises de toute taille et coûte 6,00$/utilisateur/mois.



POUR PLUS D'INFORMATIONS SUR LASTPASS

https://www.lastpass.com/

KeePass

KEEPASS EST INCROYABLEMENT PUISSANT ET BIEN SOUTENU PAR LA COMMUNAUTÉ. IL S'AGIT D'UN LOGICIEL LIBRE, DONC GRATUIT, QUI VOUS AIDE À GÉRER VOS MOTS DE PASSE DE FAÇON SÉCURITAIRE.

ON AIME

LOGICIEL LIBRE : Étant un logiciel libre, vous avez accès au code source de KeePass. Vous pouvez configurer et personnaliser votre installation vous-même grâce aux plugiciels développés par la communauté, tout en gardant le plein contrôle sur vos données.

PORTABILITÉ : Vous pouvez garder KeePass sur une clé USB puisqu'il ne nécessite aucune installation sur votre ordinateur. Il peut même s'exécuter sur des systèmes Windows sans être installé.

SÉCURITÉ À LA FINE POINTE : KeePass se surpasse en matière de sécurité. Il prend en charge les chiffrements AES et Twofish, en plus d'être chiffré par SHA-256, une fonction de hachage cryptographique sécuritaire à sens unique. Finalement, la base de données est complètement chiffrée.

MULTIPLES PLUGICIELS COMPATIBLES : L'une des forces de KeePass est qu'il prend en charge plusieurs plugiciels, car tout le monde peut développer des plugiciels pour KeePass. Si vous êtes une personne débrouillarde, vous pouvez facilement étendre les fonctionnalités de KeePass en employant d'autres méthodes d'importation et d'exportation d'autres formats de fichiers.

ON AIME MOINS

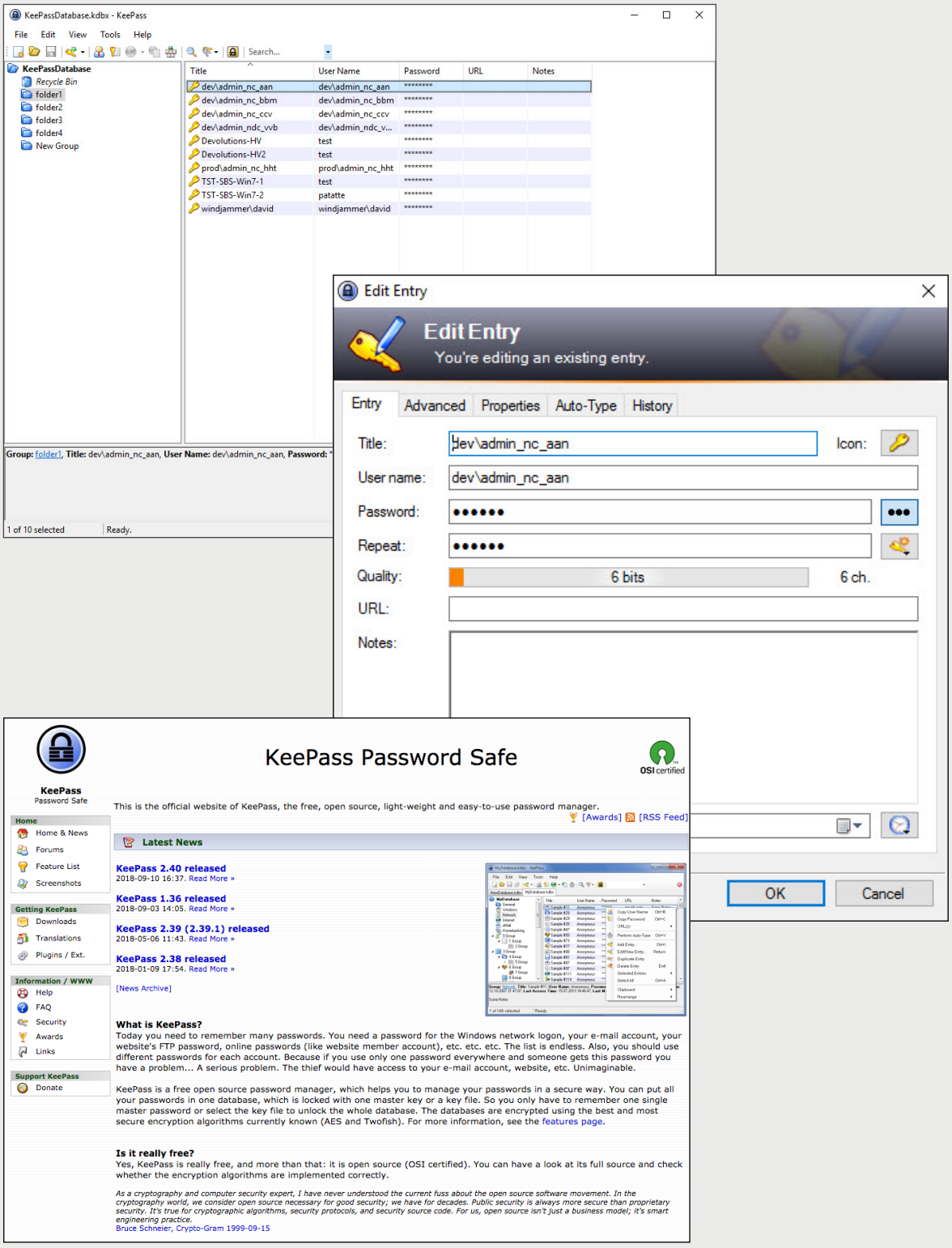
ABSENCE D'ACCOMPAGNEMENT : Lorsque vous ouvrez KeePass pour la première fois, il n'y a pas d'indices visuels sur ce que vous devez faire à la prochaine étape. Il n'y a pas non plus de configuration facile en un clic ou d'assistant d'installation.

INTERFACE DÉMODÉE : Si vous aimez les vieilles affaires, alors vous apprécierez l'interface grise qui rappelle celle de Windows 95 lorsque vous lancez KeePass. On dirait que ça n'a pas été mis à jour depuis le dernier siècle.

CLIENTÈLE CIBLE

KeePass est le meilleur gestionnaire de mots de passe pour les personnes moindrement habiles qui prendront le temps de le configurer. Elles profiteront alors d'un contrôle total de leur système personnalisé plutôt qu'utiliser une solution infonuagique nécessitant peu de configuration comme LastPass. Cette solution est parfaite pour toute personne technophile qui ne veut pas stocker ses données sur un serveur d'une partie tierce. Par contre, ce n'est pas un bon choix pour l'utilisateur moyen.

KeePass est gratuit, mais les dons sont appréciés afin de financer le développement du projet.



POUR PLUS D'INFORMATIONS SUR KEEPASS

http://keepass.info/

1PASSWORD EST CELUI QUI A LE PLUS BEAU DESIGN. IL EST OFFERT SUR WINDOWS, IOS ET ANDROID.

ON AIME

EXTENSIONS DE NAVIGATEUR : L'application Bureau de 1Password doit être installée, mais vous pouvez la lier facilement à votre navigateur avec différentes extensions. Vous pouvez donc synchroniser votre compte sur plusieurs appareils.

MODE ITINÉRANT : Le mode itinérant vous permet de supprimer temporairement les données de votre appareil mobile lors d'un voyage. Ainsi, si votre appareil est perdu, volé ou si un agent frontalier vous demande de vérifier vos appareils mobiles, personne ne pourra accéder aux données, puisqu'elles n'y seront plus! Une fois votre voyage terminé, vous n'avez qu'à restaurer vos données en une seule touche. Nous savons qu'il ne s'agit pas d'une fonctionnalité à tout casser, mais c'est une fonctionnalité unique que seul 1Password offre.

KIT D'URGENCE : 1Password fournit un PDF appelé « Kit d'urgence », qui contient votre mot de passe principal (Master Password) et la clé secrète (Secret Key) requise pour vous connecter à votre compte. Si jamais vous oubliez vos informations de connexion à votre compte 1Password, ce PDF (ou même le code QR) peut vous sauver la vie.

