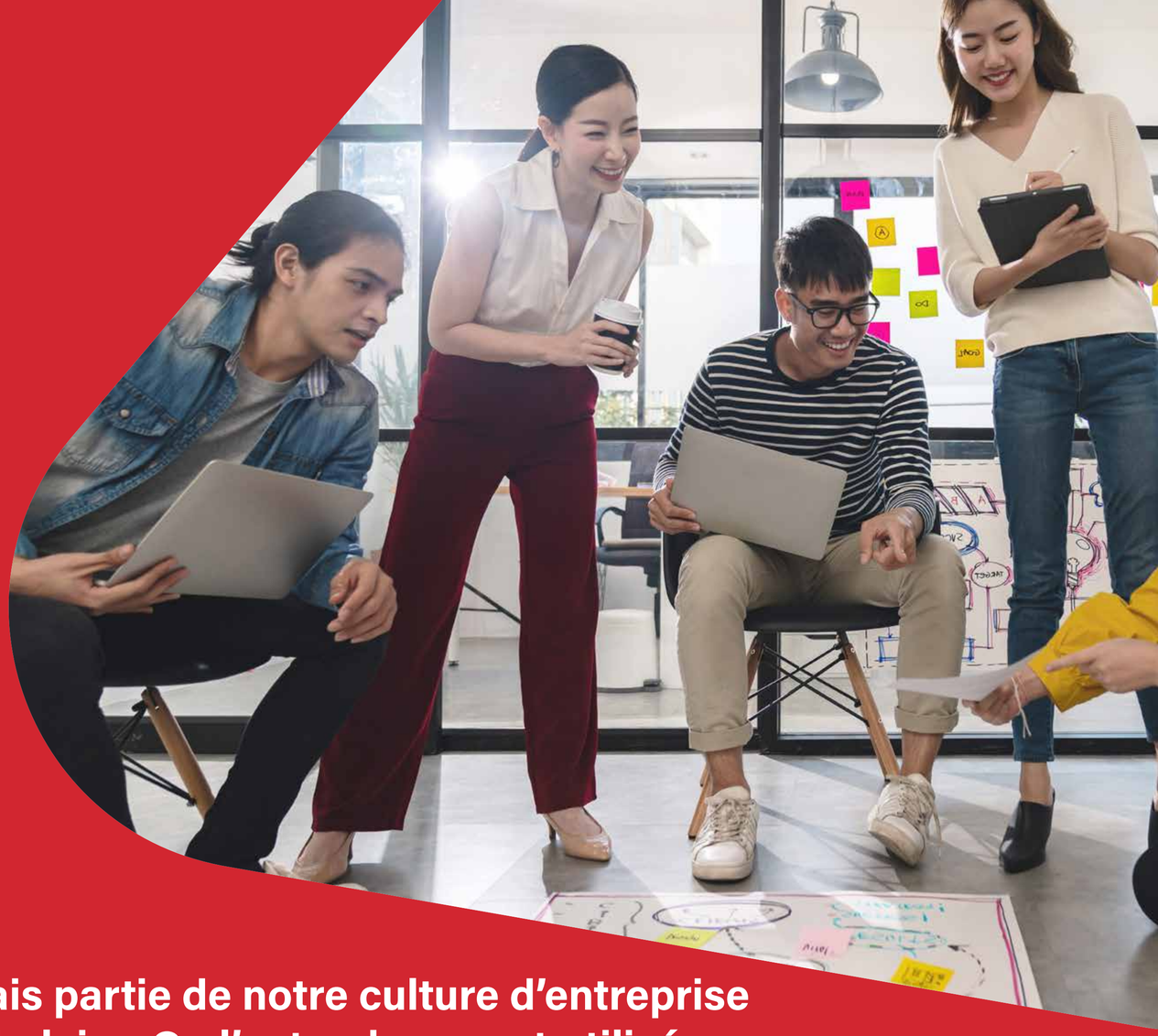
LastPass

Étude de cas : Handshakes



Handshakes

« LastPass fait désormais partie de notre culture d'entreprise et même de notre vocabulaire. On l'entend souvent utilisé sous forme de verbe dans nos bureaux, car il nous aide à effectuer nos tâches en toute sécurité. »
Kenneth Ham

Le défi

Fondée en 2011, Handshakes est une société DataTech primée qui permet aux entreprises de prendre des décisions avisées en exploitant des informations pertinentes provenant de données fiables. Présente dans six pays, incluant Singapour, l'Australie et Taiwan, la société a forgé des partenariats avec des entreprises comme Microsoft.

