

La finance se concentre sur la réduction des risques tout en intégrant son infrastructure IAM



Les services financiers gèrent des données d'un genre particulièrement sensible : l'argent. Le secteur financier est confronté à des enjeux plus importants que la plupart des marchés verticaux, ce qui affecte inévitablement sa manière de gérer les accès et l'authentification des employés.



Réduire les risques est une priorité.



Notre avis : En raison de la nature hautement sensible des données et de la réglementation associée, comme le **Financial Action Task Force (TASF)**, le **Bank Secrecy Act (BSA)** et la **5e directive anti-blanchiment d'argent (SAMLd)** de l'UE, il n'est pas surprenant que la réduction des risques soit une priorité IAM plus importante sur le secteur de la finance.

Des pirates ont pénétré mon organisation.



Notre avis : Toutefois, lorsque l'on considère le piratage informatique, la finance est en difficulté. Le secteur financier a toujours été visé par des attaques très diverses, qu'elles ciblent les institutions ou leurs clients, et **la cybercriminalité lui coûte plus cher que dans tous les autres secteurs**, avec une moyenne de \$18,3 millions par an¹.

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



Notre avis : En matière d'améliorations, **le secteur financier place les intégrations en tête**, dans le but d'obtenir une vision globale des accès et de l'authentification des utilisateurs, afin de réduire le pourcentage inquiétant de piratages réussis.

Les budgets d'IAM insuffisants sont un défi.



Notre avis : S'il y a bien un domaine qui ne pose pas de problème au secteur financier, c'est le budget. **La finance mesure les risques élevés liés à la gestion de l'argent** et consacre jusqu'à 14 % de son budget informatique annuel aux programmes de cybersécurité².

J'ai déjà investi dans la MFA.



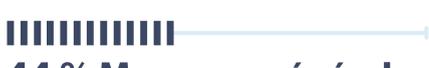
Notre avis : En matière d'affectation de ce budget, **la MFA est la technologie la mieux dotée**. C'est sans doute une conséquence de la norme NIST (National Institute of Standards and Technology) qui recommande l'utilisation de la MFA pour renforcer la sécurité de chaque tentative de connexion.

Je compte investir dans la gestion des mots de passe.



Notre avis : **Le secteur financier accorde une priorité de 10 % plus élevée à la gestion des mots de passe que les autres secteurs**, sans doute parce que leurs employés partagent des identifiants sensibles. La gestion des mots de passe permettra au secteur financier de gérer et partager les mots de passe pour atteindre son objectif de réduction des risques.

J'ai besoin d'un système intégré pour gérer, surveiller et définir des règles.



Notre avis : Dans une solution IAM idéale, **la finance cherche un moyen de gérer les accès et l'authentification des utilisateurs** compatible avec leurs priorités en matière d'intégration. Cela permettra au secteur financier de simplifier la gestion de l'IAM à l'échelle de l'organisation.

NOS RECOMMANDATIONS POUR LA FINANCE :



Ajouter la MFA partout.

La MFA au niveau des applications, des postes de travail et du VPN est un moyen simple de réduire les risques, et elle simplifie également les audits et le respect de la réglementation.



Se concentrer sur les intégrations et la souplesse.

Envisagez des technologies d'IAM qui offrent un large éventail d'intégrations pour un maximum de souplesse dans l'utilisation de vos outils de prédilection.



Unifier l'IAM lorsque c'est possible.

Une vue unifiée des accès et de l'authentification des utilisateurs permet aux entreprises de mieux se prémunir contre les risques potentiels.

En savoir plus : <https://www.lastpass.com/fr/products/identity>