La valeur stratégique de l'identité pour les DSI

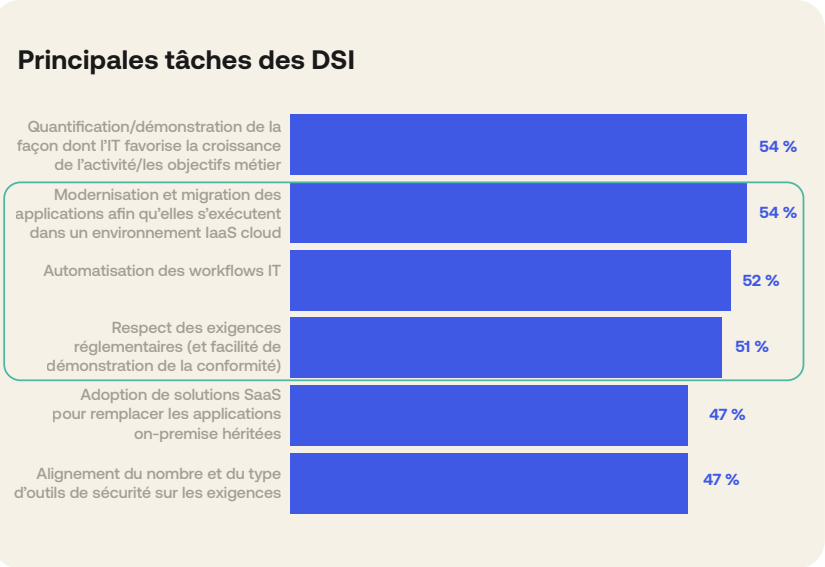
À mesure que les entreprises migrent vers le cloud et cherchent activement à gagner un avantage concurrentiel en augmentant l'efficacité IT, l'identité devient un facteur critique – et bien souvent un goulet d'étranglement – pour les DSI dans une démarche de business enablement. Cette présentation est 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 gestion des identités pour les DSI :

1. Le défi majeur des DSI est de trouver le juste équilibre entre business enablement et protection de l'entreprise.
2. Les lacunes en matière d'automatisation de l'identité entravent l'efficacité IT.
3. Les programmes d'identité sont un facteur décisif en matière de business enablement.
4. La fragmentation constitue un obstacle sous-estimé à la gestion des identités.
5. Les DSI reconnaissent le besoin urgent de rationaliser l'identité.

