

# LastPass Identity protège tous les points d'accès à l'aide d'une sécurité intelligente.

Dans un monde hyper mobile toujours connecté, le SI est mis au défi de sécuriser les activités des entreprises. Malgré la montée des cybermenaces, les employés demandent une technologie rapide, pratique et simple à utiliser. Il y a toujours plus d'appareils, d'apps, de réseaux et même d'utilisateurs dans votre écosystème d'entreprise, à l'intérieur et à l'extérieur de vos bureaux, ce qui signifie que la gestion et la protection des accès utilisateurs sont plus complexes que jamais. La complexité intensifiée dans votre écosystème d'entreprise est synonyme d'obstacles supplémentaires pour sécuriser les accès dans votre organisation.

Face à ces enjeux, le SI est rapidement débordé. Quelles sont les façons de protéger les accès utilisateur et l'authentification de manière automatisée, sécurisée et abordable ? Les entreprises ont besoin d'une solution d'identification exhaustive, simple, intégrée et transparente avec une sécurité renforcée.

LastPass Identity fournit un contrôle simple et une visibilité unifiée pour tous les points d'entrée de votre entreprise, avec un accès intuitif et une expérience d'authentification à plusieurs facteurs qui fonctionne à tous les niveaux, du nuage aux apps mobiles aux outils anciens sur site. De l'authentification unique à la gestion de mots de passe à l'authentification adaptative, LastPass Identity propose une fonctionnalité de contrôle performante au SI et un accès sans points de friction aux utilisateurs.



## Contrôle unifié pour les administrateurs

Offrir au SI une vue d'ensemble des activités utilisateur à partir d'un tableau de bord simple à utiliser. Gérer l'inscription et la radiation des utilisateurs à l'aide de votre annuaire, déployer des méthodes d'authentification, activer la surveillance, afficher des alertes de sécurité exploitables et définir des règles de sécurité. LastPass Identity permet au SI d'attribuer un accès adapté aux bonnes personnes au moment adéquat. Éliminer les tâches manuelles fastidieuses et fournir au SI une visibilité sur la sécurité des accès dans toute l'entreprise.

## Gestion simplifiée pour le SI

Le déploiement d'outils de gestion d'identité et d'accès n'a jamais été aussi simple. Exploiter les annuaires utilisateur existants pour les inscriptions et les radiations faciles ainsi que la gestion de groupe. Un besoin de gestion limité au quotidien permet de libérer du temps pour des projets informatiques à haute valeur ajoutée.

## Contrôles granulaires et personnalisés

Une sécurité globale sans complexité. LastPass Identity offre plus de 100 règles pour gérer les utilisateurs au niveau applicatif, individuel, collectif ou organisationnel, pour que vous puissiez personnaliser les exigences d'accès et d'authentification selon les besoins de votre entreprise. Assurez-vous que les règles sont cohérentes entre l'authentification unique, la gestion des mots de passe et l'authentification à plusieurs facteurs.

## Gestion d'accès universel

LastPass Identity sécurise l'accès à tous les outils utilisés par les employés, depuis les apps dans le nuage ou mobiles, aux formulaires de connexion et aux apps anciennes sur site. Un portail unique permet de déverrouiller l'accès employé à toutes les apps pour une journée de travail simplifiée et plus sécurisée.



**Solution d'accès tout-en-un**



**SSO prêt-à-l'emploi**



**Gestion universelle des mots de passe**



**Authentification à plusieurs facteurs**



**Sécurité zéro-connaissance**

### Accès sans mot de passe

Les mots de passe représentent une source infinie de frustrations et de risques. À l'aide de données biométriques et d'authentification adaptative, LastPass Identity peut éliminer les mots de passe et rationaliser l'accès employé aux apps de travail pour améliorer la productivité.

### Authentification à plusieurs facteurs flexible

LastPass Identity offre des méthodes d'authentification versatiles qui s'adaptent en fonction des profils utilisateur, avec des règles personnalisables aux niveaux utilisateur ou groupe, pour offrir une assistance à chaque utilisateur dans l'entreprise sans compromettre la sécurité.

### Risques d'accès limités

Un employé partage en général six mots de passe avec ses collègues, c'est pourquoi une fonctionnalité de partage rapide et flexible est essentielle. Du service informatique au marketing, LastPass Identity simplifie la prise de responsabilité et la sécurité avec le partage d'accès.

### Sécurité zéro-connaissance

La sécurité et la confidentialité ne sont pas négociables. LastPass est conçu pour sécuriser les données sensibles avec une approche zéro-connaissance. Des données biométriques et des clés de chiffrement ne quittent jamais l'appareil de l'utilisateur, ainsi les données personnelles restent sécurisées et confidentielles.

## Ces fonctionnalités offrent le contrôle exigé par le SI et la commodité demandée par les utilisateurs :

<b>Contrôle centralisé pour les administrateurs</b>	Le tableau de bord d'administration offre au SI une vue unifiée de l'accès dans toute l'entreprise et centralise la gestion des utilisateurs, des règles, des rapports et d'autres encore.
<b>Authentification à plusieurs facteurs adaptative</b>	Élimine les mots de passe tout en renforçant la sécurité en associant des données biométriques et des facteurs contextuels pour adapter les exigences d'authentification à différentes situations.
<b>Authentification unique</b>	Avec un catalogue de plus de 1 200 apps préintégrées, le SI peut simplifier l'accès des employés aux outils métier critiques à travers un portail pratique.
<b>Sécurisation des mots de passe en coffre-fort</b>	Pour les apps que le SI ne connaît pas, LastPass Identity offre des fonctionnalités de gestion de mots de passe qui capturent, stockent et remplissent les identifiants pour toute connexion basée sur le web.
<b>Intégrations des annuaires utilisateur</b>	Automatisent l'inscription et la radiation, la gestion des groupes et plus encore avec AD, Azure AD, Okta, OneLogin ou une API personnalisée.
<b>Plus de 100 règles de sécurité</b>	Appliquent les bonnes pratiques et contrôlent les comportements relatifs aux mots de passe dans toute l'entreprise.
<b>Rapports de sécurité détaillés</b>	Associent les actions aux individus grâce aux rapports détaillés automatisés qui aident votre entreprise à être en conformité.
<b>Partage sécurisé des mots de passe</b>	Donnent aux équipes un moyen souple et sûr de partager l'accès aux apps, sans sacrifier la traçabilité ou la sécurité.



Consultez [www.lastpass.com/products/identity-as-a-solution](http://www.lastpass.com/products/identity-as-a-solution) pour en savoir plus