LastPass •••|
by LogMeIn

LE B-A-BA DE L'IDENTITÉ EN ENTREPRISE

Guide des avantages et fonctionnalités des solutions d'identité

L'ENVIRONNEMENT PROFESSIONNEL D'AUJOURD'HUI EST TOUT SAUF SIMPLE.

Les attentes des employés sont élevées. Une main-d'œuvre toujours connectée et mobile exige plus de souplesse en voulant travailler où et quand elle le souhaite, sur tout appareil.

Les employés d'aujourd'hui n'hésitent pas non plus à essayer de nouvelles applications. L'employé moyen utilise activement **36** services en ligne au travail[1]. Il veut que les technologies soient rapides, pratiques et simples à utiliser, et il en cherche par lui-même en cas de besoin. **77 %** des employés utilisent une app tierce dans le cloud à l'insu du SI[2].

L'employé moyen n'est plus forcément là pour longtemps. Changer d'emploi est la nouvelle norme. **50 %** des actifs ont entre 18 et 24 ans et **plus de la moitié** d'entre eux ont déjà eu au moins trois emplois[3].

Bref, vous devez gérer et connecter davantage d'appareils, d'applications, de réseaux et d'utilisateurs dans un environnement de travail en constante évolution.

Il n'est donc pas étonnant que fournir aux employés un accès aux systèmes et aux données de l'entreprise n'a jamais été aussi difficile.

L'AUGMENTATION DES CYBERMENACES NE FAIT QUE COMPLIQUER LA SITUATION.

Gérer l'environnement de travail hybride d'aujourd'hui est un sacré défi, mais sécuriser cet environnement est tout aussi important et compliqué.

Le modeste mot de passe reste un obstacle pour les employés, une perte de productivité pour le SI et une menace pour la sécurité de l'entreprise.

80 % des fuites de données connues sont dues aux identifiants faibles, réutilisés ou volés[4]. Lorsque **59 %** des gens utilisent souvent ou toujours le même mot de passe[5], il n'est pas surprenant qu'un seul mot de passe piraté puisse entraîner une fuite. L'employé moyen lutte pour jongler **plus de 100** mots de passe, et **76 %** d'entre eux rencontrent régulièrement des problèmes liés aux mots de passe.

80 %

des fuites de données connues sont dues aux identifiants faibles, réutilisés ou volés.

76 %

des employés rencontrent régulièrement des problèmes de mots de passe.

Les contrôles d'accès déficients ne font qu'aggraver le problème. Lorsque les employés ont un accès illimité aux données et aux ressources, leur mauvaise utilisation et les pertes de données sont inévitables. Cela simplifie aussi la tâche des pirates qui peuvent abuser d'accès privilégiés aux systèmes stratégiques.

En moyenne, les équipes de sécurité informatique consacrent **4 heures** par semaine à des problèmes liés à la gestion des mots de passe, et elles reçoivent **96** demandes relatives aux mots de passe par mois[6]. Certaines équipes informatiques reçoivent plus de **25** demandes de mots de passe oubliés **par jour**[7] !

Lorsque l'on sait que **43 %** des cyberattaques touchent les petites entreprises[8] et que **53 %** des moyennes entreprises ont subi une faille de sécurité[9], prendre des mesures de sécurité de base est devenu obligatoire. Mais tout espoir n'est pas perdu : **93 %** des cyberincidents peuvent être évités avec les bons outils.

4 heures

consacrées par semaine aux problèmes de gestion des mots de passe par les équipes informatiques.

96

demandes liées aux mots de passe envoyées aux équipes de sécurité informatique par mois.

GÉRER LES IDENTITÉS ET LES ACCÈS DIMINUE LES RISQUES ET ÉLIMINE LES OBSTACLES.

En fin de compte, vous devez connecter vos utilisateurs, qu'il s'agisse d'employés, de sous-traitants ou de partenaires, à la bonne technologie au bon moment et de façon sécurisée. Pour travailler efficacement, les utilisateurs doivent avoir accès aux ressources nécessaires, lorsqu'ils en ont besoin, où qu'ils se trouvent et sans mettre l'entreprise en danger.

Pour donner un accès aux bonnes personnes, vous devez d'abord disposer d'un moyen de savoir qui elles sont. Bâtir une « identité » unique pour chaque utilisateur de votre environnement vous permet de fournir un accès sécurisé en vérifiant de façon fiable et systématique qu'il s'agit du bon utilisateur.

