LastPass •••|
by LogMeIn

LE GUIDE DE L'IDENTITÉ MODERNE

Combler le fossé entre mots de passe et identité

INTRODUCTION

En tant que professionnel du SI et de la sécurité, vous avez certainement plus de responsabilités que jamais auparavant. Vous jonglez peut-être des priorités qui se font concurrence, du service d'assistance à la maintenance de réseau à la gestion de l'accès utilisateur et la sécurisation des identités des employés. Mais qu'est-ce qu'une identité, et de quelles informations avez-vous besoin pour optimiser la sécurité et la productivité avec les solutions de gestion d'identité et d'accès ? Surtout lorsque votre organisation ne dispose pas forcément des ressources nécessaires.

LassPass a mandaté le cabinet d'études de marché Vanson Bourne pour présenter un aperçu de la situation actuelle de la gestion d'identité. Nous avons interrogé 700 professionnels de l'informatique et de la sécurité dans des entreprises de 250 à 2 999 employés, dans différentes industries en Amérique du Nord, Europe et Asie-Pacifique. Les participants à l'enquête occupent une variété de fonctions dans le domaine de la sécurité informatique, dont 37 % à des postes de direction, 40 % à des postes d'encadrement et 23 % à des postes administratifs.

Dans ce rapport, nous avons rassemblé les conclusions de Vanson Bourne avec les enseignements tirés des expériences de nos clients. Dans les pages suivantes, nous offrons une définition de l'identité, une compréhension des différentes technologies de l'identité, un aperçu des méthodes utilisées par les organisations pour aborder l'identité et un examen des défis uniques auxquels elles sont confrontées.

Notre objectif est de vous apporter de la clarté au sujet de la gestion d'identité et d'accès (IAM) et des mesures concrètes pour appliquer ces connaissances afin d'améliorer le programme IAM au sein de votre organisation.

TABLE DES MATIÈRES

1. QU'EST-CE QUE L'IDENTITÉ ?

L'identité c'est **vous**. Ce sont les comportements, les appareils, les accès et les attributs qui vous sont propres en tant qu'individu. Votre identité vous permet de prouver que vous êtes la personne que vous prétendez être. Sur le lieu de travail, votre identité vous associe aux ressources correctes sur les appareils adéquats au bon moment, pour pouvoir travailler en toute sécurité et efficacité.

Mais l'identité est un sujet complexe. 24 heures sur 24, les employés utilisent de nombreuses applications, autorisées ou non, sur une variété d'appareils, de réseaux et localisations. Les menaces sont omniprésentes et en pleine évolution. Chaque employé a sa propre identité, par conséquent chaque identité doit être correctement gérée. Sans quoi, des utilisateurs non autorisés peuvent accéder à des applications et ressources auxquelles ils ne devraient pas avoir accès, conduisant à des failles de sécurité et des inefficacités organisationnelles.

Les technologies peuvent renforcer la complexité de l'identité, mais elles sont essentielles pour une gestion efficace de celle-ci. Comme nous le verrons dans les sections suivantes, différentes solutions peuvent être utilisées pour vous donner une plus grande visibilité sur les accès utilisateur dans toute l'organisation, et un meilleur contrôle sur ces accès.

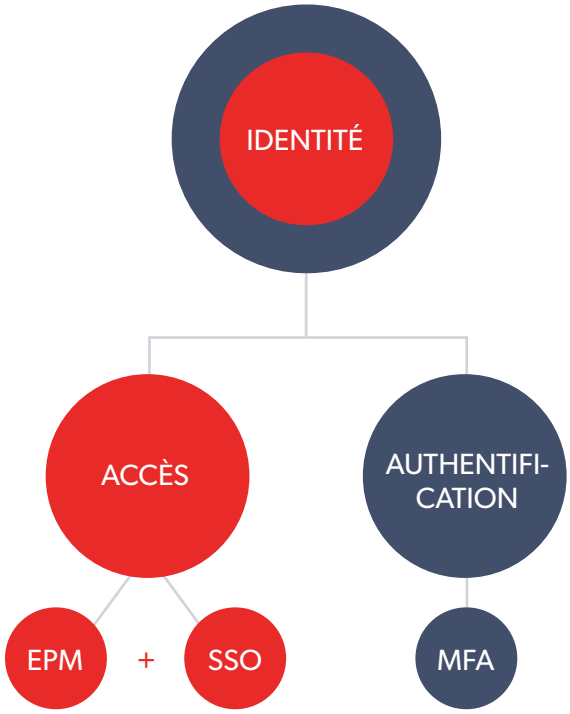
2. LA PILE TECHNOLOGIQUE DE L'IDENTITÉ MODERNE

Les technologies d'identité permettent de gérer les identités des utilisateurs de façon sécurisée afin de connecter les individus aux technologies dont ils ont besoin pour travailler.

Les technologies d'identité présentées dans ce rapport sont les suivantes :

- **L'authentification multifacteur (MFA) :** associe deux facteurs ou plus, dont un qui vous définit (inhérence), un que vous connaissez (connaissance) et un qui vous appartient (propriété), pour vérifier l'identité d'un utilisateur avant de lui accorder l'accès à un compte ou autoriser une action.
- **L'authentification unique (SSO) :** connecte les employés aux applications avec un ensemble unique d'identifiants de connexion, ce qui élimine les mots de passe pour des services clés.
- **La gestion des mots de passe entreprise (EPM) :** capture, enregistre et remplit les mots de passe pour toutes les connexions web basées sur des formulaires et simplifie le partage sécurisé des mots de passe.
- **La gestion d'accès privilégié (PAM) :** sécurise, contrôle, gère et surveille les accès aux comptes et systèmes critiques.
- **La gestion du cycle de vie :** automatise l'approvisionnement, le déprovisionnement et la gestion des identités utilisateur.

Utilisée individuellement, chaque technologie fournit aux entreprises des avantages uniques en matière de sécurité et de productivité. Associées, elles leur proposent une sécurité et une visibilité complètes sur chaque utilisateur et chaque point d'accès.



Avec des ressources plus limitées, il est particulièrement important de trouver une solution tout-en-un qui rassemble les éléments clés et optimise un investissement dans la technologie d'identité.