1PASSWORD WATCHTOWER : Cette fonctionnalité classe vos mots de passe dans les catégories suivantes : faible, vulnérable, compromis et réutilisé. Elle vous enverra également des alertes de sécurité en temps réel pour les services et les sites que vous utilisez.

ON AIME MOINS

IMPORTATION DE MOTS DE PASSE : 1Password vous permet d'importer les mots de passe des autres logiciels concurrents, mais le point faible relève du nombre restreint de gestionnaires compatibles. Il est à noter que LastPass, lui, permet d'importer les mots de passe de plus de 30 produits.

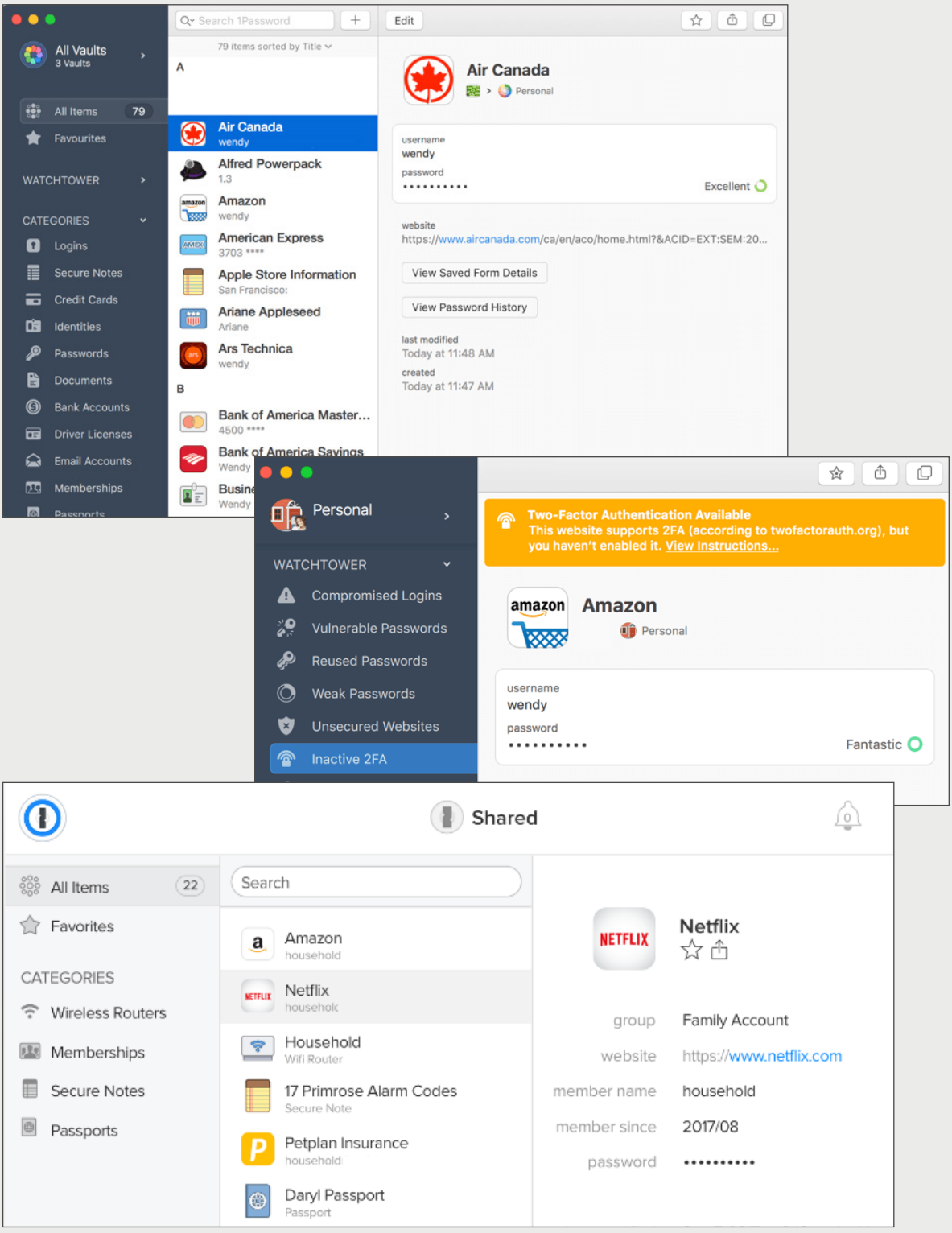
PAS DE VERSION GRATUITE : La plupart des gestionnaires de mots de passe offrent une version gratuite pour les utilisateurs individuels, même si les fonctionnalités sont limitées. L'absence d'une version gratuite est plutôt décevante.

CLIENTÈLE CIBLE

1Password est une excellente option pour une utilisation autant personnelle que commerciale grâce à son intégration fluide aux navigateurs Web, sa convivialité, son haut niveau de sécurité et un soutien technique par le biais du forum très efficace.

La licence individuelle est offerte à 2,99$/mois, ce qui inclut un nombre illimité de mots de passe et 1 Go d'espace de stockage.1Password offre également le forfait Familles, un abonnement qui comprend toutes les applications, des mises à niveau gratuites, l'accès par le Web et le partage avec 5 membres de la famille. Il se vend à 4,99$/mois.

Pour les équipes et les entreprises, 1Password offre 3 types d'abonnements :Teams, qui inclut les fonctionnalités telles que l'A2F, les commandes admin et le nombre illimité de coffres partagés pour 3,99$/utilisateur/mois; Business, qui comprend aussi les journaux d'activités et les rapports d'utilisation pour 7,99$/utilisateur/mois; Et, finalement, le plan Enterprise pour les grandes entreprises.



POUR PLUS D'INFORMATIONS SUR 1PASSWORD

https://1password.com/

DASHLANE EST UN GESTIONNAIRE DE MOTS DE PASSE ÉLÉGANT ET CONVIVIAL, COMPRENANT UN ALGORITHME DE CHIFFREMENT DE CALIBRE MILITAIRE.

ON AIME

CONNEXION AUTOMATIQUE : Dashlane vous connecte automatiquement à tous vos comptes. Il réussit à le faire même avec des systèmes de connexion plus complexes avec 2 ou 3 champs à remplir, comme les comptes bancaires. Aucun clic ni touche n'est requis.

TABLEAU DE BORD SUR LA SÉCURITÉ : Dashlane trouve tous les mots de passe faibles ou réutilisés dans le coffre de mots de passe. Il affiche également un score de sécurité à côté de ceux qui peuvent avoir été compromis. Il vous enverra une alerte si une brèche de sécurité survient.

CONTACT EN CAS D'URGENCE : Dashlane vous permet de définir une personne à contacter en cas d'urgence. Ainsi, la personne pourra avoir temporairement accès à votre compte. Cela est valable autant pour un compte personnel qu'un compte professionnel.

ACCÈS À UN RPV : Dashlane est l'un des seuls logiciels à donner accès aux utilisateurs à un RPV. En chiffrant toutes vos données sur les réseaux sans fil publics, un RPV peut contrer les pirates qui cherchent à voler vos mots de passe.

ON AIME MOINS

VERSION GRATUITE : Dashlane pourrait s'inspirer de LastPass quand il est question de version gratuite. En effet, la version gratuite est très limitée et plutôt décevante. Vous ne pouvez que stocker 50 mots de passe sur un seul appareil, puisque la fonctionnalité de synchronisation entre divers appareils n'est pas incluse.

COÛT : Dashlane est plutôt onéreux. Il s'agit en fait du logiciel le plus cher sur le marché.

