LastPass

La MFA et le SSO ne suffisent pas : Pourquoi il vous faut un gestionnaire de mots de passe

Protéger chaque point d'accès

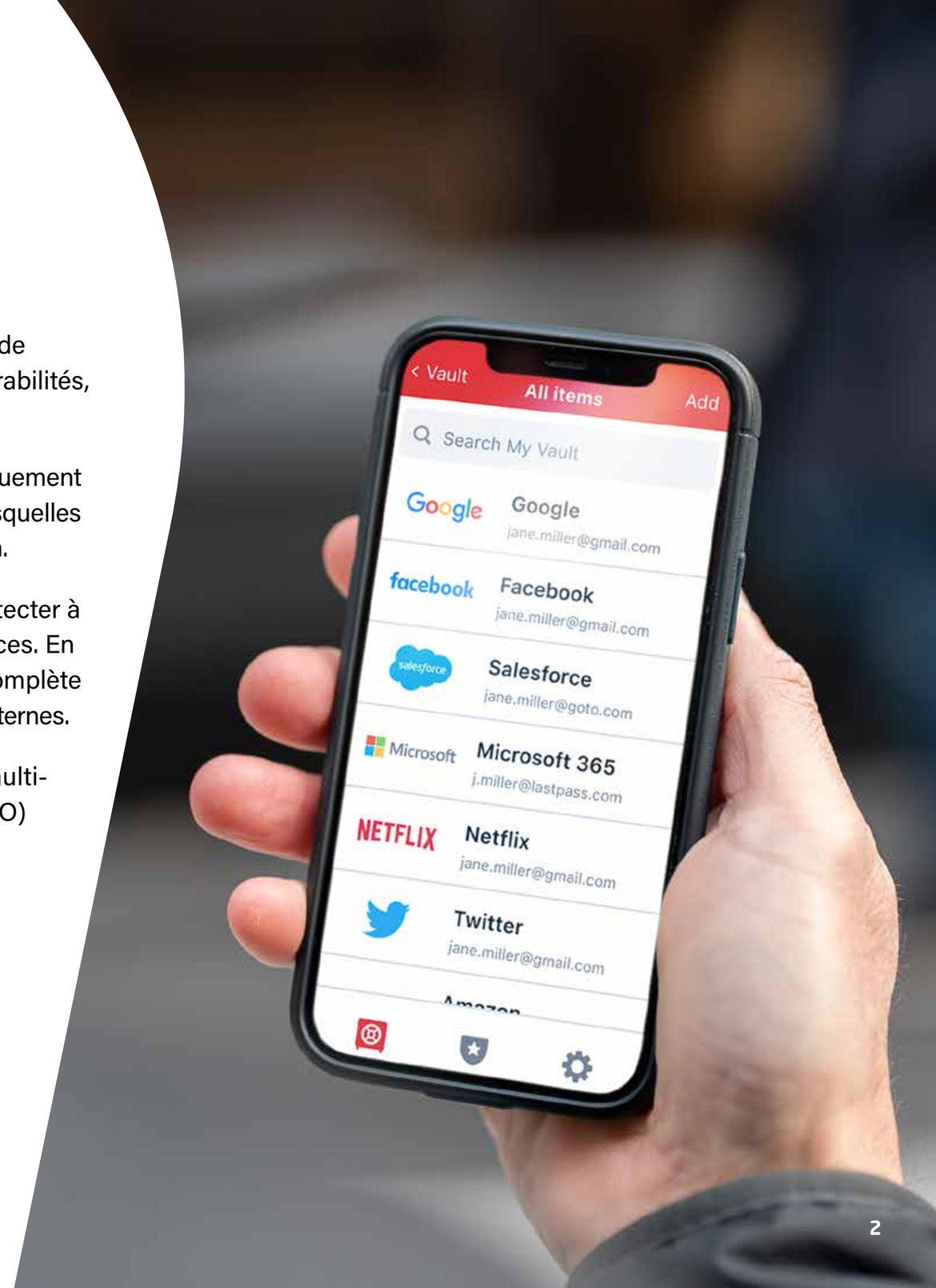
L'erreur humaine reste un facteur important en matière de cybermenaces. Il est essentiel de disposer d'une stratégie de cybersécurité exhaustive qui tient compte de toutes les vulnérabilités, qu'elles soient techniques ou humaines.

La cybersécurité est plus efficace lorsqu'elle est abordée de manière globale. Protéger uniquement certains points d'accès tout en laissant les autres vulnérables peut créer des failles dans lesquelles les cybercriminels risquent de s'engouffrer pour infiltrer l'infrastructure d'une organisation.

Les cyberattaques peuvent s'intensifier rapidement, c'est pourquoi il est primordial de détecter à temps toute activité suspecte et de réagir rapidement pour contenir et atténuer les menaces. En surveillant et en contrôlant les accès dans l'ensemble de l'organisation, une couverture complète permet d'identifier et de réduire les risques associés aux erreurs humaines et aux menaces internes.

