LastPass pour le secteur de la santé

Le secteur de la santé comprend les hôpitaux, les services médicaux, les produits pharmaceutiques, les fabricants d'appareils médicaux, les mutuelles, les prestataires de santé publique et les institutions de recherche et développement, qui s'évertuent à assurer les soins et améliorer la santé. Il intègre un réseau complexe de professionnels, d'établissements et de technologies.

Empêcher les accès non autorisés est vital pour les prestataires de santé

Les prestataires de santé ont la lourde responsabilité de protéger les données sensibles des patients et des clients, y compris les informations de santé personnelles, les dossiers médicaux et les données financières relatives aux patients, aux prestataires et aux fournisseurs. Les cybercriminels ciblent de plus en plus le secteur de la santé, réputé pour une mauvaise gestion des mots de passe et un contrôle des accès défaillant qui créent de nombreuses failles. Accorder des accès superflus ou retarder la révocation des accès des sous-traitants, des prestataires et des intérimaires augmente les risques d'accès illicites et d'aggravation des failles de sécurité.

Les organismes de santé qui adoptent une stratégie axée sur le cloud ont de plus en plus de mal à gérer les mots de passe et les accès aux différents outils et plates-formes numériques de manière sécurisée. Des infrastructures dans le cloud mal configurées, des postes de travail vétustes et des appareils partagés non sécurisés créent des failles de sécurité, tandis que l'adoption rapide et parfois incontrôlée de solutions SaaS entraîne l'utilisation d'applications non autorisées qui dégradent encore la sécurité. Sans un système centralisé de gestion des mots de passe, garder le contrôle des accès et imposer des mesures cohérentes est encore plus compliqué.

Les prestataires de santé doivent respecter des normes strictes, comme HIPAA, HITECH et ACA, ce qui nécessite des audits en continu pour prouver la conformité. Une bonne gestion des mots de passe est essentielle pour éviter les pénalités et les atteintes à la réputation. En ne sécurisant pas les identifiants et les droits d'accès, les risques en matière de confidentialité des données, de conformité et de cyberassurance augmentent et peuvent entraîner des conséquences financières importantes.

Le ministère de la Santé des États-Unis (DHHS) a constaté une augmentation des fuites de données massives de 93 % entre 2018 et 2022, et une augmentation des attaques par rançongiciel de 278 % sur la même période.

Traitez les mots de passe comme vous traitez vos patients : avec le plus grand soin.

Un leader mondial de la gestion des mots de passe et des identités, LastPass est particulièrement bien placé pour résoudre les problèmes de piratage, d'efficacité et de conformité que rencontrent les organismes de santé. Spécialement conçu pour répondre aux besoins d'un secteur qui dépend des identifiants, LastPass crée, stocke, gère et partage les identifiants à l'échelle des équipes et des services, sans sacrifier la sécurité, la confidentialité ou l'accessibilité. Les prestataires peuvent réduire les risques liés aux mots de passe faibles ou mal gérés, pour se concentrer sur la fourniture de soins de qualité, en toute sécurité.

Les organismes de santé doivent concilier une sécurité stricte et une expérience conviviale pour les administrateurs informatiques, les utilisateurs finaux et les collaborateurs tiers, comme les sous-traitants, les fournisseurs et les intérimaires. LastPass fournit une solution dans le cloud qui simplifie la gestion des identifiants tout en répondant à toutes ces exigences. Il protège les identifiants sensibles et assure la sécurité des accès et du partage à l'intérieur des équipes et avec l'extérieur. Avec LastPass, les prestataires de soins peuvent mettre en œuvre des règles de sécurité granulaires qui bloquent les accès non autorisés, atténuent les menaces internes et diminuent l'erreur humaine.

En outre, les fonctionnalités de reporting avancées donnent de la visibilité sur l'activité des utilisateurs et permettent de respecter les normes comme HIPAA ou HITECH, parmi d'autres. LastPass permet aux organisations de garder une longueur d'avance sur les problèmes de cybersécurité sur le secteur de la santé, afin d'assurer tant l'efficacité opérationnelle que le respect de la réglementation.

Les avantages de LastPass pour le secteur de la santé

Le moyen le plus simple, abordable et fiable pour les organismes de santé 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.