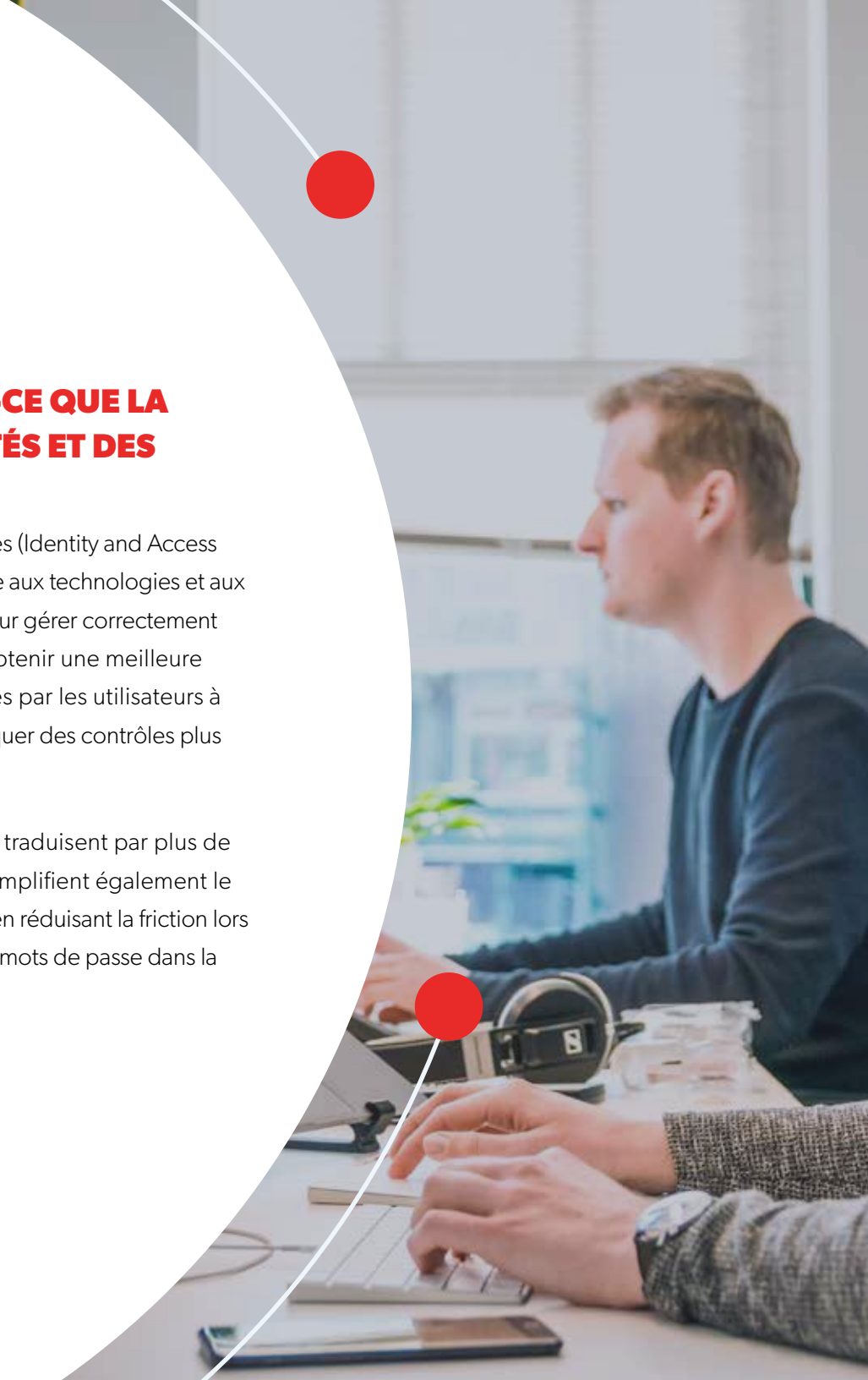
Plusieurs types de données peuvent être exploitées pour bâtir une identité, qu'il s'agisse du comportement et des appareils de l'utilisateur ou des services qu'ils utilisent et de leurs caractéristiques personnelles. Chaque utilisateur est unique, et toute méthode de gestion des identités doit donc prendre en compte un large éventail de cas d'utilisation et de scénarios d'authentification.

Bien entendu, trop de sécurité peut affecter la productivité de l'employé, mais une sécurité insuffisante peut mettre l'entreprise en danger. La clé consiste à trouver le bon équilibre entre les deux extrêmes.