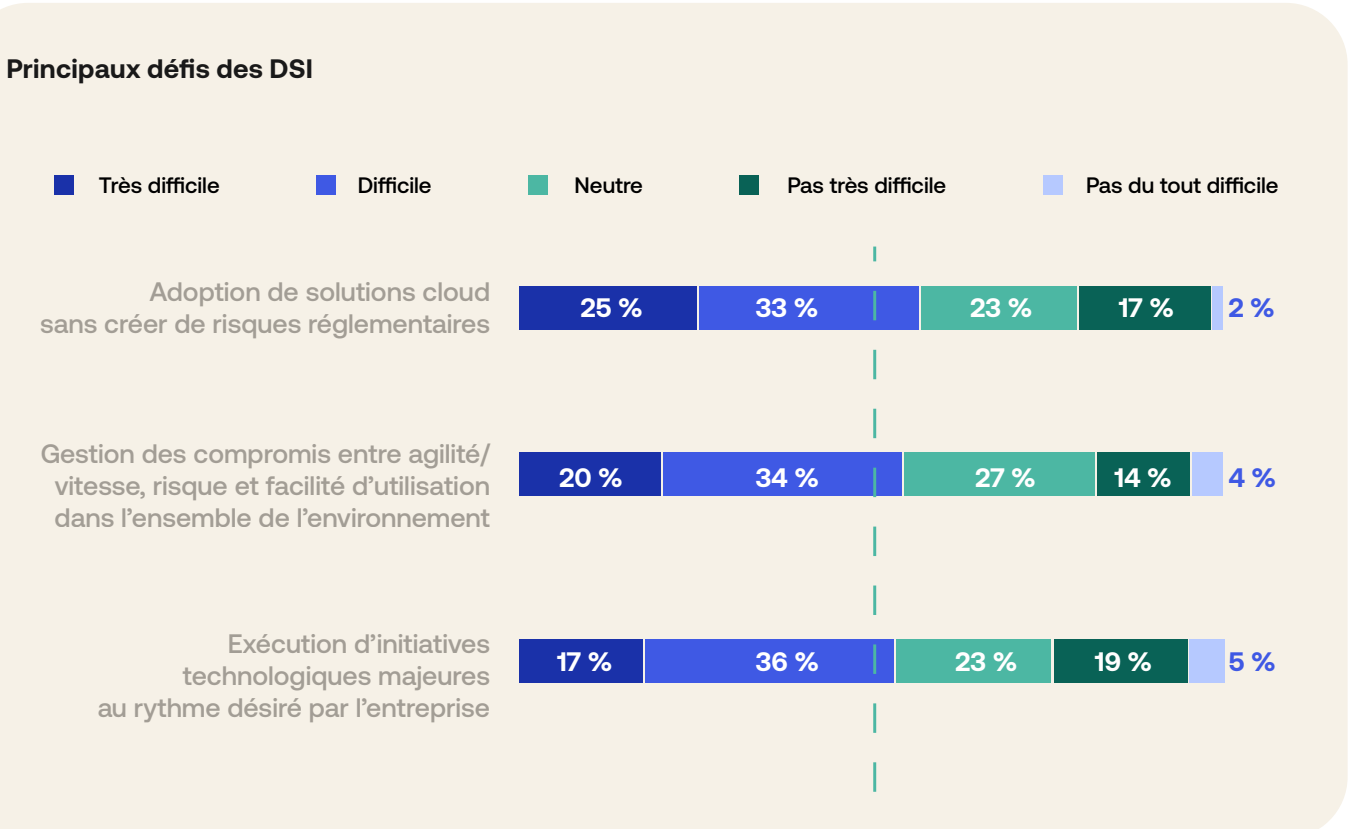
CONSTAT 1 :

Le défi majeur des DSI est de trouver le juste équilibre entre business enablement et protection de l'entreprise

Il n'est pas surprenant que la priorité absolue des DSI soit de démontrer comment les processus IT soutiennent les principaux objectifs métier et la croissance globale de l'activité. Toutefois, les réponses concernant les autres priorités révèlent une tension critique – avec l'accélération des opérations métier et l'augmentation de l'efficience d'une part, la sécurité et la conformité d'autre part.



C'est en s'intéressant aux principaux défis des DSI que l'on peut comprendre comment ils cherchent à trouver le juste équilibre entre business enablement et protection de l'entreprise – de l'adoption de solutions cloud sans créer de problèmes réglementaires, à l'identification du point d'équilibre idéal entre agilité et risque, en passant par l'accélération des initiatives technologiques majeures tout en garantissant une gouvernance et une gestion appropriées des données.

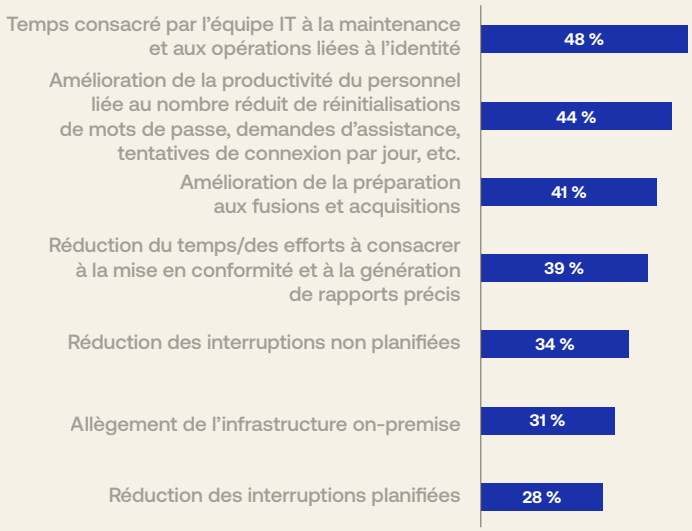


CONSTAT 2 :

