Devolutions

[NOUVEAU] Cas d'utilisation : Les avantages de l'intégration de Remote Desktop Manager et Password Hub Business

UTILISER DES OUTILS DE GESTION DE CONNEXIONS À DISTANCE ET DE MOTS DE PASSE

De plus en plus d'entreprises ont des employés qui travaillent à distance, dans différents endroits et à différents moments de la journée. De plus, certaines compagnies comme les fournisseurs de services gérés travaillent avec des gens qui passent la majorité de leur temps (dans certains cas, 100 % de leur temps) chez leurs clients.

Cela les oblige à utiliser des outils de gestion de connexions à distance et de mots de passe, rendant leurs tâches quotidiennes exténuantes et inefficaces. Cette situation est d'autant plus susceptible d'engendrer l'insatisfaction de leurs clients, puisque les problèmes urgents ne peuvent pas être résolus rapidement.

Heureusement, **il existe une solution toute simple, c'est-à-dire intégrer Remote Desktop Manager et Password Hub Business pour obtenir le meilleur des deux mondes :**

- **Avec Remote Desktop Manager**, les utilisateurs ont accès rapidement à toutes leurs connexions à distance et informations, car toutes les données sont stockés de façon sécurisée dans le nuage.
- **Avec Password Hub Business**, les utilisateurs stockent et gèrent leurs mots de passe dans une seule solution infonuagique fiable et sécurisée.

De plus, étant donné que Password Hub Business est une source de données au sein même de Remote Desktop Manager, les employés n'ont pas besoin de lancer les deux programmes. Remote Desktop Manager et Password Hub Business sont constamment mis à jour selon les dernières améliorations, ajouts et correctifs.

Dans notre nouveau cas d'utilisation, vous découvrirez **comment intégrer Password Hub Business dans Remote Desktop Manager :**

- **Productivité augmentée :** centralisez toutes les connexions, informations d'ordinateurs, mots de passe et autres données sensibles dans une plateforme infonuagique et sécurisée, accessible en tout temps.
- **Sécurité renforcée et conformité :** empêchez vos utilisateurs de stocker des mots de passe dans des feuilles de calcul et autres documents non sécurisés ou d'utiliser des gestionnaires de mots de passe personnels non approuvés pour les comptes professionnels.
- **Reprise et continuité des activités après un incident :** il n'est pas nécessaire de sauvegarder manuellement vos données, puisque toutes les données sont stockées automatiquement et de manière sécuritaire dans le nuage. Elles peuvent être récupérées instantanément en cas de panne de courant, de cyberattaque ou tout autre problème/urgence.

Cliquez ici pour télécharger le cas d'utilisation [PDF].

Cliquez ici pour accéder à la liste complète des cas d'utilisation.