LastPass •••|

FICHE PRODUIT LASTPASS BUSINESS

Gestion des mots de passe pour votre organisation tout ENTIÈRE

Une solution de gestion des mots de passe doit couvrir tous les employés, pas seulement certains services ou individus.

Limiter le déploiement d'une solution de gestion des mots de passe à certains services de votre organisation permet aux risques et vulnérabilités de perdurer, voire de s'aggraver. Dans l'environnement de travail actuel, la présence en ligne des employés n'a jamais été aussi importante, puisqu'ils y passent 70 % de temps en plus. En outre, la réutilisation des mots de passe augmente : 92 % des gens savent qu'il est risqué d'utiliser un même mot de passe ou une variation, mais ils sont 65 % à le faire quand même. Même si vous mettez en œuvre des mesures de sécurité dans votre organisation, certaines personnes continueront à avoir une mauvaise hygiène des mots de passe si elles ne sont pas équipées des bons outils pour faire autrement.

Les mots de passe sont comme des clés universelles qui ouvrent toutes les portes de votre organisation, que ces portes soient fréquemment utilisées ou non. Alors que le travail flexible se répand, de nouvelles portes sont ajoutées, et la clé est d'autant plus universelle. Prenez par exemple le fait que 50 % de comptes en ligne supplémentaires ont été créés, selon une étude réalisée deux années de suite. Et que seulement 32 % des comptes professionnels étaient protégés par un mot de passe fort.

Toute personne de votre organisation qui crée, gère ou partage des mots de passe faibles ou réutilisés partage potentiellement les clés de votre entreprise. Fournissez un gestionnaire de mots de passe à tout le monde via une licence sur site LastPass pour éliminer à la fois la lassitude à l'égard des mots de passe et une mauvaise posture de sécurité.

Collaboration sécurisée et rationalisée

Les employés peuvent partager des identifiants en accordant (et révoquant) l'accès en temps réel à des comptes individuels ou à des dossiers partagés, en interne et en externe. Masquez les mots de passe eux-mêmes en permettant aux gens de lancer le compte partagé à partir d'un coffre-fort LastPass. La collaboration n'a jamais été aussi facile, en assurant l'efficacité tout en renforçant la sécurité.

Intégration avec les technologies existantes pour combler les lacunes de sécurité

Certains pensent que déployer une solution de sécurité permet de couvrir tout l'environnement numérique, alors que ne déployer qu'une solution d'authentification unique (SSO), par exemple, ne protège qu'une partie des applications. Et le SSO est souvent déployé pour protéger des solutions professionnelles, comme Workday et Slack. Mais que se passe-t-il si vos employés utilisent leur appareil professionnel à des fins personnelles, ou inversement ? Utilisez la gestion des mots de passe pour enrichir ou intégrer les technologies les plus utilisées dans votre entreprise, pour être sûr que chaque point d'accès est sécurisé.

*Rapport sur la psychologie des mots de passe de 2021

Déployez dans toute l'entreprise, faites d'importantes économies et obtenez l'assentiment de tous

Une licence sur site LastPass fournit un compte LastPass Business à chaque employé de votre organisation à un prix forfaitaire au lieu d'un prix par poste. Cette option vous permet d'adapter votre utilisation de LastPass à la croissance de votre entreprise, sans frais supplémentaires. Vous pouvez également bénéficier de l'assistance d'un Responsable de la réussite client (CSM) lors du déploiement de LastPass dans votre organisation. En outre, chaque détenteur d'un compte LastPass Business bénéficie également d'un compte Families gratuit et de cinq autres comptes gratuits pour ses proches.

Gestion de mots de passe pour tout le monde : identifiez des cas d'utilisation courants et sécurisez votre entreprise

SI	Le service informatique gère de gros volumes de mots de passe pour sécuriser ses infrastructures techniques et de sécurité, et assurer le bon fonctionnement de l'entreprise. Pour gérer les serveurs ou les tâches administratives, le SI a besoin d'une solution simple pour sécuriser et partager des identifiants afin d'assurer la protection des données, permettre l'inscription rapide des employés, afin que les problèmes soient l'exception et pas la norme.
Ventes et développement commercial	Ces équipes utilisent un certain nombre d'outils de gestion de la clientèle, de bases de données et de logiciels d'automatisation pour gérer la relation client et les revendeurs. En outre, ces personnes ont tendance à être en déplacement, à utiliser des appareils mobiles, à se connecter à différents réseaux Wi-Fi, et donc à augmenter leur exposition aux vulnérabilités numérique.
Marketing	Les équipes marketing utilisent des sites web et des outils pour les RP, les campagnes et l'analyse de données, et interagissent fréquemment avec des partenaires externes pour obtenir d'autres services. Une étude récente de Gartner montre que les dépenses technologiques des services marketing dépassent celles du service informatique. De nombreuses personnes finissent par partager une seule licence pour ces outils.
Réseaux sociaux	L'équipe de community management gère souvent des douzaines (parfois des centaines) de comptes sur les réseaux sociaux, ainsi que des outils de création et distribution de contenus et d'analyse de données. Bon nombre de ces services ne prennent pas en charge le SSO SAML et ne peuvent donc pas être fédérés, surtout lorsque les identifiants sont partagés entre plusieurs personnes.
Ingénierie et développement	En tant que pilier de nombreux produits, cette équipe doit partager des informations confidentielles de l'entreprise, exploiter des outils et des équipes internes et externes pour réaliser des mises à jour, ou pour sortir des produits dans des délais serrés.
Ressources humaines	L'équipe des ressources humaines utilise généralement des outils de gestion du recrutement, de la paie, des prestations sociales, des performances et de la présence. Lorsque des employés rejoignent ou quittent l'équipe, ils doivent être ajoutés ou supprimés rapidement de l'annuaire.
Finance/ comptabilité/ juridique	Les équipes financières, comptables ou juridiques utilisent généralement des outils pour gérer les budgets, la trésorerie, les dépenses, les cartes bancaires de l'entreprise, les signatures électroniques et les prises de décision stratégiques, soit les données les plus confidentielles de votre entreprise.
Assistance/ service clientèle	Cette équipe utilise généralement des outils de gestion des tickets d'assistance, de signalement et de suivi de bugs et de test et de dépannage des produits. Cette équipe a souvent besoin d'un accès instantané de partout et d'un gestionnaire de mots de passe qui intègre des règles qui le permettent.
Tous les autres	Consultants, stagiaires, responsables administratifs, directeurs de l'exploitation, la liste est longue. Que votre entreprise compte quelques individus, plusieurs services ou des équipes petites ou grandes, tout le monde doit pouvoir collaborer en toute sécurité. Tout le monde a besoin d'un gestionnaire de mots de passe.

Nous contacter

Ne laissez pas un seul mot de passe réutilisé mettre l'ensemble de votre entreprise en danger.