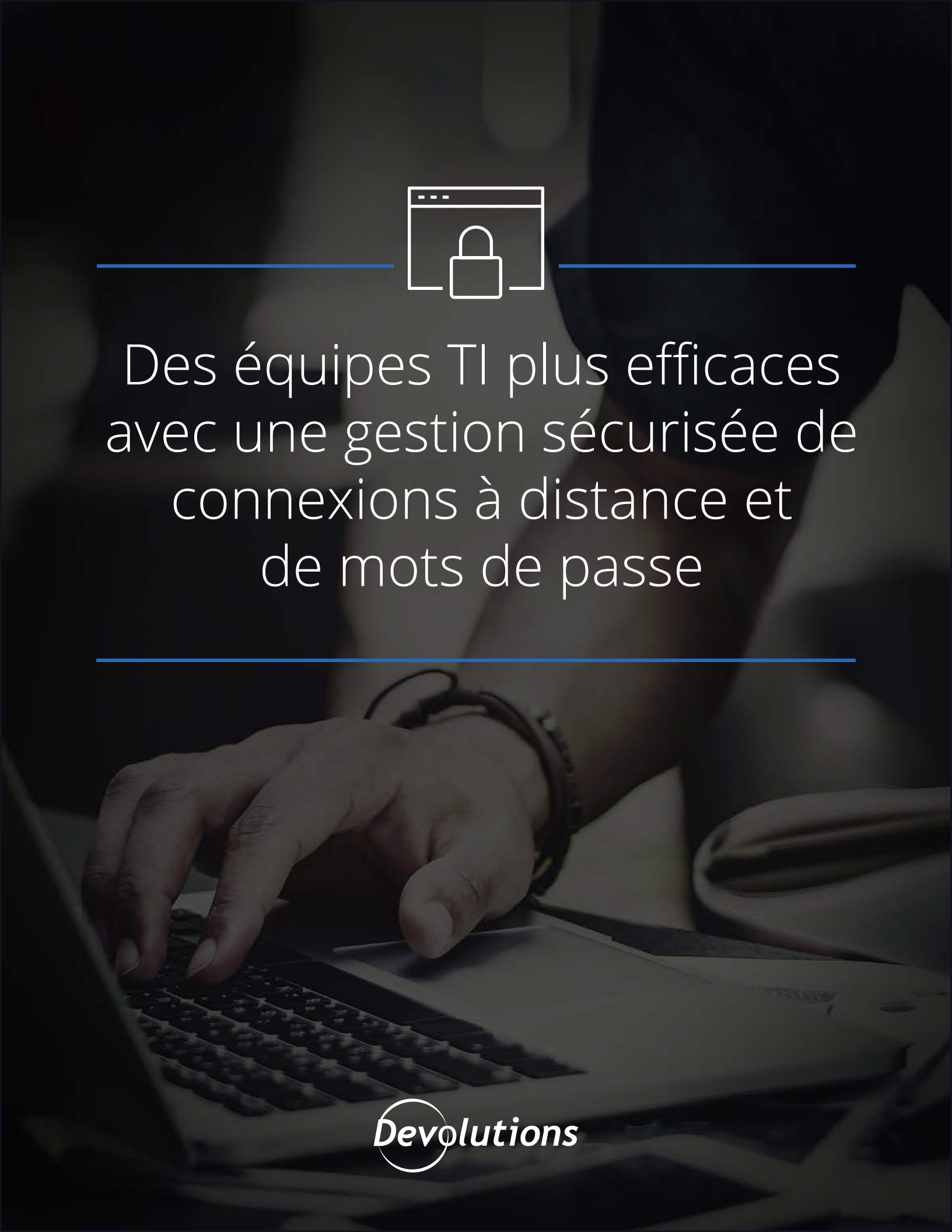