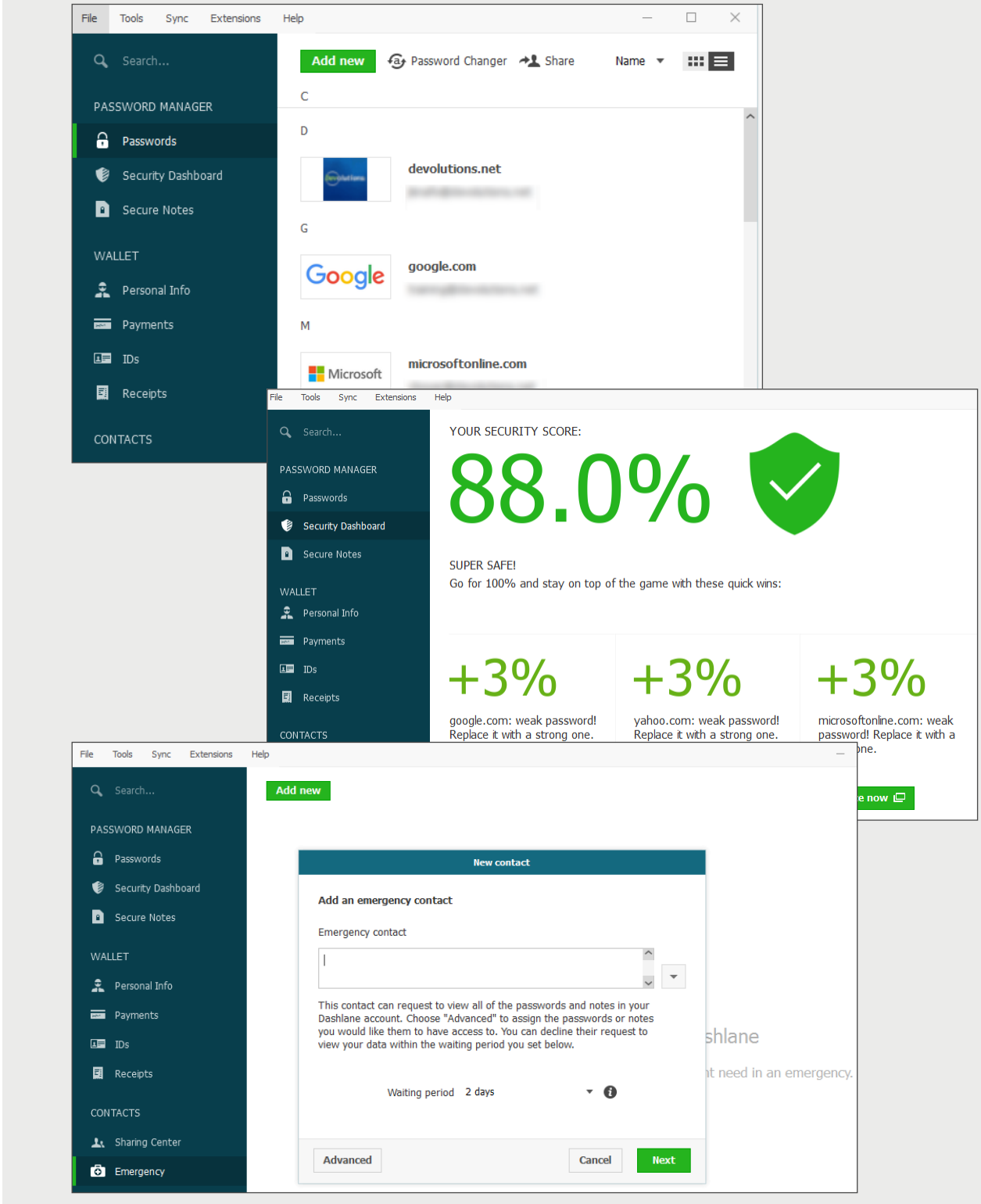
CLIENTÈLE CIBLE

Très facile à utiliser, Dashlane comprend plusieurs fonctionnalités. Sa belle interface simple convient à toute personne peu technophile.

Dashlane offre une version gratuite parfaite pour les utilisateurs qui ont moins de 50 mots de passe à gérer avec un seul appareil.

La licence Business est 4 $/utilisateur/mois.

La licence Premium coûte 3,33 $/mois et permet de stocker un nombre illimité de mots de passe sur un nombre illimité d'appareils, en plus d'offrir la surveillance du dark Web et un RPV sécurisé.



POUR PLUS D'INFORMATIONS SUR DASHLANE

https://www.dashlane.com/en/lp/neverforget-teal

Passwordstate

PASSWORDSTATE EST UNE SOLUTION WEB DE GESTION SÉCURITAIRE DE MOTS DE PASSE, CONÇUE À LA FOIS POUR LES PARTICULIERS ET LES ENTREPRISES.

ON AIME

INTERFACE DE PROGRAMMATION D'APPLICATIONS (API) : Passwordstate vous permet d'intégrer son API dans vos propres applications, mettant fin aux mots de passe codés en dur. Vous pourrez alors écrire vos propres scripts pour récupérer, mettre à jour ou ajouter des mots de passe, tout en respectant les standards en matière de vérification et les envois de notifications en temps réel.

PLATEFORMES MOBILES PRISES EN CHARGE : Le client mobile est compatible avec iOS, Android, Windows 8 et Blackberry.

CONTRÔLE D'ACCÈS BASÉ SUR DES RÔLES : Passwordstate est basé sur le concept des accès selon les rôles. Cela s'applique autant à l'accès aux mots de passe qu'à la gestion de l'application elle-même.

NOTIFICATIONS EN TEMPS RÉEL : Passwordstate a 54 notifications par courriel différentes. Elles peuvent être personnalisées ou désactivées par les administrateurs de Passwordstate. Chaque utilisateur peut spécifier quelles notifications il désire recevoir.

ON AIME MOINS

PAS DE SOLUTION INFONUAGIQUE : Certaines entreprises souhaiteraient plutôt utiliser une solution infonuagique, mais pour le moment, ce n'est pas une option offerte par Passwordstate.

INTERFACE UTILISATEUR : L'interface utilisateur est moins conviviale pour les utilisateurs finaux que la concurrence.

CLIENTÈLE CIBLE

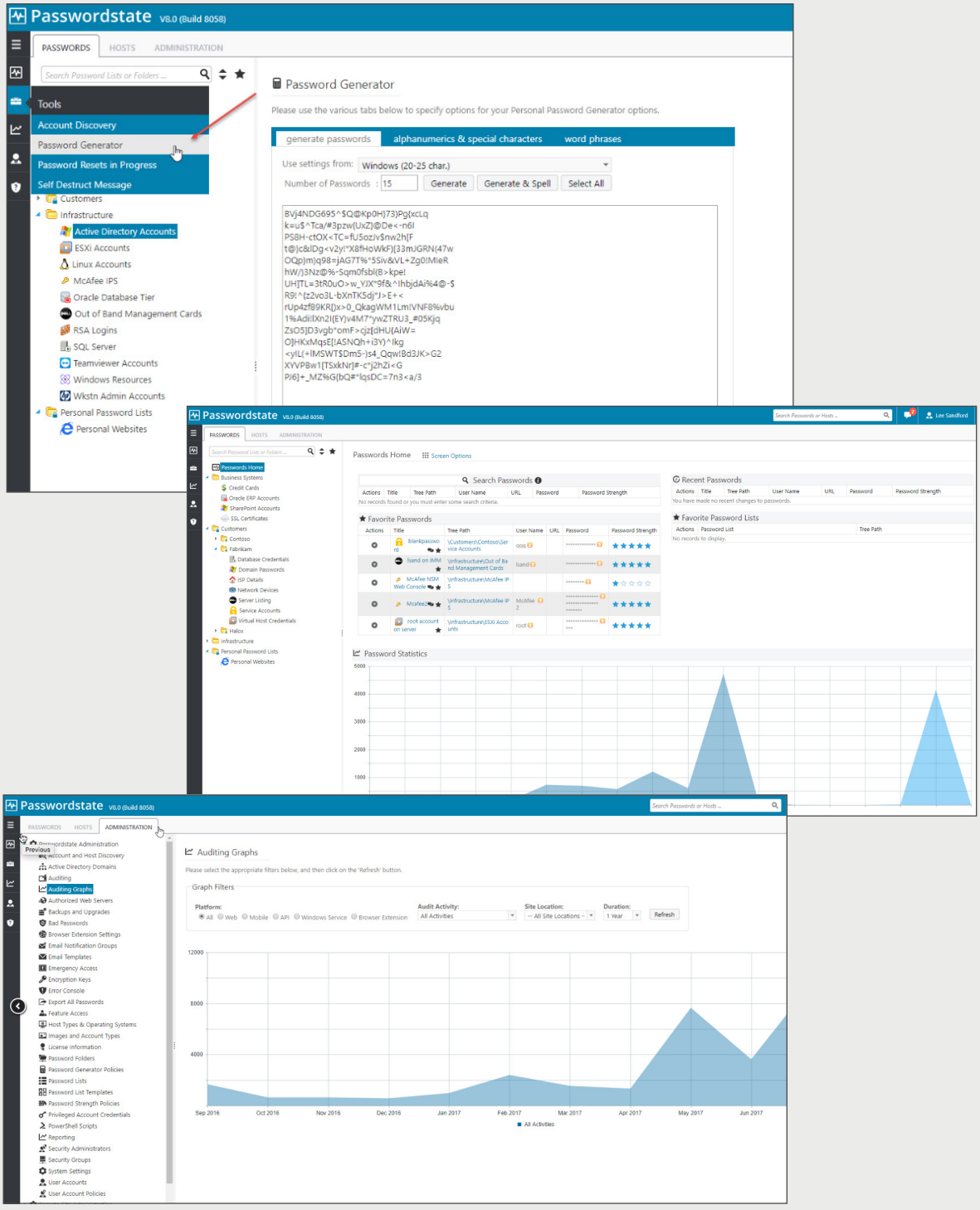
Passwordstate rend le tout facile à utiliser. Avec la version gratuite pour 5 utilisateurs, il s'agit d'un bon choix pour les petites entreprises. Les versions Enterprise et Global pourraient aussi plaire aux grandes entreprises avec toutes les fonctionnalités offertes.