Pour de nombreuses organisations, le programme de sécurité inclut l'authentification multi-facteur (MFA) pour les contrôles d'accès supplémentaires et l'authentification unique (SSO) pour l'accès aux services basé sur des permissions.

Toutefois, la MFA comme le SSO souffrent de certaines limites qui peuvent créer des brèches dans vos cyberdéfenses.



Les limites de l’authentification multifacteur

Incompatibilités :

Certains dispositifs, systèmes et applications peuvent ne pas être compatibles avec toutes les méthodes d’authentification multifacteur.

Complexité et gêne pour l’utilisateur :

Le processus d’authentification peut devenir plus complexe et prendre plus de temps selon la méthode employée.

Adoption par les utilisateurs et formation :

La mise en œuvre de la MFA nécessite de former les utilisateurs au nouveau processus d’authentification, et de s’assurer qu’ils comprennent comment l’utiliser à bon escient.

Coût et mise en œuvre :

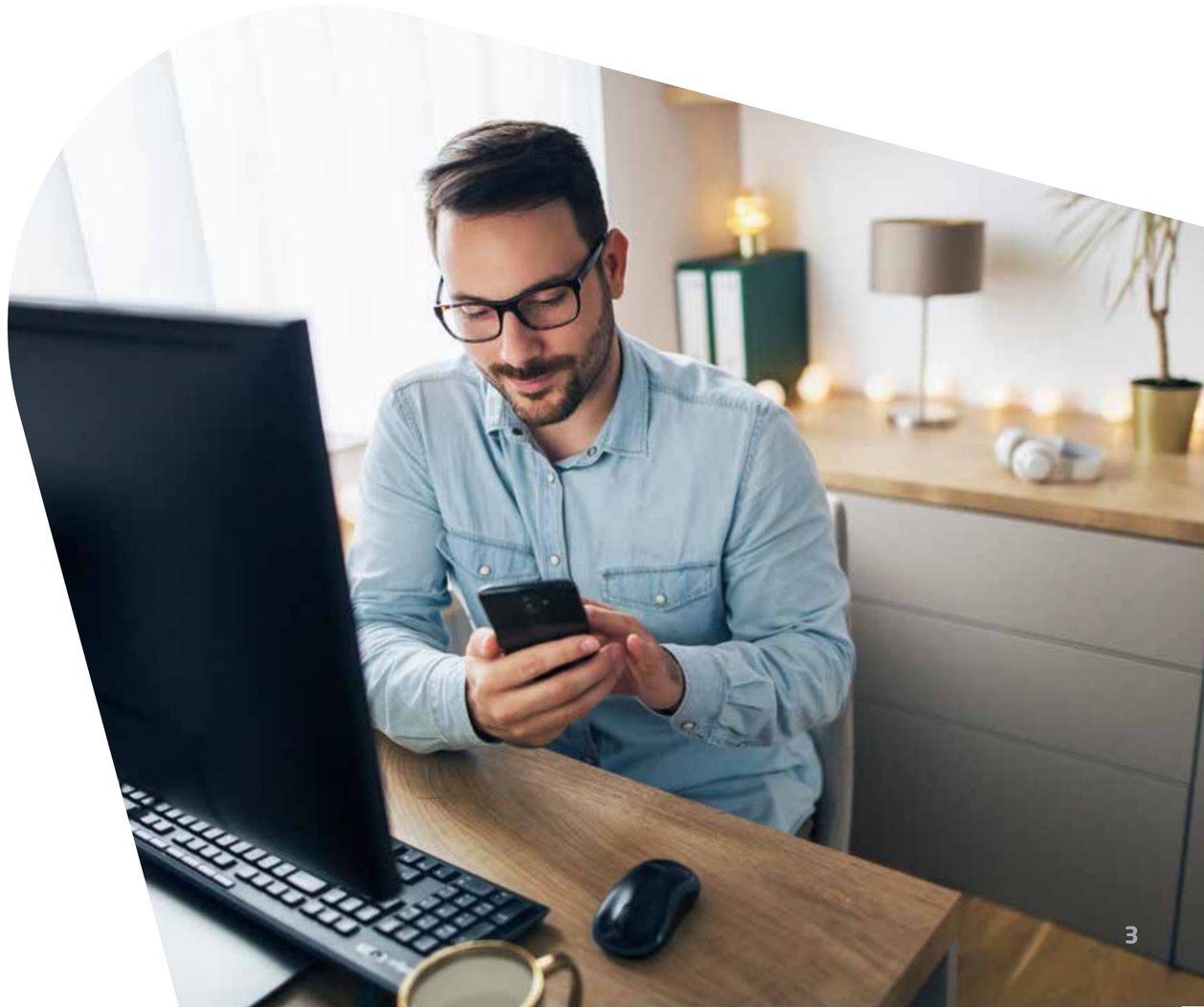
Le déploiement de solutions d’authentification multifacteur, en particulier de clés physiques ou de systèmes biométriques, peut impliquer des coûts initiaux pour la mise en œuvre de l’infrastructure nécessaire.