Les lacunes en matière d'automatisation de l'identité entravent l'efficacité IT

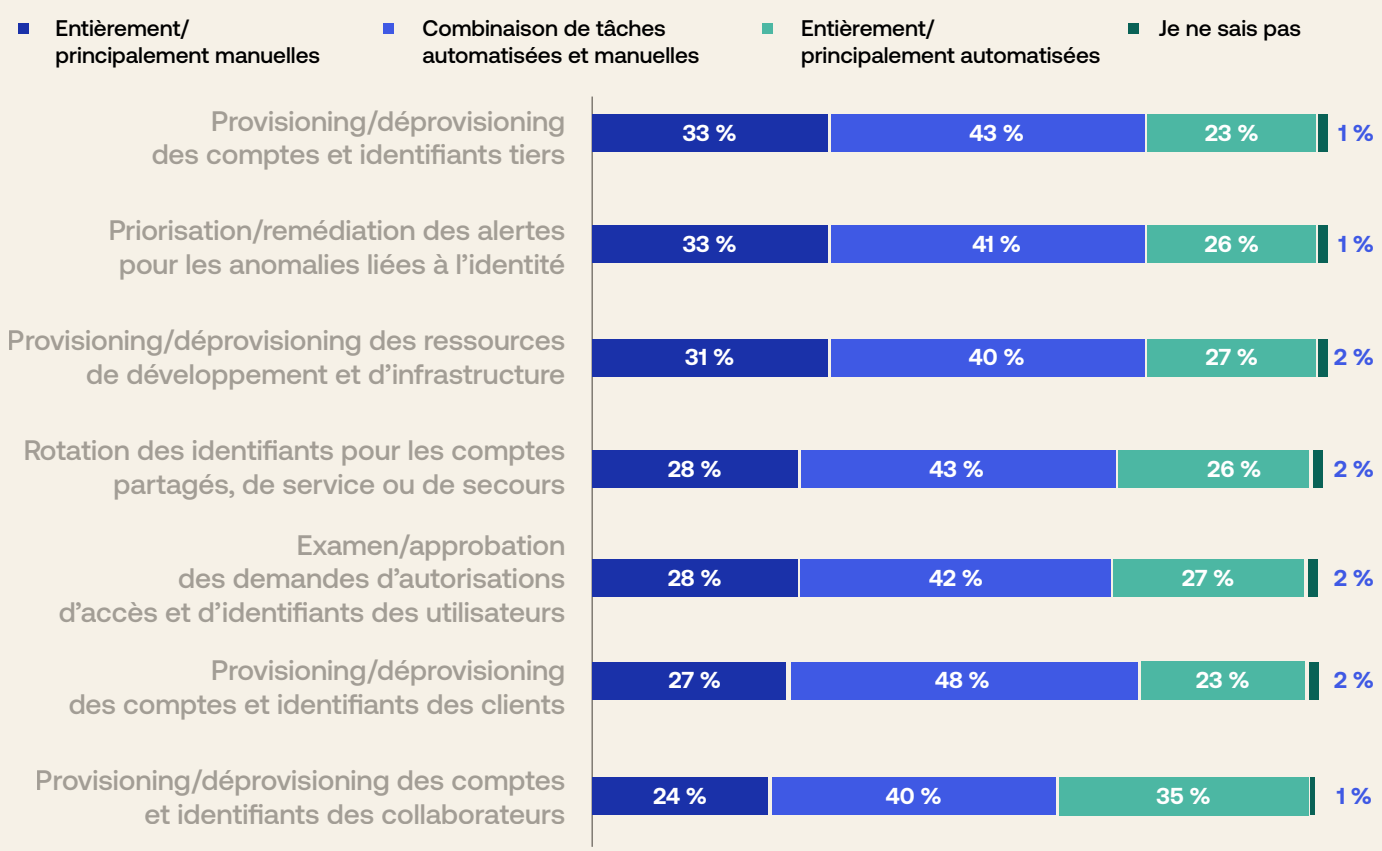
L'automatisation des workflows IT fait partie des priorités des DSI. Plus spécifiquement, les DSI interrogés dans le cadre de l'étude affirment que le temps consacré par le personnel IT à la maintenance et aux opérations liées à l'identité constitue aujourd'hui leur indicateur clé de performance (KPI) le plus critique. (En seconde position vient la réduction de l'impact des problèmes d'identité sur la productivité, par exemple les réinitialisations de mots de passe et les connexions quotidiennes excessives.) Étonnamment, ces KPI centrés sur l'identité pèsent davantage que les KPI plus conventionnels, tels que la réduction des interruptions planifiées et non planifiées, ou encore l'allègement de l'infrastructure technologique on-premise.