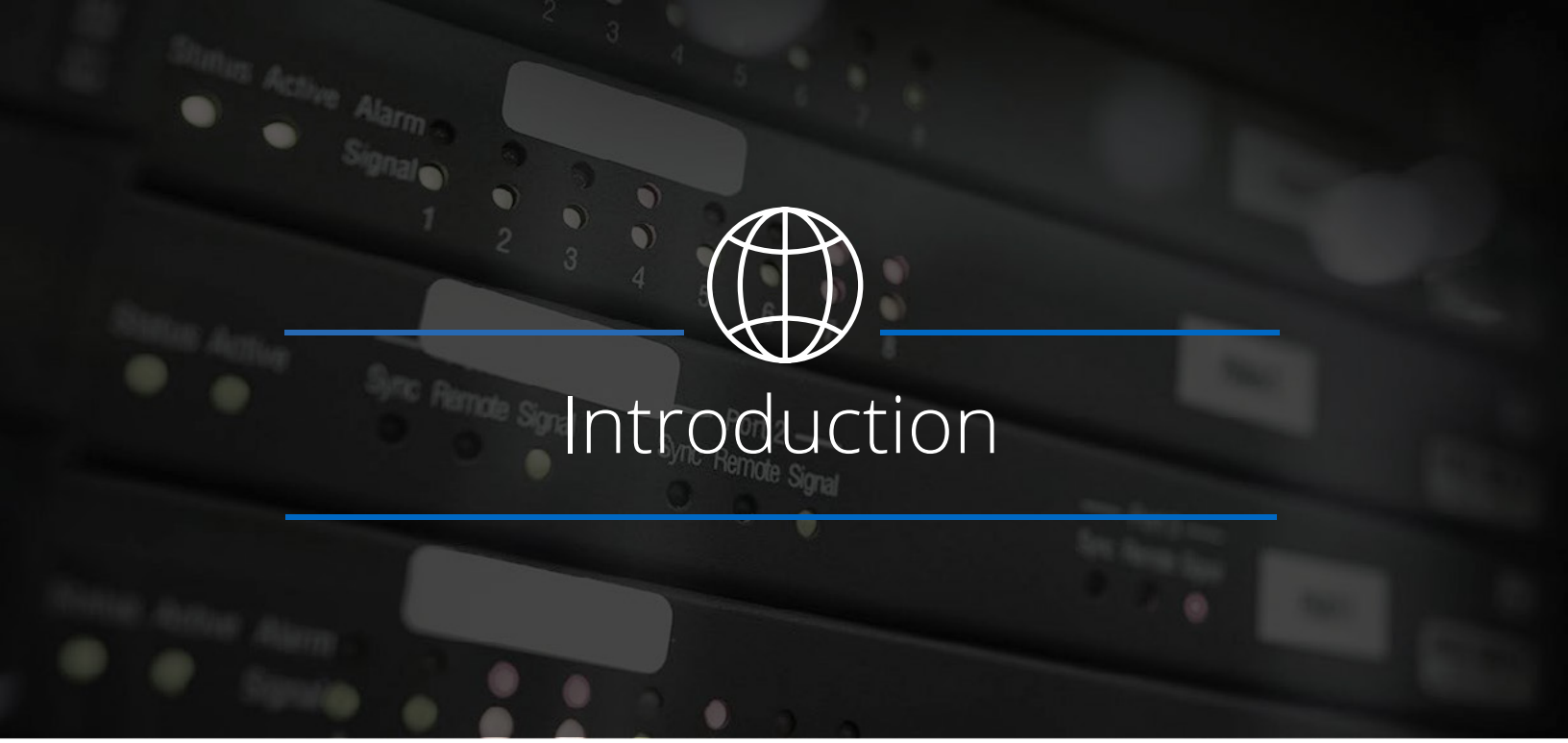