3. LA MISE À JOUR DES FONCTIONNALITÉS DE L'IDENTITÉ EST UNE PRIORITÉ ABSOLUE POUR L'ANNÉE À VENIR

En matière de sécurité, le travail d'un professionnel de l'informatique n'est jamais achevé. Que ce soit la mise à jour des technologies obsolètes, le suivi des dernières menaces ou l'identification de moyens plus efficaces pour former les employés, les équipes du SI ont du pain sur la planche.

La majorité des professionnels de l'informatique interrogés **(98 %)** estiment qu'il y a lieu d'améliorer le comportement général des employés en matière de sécurité (créer des mots de passe plus forts, partage et collaboration sécurisés), et plus de la moitié d'entre eux **(53 %)** évoquent des besoins d'améliorations importantes des comportements en matière de sécurité. Une minorité de professionnels de l'informatique **(< 5 %)** jugent que tous les organisateurs travaillent de manière complètement sécurisée. Il apparaît clairement que très peu d'entreprises crient victoire en matière de sécurité, ce qui n'est pas surprenant vu la rapidité d'évolution des menaces et des solutions de cybersécurité.

98 %

des interrogés estiment qu'il y a lieu d'améliorer le comportement général de leurs employés en matière de sécurité

53 %

évoquent des besoins d'améliorations importantes du comportement de leurs employés en matière de sécurité

<5 %

jugent que tous leurs employés travaillent de manière complètement sécurisée.

À cause de priorités opposées, les équipes du SI ont du mal à aborder leurs besoins en matière de sécurité. Une organisation type à en moyenne quatre objectifs de sécurité à atteindre dans l'année à venir, y compris la sécurisation des données **(75 %)**, la sécurisation de nouvelles technologies au fur et à mesure de leur adoption **(68 %)** et la réduction de risques **(66 %)**. **65 %** d'entre elles reconnaissent que la mise à jour de leurs capacités de gestion d'identité et d'accès est aussi un objectif prioritaire, qui peut contribuer en partie à aider les équipes du SI à atteindre les trois premiers objectifs. Le fait de garder les lumières allumées était classé en bas de la liste **(26 %)**, ce qui montre qu'en matière de sécurité, la dernière option est la complaisance.

LE TOP 4 DES OBJECTIFS DE SÉCURITÉ DU SI

75 % sécuriser les données

68 % sécuriser les nouvelles technologies au fur et à mesure de leur adoption

68 % réduire les risques

65 % mettre à jour les capacités de gestion d'identité et d'accès

4. LA PLUPART DES ORGANISATIONS SONT CONFRONTÉES AU DÉFI DE TROUVER LE JUSTE ÉQUILIBRE ENTRE LA SIMPLICITÉ D'UTILISATION ET LA SÉCURITÉ À L'HEURE D'IMPLÉMENTER UNE SOLUTION D'IDENTITÉ

Étant donné que la sécurité constitue une priorité absolue pour la plupart des organisations, il n'est pas surprenant que la plupart d'entre elles investissent dans des solutions d'identité. **Moins de 1 % (0,29 %)** des professionnels de l'informatique estiment que la gestion de l'accès utilisateur est sans effet sur la sécurité générale d'une organisation.

Malheureusement, **92 %** des organisations disent qu'elles font face à au moins un défi en matière d'identité. Une organisation type est confrontée à trois défis relatifs à l'identité : **47 %** des interrogés jugent difficile de trouver le juste équilibre entre la simplicité d'utilisation et le renforcement de la sécurité, **40 %** évoquent la sécurité générale de leurs solutions et **37 %** doivent faire face aux demandes de leurs employés pour trouver une solution simple à utiliser.

92 %

des organisations font face à au moins un défi en matière d'identité

47 %

Le juste équilibre entre simplicité d'utilisation et sécurité

40 %

La sécurité générale de leurs solutions

37 %

Les employés demandent une plus grande simplicité d'utilisation

Les défis varient aussi selon les pays. Le juste équilibre entre la simplicité d'utilisation et la sécurité renforcée est une priorité absolue en France **(56 %)**, au Royaume-Uni **(49 %)** et aux États-Unis **(47 %)** alors que la sécurité des solutions de gestion d'identité et d'accès arrive en tête de liste en Allemagne **(50 %)** et en Australie **(49 %)**.