MAIS ALORS, QU'EST-CE QUE LA GESTION DES IDENTITÉS ET DES ACCÈS ?

La gestion des identités et des accès (Identity and Access Management ou IAM) fait référence aux technologies et aux règles qui peuvent être utilisées pour gérer correctement l'identité de chaque utilisateur, obtenir une meilleure visibilité sur les éléments consultés par les utilisateurs à l'échelle de l'organisation et appliquer des contrôles plus stricts sur ces accès.

Plus de visibilité et de contrôle se traduisent par plus de sécurité, mais les solutions IAM simplifient également le travail des employés au quotidien en réduisant la friction lors de la connexion et en éliminant les mots de passe dans la mesure du possible.



LES SOLUTIONS D'IDENTITÉ OFFRENT DES AVANTAGES CONSIDÉRABLES.

Les solutions IAM permettent de définir les rôles des utilisateurs, gérer les privilèges et décider lorsque les employés se voient accorder ou refuser les accès, mais elles offrent aussi des avantages conséquents pour l'organisation dans son ensemble.

UNE SOLUTION D'IDENTITÉ IDÉALE VOUS CONFÈRE :

Visibilité : Suivez l'activité des utilisateurs, créez des rapports sur cette activité, obtenez une compréhension approfondie des ressources consultées par les utilisateurs ainsi que leurs comportements en matière de sécurité.

Contrôle : Appliquez des règles adaptées aux objectifs de sécurité de l'entreprise et qui respectent la réglementation, et vérifiez que les accès sont adaptés au rôle de chaque utilisateur.

Automatisation : Intégrez les technologies et infrastructures existantes pour accélérer le déploiement, simplifiez la gestion quotidienne et standardisez la radiation des utilisateurs.

Unification : Réunissez accès et authentification au sein d'une solution unique qui fournit une vue complète de chaque point d'accès et de chaque action des utilisateurs.

Sécurité : Imposez des autorisations basées sur les rôles pour que chaque utilisateur ait l'accès le moins privilégié possible pour pouvoir faire son travail. Éliminez les mots de passe, renforcez ceux qui restent et ajoutez des protections avec des facteurs d'authentification supplémentaires.

Efficacité : Supprimez les obstacles liés aux mots de passe et offrez aux utilisateurs un moyen plus simple et fluide d'accéder aux outils dont ils ont besoin pour travailler.

SSO, GME, AMF : DESCRIPTION DES TECHNOLOGIES DE GESTION DES IDENTITÉS ET POURQUOI IL FAUT LES CONJUGUER.

De nombreuses technologies relèvent de l'IAM. Ce guide est consacré à quelques technologies clés qui, ensemble, peuvent aider votre entreprise à bâtir ou à moderniser son programme d'identité.

Accès

Les solutions d'**accès** se concentrent sur la connexion des utilisateurs aux applications et services appropriés par mot de passe et d'autres protocoles. Les technologies clés sont l'authentification unique (Single Sign-On ou SSO) et la gestion des mots de passe en entreprise (GME).

Authentification

Les solutions d'**authentification** se concentrent sur la validation et l'autorisation sécurisée des utilisateurs lorsqu'ils demandent un accès à une ressource. L'authentification multifacteur est une technologie clé dans ce domaine. Diverses options sont disponibles, dont les codes par SMS, les clés matérielles, la biométrie ou encore des méthodes contextuelles.

Identité

Les solutions d'**identité** associent plusieurs technologies d'accès et d'authentification pour répondre de manière globale aux besoins IAM de l'entreprise.

Les technologies d'identité peuvent être déployées en interne (gérées sur site) ou dans le cloud (conçues et exploitées par un fournisseur tiers). Opter pour une solution dans le cloud présente de nombreux avantages : Elles coûtent moins cher, nécessitent moins de ressources et d'expertise en interne et font reposer la sécurité sur des experts qui desservent des milliers d'organisations. C'est pour ces raisons que nous recommandons une solution dans le cloud pour les organisations qui cherchent à créer ou à moderniser leur programme d'identité.

COMMENT LES SOLUTIONS D'ACCÈS DIMINUENT LE RECOURS AUX MOTS DE PASSE ET SÉCURISENT TOUS LES POINTS D'ACCÈS.