Des équipes TI plus efficaces avec une gestion sécurisée de connexions à distance et de mots de passe

Devolutions

Table des matières

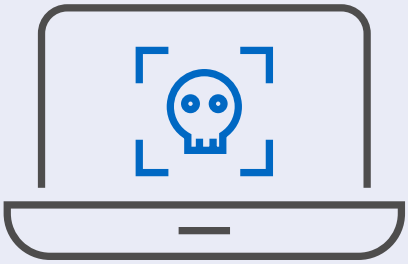
Introduction	3
Identifier les points faibles des TI	5
Choisir une solution sécurisée de gestion de connexions à distance et de mots de passe	10
Mettre de l'ordre dans le chaos informatique	15



Introduction

Nous entendons souvent des histoires qui confirment le fait que la sécurité est un énorme défi pour les équipes TI. De nouveaux records ont été battus pour le nombre de brèches et de fichiers volés en 2016. Sur 4 149 violations de données confirmées, plus de 4,2 milliards de dossiers ont été exposés, soit environ 3,2 milliards de plus qu'en 2013, l'année qui détenait précédemment tous les records. Les entreprises ont été les plus durement touchées avec 55 % des violations de données. Elles sont suivies par les institutions médicales et les agences gouvernementales.[2]

La brèche rapportée par Yahoo l'année dernière montre à quel point les entreprises sont vulnérables face au piratage : 500 millions de comptes d'utilisateurs ont été piratés en 2014 et plus d'un milliard de comptes ont été piratés en 2013. Quelle est la première défense contre ce genre d'attaques? Ne jamais utiliser le même mot de passe pour différents comptes. Cela est particulièrement critique pour les environnements de travail où les utilisateurs se connectent à de nombreux systèmes et comptes différents. Faire en sorte que les utilisateurs suivent cette pratique est toutefois tout un défi, demandez à n'importe quel expert de l'informatique.



4 149

violations de données confirmées en 2016

Le problème devient encore plus complexe quand on considère qu'il existe de plus en plus de programmes BYOD (apportez votre propre appareil), que la diversité technologique est bien acceptée et que les entreprises doivent composer avec une variété d'appareils qui sont connectés à différents terminaux de l'entreprise. Le département des TI doit pouvoir accéder à tous les appareils et ces derniers peuvent se trouver partout dans le monde. Comment les équipes TI sont-elles en mesure de gérer toutes ces connexions à distance ainsi que chaque mot de passe utilisateur différent (ou pas assez différent), tout en protégeant les données de l'entreprise contre les attaques?

Quand nous parlons de solutions de gestion de connexions à distance et de mots de passe, il existe un mantra que nous devrions tous respecter : plus la solution est simple, mieux c'est. Savoir quoi chercher dans ce type de solution peut toutefois être difficile. D'un point de vue informatique, une solution de connexion à distance doit non seulement faciliter la visualisation de l'ordinateur d'un utilisateur distant, mais également garantir la sécurité du réseau, des mots de passe et autres informations d'identification.

Ce document technique explore certains des défis auxquels sont confrontés les experts TI au quotidien dans les environnements de bureau à distance, ainsi que les types de fonctionnalités à prendre en considération quand vient le temps de choisir une solution. Avec les bons outils, les professionnels de l'informatique d'aujourd'hui peuvent fournir un service d'assistance rapide et efficace et aider leur organisation à devenir plus agile et connectée.

Avec les bons outils, les professionnels de l'informatique d'aujourd'hui peuvent fournir un service d'assistance rapide et efficace et aider leur organisation à devenir plus agile et plus connectée.

Identifier les points faibles des TI

Que votre entreprise possède des bureaux dans le monde entier, dans tout le pays ou dans une seule ville, votre équipe TI doit fort probablement se connecter à des appareils ou des systèmes qui peuvent se trouver un peu partout. La gestion sécurisée des protocoles de connexion, des mots de passe, des paramètres de configuration et de l'accès aux appareils est pratiquement impossible sans la bonne solution.

Les professionnels de l'informatique sont confrontés à des défis universels.

- **Mots de passe et données mal conservés**
- **Gestion de différentes technologies de connexion à distance et de protocoles**
- **Contrôles d'accès, autorisations et paramètres de session non surveillés**
- **Systèmes confus et désorganisés**

Mots de passe et données mal stockés

Sécurité des appareils, chiffrement et gestion des mots de passe… Ces trois éléments font partie des préoccupations constantes des experts TI. Lors d'une journée normale, une organisation peut avoir des centaines d'informations d'identification à gérer et d'autres types de données sensibles comme des numéros de compte, des informations de carte de crédit, des codes de licence, etc. Ces données doivent être gérées de manière sécurisée tout en étant facilement accessible, en respectant les mandats de réglementation et de conformité en place.

Les problèmes fréquents liés aux mots de passe incluent le choix de mots de passe faibles, la réutilisation des mots de passe, la rotation des mots de passe, le refus de changer les mots de passe et le partage de mots de passe, que ce soit volontairement ou par inadvertance (par exemple, des notes autocollantes sur un écran). Advenant une faille de sécurité, il y a de fortes chances que le pirate pénètre dans le réseau en utilisant des mots de passe faibles, partagés ou réutilisés. Le service informatique doit pouvoir être sûr que, quel que soit le choix des utilisateurs, il y a une solution de gestion de mots de passe solide qui veille au grain.