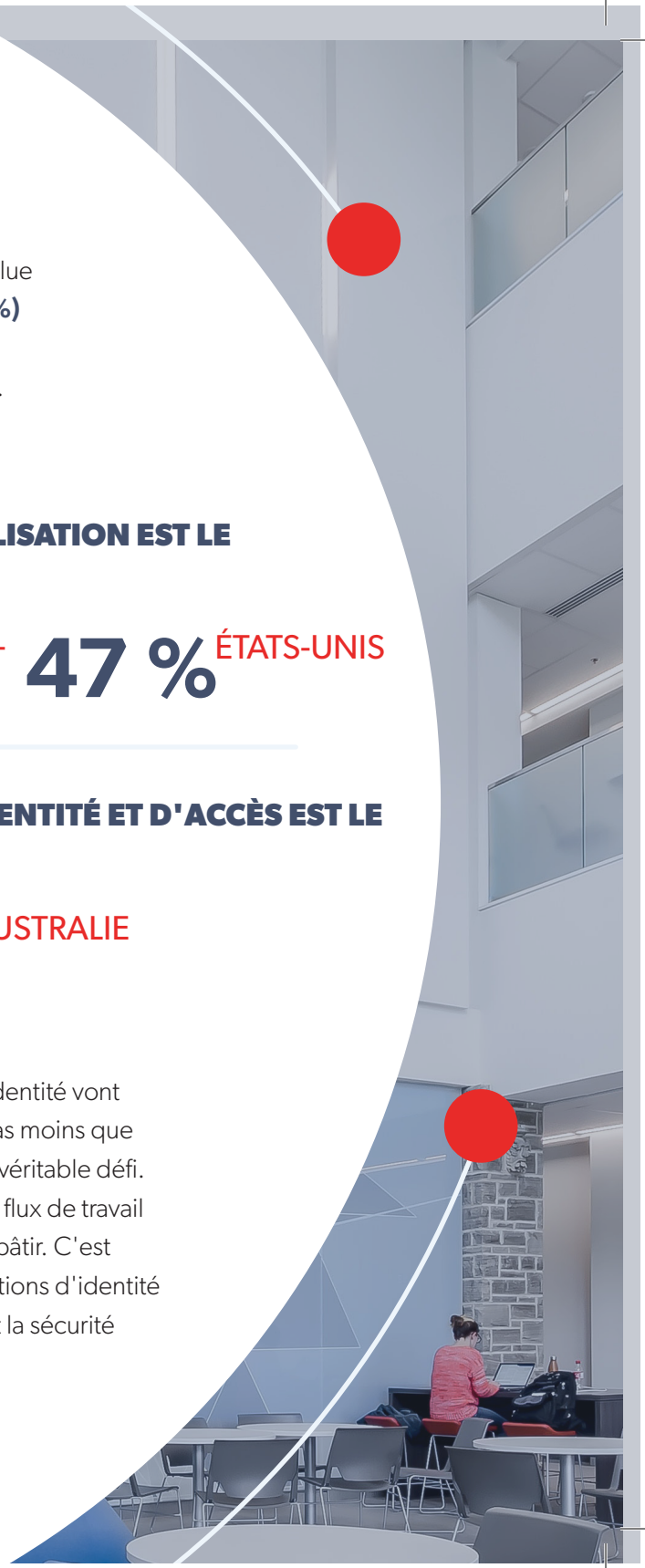
LE JUSTE ÉQUILIBRE AVEC LA SIMPLICITÉ D'UTILISATION EST LE DÉFI PRINCIPAL

56 % FRANCE **49 %** ROYAUME-UNI **47 %** ÉTATS-UNIS

LA SÉCURITÉ DES SOLUTIONS DE GESTION D'IDENTITÉ ET D'ACCÈS EST LE DÉFI PRINCIPAL

50 % ALLEMAGNE **49 %** AUSTRALIE

Même si les équipes du SI reconnaissent que les technologies d'identité vont beaucoup augmenter la sécurité des organisations, il n'en reste pas moins que trouver une solution que les employés sont prêts à adopter est un véritable défi. Toute technologie complexe à utiliser ou susceptible de ralentir le flux de travail d'un utilisateur constitue un obstacle et son adoption risque d'en pâtir. C'est pourquoi il est essentiel que les organisations choisissent des solutions d'identité simples à utiliser et adopter pour les utilisateurs, tout en renforçant la sécurité générale de l'entreprise.

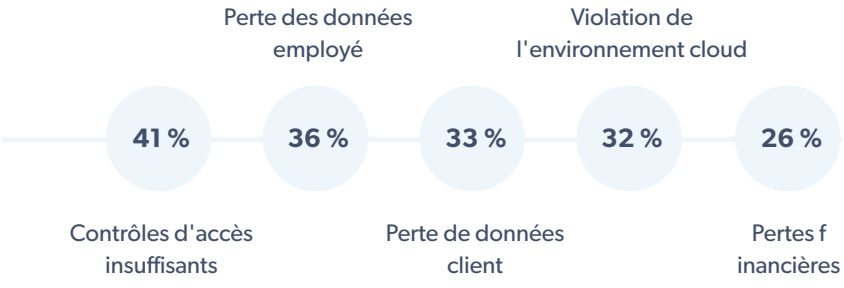


5. LES PRO DU SI RECONNAISSENT QUE LES MAUVAISES PRATIQUES EN MATIÈRE D'IDENTITÉ EXPOSENT LEURS ENTREPRISES À DES RISQUES

Les équipes du SI sont en général motivées pour mettre la priorité sur la sécurité et investir dans l'identité parce qu'elles sont témoin des conséquences de tout manquement. **82 %** des interrogés indiquent que leur entreprise a déjà été exposée à un risque suite à de mauvaises pratiques de gestion d'identité et d'accès, y compris des contrôles d'accès insuffisants **(41 %)**, la perte de données employé **(36 %)**, la perte de données client **(33 %)**, des pertes financières **(26 %)** et la violation de leur environnement cloud **(32 %)**. Le risque de contrôles d'accès insuffisants est arrivé en tête dans tous les pays sauf l'Australie, qui a classé le risque de violation de l'environnement cloud comme le plus élevé **(40 %)**.

82 %

déclarent que leur entreprise a été exposée à des risques en raison d'une gestion d'identité et d'accès insuffisante



Comme on peut s'y attendre, les organisations qui ont des besoins d'améliorations importantes au niveau du comportement général des employés en matière de sécurité sont celles qui sont susceptibles d'avoir été confrontées à la majorité des risques, surtout des contrôles d'accès insuffisants **(46 %)** et la perte des données client **(46 %)**.

UN COMPORTEMENT HASARDEUX EN MATIÈRE DE SÉCURITÉ AUGMENTE LES RISQUES

Organisations types* :

- Contrôles d'accès insuffisants — **41 %**
- Perte de données client — **36 %**

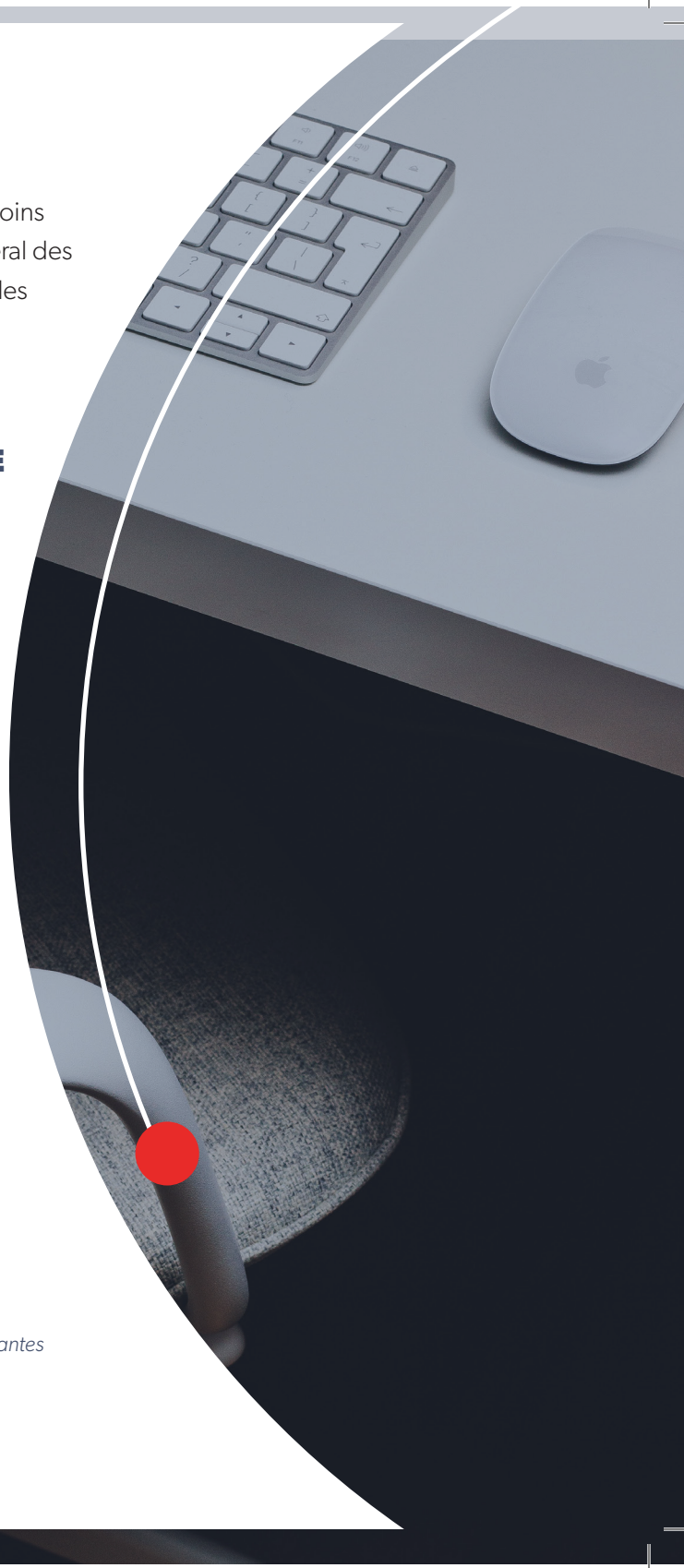
Organisations avec un faible niveau de sécurité* :