Passwordstate est gratuit pour 5 utilisateurs. Pour un accès complet, incluant du soutien technique et des mises à niveau, le montant est de 60 $/licence/utilisateur (plus vous ajoutez des utilisateurs, plus le prix diminue).

La licence Enterprise est 5700 $, et vous pouvez ajouter un plan annuel de soutien technique et de mises à niveau pour 1140 $/année.

La licence Global, tout inclus, coûte 15 100 $, et le plan annuel de soutien technique et de mises à niveau se détaille à 2020 $/année.

Passwordstate offre également un module de haute disponibilité (High Availability module), qui roule en mode lecture seule sur un serveur de redondance pour 1750 $.



POUR PLUS D'INFORMATIONS SUR PASSWORDSTATE

https://www.clickstudios.com.au/

KEEPER EST L'UN DES GESTIONNAIRES LES PLUS TÉLÉCHARGÉS. IL PROTÈGE ET GÈRE VOS MOTS DE PASSE SUR DES TÉLÉPHONES INTELLIGENTS, DES TABLETTES ET DES ORDINATEURS.

ON AIME

KEEPER DNA : La plupart des applications prennent en charge l'authentification à 2 facteurs (2FA), mais Keeper a dépassé nos attentes. Plutôt qu'envoyer un code à un appareil, Keeper DNA utilise un objet connecté de la personne pour créer un profil unique (Keeper DNA Profile). Keeper prend en charge les montres intelligentes Apple Watch et Android Wear.

BREACHWATCH : BreachWatch surveille le dark Web, à la recherche de comptes compromis. Si un mot de passe ou un compte a été compromis, Keeper vous offre des façons de changer vos mots de passe pour vous protéger.

KEEPER CHAT : Keeper Chat est un service de messagerie qui ressemble à WhatsApp. Il est conçu pour stocker des messages, des photos et des vidéos dans un coffre sécurisé. Ainsi, vous ou votre entreprise pouvez maintenant communiquer par le biais d'une plateforme de messagerie sécurisée et chiffrée.

CONSOLE ADMINISTRATIVE : La console administrative vous donne accès aux rôles, aux équipes, aux utilisateurs, aux paramètres de A2F et au provisionnement des utilisateurs. Vous pouvez également voir la force globale des mots de passe de tout le monde inclus dans le plan.

ON AIME MOINS

PRIX : La stratégie de la boutique est à revoir, car, au moment d'acheter une licence personnelle de Keeper, les utilisateurs doivent se méfier. Lorsqu'on clique sur le bouton « Achetez maintenant », la facture grimpe soudainement de 29,99 $ à 59,97 $, ajoutant automatiquement un ensemble de fonctionnalités. Keeper devrait vraiment s'améliorer.

SYNCHRONISATION ENTRE LES APPAREILS : Keeper devrait s'inspirer de LastPass quant à sa version gratuite. En effet, la version gratuite ne permet qu'une seule installation, donc il est impossible de synchroniser les données entre différents appareils. Toutefois, le stockage de mots de passe est illimité.