Lors d'une faille de sécurité, il y a de fortes chances que le pirate pénètre dans le réseau en utilisant des mots de passe faibles, partagés ou réutilisés.

Gérer différentes technologies de connexion à distance et de protocoles

Chaque ticket d'aide peut être différent. Avec des dizaines de gestionnaires de bureau et de types de connexion parmi lesquels choisir, l'écran d'un spécialiste de l'informatique peut devenir un chaos de fenêtres ouvertes qui exécutent RDP, des services de terminaux, Citrix, LogMeIn, Putty, TeamViewer, FTP, HP RGS, VNC, des RPV, LastPass, KeePass et plus encore.

La connexion manuelle sur tous ces systèmes peut prendre du temps, surtout quand d'autres tâches s'accumulent. Au-delà de la charge de travail, rester à jour sur les coûts et les exigences des licences logicielles est un autre travail en soi. Pas besoin de mentionner que ce n'est pas l'idéal de découvrir qu'une licence a expiré lorsqu'on tente de se connecter.

La diversité des interfaces d'utilisateurs et des systèmes d'exploitation offerts aujourd'hui ne fait qu'ajouter au défi. Si une solution basée sur Microsoft avait pu être suffisante dans le passé, les départements informatiques d'aujourd'hui doivent composer non seulement dans les environnements de bureau Microsoft et Apple, mais également dans des environnements mobiles tels qu'Android ou iOS. Avant de contacter un utilisateur pour résoudre un problème, le service informatique doit disposer des bonnes informations sur son appareil pour s'assurer qu'il n'est pas en train de résoudre un problème PC sur un ordinateur Apple.

Contrôles des accès, des autorisations et des paramètres de session non surveillés

Peu importe le nombre d'utilisateurs dans une entreprise, la sécurité informatique est toujours un enjeu, et cela va de soi pour les TI. Lorsque vous travaillez dans des environnements de bureau à distance, le partage des paramètres de connexion et des informations d'identification peut prendre du temps : surtout quand il y a un problème délicat qui nécessite l'aide immédiate d'un collègue. En même temps, quand il est question de sécurité, certaines tâches et autorisations doivent être séparées pour garantir que certains membres de l'équipe ne voient que ce qu'ils sont autorisés à voir.

S'il est possible qu'un membre de l'équipe TI ait besoin de l'aide d'un collègue pour résoudre un problème, le partage d'écran ou d'interface peut entraîner des fuites d'informations sensibles ou accorder à un utilisateur des accès qu'il n'est pas censé avoir. Si le contrôle des accès, les autorisations et les paramètres de session ne sont pas définis pour prendre en compte chaque utilisateur spécifique, vous créez des lacunes dans vos protocoles de sécurité qui peuvent exposer votre organisation à des risques.

S'il est possible qu'un membre de l'équipe TI ait besoin de l'aide d'un collègue pour résoudre un problème, le partage d'écrans ou d'interfaces peut entraîner des fuites d'informations sensibles ou accorder à un utilisateur l'accès à des niveaux du système auxquels il n'a pas accès sur ses propres ordinateurs.

Systèmes désorganisés

Avec plusieurs (et parfois des milliers) d'appareils et de mots de passe à gérer, la confusion peut rapidement s'installer et diminuer la productivité. Lorsque les professionnels de l'informatique doivent se déplacer entre des sessions et des paramètres différents, non seulement il y a beaucoup de mots de passe et d'identifiants à enregistrer et à mémoriser, mais il est très probable que des raccourcis soient pris. Cela expose l'organisation à des risques de sécurité. Sans oublier que des flux de travail inefficaces peuvent entraîner une perte de temps et de productivité. C'est particulièrement le cas lorsque des informations importantes sont stockées dans des systèmes disparates qui ne communiquent pas bien entre eux ou ne peuvent pas communiquer du tout.

