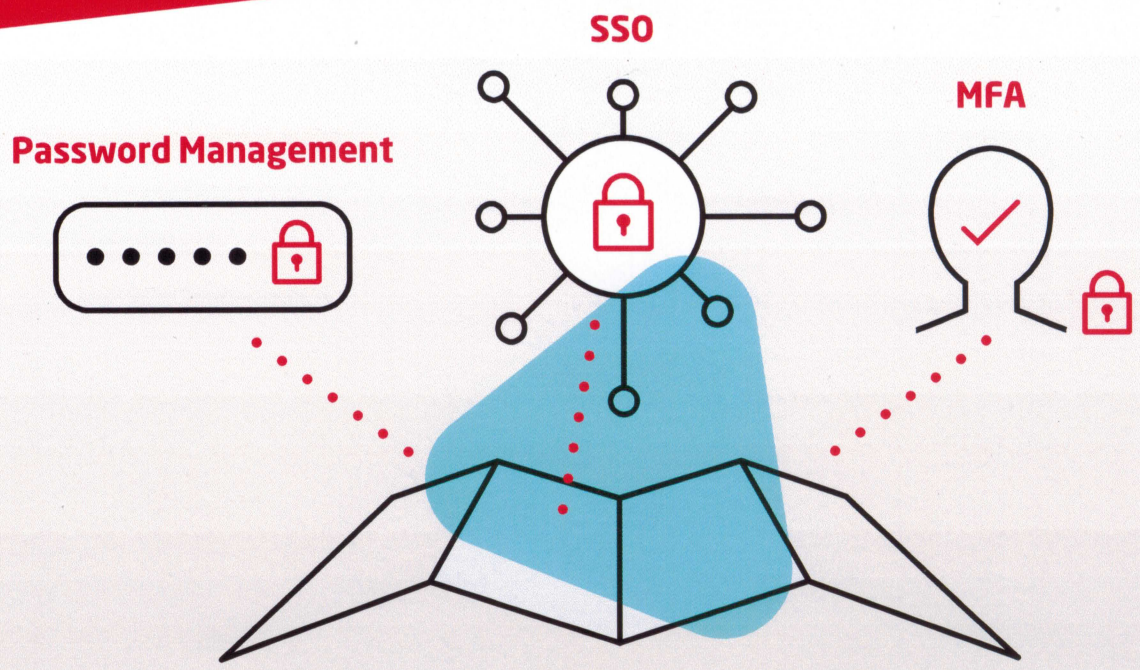
LastPass •••|

Always-on security for an always-on world.



LastPass •••|

Access & Authentication



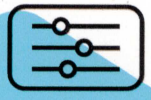


LastPass •••|

Connecter simplement et en toute sécurité les employés à leur travail.

Le service informatique doit assurer la sécurité de l'entreprise, sans nuire à la productivité.

De l'authentification à l'accès aux mots de passe, LastPass gère chaque point d'entrée dans votre entreprise, afin que vous puissiez atténuer les risques tout en améliorant la productivité des employés.



Contrôles de sécurité complets



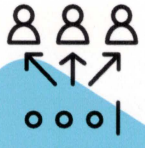
Intégrations plug-and-play



Authentification adaptative



Gestion et rapports faciles pour les utilisateurs



Partage de mot de passe pratique



Expérience utilisateur fluide



Surveillance du Dark Web



Conçu pour la sécurité avant tout



Déploiement, gestion et expérience transparents



Plus de 85 000 entre-prises utilisent LastPass



Plus de 30 millions d'utilisateurs



Un compte familial gratuit pour les employés

Protéger tous les points d'entrée de votre entreprise



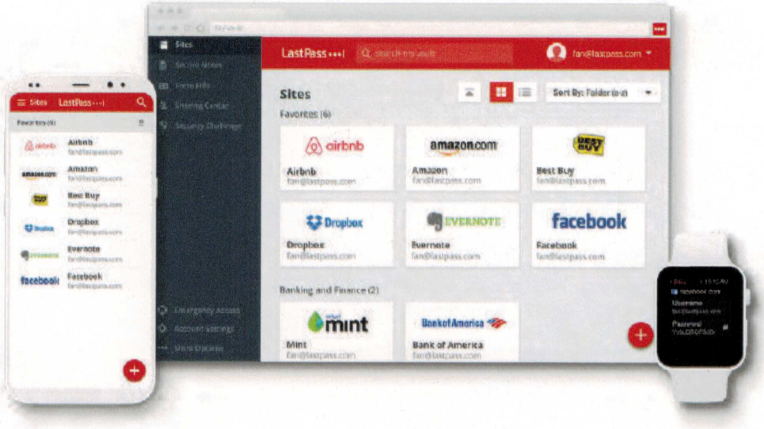
LastPass fournit des solutions d'accès et d'authentification pour les entreprises, qui offrent contrôle et visibilité aux administrateurs tout en connectant les employés à leurs tâches de façon transparente. Voici une comparaison détaillée des fonctionnalités de Teams et Business.

