LastPass pour le commerce de détail

Les détaillants assurent la vente de biens et de services directement aux consommateurs pour leur usage personnel ou domestique. Il peut s'agir de petits commerces de proximité comme de grandes enseignes de détail internationales. Les entreprises du secteur se distinguent par des enseignes physiques de toutes tailles, des sites de e-commerce ou encore des magasins spécialisés, discount ou de proximité.

La meilleure défense des détaillants : la gestion des mots de passe.

Les détaillants de tous types sont confrontés sans relâche aux cybermenaces. Avec un volume de transactions élevé, un grand nombre d'employés et l'accès à de précieuses données de cartes bancaires, les détaillants représentent une opportunité alléchante pour le vol d'identifiants, ce qui les transforme en cibles de choix pour les acteurs malveillants qui souhaitent s'enrichir ou obtenir des données sensibles sur les clients. Les acteurs malveillants exploitent les mots de passe faibles, réutilisés ou partagés pour infiltrer les systèmes, voler des données ou entraver les opérations.

La rotation du personnel ne fait qu'aggraver le problème, car les identifiants périmés et les accès non révoqués sont autant de vulnérabilités que les pirates tentent d'exploiter. Pour les équipes informatiques et de sécurité, gérer les droits d'accès d'un personnel fluctuant et d'un nombre incalculable d'applications SaaS représente un défi permanent.

Ces risques n'affectent pas que les opérations internes. Ils affectent aussi directement l'expérience client. Sur un secteur où la fidélité aux marques n'a jamais été aussi faible, toute cyberattaque, fuite de données ou interruption de la productivité peut envoyer les consommateurs et leurs portefeuilles voir ailleurs. Un seul incident de piratage d'identifiants peut ruiner la confiance et avoir des conséquences financières et réputationnelles à long terme pour des entreprises aux marges faibles et qui affrontent une concurrence féroce.

Les petites enseignes de détail sont plus susceptibles de déclarer qu'elles sont à une attaque majeure de la fermeture définitive, avec plus d'un tiers des personnes interrogées qui répondent ainsi à la question posée par la chambre du commerce des États-Unis.

60 % des consommateurs et 74 % des consommateurs CSP+ éviteraient probablement les détaillants victimes d'une fuite récente. (Cyberint)

Ne négociez pas avec la protection des mots de passe

Un leader mondial de la gestion des mots de passe et des identités, LastPass est particulièrement bien placé pour résoudre les cybermenaces que les détaillants doivent affronter. Conçu pour le monde effréné du détail et son volume de transactions énorme, LastPass permet de créer, stocker et gérer les identifiants tout en rationalisant les accès pour les employés, les partenaires et les tiers. En éliminant les mots de passe faibles, partagés et périmés, LastPass diminue le risque de vol d'identifiants, l'une des cybermenaces les plus courantes dans le monde de détail, sans entraver le fonctionnement au quotidien.

Grâce à des outils dans le cloud simples à utiliser, LastPass allie une sécurité renforcée et une expérience intuitive, tant pour les administrateurs que les employés, quel que soit leur niveau technique. Des fonctionnalités comme le partage sécurisé d'identifiants, les inscriptions et radiations automatiques et le contrôle d'accès centralisé simplifient la gestion de la rotation du personnel, tout en bloquant les accès non autorisés aux systèmes et données sensibles. Des rapports avancés confèrent la visibilité nécessaire aux administrateurs pour imposer des règles de mot de passe, analyser les accès et démontrer la conformité.

Pour les détaillants, LastPass est la solution qui sécurise les identifiants, protège l'expérience client et assure la résilience de l'activité face à l'essor des cybermenaces.

Les avantages de LastPass pour les détaillants

Le moyen le plus simple, abordable et fiable pour les détaillants 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.