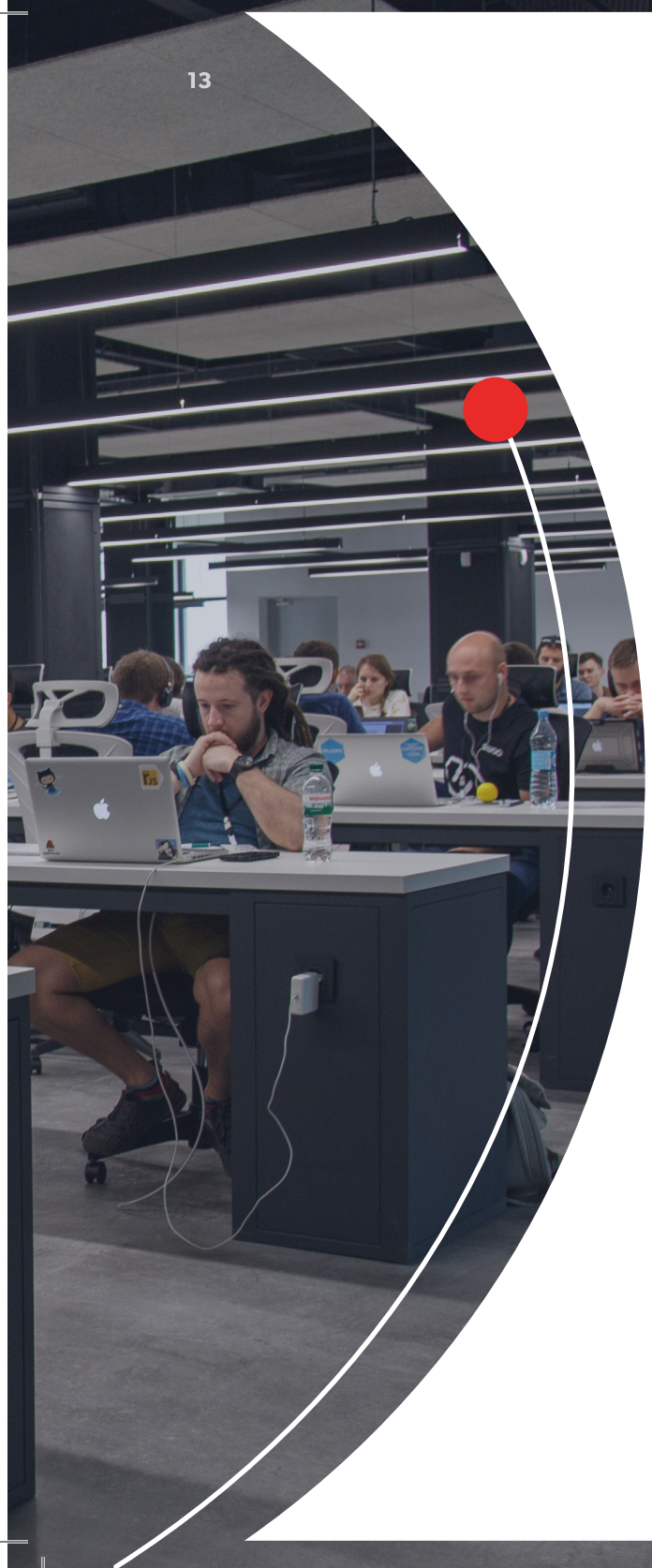
- Contrôles d'accès insuffisants — **46 %**
- Perte de données client — **46 %**

Face aux risques confrontés, et aux menaces potentielles, **81 %** des professionnels de l'informatique affirment que si leurs organisation n'implémentent pas une meilleure façon d'aborder l'identité, alors leur vulnérabilité à un large éventail de risques en matière de sécurité va augmenter. Comme on peut s'y attendre, **94 %** d'entre eux reconnaissent que la gestion d'identité et d'accès devrait constituer une priorité plus élevée dans leur organisation qu'elle ne l'est à l'heure actuelle. Les professionnels de l'informatique reconnaissent que l'utilisation des technologies d'identité pour supprimer de l'équation le comportement à risques des employés constitue un moyen efficace pour réduire les menaces visant l'organisation.