Ces fonctionnalités fournissent le contrôle exigé par les entreprises et le confort que demandent les utilisateurs :

	BASE	
	Teams	**Business**
Présentation	Conçu pour les équipes de 50 personnes maximum, LastPass Teams est une solution intuitive et légère pour créer, stocker et partager les identifiants de manière sécurisée, afin de limiter les risques de fuites de données liées aux mots de passe et d'améliorer l'hygiène des mots de passe.	Conçu pour les organisations et les équipes de toutes tailles, LastPass Business est une solution de gestion des mots de passe qui intègre toutes les fonctionnalités de LastPass Teams, ainsi que des fonctions d'administration plus étoffées pour rationaliser la gestion tout en diminuant les risques de fuites liées aux mots de passe. LastPass Business propose également des options d'authentification unique et multifacteur.
Tarif	$4 par utilisateur/mois	$6 par utilisateur/mois
Gestion des mots de passe	Tableau de bord pour capturer, stocker, remplir, générer et partager les mots de passe avec une gestion utilisateur simplifiée.	Gestionnaire de mots de passe professionnel complet pour capturer, stocker, remplir, générer et partager les mots de passe avec un tableau de bord d'administration robuste et un coffre-fort pour chaque utilisateur
Règles	Règles de sécurité standard de gestion des mots de passe	100+ règles personnalisables pour une souplesse absolue.
Rapports	Rapports de base, y compris sur l'activité des utilisateurs, les dossiers partagés et la sécurité.	Rapports avancés, y compris sur les nouveaux utilisateurs, l'activité des utilisateurs, la modification des règles, les demandes d'accès, la sécurité et les dossiers partagés.
Centre de partage	Partagez les identifiants en toute sécurité lorsque plusieurs collègues ont besoin d'un accès.	Partagez les identifiants en toute sécurité lorsque plusieurs collègues ont besoin d'un accès, et organisez les identifiants partagés par groupes.
Regroupement	-	Importez ou créez des groupes pour classer les utilisateurs et les dossiers partagés.
Intégration des annuaires	-	• LastPass AD Connector • Microsoft Azure AD • Okta • OneLogin • APIs d'approvisionnement sur mesure
Connexion fédérée	-	• Microsoft ADFS • Microsoft Azure AD • Okta

	BASE	
	Teams	**Business**
Commandes d'administration	-	Affectez des rôles particuliers aux administrateurs pour restreindre l'accès aux sections pertinentes de la console d'administration.
Authentification unique de base	-	Ajoutez 3 applications au portail intégré avec plus de 1 200 applications préintégrées.
Authentification multifacteur de base	Accès à l'application LastPass Authenticator pour bénéficier d'une protection par authentification multifacteur des coffres-forts.	Accès à l'application LastPass Authenticator pour bénéficier d'une protection par authentification multifacteur des coffres-forts et des applications à authentification unique.
Sécurité	Conçu sur un modèle de sécurité zéro connaissance.	Conçu sur un modèle de sécurité zéro connaissance.

	Offres supplémentaires : AUTHENTIFICATION UNIQUE AVANCÉE	
	Teams	**Business**
Présentation	-	Ajoutez un nombre illimité d'applications à authentification unique au portail intégré avec plus de 1 200 applications préintégrées.
Tarif	-	$2 utilisateur/mois
Nombre d'applications	-	Sécurisez un nombre illimité d'applications dans le cloud.
Rapports	-	Rapports détaillés automatisés sur les applications, les notifications ou encore les événements SAML.
Portail web	-	Moyen convivial pour les employés d'accéder à toutes leurs applications au sein du coffre-fort LastPass.



	Offres supplémentaires : AUTHENTIFICATION MULTIFACTEUR AVANCÉE	
	Teams	**Business**
Présentation	-	Fournissez une protection par authentification multifacteur aux applications à authentification unique, aux VPN, aux postes de travail et aux fournisseurs d'identité. Options d'administration supplémentaires, comme des règles de gardiennage virtuel et basées sur les adresses IP.
Tarif	-	$3 par utilisateur/mois
Règles	-	Activez des règles granulaires de gardiennage virtuel, horaires ou basées sur les adresses IP.
Méthodes d'authentification	-	• Biométrique (visage et empreintes) • Code PIN • Codes à 6 chiffres limités dans le temps • Notifications push en un toucher
Intelligence contextuelle	-	Authentification intelligente en fonction du contexte de la connexion : lieu, appareil et réseau.
Protection des terminaux	-	• Coffre-fort de mots de passe • Applications à authentification unique/dans le cloud • VPN • Postes de travail • Fournisseurs d'identité • Applications LDAP/RADIUS internes
Authentification adaptative	-	Associez intelligence biométrique et contextuelle pour bâtir des profils utilisateur individuels et adapter l'authentification à différentes situations.
Zéro mot de passe	-	En exploitant la biométrie et l'authentification adaptative, LastPass MFA élimine les mots de passe sur les postes de travail, pour l'authentification unique et les VPN.

