


# Le secteur des TI se concentre sur les avantages de l'IAM en matière de sécurité et donne la priorité à la MFA



 Les entreprises du secteur des technologies de l'information (TI) agissent sur les marchés du matériel ou des logiciels. En tant qu'entreprises technologiques et qui gèrent les données de leurs clients, il est évident que leur rapport à la technologie a un impact sur leur stratégie d'IAM.

## Sécuriser les données est la priorité.



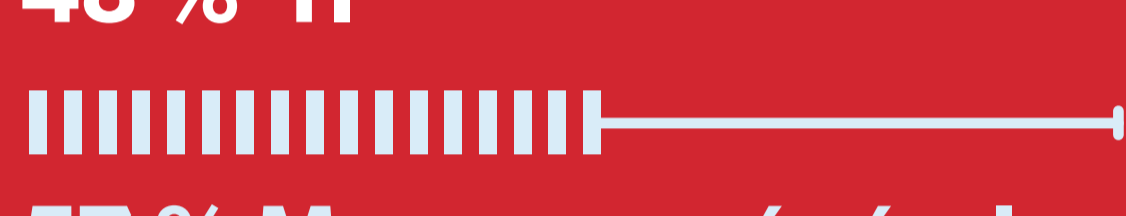
**Notre avis :** Le secteur des TI est particulièrement bien placé pour mesurer les risques liés aux pertes de données. **Les entreprises de TI gèrent souvent de gros volumes de données ;** les leurs et celles de leurs clients, surtout dans le cas du logiciel-service.

## Mettre à niveau l'IAM est une priorité.



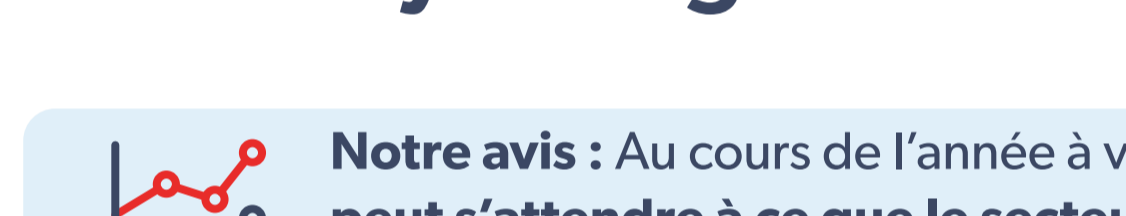
**Notre avis :** Il est surprenant de constater **qu'améliorer l'IAM est moins prioritaire.** Les entreprises de TI ont peut-être déjà mis à niveau leurs solutions d'IAM, ou alors ce n'est pas un domaine qu'elles évaluent pour l'instant.

## C'est dans l'intégration des infrastructures de sécurité que je dois progresser le plus.



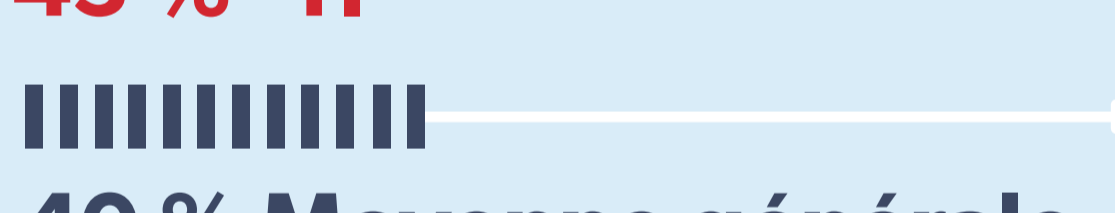
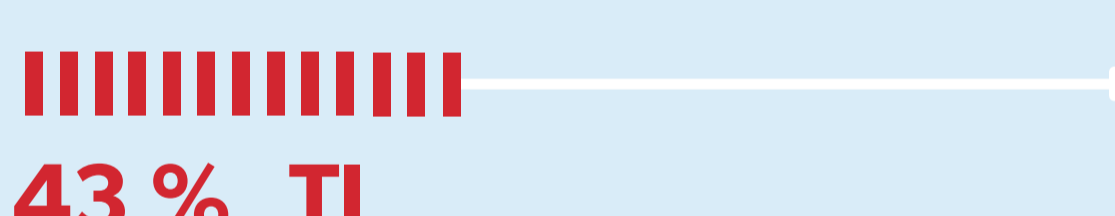
**Notre avis :** Le secteur des TI se soucie moins de l'intégration, ce qui suggère que les solutions d'IAM ont effectivement déjà été mises à niveau. C'est ce qu'indique notre Rapport mondial sur la sécurité des mots de passe de 2019, qui montre que les entreprises de TI sont en tête en matière d'adoption de la MFA et de posture de sécurité<sup>1</sup>.

## L'IAM peut améliorer l'efficacité des employés.



**Notre avis :** Au cours de l'année à venir, l'on peut s'attendre à ce que le secteur des TI se focalise sur l'amélioration de la sécurité grâce à l'IAM, car les avantages en matière de productivité sont moins prioritaires. Cela permettra également au secteur des TI de répondre à sa priorité qui est la sécurisation des données.

## La sécurité de nos solutions IAM est un défi.



**Notre avis :** Il n'est pas surprenant que la productivité des employés préoccupe moins le secteur des TI, puisque la sécurité est son principal défi. Les fuites de données ont exposé 4,1 milliards d'enregistrements au cours du premier semestre 2019<sup>2</sup>, et alors que le secteur des TI gère de plus en plus de données sur les clients, conserver le contrôle sur chaque point d'accès devient de plus en plus complexe.

## L'IAM devrait être une priorité plus élevée dans mon organisation.



**Notre avis :** Toutefois, le secteur des TI est conscient que **l'IAM doit être plus prioritaire.** En moyenne, chaque employé a accès à 17 millions de fichiers<sup>3</sup>, et lorsque les entreprises de TI gèrent aussi les données de leurs clients, ce nombre augmente, tout comme la nécessité de contrôles plus stricts.

## Je compte investir dans la MFA.



**Notre avis :** On peut s'attendre à ce que le secteur des TI se concentre sur la MFA au cours de l'année à venir, ce qui l'aidera à atteindre ses objectifs en matière de sécurité, puisque la MFA permet de s'assurer que seuls les bons employés ont accès aux données sensibles.

## NOS RECOMMANDATIONS POUR LES TI :



### Privilégier la facilité d'utilisation pour les employés.

Une stratégie IAM étant déjà en place, le moment est venu pour les entreprises de TI de se concentrer sur le comportement des employés afin d'accroître l'adoption, et ainsi de renforcer la sécurité de l'entreprise.



### Évaluer si l'approche IAM est globale.

Les entreprises de TI doivent déterminer si leur programme IAM actuel couvre l'ensemble du cycle de vie des employés et tous les points d'accès à l'organisation.



### Évoluer vers la MFA adaptative.

La MFA adaptative complique les tentatives de connexion anormales, tout en permettant aux employés de s'authentifier de façon transparente. Cela renforcera la confiance des entreprises de TI envers leurs utilisateurs, sans gêner ces derniers dans leur travail.

En savoir plus : [www.lastpass.com/fr/products/identity](http://www.lastpass.com/fr/products/identity)

Sources:  
1. <https://www.lastpass.com/fr/state-of-the-password/global-password-security-report-2019>  
2. <https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>  
3. <https://www.varonis.com/2019-data-risk-report/>  
4. Données d'enquête LastPass