***** *La réponse type entre les 700 participants.*

***** *La réponse type des participants qui ont remarqué des améliorations importantes dans le comportement général de leurs employés en matière de sécurité.*

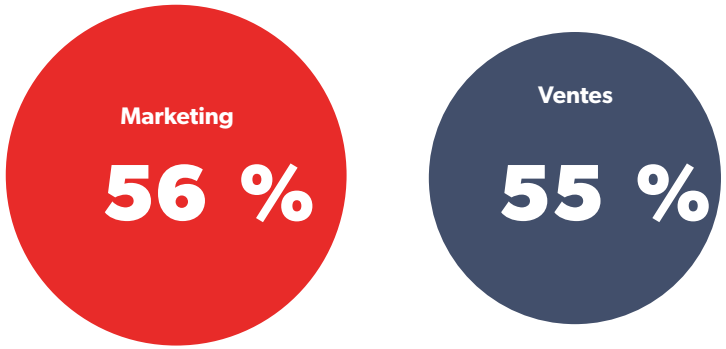




6. LES ÉQUIPES DE MARKETING ET VENTE SONT CELLES QUE L'ON ESTIME REPRÉSENTER LE PLUS DE RISQUES POUR UNE ORGANISATION

Qui met l'entreprise en danger ? **56 %** des professionnels de la sécurité informatique classent le marketing parmi les deux départements principaux les plus susceptibles d'opérer de façon non sécurisée, talonné de près par l'équipe de vente d'après **55 %** des interrogés. Pourquoi ? Il est possible que ces équipes, particulièrement le marketing, travaillent avec des prestataires ou des agences externes et ne suivent pas le protocole lors de ces démarches. Elles sont plus susceptibles de tester de nouveaux services cloud, sans l'accord du SI, pour obtenir des aperçus de données et des gains de productivité.

DÉPARTEMENTS LES PLUS ENCLINS À OPÉRER DE FAÇON NON SÉCURISÉE



DÉPARTEMENTS LES MOINS ENCLINS À OPÉRER DE FAÇON NON SÉCURISÉE

Finance

31 %

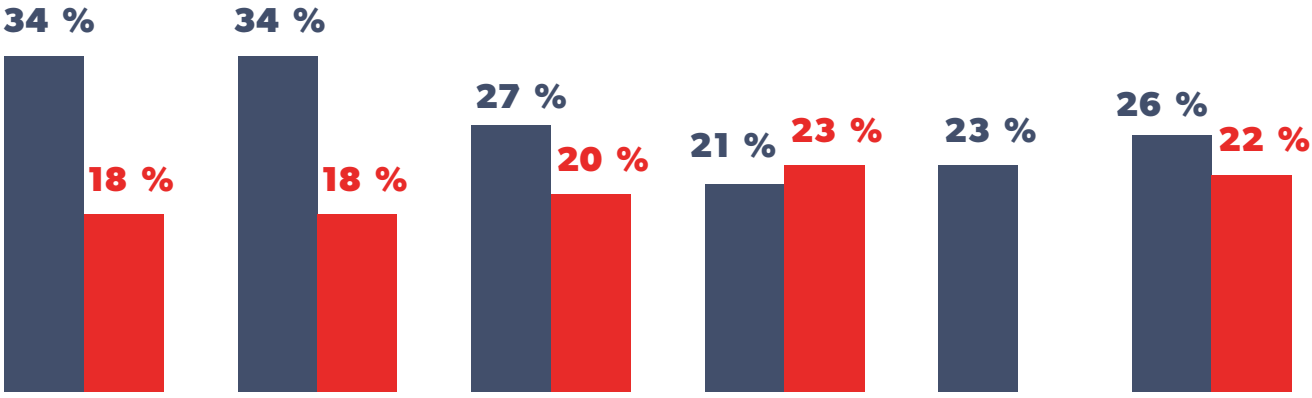
Le département financier est celui qui est le moins susceptible **(31 %)** d'être considéré comme étant un département à risques. Cette réputation est probablement liée aux nombreuses règles mises en œuvre pour cadrer les comportements au vu des données sensibles traiter de façon régulière par ce service.

Étant donné que les employés de tous les niveaux, dans tous les départements, peuvent poser un risque à l'organisation, il est essentiel que les équipes du SI implémentent des technologies d'identité simples à utiliser qui peuvent être déployées pour tout le personnel. Les solutions d'identité peuvent minimiser ou éliminer les comportements à risques, tels que la réutilisation de mots de passe ou le partage d'accès à des comptes sans surveillance administrative.

7. LES MOTS DE PASSE CONTINUENT DE CAUSER DES FRUSTRATIONS, ET DES RISQUES

Malheureusement, les équipes du SI continuent de passer un temps et des ressources précieuses pour gérer des tickets relatifs à des problèmes de mots de passe et des soucis de sécurité.

LA PLUPART DES ÉQUIPES DU SI REÇOIVENT DES TICKETS POUR LES PROBLÈMES SUIVANTS :



Identifiants perdus ou volés mensuellement ou deux fois par mois (18 %)

Identifiants piratés mensuellement, même si 18 % déclarent ne pas connaître le nombre de fois que des identifiants piratés sont signalés

Partage accidentel d'identifiants avec une personne non autorisée mensuellement ou deux fois par mois (20 %)

Mots de passe oubliés tous les jours ou deux fois par semaine (23 %)

Mises à jour de mots de passe sans notifications mensuellement

Soucis avec les notifications de mises à jour des mots de passe mensuellement ou une fois par mois (22 %)

En moyenne, les équipes de sécurité informatique passent **4 heures par semaine** sur des problèmes uniquement relatifs à la gestion des mots de passe et reçoivent **96 demandes relatives aux mots de passe par mois**. Certaines équipes du SI reçoivent plus de 25 requêtes de mots de passe oubliés par jour. Une organisation signale même que ses équipes du SI consacrent jusqu'à 30 heures par semaine à la gestion des mots de passe !

Compte tenu de la charge des mots de passe sur les ressources d'une organisation, il n'est pas surprenant que la plupart **(95 %)** des professionnels de la sécurité informatique déclarent que leur organisation devrait donner plus d'importance aux comportements visant à renforcer les mots de passe. Ce point de vue est surtout répandu en Allemagne pour **98 %** des participants.

Une vaste majorité de participants dont les organisations ont investi, ou qui planifient d'investir dans une solution de gestion des mots de passe entreprise, reconnaissent que ce type de solution pourrait apporter une sécurité organisationnelle renforcée **(54 %)**, un gestion simplifiée des profils utilisateurs et des identifiants **(47 %)** et une augmentation de la productivité des employés **(43 %)**.

