LastPass pour les agences d'assurance

Les agences d'assurance, qui servent d'intermédiaires entre les compagnies d'assurance et les clients, offrent des conseils de choix de police, vendent divers produits d'assurance, aident à gérer les sinistres, fournissent une assistance clientèle et évaluent les risques afin de déterminer la couverture adaptée.

Les agences d'assurance doivent protéger les mots de passe comme leurs autres actifs : avec assurance.

Les données d'assurance sont intrinsèquement sensibles et confidentielles, et sont ainsi des cibles de choix pour les cyberattaques qui exploitent les identifiants. Les acteurs malveillants exploitent souvent les identifiants faibles ou volés en utilisant des techniques comme l'hameçonnage ou l'ingénierie sociale pour obtenir un accès illicite aux systèmes en exploitant les mots de passe et les identités, entraînant de possibles détournements de comptes et fuites de données. Ces incidents font courir un risque important aux agences comme à leurs clients en ruinant la confiance et en exposant des informations personnelles et financières à un usage malveillant.

La transformation numérique du secteur de l'assurance a créé des problèmes complexes de gestion des identités et des accès. Qu'il s'agisse du stockage de données sur des plates-formes dans le cloud ou de la gestion des droits d'accès des employés et des collaborateurs tiers, les agences doivent plus que jamais se prémunir contre les accès non autorisés.

Une dépendance excessive sur des systèmes obsolètes associée à une gestion inadéquate des identifiants amplifie ces vulnérabilités. La conformité avec des réglementations comme le RGPD, CCPA et HIPAA est obligatoire pour éviter les pénalités financières et des conséquences juridiques. Assurer une gestion robuste des mots de passe n'est plus une option. C'est une condition nécessaire pour protéger le fonctionnement et conserver la confiance des clients. Des dangers comme la perte de productivité, les rançongiciels, l'atteinte à la réputation et des sanctions réglementaires pèsent également sur les organisations.

De fait, plus de 88 % des leaders de l'assurance utilisent des fournisseurs tiers pour certains services, et les agences s'appuient de plus en plus sur la technologie pour fournir des solutions personnalisées en temps réel, ce qui élargit leur surface d'attaque.

Empêcher les accès non autorisés et les pertes de données

Un leader mondial de la gestion des mots de passe et des identités, LastPass est particulièrement bien placé pour résoudre les cybermenaces que les agences d'assurance doivent affronter. En se concentrant sur la protection des données sensibles, LastPass permet aux agences de créer, stocker, partager et protéger les identifiants de manière transparente, assurant la confidentialité et la disponibilité sans sacrifier la sécurité. Conçu pour répondre aux exigences d'un secteur basé sur la confiance et la confidentialité, LastPass fournit une solution centralisée pour la gestion robuste des identifiants afin de diminuer les risques associés aux fuites de données provoquées par le piratage d'identifiants.

Les agences d'assurance doivent concilier des exigences de conformité strictes et de collaboration efficace entre les employés et les fournisseurs tiers**.** LastPass fournit une plate-forme dans le cloud qui simplifie l'accès et le partage sécurisés, impose des règles sur mesure et fournit une visibilité en temps réel sur l'utilisation des identifiants. Les rapports avancés permettent aux agences de démontrer facilement qu'elles respectent les normes comme le RGPD, CCPA ou HIPAA, et d'identifier et traiter les risques avant qu'ils ne s'aggravent. Avec LastPass, les agences d'assurance peuvent protéger leur activité et leurs clients en toute confiance, et créer une base solide pour assurer croissance et fiabilité dans un monde de plus en plus dématérialisé.

Les avantages de LastPass pour les agences d'assurance

Le moyen le plus simple, abordable et fiable pour les agences d'assurance 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.