KPI les plus importants pour les DSI



Pourtant, les lacunes en matière d'automatisation entravent l'efficacité IT au sens large. En ce qui concerne les workflows d'identité, l'automatisation reste l'exception, et loin d'être la norme. Moins d'un DSI sur trois interrogé pour les besoins de l'étude déclare avoir automatisé ses tâches d'identité essentielles.

Dans quelle mesure les tâches d'identité essentielles sont-elles automatisées ?



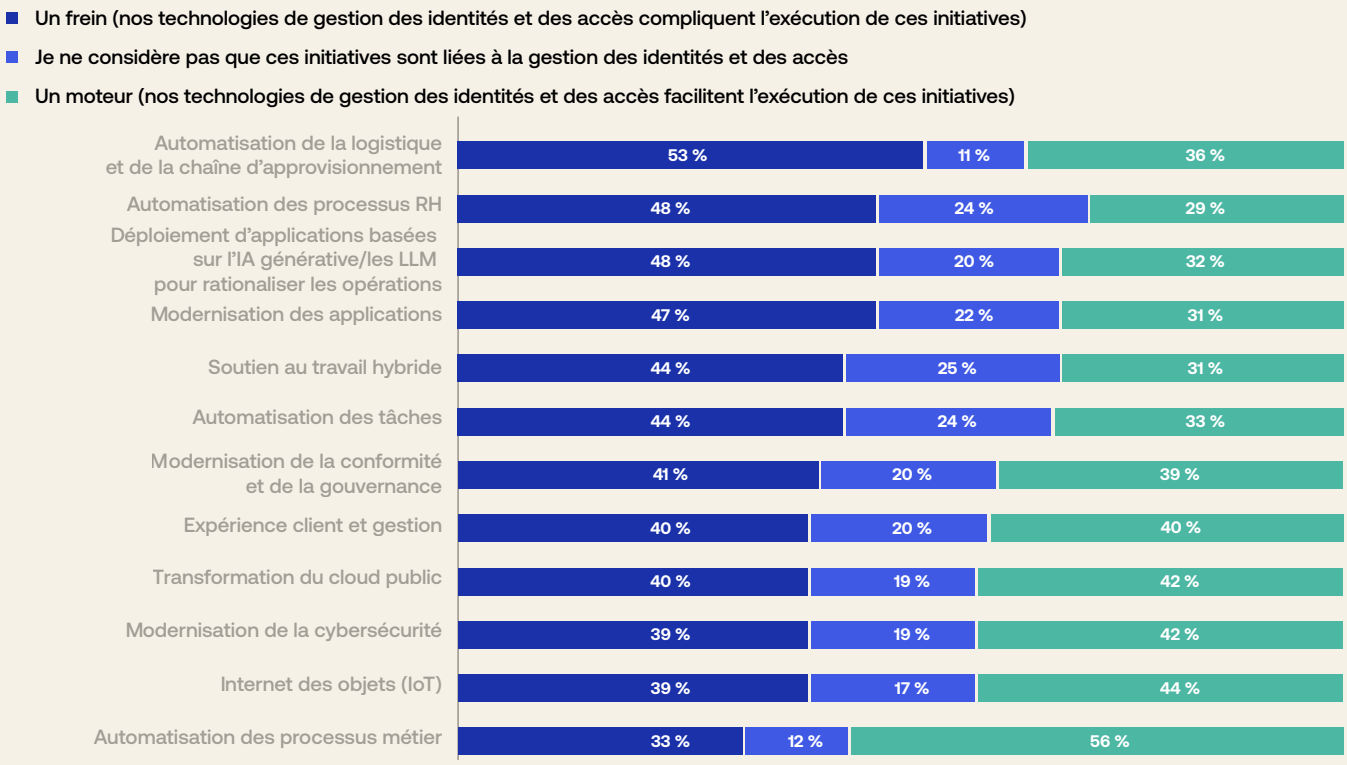
CONSTAT 3 :