En prévision de leur croissance dans un environnement en pleine transformation, Kenneth Ham, directeur technique chez Handshakes, cherchait un outil de gestion des mots de passe qui pourrait aider l'organisation à améliorer son hygiène des mots de passe. Face à l'augmentation des cybermenaces, comme les attaques par « rançongiciels » et les tentatives d'hameçonnage, Kenneth Ham a compris l'importance de la sécurisation des mots de passe, et son rôle dans la protection des informations personnelles identifiables (IPI).

Kenneth Ham explique : *« Dès que nous avons mesuré le risque que posait une mauvaise hygiène des mots de passe pour notre entreprise, je savais qu'un gestionnaire de mots de passe avec un environnement Zero Trust serait la solution à nos problèmes. »*

La solution

LastPass est rapidement arrivé en tête des prétendants, puisque les clients et les partenaires de Handshakes avaient déjà plaidé en sa faveur. En travaillant avec leurs clients, ils ont découvert les avantages de LastPass pour travailler de manière sécurisée, notamment en utilisant des fonctionnalités comme le partage de mots de passe et les dossiers partagés. En étudiant l'offre disponible, Kenneth Ham s'est rendu compte qu'avec son éventail de fonctionnalités, dont plus de 100 règles personnalisables, une infrastructure de chiffrement zero knowledge et sa conformité réglementaire (SOC2, SOC3, C5, ISO 27001 et GDPR), LastPass répondait à leurs besoins.

Handshakes a immédiatement activé des fonctionnalités comme le générateur de mots de passe, le partage de mots de passe avec accès restreint de l'extérieur et les alertes de surveillance du dark web. L'objectif était d'améliorer l'hygiène des mots de passe en incitant les employés à faire de LastPass l'unique centre d'accès pour les principaux identifiants, à éliminer la réutilisation des mots de passe et à décourager le partage de données sensibles sur les serveurs par messagerie ou par e-mail.

« Avec LastPass, notre équipe a intégré l'hygiène des mots de passe à ses habitudes. »

Le résultat

Handshakes peut faire valoir avec confiance son engagement en faveur de la protection des IPI de ses clients et partenaires avec LastPass, d'autant plus que ses infrastructures sont fréquemment soumises à des audits, et respectent plusieurs normes réglementaires. L'architecture zero knowledge est conçue pour assurer que personne ne puisse accéder à vos mots de passe ou aux données stockées dans votre coffre-fort, puisque le chiffrement est effectué exclusivement sur l'appareil. Kenneth Ham remarque : *« Ni LastPass ni nos administrateurs ne peuvent accéder au coffre-fort d'un individu, et je pense que c'est très important, car un environnement Zero Trust est essentiel pour inciter les équipes à adopter le produit en toute confiance. »* C'était nécessaire pour l'équipe de développement de qui a activé la fonction de partage de mots de passe pour mutualiser et surveiller les accès à l'environnement de production.

À l'issue du déploiement, Handshakes a commencé à former ses équipes à la cybersécurité pour souligner les faiblesses, ainsi que le rôle que peut jouer un gestionnaire de mots de passe pour limiter les risques. L'interface simple et facile fut un succès immédiat, les employés ayant adopté LastPass sans difficulté pour gérer leurs mots de passe au quotidien. LastPass fait désormais partie de la culture chez Handshakes, et la solution fait désormais partie de son vocabulaire lorsque les employés veulent collaborer de manière sécurisée.

L'équipe du SI dispose d'une meilleure visibilité grâce à la console d'administration, qui leur permet de fédérer la connexion des utilisateurs, d'activer la surveillance du dark web et de générer des rapports de sécurité pour identifier les lacunes ou les marges d'amélioration. En surveillant le score de sécurité des employés au quotidien, ils ont éliminé les risques associés ou mots de passe faibles, réutilisés ou piratés, et les cyberattaques associées. L'intégration transparente de LastPass avec Microsoft Azure a également permis à Handshakes d'adopter l'authentification unique (SSO) pour fournir une expérience de gestion des identifiants de connexion optimale aux employés.

Kenneth Ham note : *« Nos équipes ont découvert qu'avec LastPass, il suffit de quelques clics pour accéder à leurs tâches. Nous sommes absolument ravis et nous le recommanderions à n'importe quelle entreprise, car il protège véritablement les équipes tout en simplifiant la cybersécurité. »*

Nous contacter