Les données précédentes démontrent clairement que de nombreuses entreprises n'ont pas fini de gérer les obstacles relatifs à la gestion des mots de passe et aux risques de sécurité au sein de leur organisation. Étonnement, **90 %** des participants qui estiment que des améliorations importantes s'imposent au niveau du comportement général des employés de leur organisation en matière de sécurité, déclarent qu'ils ont mis en œuvre une solution de niveau entreprise, ce qui sous-entend que la gestion des mots de passe entreprise n'est que le point de départ de la gestion d'identité.

4 heures

consacrées par semaine à des problèmes relatifs à la gestion des mots de passe

95 %

des professionnels de la sécurité informatique estiment que leur société ferait bien de donner plus d'importance aux comportements visant à renforcer les mots de passe

93 %

des professionnels de l'informatique déclarent bien ou parfaitement comprendre les solutions de gestion de mots de passe entreprise

8. L'AUTHENTIFICATION UNIQUE EST ESSENTIELLE, MAIS ELLE CRÉE UN FOSSÉ CRITIQUE LORSQU'ELLE EST MISE EN ŒUVRE DE MANIÈRE ISOLÉE

La plupart des professionnels de l'informatique reconnaissent l'importance de la gestion de l'accès utilisateur. En réalité, **90 %** d'entre eux disent que la gestion de l'accès utilisateur est soit critique, soit très importante dans le cadre de la sécurité générale d'une organisation. Ce point de vue est surtout répandu chez les participants du Royaume-Uni **(93 %)**. Compte tenu des risques et de la charge sur les ressources associés aux mots de passe, les solutions d'authentification unique (SSO) offrent l'avantage d'éliminer les mots de passe dans les apps installées par le SI et de simplifier le processus de connexion pour les employés qui accèdent aux apps clés dans le cloud ou derrière le pare-feu.

La plupart des organisations ont déjà investi dans un type d'authentification unique, et **74 %** des participants ont indiqué avoir déjà mis en œuvre une telle solution. Ce n'est donc pas surprenant que de nombreux professionnels de l'informatique évoquent une très bonne sensibilisation aux solutions d'authentification unique, que **54 %** estiment parfaitement comprendre, et **40 %** bien comprendre. Ce niveau de sensibilisation est le plus élevé aux États-Unis avec **63 %** des participants déclarant parfaitement comprendre ces solutions, et le plus faible en Australie où seulement **39 %** des participants répondent la même chose.

La moitié des professionnels de la sécurité informatique **(49 %)** dont les organisations ont investi ou planifient d'investir dans une solution d'authentification unique, reconnaissent que ce type de solution pourrait apporter une gestion simplifiée des profils utilisateurs et des identifiants **(49 %)**, une sécurité organisationnelle renforcée **(48 %)** et une augmentation de la productivité des employés.

Même si l'authentification unique permet de réduire les risques des comportements des employés relatifs aux mots de passe en éliminant ceux-ci, de nombreux professionnels de l'informatique estiment que cette technologie constitue une simplification du processus de connexion des employés grâce à la mémorisation d'un seul mot de passe unique. Notons également que la visibilité ne fait pas partie des gains attendus (**seulement 31 %**), ce qui signifie que de nombreux professionnels de l'informatique reconnaissent que les solutions d'authentification unique utilisées de façon indépendante n'offrent pas d'aperçus complets des accès utilisateurs dans une entreprise.

Malheureusement, l'authentification unique n'est pas une panacée, et **38 %** des professionnels de l'informatique interrogés affirment qu'entre toutes les technologies couvertes dans ce rapport, l'authentification unique utilisée de manière isolée constitue la pire approche pour aborder la gestion d'identité. De nombreuses apps ne sont pas intégrées avec une solution d'authentification unique, soit parce qu'elles ne sont pas compatibles, leur niveau de priorité n'est pas assez élevé pour que le SI configure ce type d'authentification ou le SI ne sait même pas qu'elles sont utilisées. C'est pourquoi **80 %** des professionnels de l'informatique affirment que compter uniquement sur les solutions d'authentification unique augmente la vulnérabilité d'une variété d'apps du cloud et de comptes privilégiés. L'association de technologies d'authentification unique avec une solution de gestion de mots de passe entreprise garantit que chaque point d'accès est sécurisé, tout en éliminant presque, voire tous les obstacles relatifs aux accès auxquels sont confrontés les employés.

49 %

des organisations utilisant une solution d'authentification unique reconnaissent qu'elle simplifie la gestion de l'utilisateur et des identifiants

80 %

affirment que compter uniquement sur l'authentification unique augmente la vulnérabilité d'une variété d'apps du cloud et de comptes privilégiés

38 %

des professionnels de l'informatique affirment que l'authentification unique utilisée de manière isolée constitue la pire approche pour aborder la gestion d'identité

9. RENFORCER L'AUTHENTIFICATION UTILISATEUR AVEC L'AUTHENTIFICATION MULTIFACTEUR CONSTITUE UNE PRIORITÉ ÉLEVÉE

L'authentification multifacteur (MFA) connaît un regain de popularité ces dernières années au moment où les organisations reconnaissent l'inefficacité des mots de passe seuls pour protéger leurs activités. La plupart des organisations ont investi dans des solutions authentification multifacteur (MFA), dont **73 %** déclarent déjà avoir mis en œuvre une technologie MFA, et **19 %** s'attendent à ce que leurs organisations investissent dans ce système dans l'année à venir. En se basant sur des facteurs supplémentaires pour prouver l'identité de l'utilisateur avant d'accorder l'accès, l'authentification multifacteur protège les entreprises des risques posés par les mots de passe faibles ou piratés.

73 %

des organisations déclarent avoir mis en œuvre une technologie d'authentification multifacteur

19 %

s'attendent à investir dans une solution d'authentification multifacteur dans l'année à venir

59 % des professionnels de l'informatique reconnaissent que le renforcement de l'authentification utilisateur est critique et évoque cette stratégie comme leur priorité clé pour améliorer leurs capacités en matière d'identité. L'authentification multifacteur est une priorité absolue surtout en Allemagne, où **63 %** des professionnels de l'informatique la reconnaissent comme un de leurs objectifs clés de gestion d'identité et d'accès. Il n'est pas surprenant qu'un tiers des participants **(35 %)** disent que l'authentification multifacteur est la meilleure façon d'amorcer le thème de l'identité.