Ajoutez les deux offres à LastPass Business pour bénéficier d'un tarif groupé de $9 par utilisateur/mois.

Nous contacter

En savoir plus sur LastPass Business


LastPass
While employees work anywhere. You protect them everywhere.

LastPass •••|

Éliminez le risque. Éliminez la frustration. Éliminez les mots de passe des employés.

Chaque mot de passe faible représente un risque pour l'entreprise.

- **80 %** des failles sont attribuables aux mots de passe faibles, réutilisés ou piratés.[1]
- Le partage et la réutilisation des mots de passe restent endémiques dans la plupart des entreprises, puisque les employés réutilisent en moyenne **13 fois** un même mot de passe.[2]
- Les employés de PME gèrent en moyenne **85** mots de passe.[2]

La réinitialisation des mots de passe comme les comptes verrouillés font grimper la frustration et les coûts informatiques.

- **4 heures par semaine** sont consacrées rien qu'aux problèmes liés à la gestion des mots de passe, avec 96 demandes relatives aux mots de passe par mois.[4]
- L'employé moyen utilise activement **36 services cloud** au travail.[3]
- **34 %** des employés sont confrontés chaque mois à des identifiants perdus ou volés.[2]



Le lancement de l'authentification sans mot de passe.

L'authentification sans mot de passe élimine le mot de passe de l'expérience de connexion des employés, leur offrant une façon plus fluide et sûre de se connecter à leur environnement de travail.

Cela ne signifie pas que les mots de passe ont disparu, mais qu'ils fonctionnent en coulisses, de sorte que les employés n'ont plus à les saisir.

57 % des entreprises dans le monde ont des employés qui utilisent l'authentification multifacteur (MFA), une hausse de **12 %** par rapport à 2018.[2]

36 % des responsables informatiques considèrent que la mise en œuvre de l'authentification multifacteur biométrique est une priorité.[4]

Pourquoi passer au zéro mot de passe ?

98 % des responsables informatiques estiment que leurs employés pourraient faire mieux en matière de comportements de sécurité.[4]

82 % des responsables informatiques reconnaissent que les mauvaises pratiques en matière d'identité exposent leur entreprise à des risques.[4]

59 % des responsables informatiques reconnaissent que le renforcement de l'authentification des utilisateurs est essentiel et évoquent cette stratégie parmi leurs priorités clés pour améliorer leurs capacités en matière de gestion d'identité.[4]

Optimiser l'expérience utilisateur

Éliminer les risques liés aux mots de passe

Privilégier l'authentification plus sûre

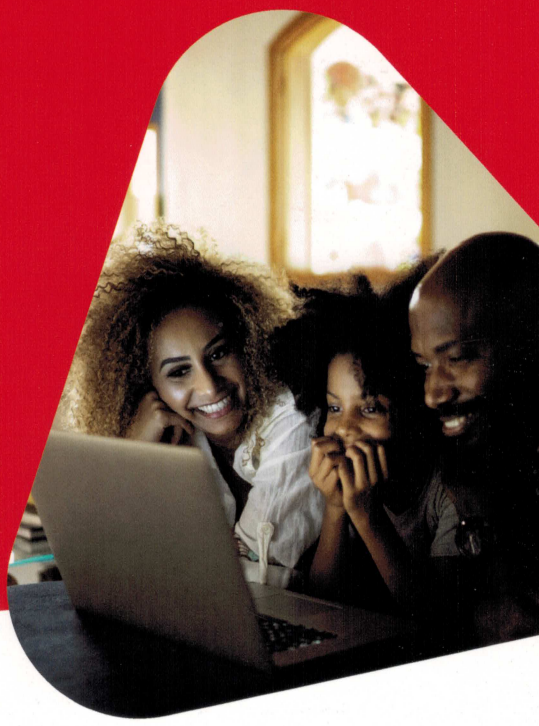
LastPass est la seule solution capable d'éliminer le mot de passe de l'expérience de connexion des employés tout en sécurisant chaque mot de passe utilisé grâce à la gestion des mots de passe.

Sources:
1. Verizon DBIR
2. Rapport mondial LastPass sur la sécurité des mots de passe
3. McAfee CASB : MVISION Cloud
4. Étude Le guide de l'identité moderne de LastPass

LastPass •••|

Utilisation de LastPass Families as a Benefit

Quelle que soit votre définition de la famille, nous assurons vos arrières.



Qualité et quantité : un bel avantage pour vos employés !