Une solution d'accès permet à votre entreprise d'atteindre deux objectifs : Éliminer les problèmes de connexion des employés et augmenter la visibilité et le contrôle du SI sur chaque point d'accès de l'organisation. Après tout, tout ce qui nécessite un mot de passe est un point d'entrée à votre entreprise et doit être géré en conséquence.

Il existe deux technologies d'accès principales : l'authentification unique (SSO) et la gestion des mots de passe en entreprise (GME).

SSO + GME

Bien qu'elles puissent être utilisées séparément, elles sont plus efficaces lorsqu'elles sont utilisées ensemble pour protéger tous les points d'accès de l'entreprise.

L'AUTHENTIFICATION UNIQUE RELIE LES EMPLOYÉS AUX OUTILS ESSENTIELS DE L'ENTREPRISE.

Avec l'authentification unique, les employés ne mémorisent qu'un seul jeu d'identifiants. Tous les autres mots de passe sont remplacés en coulisses par un protocole comme SAML 2.0. Une fois qu'un employé s'authentifie sur son portail SSO, il peut lancer les apps professionnelles qui lui sont affectées et s'y connecter en contournant les formulaires de saisie de mots de passe.

PRINCIPALES FONCTIONNALITÉS DES SOLUTIONS SSO :

- **Un seul mot de passe** qui déverrouille l'accès à toutes les apps
- **Un portail** où les employés peuvent voir et lancer des apps
- **Élimination des mots de passe** en utilisant SAML 2.0
- **Catalogue d'apps préintégrées** pour un déploiement simplifié pour les administrateurs
- **Prise en charge** des apps dans le cloud, mobiles et internes
- **Intégrations** avec les annuaires et d'autres technologies pour automatiser et simplifier la gestion
- **Règles** pour appliquer les normes de sécurité et contrôler les accès

Les équipes informatiques utilisent le SSO pour les applications prioritaires utilisées à l'échelle de l'entreprise. Toutefois, **plus de 50 %** des services dans le cloud les plus populaires ne sont pas compatibles en standard avec le SSO[10], et **77 %** des employés utilisent une app tierce dans le cloud à l'insu du SI[11]. Voilà pourquoi associer le SSO à un gestionnaire de mots de passe constitue le moyen le plus efficace de sécuriser chaque point d'accès.

plus de 50 %

des services dans le cloud les plus populaires ne proposent pas l'authentification unique en standard

77%

des employés utilisent une app tierce dans le cloud à l'insu du SI.

LA GESTION DES MOTS DE PASSE EN ENTREPRISE CAPTURE, STOCKE ET REMPLIT TOUT LE RESTE.

Avec la gestion des mots de passe en entreprise (GME), les employés ont également qu'un seul mot de passe à mémoriser. Tous les autres mots de passe sont capturés et stockés dans le gestionnaire de mots de passe, qui les saisit lorsque l'employé doit se connecter quelque part. Un gestionnaire de mots de passe simplifie d'autres tâches liées aux mots de passe, comme générer des mots de passe, partager des identifiants ou changer d'anciens mots de passe.

PRINCIPALES FONCTIONNALITÉS DES SOLUTIONS GME :

- **Un seul mot de passe** qui déverrouille l'accès à tous les identifiants
- **Un coffre-fort** pour stocker, consulter, gérer, modifier et insérer les identifiants de connexion
- **Capture et remplissage automatique** de tout formulaire de connexion (dont ceux que le SI ne connaît pas)
- **Partage chiffré des mots de passe**
- **Générateur de mots de passe** qui crée des mots de passe longs et uniques
- **Tableau de bord d'administration centralisé** avec règles, rapports et intégrations pour donner visibilité, automatisation et contrôle au SI

La GME peut améliorer considérablement la posture de sécurité d'une entreprise en identifiant en éliminant les mots de passe faibles et réutilisés. Le SI obtient une meilleure visibilité sur tous les services et toutes les apps utilisées, et peut imposer des mots de passe forts pour protéger l'accès à tous les services masqués (informatique parallèle).

COMMENT LES SOLUTIONS D'AUTHENTIFICATION AJOUTENT UNE SÉCURITÉ INTELLIGENTE À CHAQUE POINT D'ACCÈS.

Lorsque quelqu'un veut accéder à un système ou une ressource, il est essentiel 1) de prouver que la personne est qui elle prétend être et 2) de vérifier qu'elle est autorisée à accéder à l'élément concerné. C'est précisément ce que fait une solution d'authentification en validant l'identité de l'utilisateur en fonction de données uniques, puis en autorisant un accès sécurisé après vérification de ses privilèges.

