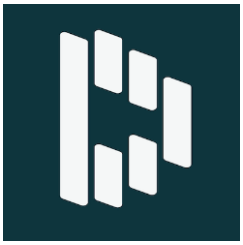
Etude gestionnaire de mot de passe

Problèmatique : *Keepass est actuellement utilisé au sein de la société Chavanel dans le service informatique uniquement, il n'existe pas encore de gestionnaire de mot de passe pour les utilisateurs. Keepass n'a pas de support professionnel étant open source, il n'est pas centralisé, il demande une synchronisation manuelle et l'interface peut paraître complexe ou vieillissante.*

Sommaire :



DASHLANE

https://www.dashlane.com/fr

Inconvénients :

1. ***Coût :*** Service payant, et le coût peut augmenter en fonction du nombre d'utilisateurs.
2. ***Dépendance à Internet :*** Nécessite une connexion Internet pour fonctionner correctement, ce qui peut poser problème en cas de perte de connectivité.
3. ***Configuration Initiale :*** La configuration initiale pour une utilisation en entreprise peut être complexe, en particulier sur un environnement RDS, et nécessite une expertise technique.
4. ***Dépendance au Logiciel Client*** : Les utilisateurs doivent installer et mettre à jour le logiciel Dashlane sur leur RDS, ce qui peut ajouter une charge administrative.
5. ***Sécurité Dépendante de la Configuration*** : La sécurité des mots de passe dans Dashlane dépend de la configuration appropriée, et des erreurs de configuration peuvent potentiellement compromettre la sécurité.

Avantages :

1. ***Sécurité Améliorée :*** Offre des fonctionnalités de sécurité avancées, telles que la génération de mots de passe forts, l'audit de la sécurité des mots de passe et la surveillance de la sécurité du dark web.
2. ***Partage Sécurisé :*** Partager des mots de passe et des informations d'identification de manière sécurisée avec les membres de l'équipe, ce qui facilite la collaboration tout en maintenant la sécurité.
3. ***Authentification Multifacteur (MFA) :*** Prend en charge l'authentification multifacteur, ce qui renforce la sécurité de l'accès aux mots de passe et aux comptes.
4. ***Stockage de Données Sensibles :*** Permet de stocker d'autres informations sensibles telles que les informations de carte de crédit, les informations d'identification de compte bancaire, etc.
5. ***Conformité et Audit :*** Offre des fonctionnalités de journalisation et d'audit qui peuvent aider les entreprises à maintenir la conformité avec les normes de sécurité et à effectuer des vérifications de sécurité.

Coût :

Variable en fonction du nombre d’utilisateurs. (Formule Business 8 € par mois)

BIT WARDEN

https://bitwarden.com/

Inconvénients :

1. ***Dépendance à Internet :*** Nécessite une connexion Internet pour fonctionner correctement, ce qui peut poser problème en cas de perte de connectivité.
2. ***Formation des Utilisateurs :*** Les utilisateurs doivent être formés à l'utilisation de Bitwarden, ce qui peut prendre du temps et des ressources supplémentaires.

Avantages :

1. ***Sécurité des Mots de Passe :*** Offre un stockage sécurisé des mots de passe, y compris le chiffrement de bout en bout, garantissant la sécurité des informations d'identification de l'entreprise.
2. ***Gestion Centralisée des Mots de Passe :*** Gérer l'accès aux mots de passe de manière centralisée, en attribuant des rôles et des autorisations aux utilisateurs, ce qui facilite la gestion des mots de passe.
3. ***Partage Sécurisé :*** Permet de partager des mots de passe et des informations d'identification de manière sécurisée avec les membres de l'équipe, ce qui facilite la collaboration tout en maintenant la sécurité.
4. ***Authentification Multifacteur (MFA) :*** Prend en charge l'authentification multifacteur, ce qui renforce la sécurité de l'accès aux mots de passe et aux comptes.
5. ***Open Source :*** Bitwarden est open source.
6. ***Accès depuis un RDS :*** Permet aux utilisateurs d'accéder à leurs mots de passe stockés depuis un emplacement centralisé.
7. ***Stockage de Données Supplémentaires :*** Permet de stocker d'autres informations sensibles, telles que des notes sécurisées, des cartes de crédit, etc.

Coût :

Existe une version gratuite mais aussi une version plus complète dite “Business” payante. (Formule Entreprise 5 $ par mois)

LASTPASS ENTREPRISE

https://www.lastpass.com/fr/solutions/enterprise-password-management

Inconvénients :

1. ***Dépendance à Internet :*** Nécessite une connexion Internet pour fonctionner correctement, ce qui peut poser problème en cas de perte de connectivité.

Avantages :

1. ***Sécurité des Mots de Passe :*** Chiffre les mots de passe et offre une sécurité renforcée grâce à des politiques de sécurité personnalisables, telles que la complexité des mots de passe et les exigences de renouvellement.
2. ***Partage Sécurisé :*** Partager des mots de passe et des informations d'identification de manière sécurisée avec les membres de l'équipe, facilitant la collaboration tout en maintenant la sécurité.
3. ***Authentification Multifacteur (MFA) :*** Prend en charge l'authentification multifacteur, renforçant ainsi la sécurité des comptes et des mots de passe.
4. ***Accès depuis plusieurs appareils :*** Les utilisateurs peuvent accéder à leurs mots de passe et informations d'identification depuis divers appareils, améliorant ainsi la mobilité et la flexibilité.

Coût :

Outil payant et dépend du nombre d’utilisateurs. (Formule Business 6.50 € par mois)

1PASSWORD

https://1password.com/fr

Inconvénients :

1. ***Dépendance à Internet : N***écessite une connexion Internet pour fonctionner correctement, ce qui peut poser problème en cas de perte de connectivité.
2. ***Configuration Initiale :*** La configuration initiale de 1Password pour une utilisation en entreprise peut être complexe, en particulier sur un environnement RDS, et nécessite une expertise technique.

Avantages :

1. ***Politiques de Sécurité Personnalisables :*** Définir des politiques de sécurité personnalisées, telles que des exigences de complexité des mots de passe et de renouvellement, pour renforcer la sécurité.
2. ***Partage Sécurisé :*** Permet de partager des mots de passe et des informations d'identification de manière sécurisée avec les membres de l'équipe, ce qui facilite la collaboration tout en maintenant la sécurité.
3. ***Authentification Multifacteur (MFA) :*** Prend en charge l'authentification multifacteur, renforçant ainsi la sécurité des comptes et des mots de passe.

Coût :

Variable en fonction du nombre d’utilisateurs. (Formule Business : 7.99 $ par mois)