Les programmes d'identité sont un facteur décisif en matière de business enablement

Si l'on prend un peu de hauteur, on constate qu'une grande majorité des DSI interrogés reconnaissent que les programmes d'identité jouent un rôle déterminant dans le succès ou l'échec de leurs initiatives de business enablement. Malheureusement, près de la moitié d'entre eux affirment considérer leur pile d'identité actuelle comme un frein important à leurs initiatives.

De nombreux DSI affirment que leur approche actuelle de l'identité entrave les initiatives qu'ils aimeraient faire avancer

Pour ces initiatives clés, entre 39 et 48 % d'entre eux déclarent que leur pile d'identité les limite. Entre 75 et 81 % affirment que leur pile d'identité facilitera ou entravera leurs initiatives métier clés.



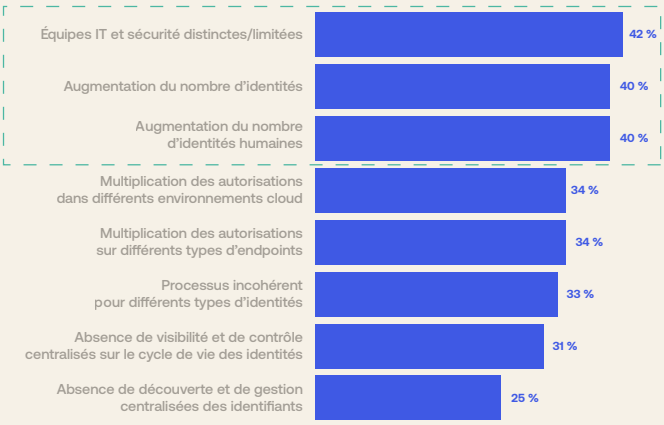
CONSTAT 4 :

La fragmentation constitue un obstacle sous-estimé à la gestion des identités

Sans surprise, les DSI affirment que la prolifération des identités humaines et non humaines représente un défi majeur pour la gestion des identités et des accès. Le volume croissant d'identités est la cause immédiate de la multiplication des autorisations, qui apparaît également dans la liste des principaux défis.

Autre problème de taille : la fragmentation des équipes et des technologies chargées de la gestion de toutes ces identités et autorisations. Les DSI citent les équipes IT et sécurité cloisonnées comme principal facteur de complication de la gestion des identités et des accès (IAM), et l'absence de découverte, visibilité, contrôle et gestion centralisés des identités et des identifiants complète la liste.