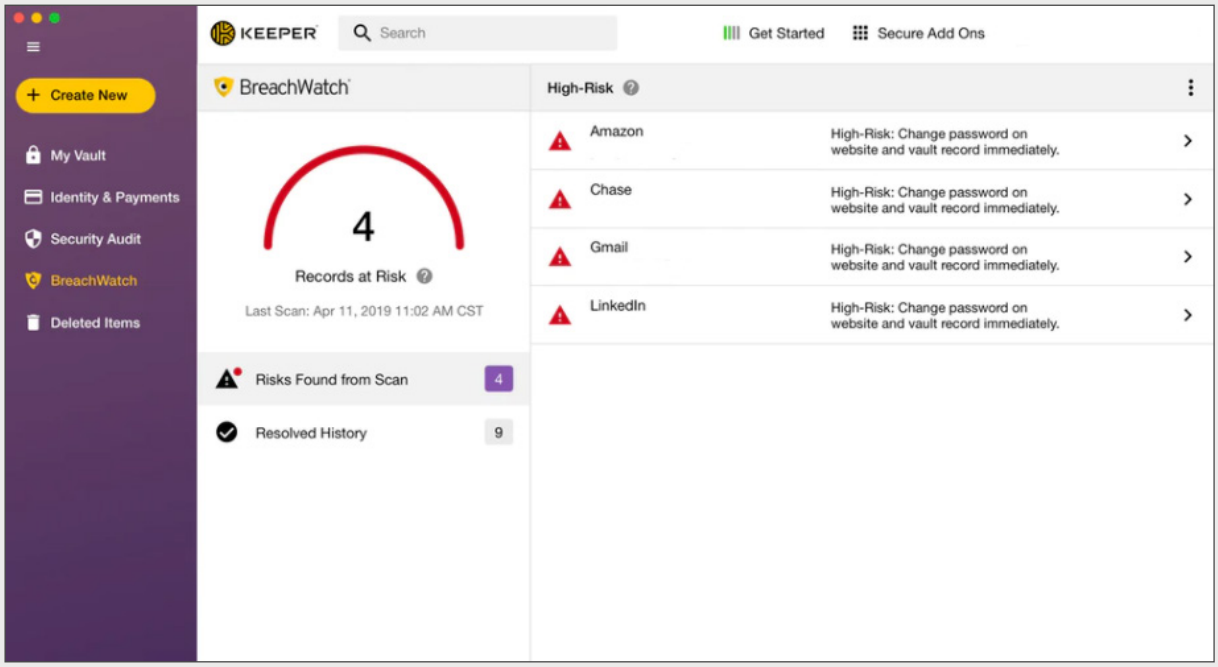
CLIENTÈLE CIBLE

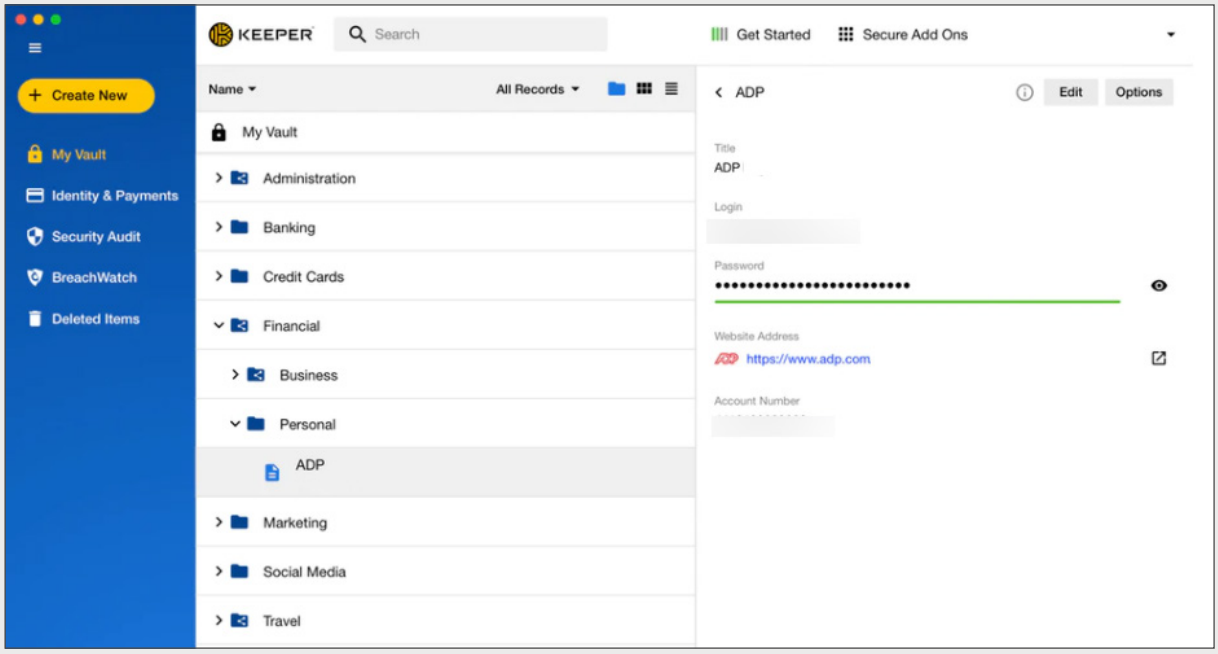
Keeper excelle dans son offre commerciale. Aussi, son interface conviviale convient parfaitement aux particuliers et aux familles.

Keeper peut être téléchargé gratuitement, vous donnant accès à leurs fonctionnalités de base sur un appareil, sans la protection d'une copie de sauvegarde. Keeper offre des plans différents pour les particuliers et les entreprises. Vous pouvez choisir entre le plan Personnel, offert à 2,50 $/utilisateur/mois, ou le plan Famille, qui coûte 5 $/mois pour 5 utilisateurs.

Les étudiants ont un rabais de 50 % sur une licence Keeper.

Pour les entreprises, il y a deux licences : la licence Business, qui coûte 2,50 $/utilisateur/mois, et la licence Enterprise à 3,75 $/utilisateur/mois, pour ceux qui ont besoin de l'intégration d'Active Directory.





POUR PLUS D'INFORMATIONS SUR KEEPER

https://keepersecurity.com/

STICKY PASSWORD VOUS PERMET DE GÉRER FACILEMENT TOUS VOS MOTS DE PASSE DE FAÇON SÉCURISÉE.

ON AIME

CHOIX DE SYNCHRONISER PAR LE RÉSEAU SANS FIL OU PAR LE NUAGE : Sticky Password permet aux utilisateurs de choisir parmi 3 options de synchronisation, soit par les serveurs infonuagiques de Sticky Password, soit par le réseau sans fil local ou encore manuellement. La synchronisation par réseau sans fil vous permet de synchroniser les appareils directement entre eux lorsqu'ils sont sur le même réseau local. Le grand avantage de cette méthode est que vos données ne se retrouveront jamais dans le nuage, donc elles ne quittent pas l'appareil.

PORTABILITÉ : La portabilité vous permet d'apporter vos mots de passe sur une clé USB partout où vous allez. L'outil USB peut aussi être utilisé pour vous connecter à tous vos sites Web enregistrés.

AUTHENTIFICATION BIOMÉTRIQUE : L'authentification par empreinte digitale fonctionne sur les appareils iOS et Android. Le propriétaire du compte n'a qu'à glisser son doigt pour déverrouiller l'application!

SAUVEZ LES LAMANTINS : Sticky Password est le seul gestionnaire de mots de passe qui encourage une belle cause! En effet, ce ne sont pas toutes les compagnies en informatique qui s'impliquent pour sauver une espèce en voie d'extinction. À chaque licence Premium vendue, une partie du montant va à un organisme pour sauver les lamantins.

ON AIME MOINS

PAS DE CHANGEMENT AUTOMATIQUE : Le tableau de bord sur la sécurité affiche les mots de passe faibles et réutilisés, mais il n'est pas possible de tous les changer automatiquement. Il faudrait donc le faire manuellement, un par un.

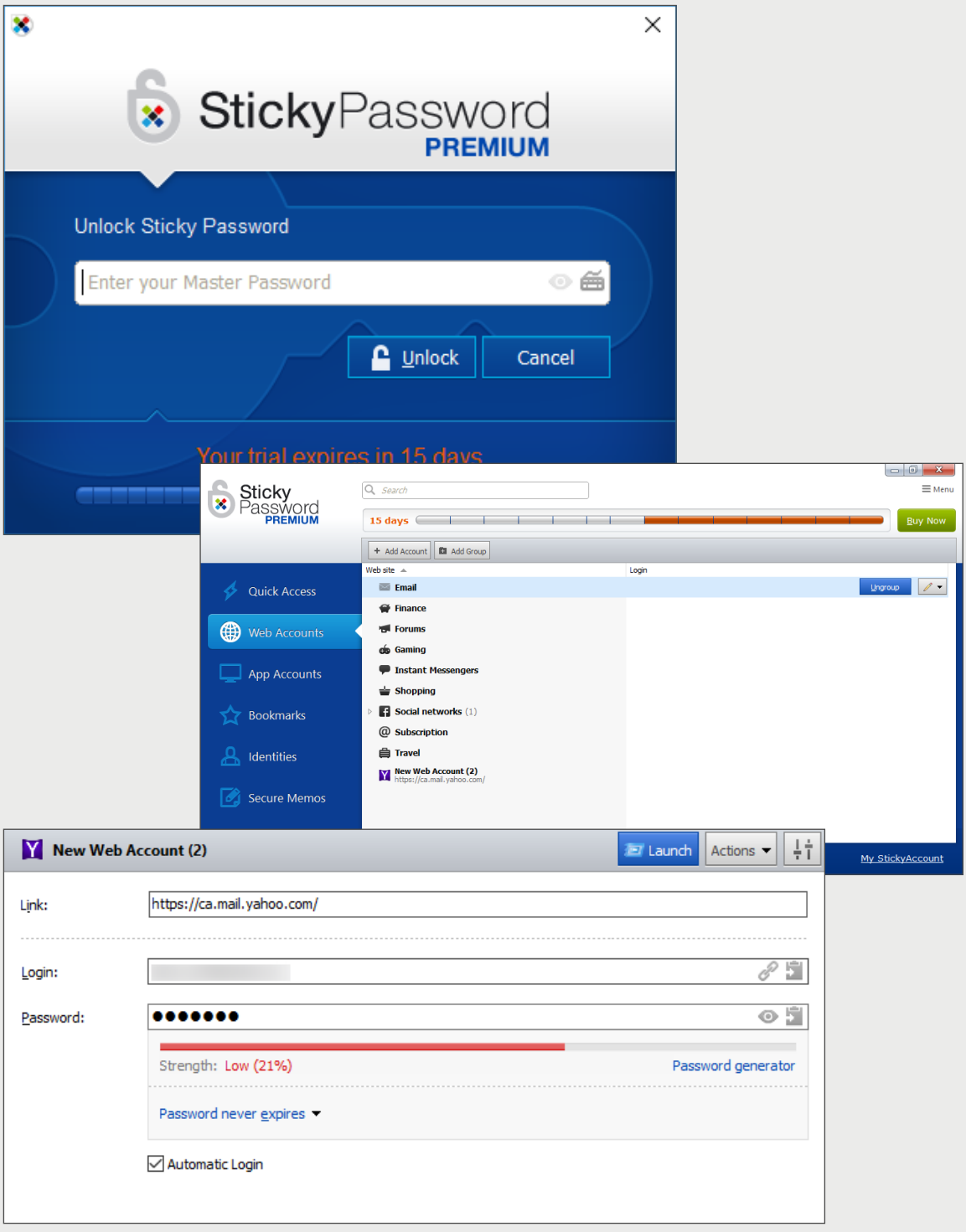
SIGNETS : La fonctionnalité des signets doit être améliorée. Pour le moment, il est impossible de sauvegarder les signets à partir de l'extension de navigateur, alors que c'est là qu'on aimerait les utiliser.