Les mots de passe ont beau être la première ligne de défense pour la plupart des organisations, 80 % des piratages sont liés à l'utilisation d'identifiants volés[12]. Une fois qu'un mot de passe est dérobé, si aucune autre mesure n'est en place pour détecter et bloquer l'accès non autorisé, une fuite est inévitable. S'appuyer sur les mots de passe seuls, ce qui est une forme d'authentification à un seul facteur, ne suffit pas.

C'est pourquoi les entreprises ont besoin de l'authentification multifacteur.

L'AUTHENTIFICATION MULTIFACTEUR DÉJOUE LES PIRATES SANS RALENTIR LES EMPLOYÉS.

Avec l'authentification multifacteur (AMF), plusieurs informations ou facteurs sont exigés pour valider l'identité des utilisateurs et les connecter aux technologies qu'ils utilisent dans le cadre de leur travail.

CES FACTEURS PEUVENT ÊTRE UNE COMBINAISON DE :

1 Quelque chose que vous savez

(un facteur de connaissance) comme un mot de passe, un code PIN ou une question de sécurité

2 Quelque chose que vous êtes ou faites

(un facteur d'inhérence) comme une empreinte digitale, le visage, la rétine ou la voix

3 Quelque chose que vous avez

(un facteur de possession) comme une carte d'identité, un jeton matériel ou un jeton logiciel

De nombreuses entreprises connaissent l'authentification à deux facteurs (A2F), généralement un mot de passe (connaissance) et un code généré par une application sur un smartphone (possession).

Toutefois, les inconvénients de l'A2F standard sont la non-prise en charge d'un large éventail de cas d'utilisation (impliquant des apps anciennes, mobiles, internes et dans le cloud), et l'incapacité à s'adapter à des scénarios particuliers (les mêmes facteurs sont exigés, quelle que soit la situation). C'est pourquoi une solution AMF qui exploite plusieurs types de données disponibles et qui prend en compte différents comportements, appareils personnels, niveau d'accès et attributs est bien plus efficace.

PRINCIPALES FONCTIONNALITÉS DES SOLUTIONS D'AMF :

- **Authentification biométrique** à l'aide de facteurs physiques comme le visage, les empreintes digitales, la voix ou l'iris
- **Authentification contextuelle** à l'aide de facteurs cachés comme l'emplacement, l'adresse IP ou l'ID d'un téléphone
- **Authentification adaptative** qui exploite l'intelligence biométrique et contextuelle pour adapter les exigences de connexion aux utilisateurs et scénarios particuliers
- **La possibilité** de remplacer les mots de passe par l'AMF
- **La protection de tous les points d'accès,** y compris les apps anciennes, dans le cloud, mobiles et internes
- **Contrôle granulaire centralisé** depuis un tableau de bord d'administration simple à utiliser
- **Intégration avec les annuaires** et d'autres technologies pour simplifier le déploiement et la gestion
- **Chiffrement efficace** des données biométriques pour assurer la confidentialité et la sécurité

L'AMF va plus loin que l'approche indifférenciée de l'A2F afin d'offrir aux organisations un moyen plus intelligent de protéger chaque point d'entrée. Mais au lieu de ralentir les employés avec des formulaires et des codes fastidieux, les meilleures solutions d'AMF exploitent des facteurs cachés et physiques pour identifier et authentifier les utilisateurs via une expérience de connexion fluide.

ADMINISTRATEURS ET UTILISATEURS : LA SÉCURITÉ SANS SACRIFIER LA CONVIVIALITÉ.

Pour qu'une solution d'identité soit adoptée avec succès dans votre entreprise, vous devez répondre aux besoins des administrateurs informatiques comme des utilisateurs finaux. Lésiner sur les fonctionnalités ou la convivialité pour les uns ou les autres suscitera résistance et insatisfaction.