Votre employeur utilise LastPass Business pour stocker, gérer, utiliser et partager en toute sécurité les identifiants et les données sensibles, afin que vous et vos collègues puissiez travailler de façon sûre et efficace. Grâce à votre entreprise, vous et 5 de vos proches pouvez désormais faire de même avec LastPass Families as a Benefit, et c'est gratuit.

Grâce à cet avantage, chaque proche que vous invitez reçoit son propre compte LastPass où il peut **stocker ses mots de passe personnels et spécifier ceux qu'il souhaite partager avec les autres.**

Célébrer et protéger toutes les familles :

Les familles se suivent et ne se ressemblent pas, mais elles peuvent toutes profiter de LastPass Families, qu'elles englobent des conjoints, des partenaires, des parents, des enfants, des cousins éloignés, des amis ou des colocataires. Stockez tout ce que vous voulez, des mots de passe aux passeports, et partagez vos identifiants de streaming, connectez-vous pour payer des factures partagées, et ne vous retrouvez plus jamais à la porte d'un compte personnel ou partagé.

Soyez toujours préparé, en disposant de tous les identifiants et documents importants à portée de main, et sans dépendre d'une personne responsable de la gestion du foyer ou de certains aspects de la vie numérique.

Sécurisez votre univers numérique :

Le monde connecté évolue à mesure que l'on passe de plus en plus de temps en ligne, pour l'école, le travail ou échanger avec ses proches. Les pirates et autres cybercriminels suivent le mouvement, et font monter les risques associés à votre vie connectée, surtout si votre hygiène des mots de passe laisse à désirer.

Le saviez-vous ?



Dans une étude récente, **91 %** des personnes interrogées disent qu'ils savent qu'utiliser un même mot de passe ou une variante d'un même mot de passe est risqué ; mais elles sont **66 %** à dire qu'elles le font quand même !



Un comportement à risque en matière de mots de passe peut avoir de graves conséquences. Et de fait, **85 % des fuites intègrent un facteur humain,** y compris lorsqu'il s'agit de cyberattaques impliquant une manipulation sociale, comme l'hameçonnage, un vol d'identifiants ou une erreur humaine.



Qu'est-ce qui est pire ? Les conséquences sont souvent financièrement désastreuses. **La motivation financière est la principale motivation observée dans 70 % des fuites.**

Les gestionnaires de mots de passe sont le moyen le plus sûr de suivre les mots de passe et de protéger les individus et les familles contre les cybermenaces.

Protégez votre famille en quelques minutes :

En tant que détenteur d'un compte d'entreprise, vous pouvez obtenir votre compte Familles dès aujourd'hui ! Allez dans votre coffre-fort professionnel, et sélectionnez « Avantages du compte » dans le menu de gauche. Activez et configurez votre compte Familles en suivant les instructions détaillées.

Validez et démarrez :



Une fois que vous avez activé avec succès votre compte Familles, vous recevez une notification de vérification et de confirmation. Vous pouvez alors commencer à utiliser votre compte Familles sans attendre, y compris pour inviter 5 proches à vous rejoindre ! Vous pouvez également gérer votre compte Familles et inviter des membres dans votre Tableau de bord familial.



Gérez votre compte Familles dans l'onglet « Avantages du compte », par exemple pour associer ou dissocier votre compte personnel et votre compte professionnel, **qui n'est pas obligatoire pour utiliser votre compte familial.**



LastPass est aussi simple à configurer qu'à utiliser. Que vous décidiez ou non d'associer votre compte Business ou Familles, vous gardez le contrôle. **Vous spécifiez ce qui doit être partagé, tout en assurant la confidentialité du reste.**
Avec notre modèle de sécurité zéro connaissance, personne ne connaît jamais vos mots de passe !



Si vous quittez votre entreprise, votre compte LastPass Families vous accompagne où que vous alliez ! Vous aurez la possibilité d'acheter votre compte LastPass Families. Si vous n'optez pas pour ce choix, vous et vos proches serez transférés vers LastPass free, sans perte d'identifiants.



Votre compte Families as a Benefit comprend l'assistance LastPass de base et personnelle. Accédez 24x7 à notre centre d'assistance avec des ressources en libre-service et la Communauté LastPass, surveillée par des spécialistes LastPass. Besoin d'aide supplémentaire ?
Vous pouvez contacter l'assistance par e-mail et parler à notre équipe de service clientèle !

LastPass •••|

PRÉSENTATION

Sécurisation de chaque application avec LastPass et Okta



Avec l'adoption rapide des services web et apps dans le cloud, de nombreuses organisations doivent assurer la transparence et la sécurité des accès des employés. Pour ce faire, les entreprises utilisent des solutions d'authentification unique (SSO) pour centraliser la gestion des identités des salariés et assurer un accès sécurisé aux applications professionnelles dans le cloud.

