LastPass pour les services financiers

Les services financiers constituent un sous-ensemble d'une infrastructure essentielle qui englobe les comptables, les banques, les courtiers, les banques coopératives, les services de cryptomonnaie, les gestionnaires de patrimoine, les FinTech, les sociétés d'investissement, les plates-formes, etc.

Les mots de passe présentent un risque particulier pour les services financiers

Les fournisseurs de services financiers sont des cibles de choix pour les cyberattaques, car en raison de la nature transactionnelle du secteur, ces organisations sont confrontées à un rythme effréné tout en devant gérant des données sensibles sur les clients et les actifs financiers. Les acteurs malveillants ont recours à des tactiques comme les infostealers et les campagnes d'ingénierie sociale par IA pour pirater les mots de passe et les identités, aboutissant souvent à des détournements de comptes et des attaques par rançongiciel.

En outre, ces organisations adoptent de plus en plus souvent des stratégies axées sur le cloud et utilisent de nombreux logiciels-services (SaaS), compliquant d'autant la gestion sécurisée des mots de passe et des accès. L'essor souvent incontrôlé de ces applications favorise le Shadow IT, lorsque les employés utilisent des outils et des applications non autorisées, créant ainsi des problèmes de visibilité et des failles de sécurité supplémentaires.

La transition vers le travail à distance et hybride n'a fait qu'amplifier les risques liés à la collaboration et aux accès, et les failles qui sont exploitées par les pirates. Peu d'outils de collaboration à distance offrent une supervision centralisée, ce qui complique le suivi et le contrôle de l'activité des utilisateurs, et lorsque les employés utilisent des applications ou des outils non autorisés pour collaborer (comme des applications de messagerie personnelles), ils contournent les protocoles de sécurité et exposent les données à des risques. Ensemble, tous ces facteurs exposent les clients à des tentatives de fraude et d'ingénierie sociale, les employés à des inefficacités et des pertes de productivité, et les organisations à des fuites de données, des attaques par rançongiciel, une atteinte à leur réputation et des pénalités réglementaires.

Selon le rapport Verizon DBIR 2024, les intrusions dans les systèmes, les erreurs diverses et l'ingénierie sociale sont à l'origine de 78 % des fuites de données sur le secteur des services financiers.

Protection des mots de passe avancée et sécurité transparente

Un leader mondial de la gestion des mots de passe et des identités, LastPass est particulièrement bien placé pour résoudre les problèmes de cybersécurité et de productivité que rencontrent les fournisseurs de services financiers. Conçu pour répondre aux exigences complexes d'un secteur particulièrement dépendant des identifiants, LastPass permet aux organisations de créer, stocker, gérer, partager et protéger les identifiants de manière transparente, sans transiger sur la sécurité, la confidentialité ou l'accessibilité.

Les institutions financières doivent concilier sécurité et exigences de conformité strictes avec le besoin de fournir une expérience fluide tant aux administrateurs qu'aux utilisateurs finaux, y compris aux collaborateurs tiers. LastPass fournit une solution dans le cloud conçue pour répondre à ces exigences, en protégeant les identifiants sensibles, en sécurisant les accès et le partage en interne et en externe, et en imposant des règles d'accès sûres qui renforcent la visibilité et le contrôle afin d'assurer la conformité.

Grâce aux rapports avancés, les intervenants clés restent informés et sont parés pour tout audit. LastPass est ainsi un outil indispensable pour empêcher les accès non autorisés et préparer votre organisation à résister aux menaces en constante évolution.

Les avantages de LastPass pour les services financiers

Le moyen le plus simple, abordable et fiable pour les fournisseurs de services financiers de diminuer radicalement les risques de cyberattaques et opérationnels consiste à standardiser la gestion des mots de passe avec LastPass dans toute 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	**Standardiser la protection par mot de passe**	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.
	Renforcer la gestion sécurisée des accès	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.