LastPass pour les services professionnels

Ce secteur comprend la comptabilité et les audits, le conseil, l'ingénierie et l'architecture, les technologies de l'information, les services juridiques ou encore le marketing et la publicité.

Les pratiques à risque en matière de mots de passe sont doublement problématiques pour les services professionnels

Les entreprises sur le secteur des services professionnels fournissent à leurs clients des services spécialisés et fondés sur des savoirs particuliers, qui passent par une relation contractuelle et un fonctionnement en prolongement des équipes internes. Elles sont responsables de la gestion et de la protection de leurs données et de celles de leurs clients, et sont donc une cible potentiellement lucrative pour les cybercriminels.

Le piratage d'identifiants est le moyen le plus simple d'obtenir un accès illicite à ces informations, et il ouvre la voie à des fuites de données, des détournements de fonds et des atteintes à la réputation. Pour les clients, ces fuites peuvent entraîner une perte de confiance, des pertes financières et l'exposition d'informations confidentielles, avec des effets domino pour d'autres entreprises ou secteurs d'activité.

Au-delà des risques de sécurité, les besoins en matière d'accès et de collaboration posent également des problèmes conséquents sur ce secteur. Les échanges d'informations sont monnaie courante, comme les identifiants d'accès aux applications, aux comptes sur les réseaux sociaux ou encore aux bases de données, tant par des collaborateurs internes qu'externes. Sans outils efficaces pour accorder, gérer et révoquer les accès, l'exploitation peut souffrir d'inefficacités, de pertes de productivité et de failles de sécurité involontaires.

74 % des fuites intègrent un facteur humain, comme l'utilisation d'identifiants volés, l'ingénierie sociale ou des erreurs.

10 % de la cybercriminalité dans les services professionnels résulte d'erreurs.

Une gestion des accès pratique et sûre

Parmi les leaders mondiaux de la gestion des mots de passe et des identités, LastPass est particulièrement bien placé pour résoudre les problèmes d'identifiants que rencontrent les fournisseurs de services professionnels. Conçu pour répondre aux exigences d'un secteur particulièrement collaboratif et dépendant des identifiants, LastPass permet aux organisations de créer, stocker, gérer, partager et protéger les identifiants sensibles sans sacrifier la sécurité, la confidentialité ou la convivialité. En fournissant une plate-forme centralisée et sécurisée, LastPass élimine le risque d'une mauvaise gestion des identifiants, et assure la protection des données métier et client contre les accès non autorisés.

LastPass simplifie la collaboration en permettant le contrôle et la sécurisation des accès aux identifiants partagés par les équipes internes et les sous-traitants. Grâce à une gestion simple des accès, les membres des équipes ne voient que ce dont ils ont besoin, tandis que la révocation automatique garantit la suppression rapide des accès lorsqu'ils ne sont plus nécessaires. En outre, LastPass fournit des outils de reporting et de visibilité avancés qui aident les entreprises à assurer la conformité et à surveiller l'utilisation des identifiants. Avec LastPass, les fournisseurs de services professionnels peuvent rationaliser la collaboration et renforcer la sécurité pour protéger en toute confiance leur activité comme leurs clients.

Les avantages de LastPass pour les services professionnels

Le moyen le plus simple, abordable et fiable pour les fournisseurs de services professionnels de diminuer radicalement les risques de cyberattaques et opérationnels consiste à standardiser la gestion des mots de passe avec LastPass à l'échelle de l'entreprise.

Sécuriser	**Empêcher les accès non autorisés**	Empêchez les acteurs malveillants et les utilisateurs non autorisés d'accéder aux applications, aux comptes en ligne et aux informations et systèmes sensibles.
	Stopper les détournements de comptes et les fuites de données	Assurez la fiabilité et l'accessibilité des comptes et applications en ligne, et la confidentialité des identifiants.
	Contrôler le shadow IT	Donnez aux organisations une visibilité et la maîtrise des applications SaaS non approuvées et surprovisionnées, en permettant aux administrateurs de suivre le partage d'identifiants, de gérer les droits d'accès et de repérer les vulnérabilités.
	Renforcer la gestion sécurisée des accès	Intégrez de manière transparente avec les principaux fournisseurs d'identité (IdP) comme Microsoft Entra, pour améliorer la gestion des utilisateurs tout au long du cycle de vie des employés.
Se conformer	**Répondez aux conditions de cyberassurance**	Simplifiez la tâche aux organisations qui doivent répondre aux exigences de gestion des mots de passe et des accès pour obtenir une cyberassurance.
	Favoriser la conformité	Aide les organisations à répondre aux normes de conformité et réglementaires comme RGPD, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA et SOX, ainsi que les cadres de cybersécurité comme NIST, CISA, Zero Trust et NERC-CIP.
	Répondre aux exigences de sécurité des partenaires	Aide les organisations à respecter les normes de sécurité strictes de partenaires grâce à un contrôle efficace des accès, des règles de partage de mots de passe, des mécanismes d'authentification forte et des rapports exploitables.
Rationaliser	**Offrir une expérience intuitive à chaque utilisateur**	Fournit des centaines de stratégies personnalisables, des autorisations souples, des rapports détaillés et plusieurs options d'authentification, pour devenir un outil indispensable de la pile technologique.
	Standardiser la protection par mot de passe	Simplifiez la gestion des identifiants pour les employés à l'échelle de l'organisation.
	Alléger la frustration du service d'assistance	Diminuez le fardeau du service d'assistance informatique dû aux problèmes de mots de passe, comme les mots de passe oubliés et les comptes verrouillés.
Collaborer	**Maximiser le travail d'équipe grâce au partage**	Rationalisez le partage de mots de passe et d'informations à l'intérieur et à l'extérieur de l'organisation, pour stimuler la productivité et l'efficacité des partenaires, des indépendants et des télétravailleurs.
	Maximiser adoption et l'utilisation	Boostez l'adoption et l'utilisation chez les employés en offrant une interface utilisateur intuitive qui simplifie les tâches de gestion des mots de passe.
	Promouvoir une culture de la sécurité	Aidez les administrateurs à s'assurer que tous les employés contribuent activement à une culture de la sécurité, pour se protéger contre les menaces courantes comme le vol ou le piratage d'identifiants afin d'assurer la responsabilité fiduciaire.