La majorité des professionnels de l'informatique déclarent bien comprendre **(45 %)** ou parfaitement comprendre **(48 %)** l'authentification multifacteur. Cependant, seuls **35 %** des professionnels en France et en Australie déclarent parfaitement comprendre l'authentification multifacteur. Par conséquent une meilleure sensibilisation est nécessaire pour augmenter la confiance dans l'utilisation et le déploiement de ces solutions.

L'implémentation des données biométriques est une priorité pour **36 %** des organisations des participants, et elle constitue une fonctionnalité spécifique de l'authentification multifacteur. La priorité est mise sur les données biométriques surtout en Allemagne pour **39 %** des participants. Nous nous attendons à une croissance continue de l'utilisation des données biométriques dans les années à venir, à mesure qu'elles deviennent plus disponibles grâce aux smartphones et que les employés s'habituent aux options d'authentification comme les empreintes digitales, la reconnaissance vocale et faciale. Les entreprises cherchant à déployer des solutions d'authentification multifacteur comportant des données biométriques doivent comprendre comment les données sont utilisées et conservées et s'assurer de la compatibilité avec tous les cas d'utilisation au sein de leur organisation.

59 %

des professionnels de l'informatique reconnaissent que le renforcement de l'authentification utilisateur est un élément critique

93 %

des professionnels de l'informatique déclarent bien ou parfaitement comprendre les solutions d'authentification multifacteur

36 %

des organisations pour qui travaillent les participants estiment que l'implémentation des données biométriques constitue une priorité

Les professionnels de la sécurité informatique dont les organisations ont investi ou planifient d'investir dans les solutions d'authentification multifacteur estiment que les avantages principaux sont une sécurité organisationnelle renforcée **(60 %)**, une diminution des incidents d'accès non autorisés à des informations confidentielles **(48 %)** et une baisse des risques de vols d'identifiants/mots de passe **(47 %)**. Encore une fois, la visibilité n'est pas un gain attendu des solutions d'authentification multifacteur (seulement **33 %**des interrogés). C'est pourquoi une solution qui proposerait un aperçu plus détaillé de l'authentification à travers l'entreprise apporterait beaucoup de valeur si elle était associée à l'authentification multifacteur.

Avec juste **1 %** des participants estimant que les solutions d'authentification multifacteur n'apportent aucun avantage, la plupart des professionnels de l'informatique et de la sécurité reconnaissent l'utilité et la nécessité de la technologie d'authentification multifacteur. Elle augmente significativement la sécurité des organisations en demandant aux utilisateurs de fournir des facteurs supplémentaires pour obtenir l'accès aux systèmes. Des fonctionnalités clés telles que les données biométriques et l'authentification adaptative offrent davantage de souplesse et une sécurité renforcée aux équipes du SI, même si les organisations souhaitent trouver des solutions avec un coût total de possession raisonnable et une gestion quotidienne minimale.

60 %

considèrent une sécurité organisationnelle renforcée comme l'avantage le plus évident des solutions d'authentification multifacteur

1 %

des participants déclarent que la technologie d'authentification multifacteur n'apporte aucun avantage

10. L'AUTOMATISATION DE LA GESTION DE L'IDENTITÉ EST EN PLEIN ESSOR

L'automatisation des tâches associées à la gestion de l'identité vous permet d'économiser du temps et des ressources. En moyenne, **40 %** de tous les participants classent l'automatisation des processus d'identité comme un objectif clé, avec la moitié des interrogés en Allemagne **(47 %)** et en Australie **(46 %)** focalisés sur l'amélioration de l'automatisation.

Nous nous attendons à voir un essor du rôle de l'automatisation à mesure que plus d'entreprises déploient des programmes de gestion d'identité dans leur organisation. Les solutions de gestion du cycle de vie peuvent automatiser l'approvisionnement et le déprovisionnement des identités pour automatiquement accorder aux utilisateurs l'accès associé à leur rôle ou supprimer le compte lorsque l'utilisateur quitte l'organisation ou change de rôle.

40 %

de tous les participants mettent la priorité sur l'automatisation des processus d'identité comme objectif clé

Focalisés sur l'amélioration de l'automatisation

Allemagne **47** % Australie **46** %

11. LES PROFESSIONNELS DE L'INFORMATIQUE RECONNAISSENT LES AVANTAGES EN MATIÈRE DE SÉCURITÉ DE LA GESTION D'ACCÈS PRIVILÉGIÉ

Plus de la moitié **(60 %)** des interrogés ont investi dans la gestion d'accès privilégié (PAM). **51 %** de la moyenne des interrogés déclarent parfaitement comprendre la gestion d'accès privilégié, les participants en Allemagne étant les moins sensibilisés, avec seulement **40 %** estimant parfaitement comprendre cette solution. En outre, **38 %** des professionnels affirment bien comprendre cette technologie. De manière générale, une sensibilisation supplémentaire relative à la gestion d'accès privilégié serait utile aux professionnels de l'informatique au niveau mondial.

51 %

des professionnels de l'informatique avec une expérience de gestion de l'accès privilégié reconnaissent qu'elle fournit une sécurité organisationnelle renforcée

Les professionnels de l'informatique dont les organisations ont investi ou planifient d'investir dans des solutions de gestion d'accès privilégié reconnaissent que les avantages principaux de ces solutions sont une sécurité organisationnelle renforcée **(51 %)**, une diminution des incidents d'accès non autorisés à des informations confidentielles **(45 %)** et une augmentation de la productivité des employés **(42 %)**. En outre, **26 %** d'entre eux planifient d'investir dans des solutions de gestion d'accès privilégié dans l'année à venir.

12. LES ORGANISATIONS ONT BESOIN D'UNE SOLUTION EXHAUSTIVE SIMPLE À IMPLÉMENTER ET FACILE À ADOPTER PAR LES UTILISATEURS

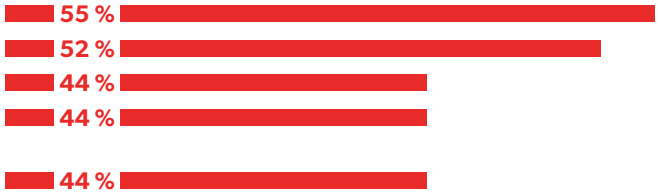
À l'heure de regarder les données mises en relief dans ce rapport, une chose est claire : alors que les professionnels de l'informatique estiment comprendre le besoin de gestion d'identité, il leur reste encore à présenter une solution exhaustive de gestion d'identité à leur organisation. Mais plutôt que d'investir dans des solutions **93 %** des professionnels de l'informatique reconnaissent que rassembler les différents aspects de la gestion d'identité et d'accès en une solution peut représenter un avantage pour la sécurité générale de toute l'organisation. Au vu des contraintes relatives aux ressources, nous reconnaissons que les organisations ont besoin d'une solution tout-en-un.