L'expérience utilisateur est un autre problème. Alors que les employés s'attendent de plus en plus à une « expérience consommateur » avec leurs outils de travail, les systèmes technologiques dont ils héritent au travail peuvent les repousser. Il est vrai que les systèmes peuvent parfois être frustrants à utiliser, surtout quand une simple tâche du quotidien nécessite une formation spécifique. La technologie évolue rapidement. Il est donc préférable d'avoir des systèmes conçus pour évoluer avec l'organisation au fil du temps, et non de maintenir les gens enfermés dans des flux de travail et des processus inefficaces.

Comment les experts TI, déjà surchargés, peuvent-ils suivre et sécuriser tous ces morceaux de casse-tête sans investir dans un autre système complexe et coûteux?

Choisir une solution de gestion de connexions à distance et de mots de passe sécurisée

Les solutions de gestion de connexions à distance et de mots de passe se présentent sous différentes formes, avec des fonctionnalités qui varient en complexité. Alors que les solutions de gestion des accès privilégiés (de l'anglais *Privileged Access Management* ou PAM), par exemple, peuvent fonctionner pour certaines organisations, la réalité est que les budgets sont presque toujours serrés et il n'y a souvent pas assez d'employés au sein des départements informatiques. En revanche, personne ne peut se permettre un réseau non sécurisé.

Une solution de gestion de connexions à distance et de mots de passe facile à utiliser, abordable et robuste peut donc être une bonne option. Cette solution peut protéger contre les failles de sécurité, simplifier le flux de travail quotidien des départements informatiques, sécuriser tous les mots de passe et augmenter la productivité à l'échelle de l'organisation, tout en réduisant les coûts et la complexité. Idéalement, la bonne solution faciliterait également l'ajout de fonctionnalités quand cela est nécessaire, parce que les besoins de l'entreprise évoluent au fil du temps.

Voici les fonctionnalités les plus importantes que les professionnels TI devraient prendre en compte quand vient le temps de choisir une solution :

Stockage de données et de mots de passe unifié

Liberté de travailler dans différents environnements distants

Contrôle d'accès basé sur les rôles

Interface utilisateur intuitive et conviviale

Stockage de données et de mots de passe unifié

En centralisant tous les mots de passe et les données de votre entreprise dans un emplacement sécurisé, votre département informatique peut accéder rapidement aux informations dont il a besoin, quand il en a besoin, tout en assurant la sécurité des sessions à distance. Lorsque vous recherchez une solution de gestion de connexions à distance et de mots de passe, assurez-vous que votre système permet l'intégration avec d'autres gestionnaires de mots de passe existants. De cette façon, le département informatique y a toujours accès, même lorsque les utilisateurs stockent leurs noms d'utilisateur et mots de passe dans d'autres outils.

Cette intégration peut également offrir une flexibilité et des options de sécurité améliorées pour la connexion automatique, ce qui permet de gagner du temps et de protéger les données.

Les utilisateurs ont aussi différentes préférences de navigateur Web. La solution que vous choisissez doit avoir des extensions qui fonctionnent de la même manière, quel que soit le navigateur dans lequel les employés travaillent (Edge, Google Chrome, Firefox, etc.). À noter que les utilisateurs et le département informatique gagnent du temps si la solution peut remplir automatiquement des formulaires Web.

En centralisant tous les mots de passe et les données de votre entreprise dans un emplacement sécurisé, votre département informatique peut accéder rapidement aux informations dont il a besoin, quand il en a besoin, tout en assurant la sécurité des sessions à distance.

Liberté de travailler dans différents environnements distants

Si vous passez souvent d'une session de bureau à distance à une autre, assurez-vous de choisir une solution qui vous facilite la tâche. Avec une interface unique, le service informatique peut gagner du temps en passant à différentes sessions, accéder rapidement aux bons outils et fournir une meilleure assistance.

La solution doit simplifier la gestion des connexions en autorisant les connexions automatiques pour différents types de sessions. De cette façon, le service informatique peut passer d'une connexion à une autre sans avoir à rechercher ou à essayer de se souvenir des mots de passe ou des informations d'identification qui n'ont pas été utilisés depuis des mois. En enregistrant les informations d'identification dans la base de données locale ou dans une application externe, le département informatique peut être certain que les données sont conservées en toute sécurité.

