LastPass •••|

Étude de cas : HealtheConnections

healtheconnections®

« C’est sa rapidité qui rend LastPass aussi efficace. Il est aussi simple que rapide à utiliser, et c’est pourquoi nos employés l’adorent. »

Brad Sweet, responsable des systèmes réseau et de la sécurité chez HealtheConnections

Le défi

HealtheConnections est une organisation à but non lucratif qui fournit des services d'échange d'informations de santé, des ressources en faveur de la santé publique, et des solutions à valeur ajoutée pour 26 comtés de l'État de New York, ainsi que dans les États voisins. Elle aide plus de 11 000 médecins et leurs millions de patients en gérant des portails d'accès aux dossiers médicaux dans le cloud, afin que les personnels de santé puissent y accéder rapidement en cas de besoin.

Pour pouvoir gérer ce portail en tant qu'organisation à but non lucratif, HealtheConnections devait satisfaire les critères de certification HITRUST CSF v9.5 pour le portail de fournisseurs myConnections. Brad Sweet, responsable des systèmes réseau et de la sécurité chez HealtheConnections, a compris que pour répondre aux normes HITRUST, il était essentiel d'investir dans un gestionnaire de mots de passe. Christina Anastos, spécialiste de l'assistance informatique chez HealtheConnections, avait quant à elle noté que l'hygiène des mots de passe était de plus en plus problématique au sein de l'organisation, les employés ayant recours à des feuilles de calcul protégées par mot de passe, ou notant aléatoirement des identifiants sur des blocs-notes à leur bureau.

Pour répondre aux critères HITRUST et intégrer une gestion sécurisée des mots de passe à l'échelle de HealtheConnections, Brad Sweet et Christina Anastos ont investi dans LastPass, en raison de ses capacités d'intégration, de ses stratégies personnalisables et de son interface utilisateur conviviale.

La solution

La génération de mots de passe était un problème endémique chez HealtheConnections, car les équipes avaient du mal à créer systématiquement des identifiants forts, et notaient souvent leurs mots de passe sur papier. L'outil de génération de mots de passe de LastPass produit un mot de passe unique pour chaque compte créé, et peut imposer différents critères, comme une longueur d'au moins 12 caractères, et l'utilisation de lettres, de chiffres et de symboles. Christina Anastos ajoute : *« Le générateur de mots de passe de LastPass est l'une de nos fonctionnalités préférées. En effet, nous devons souvent réinitialiser les mots de passe de tous les comptes, et le générateur simplifie ce processus pour toute l'équipe. »*

HealtheConnections voulait inaugurer une méthode sécurisée de stockage des identifiants à l'échelle des équipes. LastPass stocke tous les mots de passe ainsi que d'autres informations importantes dans un coffre-fort électronique. Il s'agit d'un espace sécurisé pour conserver les mots de passe, les notes sécurisées ou encore les informations de carte bancaire. Avec l'architecture zero knowledge de LastPass, les données dans le coffre-fort sont protégées par chiffrement AES-256 et par 600 000 itérations de hachage plus salage PBKDF2-SHA-256. Le hachage convertit les données en sorties illisibles, tandis que le salage rend chaque sortie unique et plus difficile à comparer. Brad Sweet remarque : *« Nos méthodes de gestion des mots de passe précédentes nous exposaient à des vulnérabilités, tandis qu'avec LastPass, nous pouvons créer un espace sécurisé pour que les employés puissent stocker les notes importantes et les mots de passe. »*

Le résultat

LastPass a renforcé considérablement la posture de cybersécurité de HealtheConnections, qui a pu obtenir la certification HITRUST sans encombre. Quatre ans après le déploiement de LastPass, ils ont atteint un taux d'adoption de 98 % à l'échelle de l'organisation. Brad Sweet note que le processus de mise en œuvre *« était simple et transparent, et l'aide apportée par l'équipe de LastPass nous a été d'un grand secours ! »* Pour améliorer l'utilisation et l'adoption, l'équipe de sécurité est sur le pont pour aider le personnel, et pour animer des séances de formation trimestrielles dans toute l'entreprise. En outre, pour renforcer la cyber-résilience de l'organisation, HealtheConnections a intégré l'authentification multifacteur avec Duo, ce qui leur permet de générer des codes à usage unique en tant que facteur d'authentification supplémentaire, pour plus de sécurité et d'assurance.

LastPass est devenu un outil incontournable pour les tâches quotidiennes du personnel, et un composant essentiel du processus d'inscription des nouvelles embauches.

« La réinitialisation des mots de passe est tellement plus simple avec l'outil de génération de mots de passe de LastPass, qui crée instantanément des identifiants longs et uniques prêts à exploiter. »

Brad Sweet

Christina Anastos explique, *« La sécurité est non-négociable, donc il est essentiel pour nous que nos employés exploitent tout le potentiel des fonctionnalités de LastPass pour travailler en toute sécurité. »* Ils exploitent également les stratégies personnalisables de LastPass pour automatiser la radiation des employés. Brad Sweet explique : *« Nous étions ravis de pouvoir sélectionner des stratégies adaptées à notre entreprise. Supprimer les accès au départ d'un employé était un besoin essentiel, et nous avons également imposé des règles de robustesse et de réutilisation pour améliorer notre hygiène des mots de passe générale. »*

Découvrez comment HealtheConnections a renforcé sa sécurité des mots de passe avec LastPass. Nous contacter