Néanmoins, les solutions SSO laissent un manque. En plus des applications qui ne s'intègrent pas avec le système SSO, il reste d'innombrables services que les salariés peuvent apporter sur leur lieu de travail sans que le service informatique soit au courant. Chaque connexion est un point d'entrée potentiel pour un pirate – et doit être sécurisée en conséquence. La gestion des mots de passe en entreprise complète le SSO afin de sécuriser tous les points d'accès de l'organisation.

LastPass offre un portail SSO en plus de l'intégration avec tout un éventail de fournisseurs SSO, afin de conférer aux entreprises une souplesse absolue pour la gestion de chaque point d'accès : ceux qui sont intégrés au SSO, ceux qui ne le sont pas et ceux dont le SI ne connaissent même pas l'existence.

Pour les entreprises qui utilisent l'authentification unique Okta, LastPass fournit une intégration via une API SCIM qui permet aux utilisateurs d'Okta de tirer parti du gestionnaire de mots de passe LastPass, afin d'assurer que chaque point d'accès soit correctement contrôlé et sécurisé.

Comment LastPass aide les entreprises qui utilisent Okta

LastPass est une solution immédiatement utilisable de centralisation de la gestion de tous les mots de passe utilisés et partagés, que ces services aient été approuvés par le service informatique ou non.

Les entreprises investissent dans LastPass de façon à pouvoir :

- Traiter le manque laissé par les applications et services web qui ne sont pas compatibles avec le système SSO.
- Aider le service informatique à mettre en application les contrôles de sécurité pour les applications et services web introduits dans l'entreprise par les employés.
- Faciliter le partage sécurisé de mots de passe dans l'ensemble de l'entreprise.
- Résoudre les problèmes de gestion collaborative des travaux et des informations d'identification personnelles.

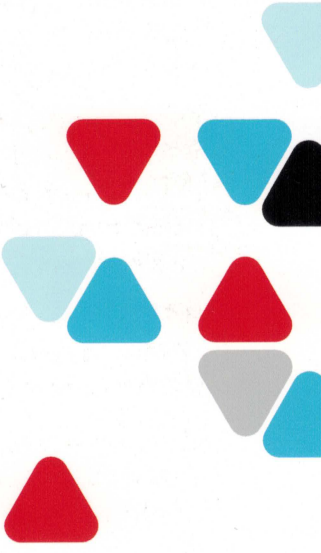
Notre façon de travailler avec Okta

Pour faciliter l'intégration et la gestion de LastPass, nous avons conclu un partenariat avec Okta qui permet le provisionnement et le déprovisionnement automatisés des utilisateurs par une API SCIM. Notre point de terminaison Okta peut être configuré pour assurer la création instantanée de comptes LastPass et la révocation en temps réel quand les salariés quittent l'entreprise. Les administrateurs informatiques profitent d'une administration sécurisée et intuitive de LastPass à travers leur annuaire Okta.

LastPass offre une sécurité souple

Pour les entreprises qui ont déjà investi dans l'authentification unique Okta, l'associer avec les fonctionnalités de gestion des mots de passe de LastPass permet de protéger tous les points d'accès de l'organisation, qu'il s'agisse de ceux qui sont intégrés avec le SSO, de ceux qui ne le sont pas et de ceux dont le SI ne connaît même pas l'existence. Grâce aux intégrations clés en main, LastPass offre de la souplesse aux équipes informatiques qui doivent protéger chaque point d'accès, tout en simplifiant la vie des employés.

LastPass offre 1 200+ apps SSO préintégrées et s'intègre avec plusieurs fournisseurs de SSO afin de donner aux entreprises une souplesse absolue pour la gestion et la sécurisation de chaque point d'accès.



En savoir plus **Démarrez un essai gratuit de LastPass Business dès aujourd'hui.**

LastPass •••|

Cas client : MV Group

" Un bon gestionnaire de mots de passe, c'est primordial aujourd'hui ! "

Grégory Lozachmeur,
Responsable Informatique de MV Group

⚠ Challenge

Avec un nombre de clients en forte hausse, il devenait indispensable de pouvoir échanger de l'information de manière sécurisée, entre les différents collaborateurs : ceux présents dès le lancement des projets et ceux arrivant au fil de leurs évolutions. Il fallait aussi être en mesure de maîtriser l'accès à l'information le jour où un collaborateur quitte le projet (fin de CDD, de stage...). Un gestionnaire de mots de passe est devenu indispensable. "C'est l'un de nos outils principaux, résume Grégory Lozachmeur, Responsable Informatique de MV Group. Si on ne l'avait pas, ce serait très compliqué de travailler comme nous le faisons." La société a donc opté pour **LastPass**, de LogMeIn.