Une minorité de participants **(23 % à 38 %)** doivent mettre à jour leurs investissements sur tous les aspects de l'identité. Seuls **24 %** des professionnels de l'informatique évoquent le budget comme un défi dans le cadre de la gestion d'identité et d'accès, alors il suffit peut-être simplement de trouver la bonne solution pour votre entreprise.

DES ENTREPRISES RECONNAISSENT L'AVANTAGE D'UNE SOLUTION UNIFIÉE DE GESTION D'IDENTITÉ ET D'ACCÈS POUR LEUR ORGANISATION

À l'heure d'évaluer les capacités d'identité actuelles, les professionnels de l'informatique entrevoient des possibilités d'amélioration avec :

Nos participants ont mis en relief différentes fonctionnalités pour leur solution de gestion d'identité idéale :



En d'autres mots, la solution idéale de gestion d'identité et d'accès supporte un large éventail de cas d'utilisation, est compatible et s'intègre avec l'écosystème technologique existant dans l'entreprise, gère l'hygiène des mots de passe et offre une souplesse de configuration de la solution aux administrateurs afin de répondre aux besoins de sécurité unique de leur organisation.

Pour mettre en pratique ces fonctionnalités idéales, les professionnels de l'informatique signalent généralement les quatre priorités clés planifiées par leur organisation relatives à l'amélioration des capacités de gestion d'identité et d'accès ; le renforcement de l'authentification utilisateur **(59 %)**, l'intégration de l'infrastructure de sécurité **(57 %)**, la surveillance des activités utilisateur **(53 %)** et la simplification de l'accès utilisateurs **(44 %)** arrivent en tête de liste. Dans la plupart des cas, ces priorités reflètent les défis principaux rencontrés par ces professionnels. Par exemple, le renforcement de l'authentification utilisateur et l'intégration de l'infrastructure de sécurité permettent de gérer le défi de sécurisation des solutions de gestion d'identité tout en simplifiant l'accès utilisateur et en répondant aux demandes des utilisateurs pour une solution simple à utiliser.

Comme nous l'avons vu au cours de ce rapport, les technologies de gestion d'identité sont censées offrir des avantages au niveau de la sécurité et de la productivité. Dans la réalité, la plupart des participants **(93 %)** reconnaissent qu'implémenter une meilleure approche de la gestion d'identité et d'accès peut augmenter l'efficacité des employés. Pour concrétiser ces avantages, il est nécessaire d'investir dans une solution complète qui offre un juste équilibre entre l'expérience utilisateur et la sécurité.

13. PROCHAINES ÉTAPES : CE QUE VOUS DEVEZ SAVOIR POUR POURSUIVRE LA MISE EN ŒUVRE DE LA GESTION D'IDENTITÉ

En tant que professionnel de l'informatique, vous vous trouverez peut-être dans différents cas de figure relatifs à votre programme d'identité. Peut-être, allez vous investir dans une technologie de gestion d'identité et d'accès et chercher comment en ajouter d'autres. Peut-être que votre organisation utilise toutes ces technologies depuis longtemps, mais que vous estimez que vos solutions ne sont plus adaptées à vos activités. Ou alors, peut-être que votre entreprise ne dispose pas d'un programme de gestion d'identité, et vous vous demandez par où commencer.

D'ABORD, NOUS VOUS CONSEILLONS DE VOUS FAMILIARISER AVEC LES ÉLÉMENTS SUIVANTS :

- **Les problèmes que vous souhaitez résoudre :** La gestion de l'accès utilisateur est-elle un obstacle ? Est-ce que les employés gèrent les mots de passe de façon sécurisée ? Est-ce que la sécurité renforcée a un impact négatif sur la productivité des employés ?
- **Vos besoins pour résoudre ces problèmes :** Quel type de solution d'identité répond au défi auquel vous êtes confronté ? Existe-t-il une solution unifiée pour répondre à tous ces défis d'un coup ?
- **Les technologies que vous utilisez pour répondre à ces besoins :** Utilisez-vous la gestion des mots de passe ? Authentification unique ? Authentification multifacteur ?
- **Lacunes actuelles dans les technologies existantes :** Utilisez-vous des technologies de gestion d'identité et d'accès de manière isolée ?
- **Technologies supplémentaires qui vous aident à gérer ces lacunes :** Comment pouvez-vous compléter vos solutions actuelles de gestion d'identité et d'accès pour gérer l'identité utilisateur de façon sécurisée ?

En clarifiant l'état actuel de l'identité dans votre organisation, vous pouvez chercher et évaluer les technologies d'identité avec plus de concentration et d'intention. Une planification et prise de décision plus attentives permettent de garantir qu'un investissement dans des solutions de gestion d'identité et d'accès va générer un maximum de gains de productivité et de sécurité.

Une solution exhaustive qui rassemble les avantages de chaque technologie de gestion d'identité et d'accès constitue la meilleure option pour tous. Une solution tout-en-un qui offre une visibilité et un contrôle unifié sur tous les points d'accès, avec une expérience utilisateur simple à apprivoiser et à utiliser, est la plus susceptible de conduire à une implémentation réussie. Avec une visibilité unifiée sur l'accès utilisateur et l'authentification à travers l'entreprise, vous pouvez tirer profit d'un équilibre entre l'expérience client et la sécurité renforcée.

GÉRER L'IDENTITÉ UTILISATEUR AVEC UNE SEULE SOLUTION

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 nuage aux apps mobiles aux outils hérités 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 centralisé pour les administrateurs
- Plus de 1 200 applications à authentification unique
- Gestionnaire de mots de passe leadeur sur le marché
- Plus de 100 règles d'accès sécurisé
- Rapports avancés
- Partage sécurisé des mots de passe
- Intégrations des annuaires utilisateur
- Authentification multifacteur adaptative
- Une solution unique

lastpass.com

LastPass •••|
by LogMeIn

Unifier l'accès et l'authentification

www.lastpass.com/fr/products/identity

© 2019 LogMeIn, Inc. Tous droits réservés.

06.26.19/PDF/ LMI0638C