Dépendance à l’égard de facteurs extérieurs :

Certaines méthodes d’authentification multifacteur, telles que les codes envoyés par SMS, dépendent de facteurs externes tels que la couverture du réseau ou la force du signal cellulaire.

Risques pour la sécurité :

Des pirates aguerris peuvent encore tenter d’inciter les utilisateurs à fournir leur deuxième facteur par le biais de techniques d’ingénierie sociale.



Les limites de l'authentification unique

Couverture limitée des applications :

Le SSO ne couvre pas toujours toutes les applications ou tous les services utilisés au sein d'une organisation, en raison de problèmes de compatibilité ou de Shadow IT.

Point de défaillance unique :

Si le système d'authentification unique subit une panne ou une faille de sécurité, l'accès à toutes les applications connectées peut être impacté.

Mise en œuvre complexe :

L'installation et la configuration initiales de l'authentification unique nécessitent une planification et des tests approfondis pour garantir un déploiement optimal.

Sécurité renforcée :

Il peut être impossible d'accéder aux applications à partir d'appareils ou de lieux où l'authentification unique n'est pas prise en charge, ou lorsque la connectivité du réseau est limitée.

Dépendance à un fournisseur :

Les organisations peuvent devenir dépendantes d'un fournisseur ou d'une solution d'authentification unique spécifique, rendant difficile le passage à une autre solution.

Problèmes de synchronisation des identifiants :

Les modifications apportées aux identifiants d'un utilisateur peuvent ne pas se synchroniser correctement entre toutes les applications connectées.

Adoption par les utilisateurs et formation :

Les utilisateurs peuvent avoir besoin d'être formés à l'utilisation de l'authentification unique afin d'en comprendre les avantages.

Combler les lacunes à l'aide d'un gestionnaire de mots de passe

Bien que la MFA et le SSO ont un rôle à jouer dans votre pile technologique, il reste des lacunes en matière de protection par mot de passe. La gestion des mots de passe comble ces lacunes, avec un effort minimal pour une sécurité maximale.

Les avantages d'un gestionnaire de mots de passe sont nombreux :

Expérience utilisateur fluide.

- Remplissage automatique des mots de passe dans le navigateur
- Capture automatique des identifiants.
- Partage sécurisé et fluide
- Synchronisation automatique pour un accès sur tous les appareils
- Prise en charge de toutes les connexions web
- Chiffrage et stockage sécurisé des identifiants et des autres données sensibles

Accent sur la sécurité.

- Chiffrement exclusivement en local
- Grand éventail de stratégies et de réglages avancés au niveau de l’administrateur
- Différents scénarios d’accès des données, en mode en ligne ou hors ligne
- Intégration de l’authentification multifacteur
- Surveillance du dark web pour surveiller, alerter et protéger les comptes

Expérience d’administration centralisée.

- Sélectionnez les administrateurs qui auront accès à des privilèges spéciaux pour gérer et sécuriser le déploiement
- Des services d’annuaire pour synchroniser et virtualiser les infos d’identité existantes
- Mises à jour automatisées du service qui demandent peu ou pas d’engagement de l’informatique
- Possibilité d’ajouter des licences en cours d’année pour accompagner l’augmentation des effectifs
- Des outils de provisionnement qui simplifient le cycle de vie de l’identité numérique des employés

Contrôles personnalisés, granulaires et axés sur des actions concrètes

- Vue d'ensemble instantanée sur les utilisateurs, leurs sites stockés et leurs comportements relatifs aux mots de passe
- Rapports de sécurité qui démontrent un impact net sur la baisse du taux de réutilisation des mots de passe
- Stratégies et les paramètres appliqués au niveau global, groupe et utilisateur
- Partage d'identifiants qui permet de relier les actions aux individus
- Journaux de reporting détaillés pour les audits et la conformité
- Fonctionnalité de récupération de compte utile lors du départ d'un employé ou en cas d'oubli du mot de passe maître

Gestion des mots de passe et LastPass

Lorsque les outils de gestion des identités traditionnels comme le SSO et la MFA ne peuvent pas sécuriser la totalité des applications dans le cloud utilisées par vos employés, protégez la surface d'attaque de votre entreprise avec LastPass.

- Faites en sorte que vos employés puissent améliorer et conserver une bonne hygiène des mots de passe, et collaborer en toute sécurité.
- Diminuez les risques et la charge du SI, tout en augmentant l'efficacité et la surveillance de la sécurité.

LastPass est un outil de gestion des mots de passe de pointe qui aide vos employés à créer des mots de passe forts à l'aide d'un générateur de mots de passe, à partager les identifiants et les informations sensibles en toute sécurité, tant en interne qu'avec l'extérieur, qui protège vos employés, et qui fournit des stratégies personnalisées et des informations sur le score de sécurité de votre entreprise.

Sécurisez chaque point d'accès avec LastPass.

Démarrer votre essai gratuit