La valeur stratégique de l'identité pour les RSSI

La disparition du périmètre réseau a fait de l'identité le point de contrôle fondamental de la cybersécurité, révolutionnant ainsi les opérations de sécurité. Cette présentation est une synthèse de l'étude* réalisée par Enterprise Strategy Group et Okta sur cette évolution. Elle nous livre cinq constats clés sur l'enjeu que représente la sécurité de l'identité pour les RSSI :

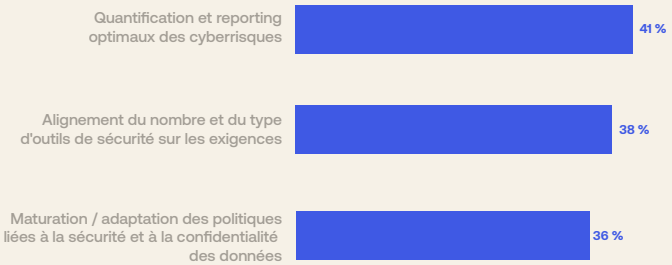
1. Le RSSI est passé d'une position défensive à l'offensive.
2. Les responsabilités du RSSI ont évolué vers un business enablement stratégique.
3. Les RSSI considèrent l'identité comme la principale vulnérabilité de leur entreprise.
4. Les RSSI ne voient pas de solution simple pour garantir la sécurité des identités.
5. La multiplication des technologies aggrave les problèmes liés à la sécurité de l'identité.

CONSTAT 1 :

Le RSSI est passé d'une position défensive à l'offensive

Les stratégies de sécurité d'entreprise traditionnelles, basées sur le périmètre, sont par nature défensives, mais une telle posture n'est plus adaptée à l'environnement de travail moderne. L'étude ESG a révélé que les principales tâches des RSSI sont toutes axées sur des stratégies proactives, à savoir la quantification / le signalement des risques, la rationalisation des contrôles et la confidentialité des données :

Principales tâches des RSSI



CONSTAT 2 :

Les responsabilités du RSSI ont évolué vers un business enablement stratégique

D'après l'étude d'ESG, les RSSI envisagent leurs responsabilités sous un angle plus stratégique et se concentrent davantage sur les résultats critiques pour l'entreprise.

Principales responsabilités des RSSI

Maturation / adaptation des politiques liées à la sécurité et à la confidentialité des données (p. ex. Zero Trust)

Les RSSI redéfinissent les métriques de réussite et ne se limitent plus aux taux d'incidents et aux délais de réponse. Ils s'intéressent davantage à l'impact de la sécurité sur l'activité, notamment sur le lien entre la fréquence ou la durée des interruptions et les incidents de sécurité.

Quantification / démonstration de la façon dont la sécurité contribue à la croissance et/ou aux objectifs de l'entreprise

Alors que cette tâche était auparavant axée sur les métriques de conformité, elle est désormais plus orientée vers une réflexion stratégique sur la productivité de l'entreprise et d'autres métriques liées aux ressources humaines.

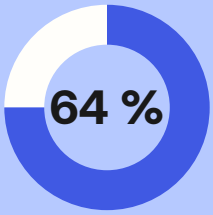
Mise en place d'une authentification forte et fluide pour l'ensemble des collaborateurs et clients

La gouvernance des identités occupe également une place prépondérante dans leurs priorités. En effet, les RSSI interrogés dans le cadre de l'étude estiment que certaines responsabilités telles que la gestion des identifiants et le contrôle des accès doivent être envisagées de façon à faciliter un accès fluide aux collaborateurs et clients.

CONSTAT 3 :

Les RSSI considèrent l'identité comme la principale vulnérabilité de leur entreprise

Malgré la transition vers des stratégies proactives et non plus réactives, environ deux tiers des RSSI interrogés dans le cadre de l'étude déclarent qu'il leur est difficile de se protéger contre les cyberattaques. Plus précisément, les RSSI considèrent la sécurité des identités comme leur principale vulnérabilité et reconnaissent être confrontés à un large éventail de défis liés à l'identité qui affaiblissent leur posture de sécurité globale. Cela n'a rien de surprenant, au vu des nombreuses études indiquant que l'identité est désormais le principal vecteur de brèches de données.



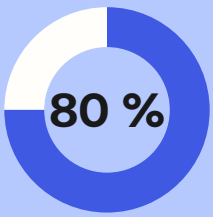
des RSSI affirment qu'il est **difficile** de bloquer les cyberattaques

2/3

des RSSI affirment que la **majorité** des **incidents de sécurité** sont dus à l'identité

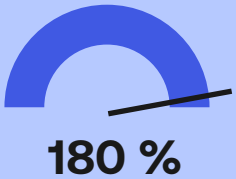
Principaux défis en matière d'identité entravant les cyberdéfenses, selon les RSSI interrogés