Principales difficultés rencontrées par les DSI en matière de gestion des identités et des accès

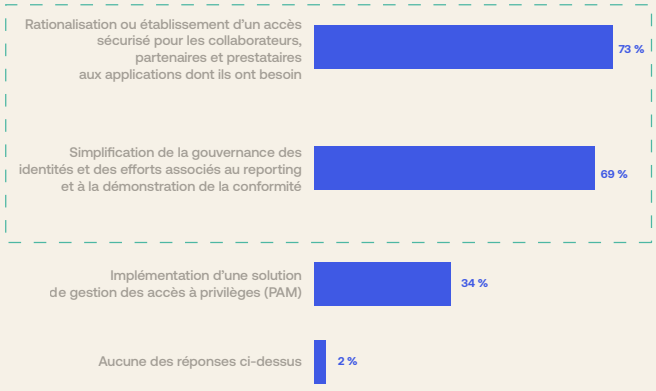


CONSTAT 5 :

Les DSI reconnaissent le besoin urgent de rationaliser l'identité

L'étude se termine sur une note positive : la grande majorité des DSI prennent des mesures décisives pour relever les défis de gestion des identités qui entravent l'efficience et le business enablement. 7 DSI sur 10 ont déclaré avoir prévu des initiatives majeures pour 2025 en vue de rationaliser l'accès sécurisé et de simplifier la gouvernance des identités. Les DSI interrogés dans le cadre de l'étude ont donc conscience du besoin critique de moderniser leurs programmes d'identité. Ils sont bien décidés à investir dans des solutions qui peuvent renforcer l'efficacité, l'automatisation et le contrôle de cet élément fondamental du business enablement favorisé par l'IT.

Les DSI prévoient d'investir dans l'identité en 2025



Les DSI considèrent la prolifération des technologies de sécurité comme un contributeur majeur aux problèmes de fragmentation, mais ils pourraient en réalité sous-évaluer l'ampleur du problème. Les DSI interrogés disent faire appel à 44 éditeurs de solutions de sécurité différents en moyenne, un chiffre qui, bien qu'alarmant, est considérablement inférieur aux estimations des RSSI (environ 60 outils de sécurité différents).

À combien d'éditeurs de solutions de cybersécurité différents les entreprises font-elles appel ?

Selon les DSI : ± 44

Selon les RSSI : ± 60

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

L'étude d'ESG démontre comment l'identité est devenue essentielle au business enablement et révèle que les programmes d'identité actuels constituent un frein persistant aux initiatives critiques – avec des frictions naissant des lacunes en matière d'automatisation et de la fragmentation omniprésente des identités. La plateforme d'identité unifiée d'Okta est spécialement conçue pour relever ces défis spécifiques, en dotant les DSI d'un toolkit d'identité moderne pour booster l'efficacité et accélérer la transformation digitale.

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

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

Le présent document et toute recommandation qu'il propose ne constituent pas des conseils juridiques, commerciaux, ou encore de confidentialité, sécurité et conformité. Le contenu de ce document revêt un caractère purement informatif et pourrait ne pas refléter les normes de sécurité, de confidentialité et les réglementations les plus récentes, ou tous les problèmes pertinents. Pour obtenir de tels conseils, il vous revient de vous adresser à votre conseiller juridique ou à tout autre conseiller professionnel en matière de sécurité, confidentialité ou conformité, et de ne pas vous en remettre aux recommandations formulées dans le présent document. Okta ne formule aucune déclaration, garantie ou autre assurance concernant le contenu de cet article. Pour en savoir plus sur les assurances contractuelles d'Okta à ses clients, rendez-vous à l'adresse okta.com/agreements. Tous les produits, fonctions et fonctionnalités référencés dans ce document qui ne sont pas encore disponibles en version GA pourraient être distribués à une date ultérieure à la date annoncée, ou annulés. Les roadmaps produits ne représentent en rien un engagement, une obligation ou une promesse d'offre de produit ou fonctionnalité, et les clients ne doivent pas se baser sur ces plans pour prendre leur décision d'achat.