CLIENTÈLE CIBLE

Avec son authentification biométrique et sa portabilité, Sticky Password est parfait autant pour une utilisation personnelle que pour les petites entreprises. L'absence d'authentification à 2 facteurs nous empêche de le recommander pour les plus grandes entreprises.

Sticky Password a une version gratuite qui comprend toutes les fonctionnalités de base. Cependant, la synchronisation entre plusieurs appareils n'est pas incluse.

L'édition Premium coûte 29,99 $ par année. Une licence valide à vie est aussi offerte au coût de 199,99 $.



POUR PLUS D'INFORMATIONS SUR STICKY PASSWORD

https://www.stickypassword.com/

Devolutions Password Hub

DEVOLUTIONS PASSWORD HUB EST UNE SOLUTION INFONUAGIQUE SÉCURISÉE ET FLEXIBLE DE GESTION DE MOTS DE PASSE, CONÇUE POUR LES DIFFÉRENTES ÉQUIPES DE L'ENTREPRISE.

ON AIME

SYSTÈME DE CONTRÔLE D'ACCÈS BASÉ SUR DES RÔLES : Devolutions Password Hub protège l'accès aux mots de passe sensibles en partageant les données seulement au besoin grâce à un système de contrôle d'accès basé sur des rôles.

RAPPORTS COMPLETS : Générez des rapports complets, incluant les journaux des activités, journaux administratifs et rapports d'utilisation, à des fins d'audit, de conformité et de gouvernance.

CONVIVIALITÉ : Avec un générateur de mots de passe robustes, un analyseur de mots de passe et une interface utilisateur intuitive, tous les utilisateurs de l'entreprise y trouveront leur compte.

OUTILS CONNEXES : Devolutions Password Hub dispose de deux outils connexes gratuits : Devolutions Launcher et Devolutions Web Login.

- **Devolutions Launcher** permet aux utilisateurs de lancer des connexions à distance sécurisées à des serveurs, des sites Web et des applications directement à partir de Devolutions Password Hub.
- **Devolutions Web Login** est une extension de navigateur qui permet aux utilisateurs d'injecter sécuritairement leurs mots de passe, stockés dans un coffre, dans des sites Web.

ON AIME MOINS

MODE HORS-LIGNE : Actuellement, Devolutions Password Hub n'offre pas le mode hors-ligne.

AUCUN PLAN POUR UNE UTILISATION PERSONNELLE : Devolutions Password Hub est conçu pour les entreprises, incluant les PME qui ont des budgets limités. Il n'y a pas de version gratuite pour le moment.

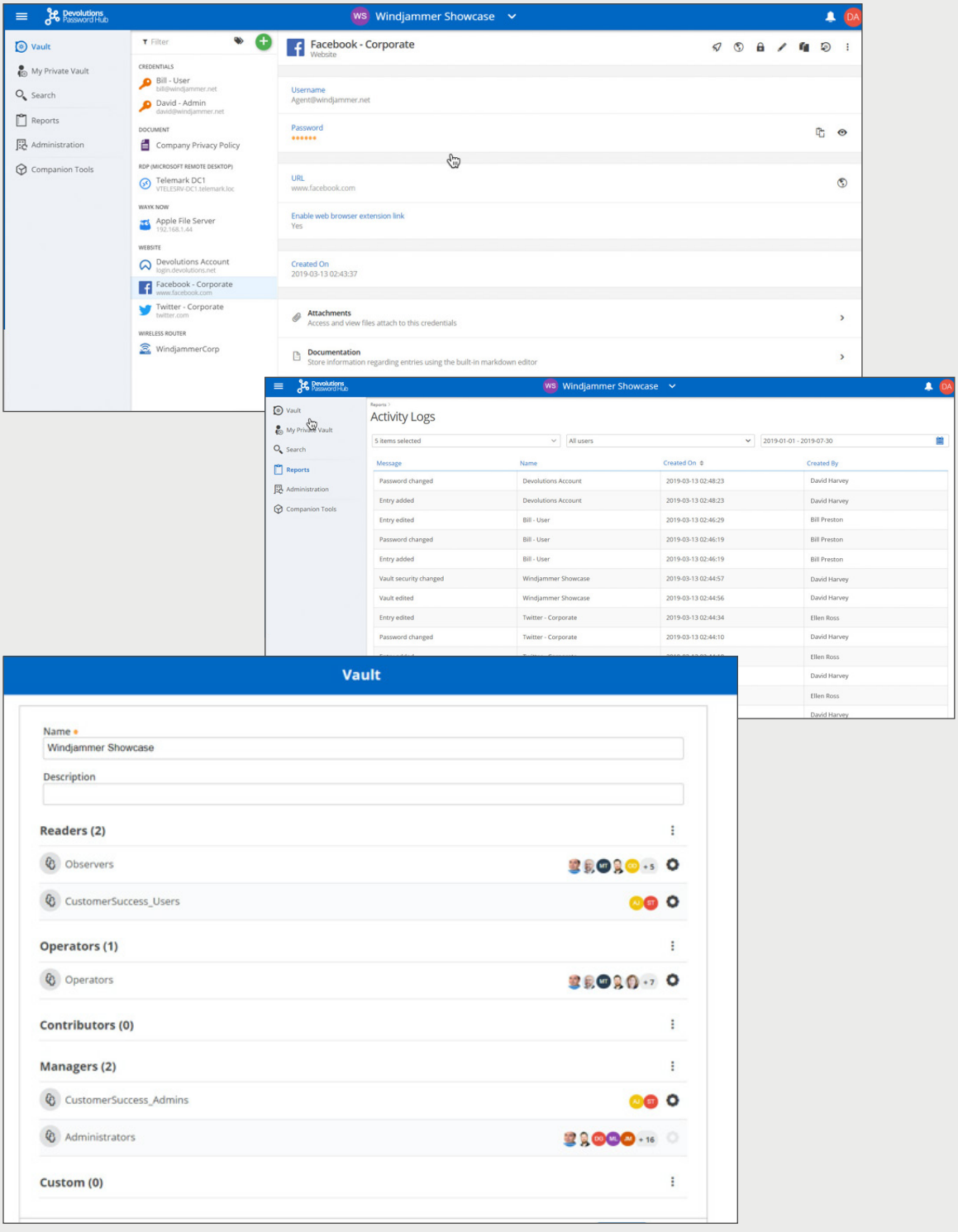
CLIENTÈLE CIBLE

Devolutions Password Hub représente un équilibre parfait entre la sécurité et la convivialité. Il est conçu pour les entreprises, incluant les PME qui ont des budgets limités.

Les licences d'abonnement incluent l'accès à Devolutions Password Hub, aux outils d'accompagnement Devolutions Launcher et Devolutions Web Login ainsi qu'un espace illimité de stockage dans le nuage.

Le prix d'une licence varie en fonction du nombre d'utilisateurs :

- 1 à 10 utilisateurs : 50 $/mois
- 11 à 25 utilisateurs : 100 $/mois
- 26 à 50 utilisateurs : 150 $/mois
- 50 à 100 utilisateurs : 200 $/mois.