1. Incapacité à identifier avec précision et à prévenir la création de comptes frauduleux et les tentatives de connexion à grande échelle
2. Pratiques incohérentes en matière de gouvernance des identités
3. Manque de soutien à l'adoption d'une authentification plus forte / dépendance excessive vis-à-vis des mots de passe
4. Gestion des identités manuelle / fragmentée
5. Implémentation lacunaire du MFA



des brèches de données commencent par **des identifiants compromis**

Verizon, 2024 Data Breach Investigations Report



Augmentation annuelle des attaques liées à l'identité

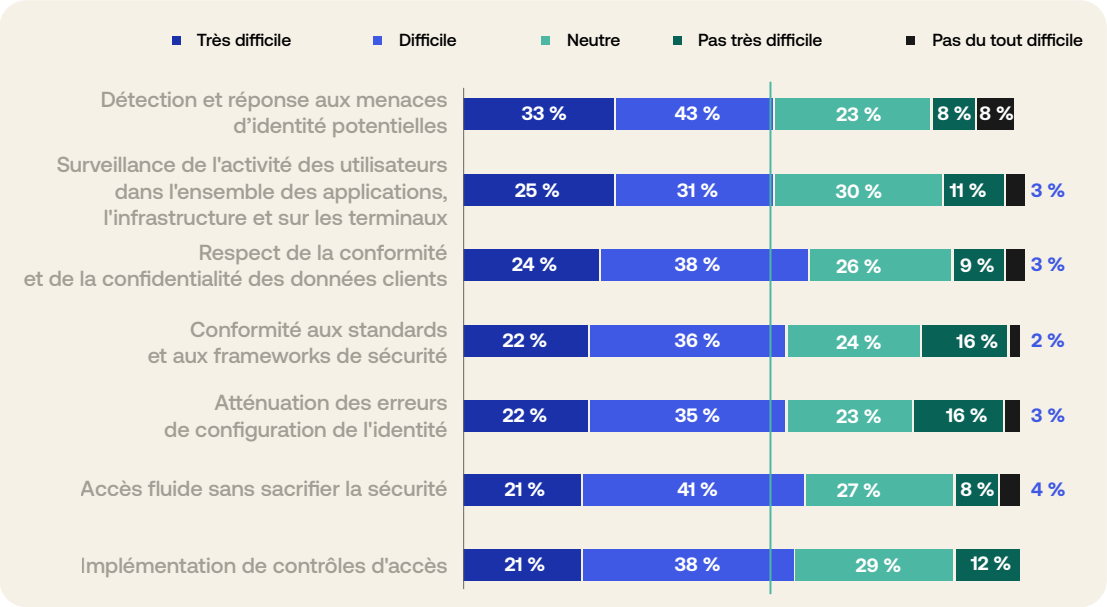
Verizon, 2024 Data Breach Investigations Report

CONSTAT 4 :

Les RSSI ne voient pas de solution simple pour garantir la sécurité des identités

Compte tenu du rôle joué par l'identité dans la majorité des brèches, il n'est guère surprenant que la vaste majorité des RSSI interrogés dans le cadre de l'étude (76 %) considèrent le renforcement de la sécurité des identités comme une priorité absolue. Pourquoi, dès lors, n'ont-ils pas remédié au problème ?

Parce que la sécurité des identités n'est pas un problème isolé mais une bataille sur plusieurs fronts, et la plupart des RSSI estiment que ***chaque aspect*** de la sécurité des identités représente un défi.



CONSTAT 5 :

La multiplication des technologies aggrave les problèmes liés à la sécurité des identités

Deux grands défis rencontrés par les RSSI, à savoir le business enablement et la protection de l'entreprise, sont encore aggravés par la prolifération des technologies. Le déploiement décentralisé des technologies et la multiplication des solutions SaaS constituent des problèmes récurrents dans les entreprises, et s'étendent désormais aux piles de sécurité. L'étude révèle que la plupart des entreprises collaborent avec plus de 50 éditeurs de solutions de cybersécurité différents. Les équipes sécurité consacrent trop de temps à orchestrer manuellement les processus et les flux de données entre les différentes solutions, tandis que les RSSI s'efforcent de créer de meilleures intégrations et d'éliminer les redondances.

Autres observations de l'étude :

Principaux risques liés à la sécurité des identités

1. Manque de visibilité sur les outils de sécurité
2. Comptes mal configurés / surprovisionnés

Principaux obstacles à un accès fluide

1. Gestion des pistes d'audit dans l'ensemble des solutions
2. Complexité de la gestion de plusieurs solutions d'identité

Une entreprise type fait appel à 60 fournisseurs de cybersécurité différents.

Okta, pour une stratégie de sécurité axée sur l'identité

L'étude réalisée par ESG démontre clairement que l'identité n'est plus une simple fonction IT mais qu'elle fait désormais partie intégrante de la sécurité des entreprises modernes. La plateforme d'identité d'Okta est spécialement conçue pour offrir l'agilité et la sécurité requises par les RSSI qui souhaitent adopter une approche proactive, axée sur l'identité. Okta permet aux RSSI d'abandonner une posture défensive pour passer à l'offensive en leur fournissant les bases de la sécurité des identités indispensables pour réduire les risques et la complexité, et aborder en toute confiance un paysage des menaces en constante évolution.

* L'étude/enquête a été réalisée par Enterprise Strategy Group en partenariat avec Okta entre janvier et février 2025. Dans ce cadre ont été interrogés plus de 150 RSSI en Amérique du Nord, dans la région EMEA et dans la région APJ.

Vous voulez en savoir plus sur la plateforme ?

Nous serions ravis de connaître les défis auxquels vous êtes confronté et de vous expliquer comment Okta peut vous aider.

En savoir plus