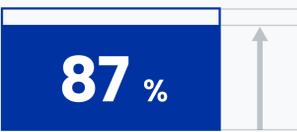
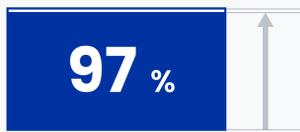


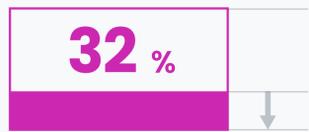
À l'ère de l'accélération numérique, la sécurité des identités est un impératif stratégique pour les entreprises



87 % des RSSI jouent un rôle de premier plan dans la gestion des identités et des accès (IAM), faisant de la sécurité des identités une priorité stratégique absolue.¹



97 % des entreprises prévoient d'investir dans des mesures de sécurité liées aux identités au cours des deux prochaines années.²

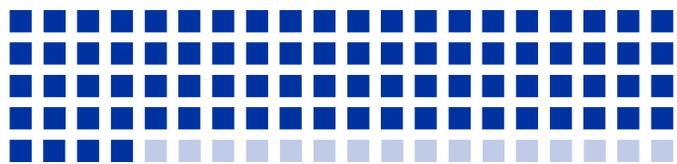


Pourtant, seules 32 % des entreprises déclarent avoir confiance dans leur propre programme de sécurité des identités.³

En matière de sécurité des identités, les objectifs de l'entreprise et ceux du business peuvent diverger en dépit d'incidences financières MAJEURES.

4,24
M\$

Coût total moyen d'une violation de données



84 % des personnes interrogées ont fait l'objet d'une violation de données liée aux identités

Le coût total moyen d'une violation de données s'élevait à 4,24 millions de dollars⁴ en 2021, et 84 % des personnes interrogées ont fait état d'une violation de données liée aux identités au cours de l'année écoulée².

Les moteurs de la sécurité des identités ont évolué :



Adoption accélérée du cloud



Renforcement de la conformité



Suivi d'une foule de nouvelles identités et de nouveaux droits

Mais les trois principaux obstacles à la mise en place d'un solide programme de sécurité des identités restent les mêmes :

Ressources limitées

56 %

56 % des entreprises estiment que, dans le domaine de la cybersécurité, les pénuries de personnel les exposent à un risque modéré ou extrême.⁵

Environnements numériques complexes

55 %

55 % des entreprises s'appuient sur des processus manuels pour ajuster les accès lorsque les environnements informatiques évoluent brusquement.⁶

Manque de visibilité sur les données d'accès

>50 %

Moins de 50 % des entreprises savent qui a accès aux ressources dans le cloud, aux terminaux et aux données non structurées.⁵

Les capacités humaines sont largement dépassées lorsqu'il s'agit d'assurer la connexion sécurisée des bonnes personnes à la bonne technologie.



L'intelligence artificielle (IA), le Machine Learning (ML) et l'analytique offrent une formidable occasion d'améliorer votre posture de sécurité des identités et de vous prémunir contre des coûts considérables liés aux violations de la sécurité.

80 %

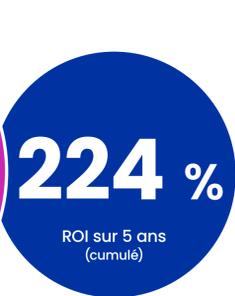
Différence de coût

Une récente étude a mis en évidence une différence de coût de 80 % associée aux violations de la sécurité dans les entreprises où l'IA et l'automatisation de la sécurité étaient entièrement déployées, par rapport à celles où elles ne l'étaient pas.⁴ L'IA et l'automatisation sont les facteurs de la sécurité qui ont eu le plus d'impact positif sur les coûts.

La solution AI-Driven Identity Security de SailPoint offre aux entreprises, de manière dynamique, rapide et à grande échelle, une visibilité à 360 degrés des accès nécessaires et de ceux présentant des risques élevés de violation de la sécurité.

La solution AI-Driven Identity Security permet aux clients de SailPoint d'obtenir des résultats opérationnels concrets.

Une entreprise du secteur de l'énergie mettant à profit les recommandations formulées par l'IA a constaté les gains suivants :



Grâce aux campagnes de certification automatisées, St. James Place a obtenu les résultats suivants :

Les certifications ne prennent plus que **1 mois**, par rapport à **1 an** auparavant

640 comptes obsolètes ont été découverts et supprimés

Les accès superflus à **380** comptes ont été révoqués

Découvrez comment l'IA et le Machine Learning mis en œuvre dans la solution AI-Driven Identity Security de SailPoint peuvent faire évoluer pour de bon votre programme de sécurité des identités.

[En savoir plus](#)