Les professionnels de l'informatique qui ont besoin d'accéder à des machines distantes doivent non seulement être certains que la connexion est sécurisée, mais aussi qu'ils peuvent se connecter à une machine sans perdre de temps. La solution de connexion à distance idéale devrait permettre tout cela en exigeant simplement un nom d'hôte et une adresse IP. Enfin, choisissez une solution qui peut facilement importer des sessions à partir d'autres outils de gestion de connexions à distance, pour que le département informatique puisse travailler de manière transparente entre les différents environnements.

Contrôle d'accès basé sur les rôles

Les TI ont besoin d'une solution capable de contrôler les autorisations et les droits des utilisateurs avec un contrôle d'accès basé sur les rôles. Cela permet aux utilisateurs de se sentir en sécurité quand ils partagent des informations, puisqu'ils savent que les contrôles appropriés sont en place. La bonne solution doit sécuriser, organiser et stocker toutes les données sensibles dans un seul système, tout en contrôlant l'accès afin que seules les bonnes personnes puissent les voir.

Pour gérer les documents, la bonne solution doit permettre un stockage centralisé des données. Mieux encore, cette solution devrait servir à la fois les utilisateurs du nuage et sur site en fournissant un accès à tout moment aux documents et aux fichiers.

Aussi, si vous avez besoin de produire des rapports, la solution doit simplifier la récupération et l'exportation des données dans un format facile à utiliser.

Cette solution devrait servir à la fois les utilisateurs du nuage et sur site en fournissant un accès à tout moment aux documents et aux fichiers.

Une interface utilisateur intuitive et conviviale

Parce que les utilisateurs sont généralement le maillon le plus faible en matière de sécurité, l'expérience utilisateur est cruciale. Une expérience utilisateur puissante et flexible peut contribuer à accroître la satisfaction et la productivité des employés. Recherchez une interface personnalisable, afin que les utilisateurs puissent travailler comme ils le souhaitent.

De plus, le fait de pouvoir stocker et accéder aux sessions précédentes peut aider le département informatique à détecter les problèmes courants et à les résoudre plus rapidement. Lorsqu'il y a plusieurs connexions, types d'appareils et environnements à gérer, cela peut devenir frustrant. Une interface d'utilisateur intuitive peut aider le département informatique à rester organisé, faciliter le stockage et l'accès aux informations tout en offrant une expérience unifiée.

Recherchez aussi une solution qui donne accès à des modèles de dépannage prédéfinis que les TI peuvent partager avec les utilisateurs, afin qu'ils puissent documenter ou même résoudre leurs problèmes eux-mêmes. Cette fonctionnalité peut vous faire gagner beaucoup de temps.

Mettez de l'ordre dans le chaos informatique

Les professionnels de l'informatique sont les gardiens d'une organisation. Leur travail consiste à assurer le fonctionnement efficace et productif de l'entreprise, tout en garantissant la sécurité des actifs matériels et logiciels. En matière de gestion de connexions à distance et de mots de passe, le service informatique a besoin des bons outils pour assurer la sécurité de son organisation, sans toutefois y passer tout son budget.

Pour les organisations qui doivent composer avec des ressources limitées, les solutions de gestion des accès et des mots de passe réduisent la complexité et fournissent une meilleure visibilité sur le comportement des utilisateurs. Ils facilitent aussi l'application des politiques de sécurité. Résultat? Le département informatique et le reste des employés sont plus efficaces.

Grâce à une solution moderne de gestion des connexions à distance et des mots de passe, le département informatique peut mieux contrôler le chaos en réduisant la complexité et les coûts associés aux autres solutions, sans sacrifier la sécurité.

En matière de gestion de connexions à distance et de mots de passe, le service informatique a besoin des bons outils pour assurer la sécurité de son organisation, sans y passer tout son budget.

Remote Desktop Manager peut vous aider

Vous souhaitez en savoir plus? Remote Desktop Manager de Devolutions vous permet de centraliser toutes vos connexions à distance, mots de passe et identifiants dans une plateforme unique qui peut être partagée en toute sécurité entre les utilisateurs.

Téléchargez une version d'essai de 30 jours ›

Devolutions

Sources

[1] https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

[2] http://www.nbcnews.com/tech/tech-news/more-4-billion-data-records-were-stolen-globally-2016-n714066

[3] https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html