LES ADMINISTRATEURS ONT BESOIN DES ÉLÉMENTS SUIVANTS :

- **Un emplacement unique pour gérer** tous les utilisateurs et points d'accès
- **Des règles qui permettent d'exercer un contrôle** sur toute l'organisation, au niveau des utilisateurs et des groupes
- **Une configuration prête à l'emploi** capable de se brancher sur l'infrastructure existante
- **La prise en compte de tous les cas d'utilisation** de l'entreprise
- **La compatibilité avec l'authentification unique**, la gestion des mots de passe en entreprise et d'autres solutions IAM
- **Une diversité de méthodes d'AMF,** qu'elles soient bio-métriques, par notification push ou encore adaptatives, et pouvant être fournies au niveau des individus ou des groupes

LES UTILISATEURS FINAUX ONT BESOIN DES ÉLÉMENTS SUIVANTS :

- Une installation en un minimum d'étapes
- Peu ou pas de formation
- Une expérience de connexion fluide qui devient vite transparente
- La confidentialité de leurs données

POURQUOI LES ENTREPRISES ONT BESOIN D'UNE SOLUTION D'IDENTITÉ GLOBALE ET TOUT-EN-UN.

Les solutions d'authentification unique, de gestion des mots de passe en entreprise et d'authentification multifacteur offrent toutes d'importants avantages en matière de sécurité et de productivité aux entreprises. Mais gérer plusieurs solutions peut s'avérer difficile. Les solutions ne cohabitent pas forcément bien, la multiplicité des outils augmente la complexité et les employés se heurtent à plus d'obstacles lors de leur travail.

Mais lorsqu'elles sont associées au sein d'une même solution, votre organisation obtient une visibilité et un contrôle unifiés sur l'ensemble des points d'accès. Et lorsque les budgets et les ressources sont limités, il va de soi qu'une solution globale et tout-en-un maximisera votre investissement IAM.

UNE SOLUTION D'IDENTITÉ EXHAUSTIVE DOIT OFFRIR :

- Un tableau de bord d'administration unique et convivial
- L'automatisation et une implication minimale du SI au quotidien
- Des règles SSO, GME et AMF personnalisables et granulaires
- Un portail pour débloquer l'accès à toutes les apps et tous les identifiants
- Une AMF souple qui prend en charge de nombreuses méthodes d'authentification
- Une authentification adaptative qui exploite les facteurs biométriques et contextuels
- Une expérience fluide pour les utilisateurs
- Conçu pour la sécurité

En résumé, une solution d'identité tout-en-un doit fournir au SI la supervision dont il a besoin pour accroître la sécurité au sein de l'organisation, tout en éliminant les obstacles liés aux accès pour les utilisateurs. Une solution facile à apprendre et à utiliser et qui simplifie la gestion au quotidien pour les administrateurs informatiques aura le plus de chances d'aboutir à une mise en œuvre réussie. Avec une visibilité unifiée sur l'accès utilisateur et l'authentification à travers l'entreprise, vous pouvez tirer parti de l'équilibre entre expérience utilisateur et la sécurité renforcée.

EN SAVOIR PLUS SUR LASTPASS IDENTITY.

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 multifacteur qui fonctionne à tous les niveaux, du cloud aux apps mobiles aux outils internes. De l'authentification unique à la gestion de mots de passe à l'authentification adaptative, LastPass Identity fournit un contrôle de haut niveau au SI et un accès fluide aux utilisateurs.

- Contrôle centralisé pour les administrateurs
- Plus de 1 200 applications à authentification unique
- Gestionnaire de mots de passe en entreprise de pointe
- Plus de 100 règles d'accès sécurisé
- Rapports avancés
- Partage sécurisé des mots de passe
- Intégrations des annuaires utilisateur
- Authentification multifacteur adaptative
- Une solution sécurisée

Sources :

1 McAfee CASB: MVISION Cloud
2 NTT Com Shadow IT Survey, 2016.
3 Forbes, 2018. « Why Your Millennials Are Leaving (And How to Keep Them) »
4 Verizon Data Breach Investigations Report (DBIR), 2019.
5 LastPass, « Psychologie des mots de passe : la négligence aide les pirates à prospérer », 2017.
6 LastPass and Vanson Bourne, « Guide de l'identité moderne : combler le fossé entre mots de passe et identité », 2019
7 LastPass and Vanson Bourne, « Guide de l'identité moderne : combler le fossé entre mots de passe et identité », 2019
8 SCORE, 2018
9 Cisco, « Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats », 2018.
10 LastPass, « L'exposé sur les mots de passe », 2017
11 NTT Com Shadow IT Survey, 2016.
12 Verizon 2019 Data Breach Investigations Report (DBIR)

LastPass •••| by LogMeIn

DÉCOUVREZ COMMENT UNIFIER ACCÈS ET AUTHENTIFICATION AVEC LASTPASS IDENTITY :

WWW.LASTPASS.COM/FR/PRODUCTS/IDENTITY

06.25.19/PDF/ LMI0638C