Solution

LastPass est utilisé par plus de 25 millions de personnes dans le monde : des particuliers ainsi que les collaborateurs de 70 000 entreprises sur toute la surface du globe. MV Group en fait partie et pour plusieurs raisons :

La Compatibilité

MV Group gère son annuaire de sécurité en local, avec Active Directory, la solution Microsoft. Mais LastPass s'interface aussi avec Azure AD, la solution cloud de Microsoft. "On avait besoin d'un outil qui pouvait synchroniser les comptes de notre annuaire local avec les comptes de sécurité de LastPass, explique Grégory Lozachmeur. Quand je crée un utilisateur sur mon annuaire local, ça remonte à LastPass via le cloud."

L'accompagnement

Avoir le bon outil, c'est une chose. Encore faut-il bien l'utiliser. Les équipes de MV Group sont en lien constant avec celles de **LogMeIn** pour former les utilisateurs et améliorer leurs performances. "Ils sont ultra réactifs, on arrive toujours à trouver des solutions."

MV GROUP
UNE RECETTE UNIQUE DANS LE DIGITAL

MV Group et ses 250 collaborateurs réunissent pas moins de 42 expertises complémentaires dans l'univers du web. Après 10 ans d'existence et des effectifs multipliés par huit en 6 ans, le groupe est présent dans 11 grandes villes de France, au travers de ses 8 filiales et totalise près de 2 000 clients : TPE, PME et grands groupes.

L'évolutivité

L'amélioration continue des fonctionnalités de **LastPass** permet à MV Group d'envisager déjà les évolutions de demain :

- l'identification unique et multi-facteurs. Objectif : que les utilisateurs soient automatiquement reconnus, sans avoir besoin de s'identifier
- la mise en place du Home Office, véritable révolution du monde du travail
- l'audit des pratiques et de la solidité des mots de passe, afin de faire si besoin une piqûre de rappel aux collaborateurs.

Résultats

Grâce à ces fonctionnalités et à la réactivité des équipes de LogMeIn, MV Group enregistre des résultats très appréciables :

Une Croissance Sereine

Dans le contexte de croissance continue qu'elle connaît depuis des années, MV Group a régulièrement besoin d'intégrer une nouvelle filiale et de nouveaux clients dans son organisation et dans ses process de sécurité informatique. Certains d'entre eux utilisent déjà LastPass. Mais pour les autres, une migration est nécessaire, et les équipes de MV Group savent qu'elles peuvent appeler les supports LastPass pour que cela se déroule en douceur.

Un Passage au Remote Facilité

Au moment de mettre en place le télétravail, aux premiers jours du confinement, MV Group a vu la différence : "c'est dans ce contexte-là et dans les usages qu'on s'est rendu compte que la sécurité, on l'avait, se rappelle Grégory Lozachmeur, responsable informatique. Le télétravail est passé pour moi comme une lettre à la Poste : sur 250 collaborateurs, j'ai reçu 3 coups de fil !".

Une Adaptation aux Enjeux de demain

Avec la démocratisation du Home Office, les utilisateurs auront besoin de leurs outils de travail, de chez eux et à partir de n'importe quel device. "LastPass a un rôle à jouer, là encore, en étant capable de s'interfacer avec n'importe quel terminal."

MV Group est ses 250 collaborateurs utilisent LastPass pour la sécurité des échanges et des projets de leurs 2000 clients. Une sécurité - et une sérénité - garanties, surtout dans un contexte de forte croissance et de télétravail.

En tant qu'éditeur de logiciels, la sécurité est non négociable. LastPass était la solution la plus adaptée aux entreprises, tant en termes de fonctionnalités que de souplesse et d'intégration.

Attila Ferencz
Directeur de l'exploitation informatique, AdNovum



Le défi

Après avoir arrêté le développement de son propre outil par souci de rentabilité, AdNovum cherchait une solution agile de gestion des mots de passe en logiciel-service.

Attila Ferencz, directeur de l'exploitation informatique chez AdNovum explique : « Pour AdNovum, la sécurité est essentielle. Nous avons donc cherché une solution clé en main qui offrirait le même niveau de sécurité que notre solution précédente. »

Une équipe d'intégration chez AdNovum a testé et évalué de façon exhaustive quatre solutions différentes de gestion des mots de passe, dont LastPass de LogMeIn, sur une période de six semaines.



La solution

M. Ferencz déclare : « LastPass a été notre préféré dès le début, tout simplement en raison de sa facilité d'utilisation et de ses fonctions de sécurité. Nous l'avons finalement choisi pour ces raisons, et pour son interface utilisateur conviviale, son intégration avec un large éventail d'applications, et son stockage des données dans l'UE, ce qui était très important pour nous. Il est par ailleurs totalement intégré aux environnements Microsoft Windows et macOS, ce qui simplifie l'accès pour tous nos utilisateurs. »

Une fois que le choix s'est porté sur LastPass, LogMeIn a collaboré étroitement avec AdNovum pour coordonner une mise en œuvre progressive, à commencer par un essai de 30 jours, que LogMeIn a prolongé pour s'assurer que toute la société était prête pour le déploiement. Grâce à la simplicité de LastPass, il n'a pas fallu beaucoup de formation avant que l'ensemble des 600 employés puissent l'utiliser au quotidien.