POUR PLUS D'INFORMATIONS SUR DEVOLUTIONS PASSWORD HUB

https://password.devolutions.net/

RoboForm

ROBOFORM EST UN GESTIONNAIRE DE MOTS DE PASSE ABORDABLE QUI EXISTE SUR LE MARCHÉ DEPUIS 16 ANS ET QUI OFFRE PLUSIEURS OPTIONS.

ON AIME

PARTAGE SÉCURISÉ D'IDENTIFIANTS : RoboForm vous permet de partager une seule entrée ou un dossier avec un autre utilisateur, tant qu'il a une version installée de RoboForm et que vous avez la paire de clés RSA correspondante. Vous ne vous soucierez plus du risque d'exposition de vos informations sensibles lors d'un partage.

REMPLISSAGE AUTOMATIQUE DE FORMULAIRES À TOUTE ÉPREUVE : RoboForm mérite une étoile dorée pour sa fonctionnalité de remplissage automatique dans un navigateur Web. Le résultat est toujours parfait, peu importe la complexité ou la non-standardisation des formulaires à remplir.

SÉCURITÉ DE HAUT NIVEAU : RoboForm offre un haut niveau de sécurité grâce au chiffrement AES-256 de vos données. Toutes vos informations sont chiffrées localement sur votre appareil, puis elles sont envoyées à RoboForm par le biais d'un canal TSL/SSL, ce qui rend l'interception ou le décryptage quasiment impossible. Mais ce n'est pas tout : vos données sont hachées des milliers de fois avec PBKDF2, les protégeant ainsi de toute attaque par force brute. RoboForm n'a pas, et n'aura jamais, accès à vos données, ce qui signifie que seulement vous pouvez voir ce que vous stockez.

EXCELLENT SOUTIEN TECHNIQUE : Par le passé, RoboForm a été critiqué pour son service à la clientèle. Ce n'est plus le cas aujourd'hui. Il offre maintenant un centre d'assistance et un mode d'emploi afin de répondre aux questions les plus communes. Vous pouvez poser vos questions par courriel ou vous pouvez leur demander de vous appeler afin de résoudre n'importe quel problème. Un représentant vous appellera dans les plus brefs délais.

ON AIME MOINS

CONVIVIALITÉ : RoboForm offre trop d'options qui n'interpelleront pas la vaste majorité des utilisateurs et qui rendent l'application trop puissante et moins conviviale pour les utilisateurs finaux. Cela pourrait être un avantage, mais comme dit le dicton : trop, c'est comme pas assez.

L'ACCÈS PAR LE WEB ET LA SAUVEGARDE DANS LE NUAGE SONT DES FONCTIONNALITÉS PREMIUM : Ce serait génial d'inclure ces fonctionnalités, en plus de la synchronisation entre plusieurs appareils, dans la version gratuite.

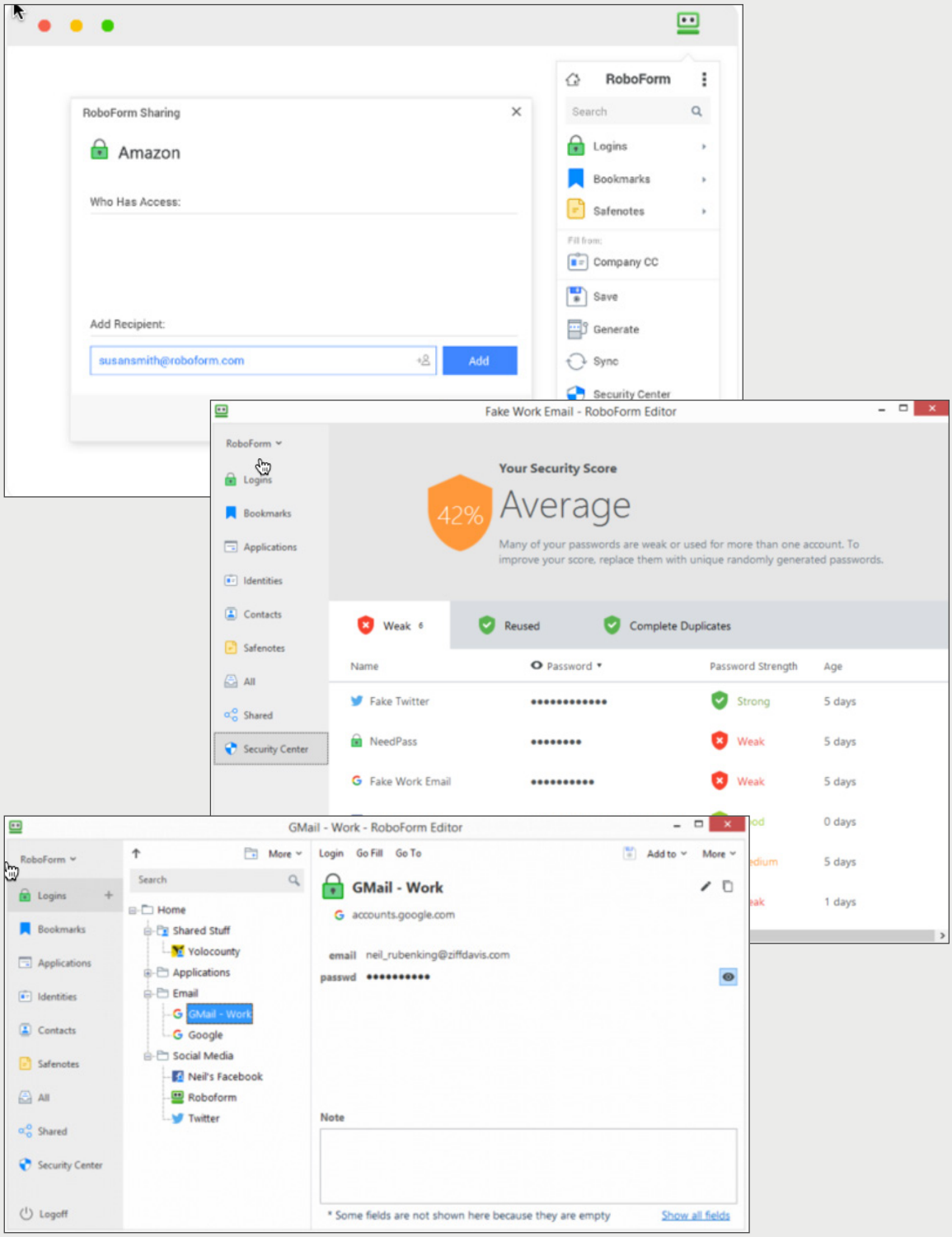
CLIENTÈLE CIBLE

RoboForm convient aux technophiles, mais pourrait décourager les non-initiés. Outre ceci, RoboForm est un gestionnaire de mots de passe solide à prix modique.

RoboForm offre une version gratuite pour les utilisateurs individuels, avec un seul appareil. Puis, il y a trois types de licences : **La licence individuelle**, qui coûte 23,88 $ pour 1 an, 71,64 $ pour 3 ans et 119,40 $ pour 5 ans.
La licence familiale, pour 5 utilisateurs, est offerte à 47,75 $ pour 1 an, 143,25 $ pour 3 ans et 238,75 $ pour 5 ans.

La licence Business, quant à elle, se décline comme suit :

- 1048,50 $, 30 utilisateurs, 1 an;
- 2695,50 $, 30 utilisateurs, 3 ans;
- 3892,50 $, 30 utilisateurs, 5 ans.



POUR PLUS D'INFORMATIONS SUR ROBOFORM

https://www.roboform.com/

NordPass

L'ENTREPRISE NORDPASS, CONNUE POUR SA SOLUTION RPV, A RÉCEMMENT LANCÉ UN GESTIONNAIRE DE MOTS DE PASSE INCLUANT D'IMPRESSIONNANTES FONCTIONNALITÉS.

ON AIME

SÉCURITÉ À LA FINE POINTE : Comparé à la plupart des gestionnaires qui utilisent la spécification Advanced Encryption Standard (AES), NordPass se sert de l'algorithme de chiffrement XChaCha20, rejoignant les poids lourds de l'industrie comme Google et CloudFlare. XChaCha20 est perçu comme le futur du chiffrement, car il est moins vulnérable à certains types de cyberattaques.