M. Ferencz ajoute : « La mise en œuvre de LastPass a été un plaisir pour tout le monde. On a donné un nouvel outil rutilant à nos utilisateurs en remplacement d'un outil qui était bien moins flexible et facile d'utilisation. »

Le résultat

L'extension LastPass est désormais installée sur tous les navigateurs chez AdNovum. Il suffit d'un clic aux utilisateurs pour se connecter et permettre à LastPass de préremplir tous leurs mots de passe, en toute sécurité. Toutes les applications utilisées au quotidien sont accessibles directement depuis LastPass, offrant aux employés un accès instantané et authentifié à tous leurs outils et applications.

LastPass permet également aux équipes de projet d'accéder aux dossiers partagés de manière simple et sécurisée, et d'ajouter ou de supprimer facilement des membres au fil de l'évolution des projets.

M. Ferencz déclare : « Tout le monde dans l'entreprise utilise désormais LastPass. Les gens peuvent l'utiliser pour le travail ainsi que pour leurs comptes personnels, ce qui est un bonus appréciable. »

Avec l'augmentation du télétravail depuis la pandémie, LastPass offre la souplesse nécessaire pour permettre aux gens de travailler de partout, sans compromettre la cybersécurité de l'entreprise.

M. Ferencz ajoute : « Les principaux avantages de LastPass pour notre entreprise sont le chiffrement avancé, le stockage des données dans l'UE et la convivialité. Pour les utilisateurs individuels, les principaux avantages sont la fonction de préremplissage et l'accès facile aux dossiers partagés, qui simplifie tellement la vie. Nous sommes ravis d'avoir ce produit dans l'entreprise, et nous avons hâte d'en tirer le meilleur parti au cours des années à venir. »

Authentification transparente

Partage de dossiers simplifié

Souplesse pour les employés

AdNovum

L'éditeur de logiciels suisse AdNovum offre une assistance exhaustive aux entreprises pour les aider à numériser leurs processus. Basé à Zurich, il emploie 600 personnes réparties dans des bureaux à Bern, Lausanne, Budapest, Lisbonne, Hô Chi Minh-Ville et Singapour.

adnovum.com

Nous contacter **Découvrez comment renforcer la sécurité des mots de passe avec LastPass.**

LastPass •••|

Témoignage client : St. Anna Children's Cancer Research Institute

« En substance, nous disposons avec LastPass d'un outil de gestion des mots de passe qui fonctionne, qui s'intègre bien et qui est simple à utiliser. Que demander de plus ? »

Dominik Achleitner
Directeur de l'informatique et de la transformation numérique, St. Anna Children's Cancer Research Institute

Le défi

L'équipe du St. Anna Children's Cancer Research Institute est composée de chercheurs qui se consacrent à la lutte contre le cancer de l'enfant. Ils s'investissent corps et âme dans leur recherche, travaillant parfois à domicile et les week-ends. C'était l'un des principaux défis, selon Dominik Achleitner, le directeur de l'informatique et de la transformation numérique au St. Anna Children's Cancer Research Institute.

« Dans le domaine de la recherche, les gens sont actifs et voyagent énormément. Ils se rendent en avion à des conférences, ils font des présentations, ou ils ont des réunions en personne avec d'autres cancérologues pour échanger des idées. Ils utilisent de nombreux outils et plates-formes. C'est pourquoi les chercheurs utilisent un grand nombre de mots de passe », explique M. Achleitner.

Ce que confirme Ingomar Schmickl, responsable informatique au St. Anna Children's Cancer Research Institute. Il estime que le problème va même encore plus loin : « L'autre défi qui nous préoccupait portait sur la sécurité des données et la manière de la garantir. »

« Nos équipes utilisent non seulement leurs ordinateurs portables professionnels, mais aussi leurs appareils personnels. Dans certains cas, nos chercheurs exploitent des données sensibles sur les patients. Nous ne voulons donc évidemment pas que nos employés se promènent avec leurs mots de passe stockés dans leur navigateur, ou pire, qu'ils laissent leur ordinateur ouvert quelque part. » Les deux experts en informatique étaient convaincus que le moment d'agir était venu. MM. Achleitner et Schmickl cherchaient un outil qui simplifierait les tâches quotidiennes de leurs collègues. Ils voulaient également mieux sensibiliser les chercheurs en matière de sécurité.