PARTAGE DE MOTS DE PASSE : NordPass rend facile le partage sécurisé d'identifiants, de cartes de crédit et de notes avec les autres utilisateurs. C'est beaucoup plus sécuritaire que de partager les données par courriel, par réseaux sociaux ou autres canaux de communication. Gardez en tête que vous devez posséder un compte Premium (payant) pour partager des informations. Cependant, avec un compte gratuit, vous pouvez recevoir des éléments partagés.

JURIDICTION RESPECTUEUSE DE LA VIE PRIVÉE : NordPass est enregistrée au Panama, pays qui prône le respect de la vie privée. Il n'y a aucune loi quant à la conservation de données, et le Panama ne fait pas partie des alliances du Groupe des cinq, du Groupe des neuf ou du Groupe des 14.

FACILE À UTILISER : NordPass est vraiment bien conçu. L'interface utilisateur est épurée, intuitive et conviviale. Contrairement à d'autres gestionnaires de mots de passe, NordPass n'essaie pas d'offrir mille choses en même temps. C'est un gestionnaire efficace et simple à utiliser : rien de plus, rien de moins.

ON AIME MOINS

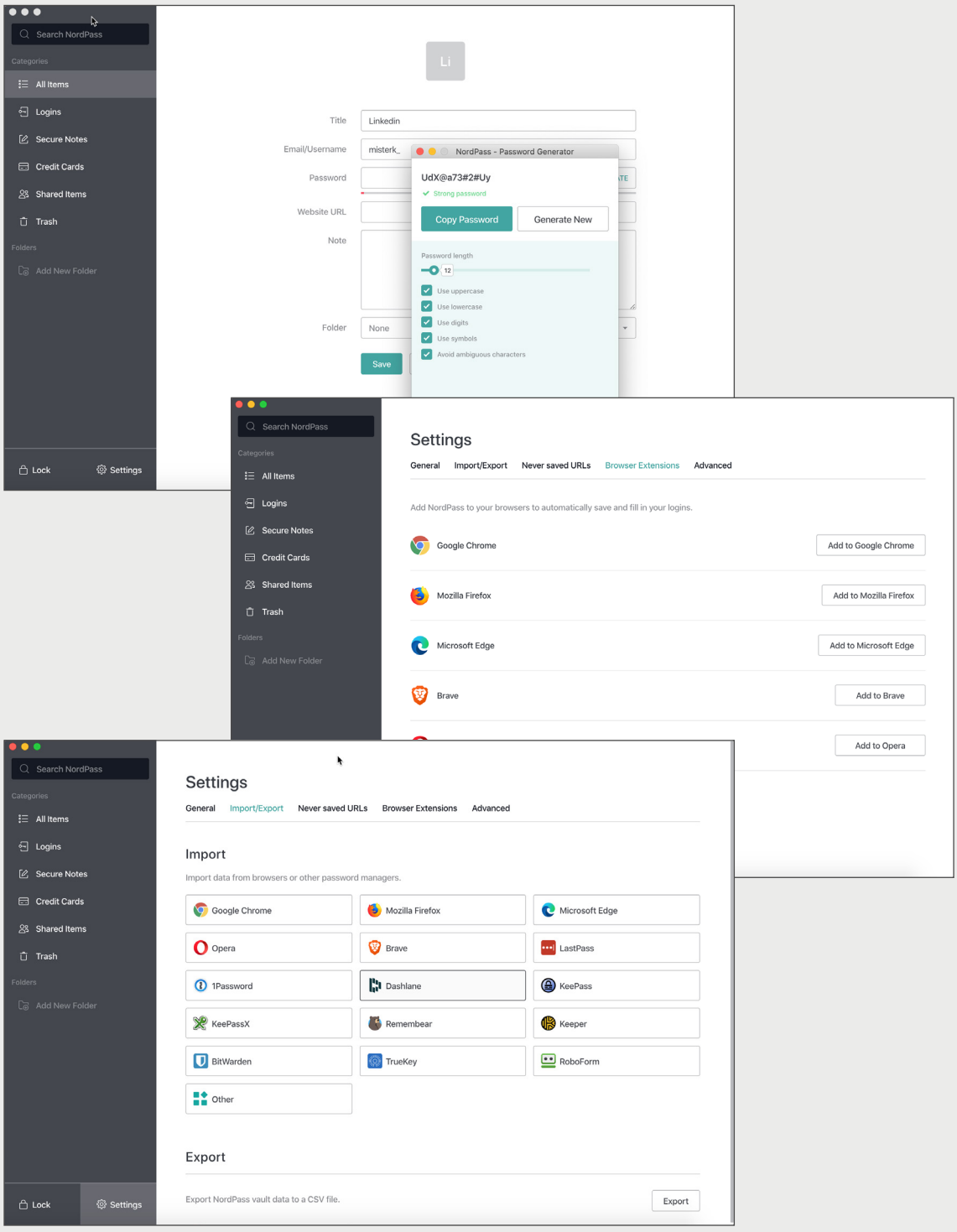
REMPLISSAGE AUTOMATIQUE PAR L'EXTENSION DE NAVIGATEUR : L'extension de navigateur ne fait que remplir les champs de connexion habituels (nom d'utilisateur et mot de passe). D'autres logiciels concurrents vont plus loin et peuvent remplir d'autres champs, comme des adresses ou des informations de cartes de crédit.

GÉNÉRATEUR DE MOTS DE PASSE SUR MOBILE : L'application mobile de NordPass n'offre pas un générateur de mots de passe. Ainsi, si vous voulez créer des mots de passe sur votre appareil mobile, NordPass les sauvegardera pour vous. Cependant, il ne pourra pas générer des mots de passe robustes et aléatoires. Cela pourrait rebuter certains acheteurs.

CLIENTÈLE CIBLE

NordPass répond aux attentes des utilisateurs qui désirent un gestionnaire de mots de passe efficace et simple à utiliser, très bien chiffré et développé par une entreprise bien réputée. Il est parfait autant pour une utilisation personnelle que commerciale.

NordPass offre une version gratuite pour les utilisateurs individuels, avec un seul appareil. Le plan Premium, qui offre des fonctionnalités additionnelles (p.ex. la possibilité de partager sécuritairement des données avec d'autres utilisateurs), coûte présentement 2,49 $/mois. NordPass peut alors être installé sur 6 appareils.



POUR PLUS D'INFORMATIONS SUR NORDPASS

https://nordpass.com/

VOICI UN TABLEAU INDIQUANT CERTAINES FONCTIONNALITÉS PLUS AVANCÉES PRISES EN CHARGE PAR LES GESTIONNAIRES DE MOTS DE PASSE.

	Lastpass	KeePass	1Password	Dashlane	Passwordstate	Keeper	Sticky Password	Devolutions Password Hub	RoboForm	NordPass
Mode hors ligne	✓		✓	✓	✓	✓	✓		✓	✓
Authentification à 2 facteurs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Navigateurs compatibles	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Remplissage automatique des formulaires	✓		✓	✓	✓	✓	✓	✓	✓	✓
Générateur de mots de passe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Alertes de sécurité	✓		✓	✓	✓	✓				
Application portable	✓	✓		✓		✓	✓		✓	
Application mobile	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Audits de sécurité	✓		✓	✓	✓	✓	✓	✓	✓	
Importation de mots de passe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Exportation de mots de passe	✓	✓	✓	✓	✓	✓	✓		✓	✓
Authentification unique (SSO)	✓					✓			✓	
Partage de mots de passe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Base de données intégrée	✓		✓	✓	✓	✓	✓		✓	
Sur site		✓	✓		✓	✓				
Infonuagique	✓		✓	✓		✓	✓	✓	✓	✓

En passant, Remote Desktop Manager intègre toutes les solutions citées ci-haut, sauf Keeper et NordPass. Au final, peu importe le choix de solution que vous ferez, l'important est d'utiliser des mots de passe robustes afin de protéger vos données.

Bon magasinage!