Un outil de gestion des mots de passe s'imposait. Et le choix évident était LastPass, la solution de gestion des identités et des mots de passe de LogMeIn.

La solution

Une nouvelle ère en matière de sécurité des données. M. Schmickl, le responsable informatique, voulait un outil web, mais qui soit sécurisé. « Cette combinaison était extrêmement importante à nos yeux, car les chercheurs travaillent au bureau, mais aussi de chez eux, ce que nous ne pouvons ni ne voulons pas interdire. »

« Si un chercheur a une idée lumineuse un samedi, vous ne voulez pas lui mettre des bâtons dans les roues en lui disant : 'il faut que tu viennes au bureau pour te connecter à ton ordinateur.' Il peut simplement tout noter, en ligne et en toute sécurité ! »

« Grâce à LastPass, nous avons renforcé la sécurité globale », confirme l'expert informatique M. Achleitner. « La sécurité mobilise toujours beaucoup de ressources et d'effort. LastPass allège considérablement ce fardeau », ajoute-t-il. St. Anna Children's Cancer Research Institute peut désormais travailler de manière plus sûre et pratique, surtout en matière informatique. « L'intégration de LastPass n'a pas augmenté la charge de travail de notre service d'assistance », se félicite M. Achleitner. « Au contraire, le nombre de demandes a considérablement baissé. »

Ce qui ne surprend pas Ingomar Schmickl. Le responsable informatique explique que la convivialité est un gros point fort de LastPass : « Le personnel n'adopte un système que s'il est simple et rapide à utiliser, ce qui est clairement le cas de LastPass. L'outil peut être intégré sur plusieurs plates-formes, et il a été bien accepté par le personnel, y compris par ceux qui ne sont pas très à l'aise avec la technologie. » M. Achleitner résume les avantages de LastPass : « En substance, nous disposons avec LastPass d'un outil de gestion des mots de passe qui fonctionne, qui s'intègre bien et qui est simple à utiliser. Que demander de plus ? »

Bien que le fonctionnement de LastPass soit évident, l'assistance et le SAV étaient des critères essentiels pour les deux responsables informatiques. Ils ont été impressionnés par LogMeIn, en collaboration avec Colited Management Consultancy, à tous les niveaux. « Nous avons pris les devants et contacté LastPass pour leur demander des renseignements, et ils nous ont fait une très bonne impression dès le début. Ils étaient très agréables, compétents et pas du tout insistants. Au bout du compte, il s'agit de pouvoir travailler avec les autres. Même le meilleur outil au monde ne me servira à rien si je dois subir des vendeurs désagréables. »

Le résultat

Grâce à LastPass, les chercheurs peuvent se consacrer pleinement à leur cœur de métier : trouver les origines du cancer chez l'enfant afin d'améliorer sensiblement le diagnostic, le traitement et les chances de survie. LastPass confère plus de souplesse et de confort au personnel, sans mettre en péril la cybersécurité du centre de recherche. « Comme nos chercheurs travaillent aussi à distance, LastPass leur offre la souplesse dont ils ont besoin. Le personnel peut utiliser l'outil tant pour leurs tâches professionnelles que personnelles », conclut M. Achleitner.

En intégrant LastPass, St. Anna Children's Cancer Research Institute a accéléré son accession au monde numérique et sécurisé du travail 2.0, de manière aussi simple que concluante.

St. Anna Children's Cancer Research Institute est l'un des principaux centres européens de recherche sur le cancer de l'enfant. En exploitant les dernières technologies, des groupes de recherche interdisciplinaires cherchent à améliorer la qualité du traitement et les chances de guérison des enfants atteints de cancer. Fondé en 1985, le centre de recherche est basé à Vienne.

ccri.at

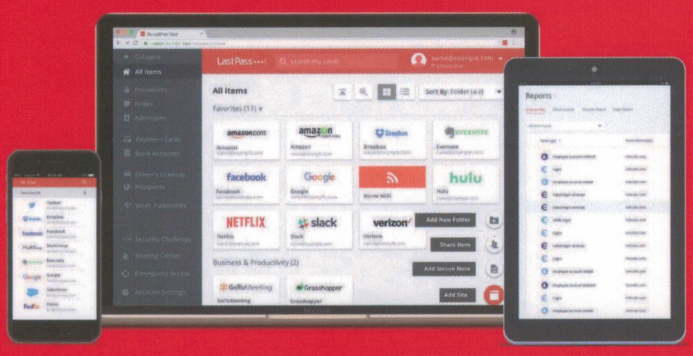
LastPass •••|

Une hygiène des mots de passe sécurisée et simplifiée

Ne plus jamais réinitialiser un mot de passe



- Authentification unique
- Gestion des mots de passe
- Accès simple et intégré



Pour en savoir plus :
lastpass.com/fr/business-solutions

©2021 LogMeIn, Inc. Tous droits réservés.