eBook

Sécurité et transformation des réseaux à l'ère du SASE

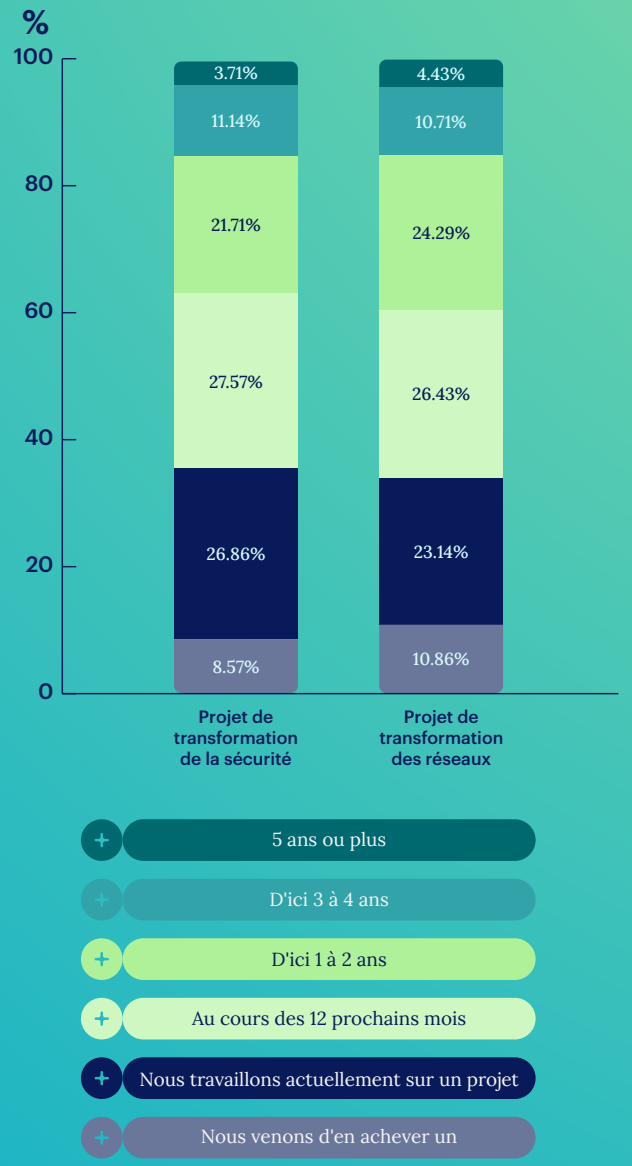
netskope

Alors que les organisations du monde entier poursuivent leur transformation numérique, de plus en plus de ressources opérationnelles sont transférées dans le cloud. Elles couvrent l'ensemble du parc informatique, et la réussite ces projets nécessitera de repenser les architectures réseau et de sécurité.

Le marché mondial de la transformation des réseaux devrait atteindre 122,73 milliards de dollars d'ici 2026, à un taux de croissance annuel composé (TCAC) de 39,7 %.[1] De même, le marché mondial de la sécurité cloud devrait atteindre 77,5 milliards de dollars la même année, avec un TCAC de 13,7 %.[2]

Le changement est clairement en marche, mais les organisations ne s'accordent guère sur la manière d'aborder leurs projets de réseau et de sécurité en ce en termes de budgets, de gestion des modifications ou de rationalisation des technologies.

Cet eBook identifie quelques-uns des principaux défis révélés par l'étude réalisée par Censuswide pour le compte de Netskope auprès d'entreprises européennes, complétée par des études tierces dans le but de dresser un tableau global. Notre objectif consiste à mieux comprendre la manière dont les responsables informatiques abordent la transformation à l'ère des architectures Secure Access Service Edge (SASE), et à montrer comment les organisations peuvent rationaliser les équipes, les processus et la technologie pour réussir dans le domaine du SASE.



[1] « Global Network Transformation Market Research Report », Market Research Future, 2021.

[2] « Cloud Security Market Report », MarketsandMarkets, janvier 2022.

Économies réalisées en transférant la sécurité dans le cloud

Une étude menée par Deloitte révèle que la sécurité et la protection des données sont désormais l'un des principaux moteurs de l'adoption du cloud au niveau mondial : 58% des responsables informatiques classent ces aspects en première ou deuxième position.[3] Une enquête menée auprès de cadres américains a quant à elle révélé que la sécurité est considérée comme le principal avantage du cloud computing par 60% des personnes interrogées.[4]

Cela transparaît également dans nos propres recherches. La grande majorité des DSI et RSSI (98%) avec lesquels nous nous sommes entretenus ont transféré au moins quelques ressources vers le cloud, même si moins d'un sur cinq (18,5%) déclare avoir transféré plus des trois quarts de son infrastructure de sécurité.

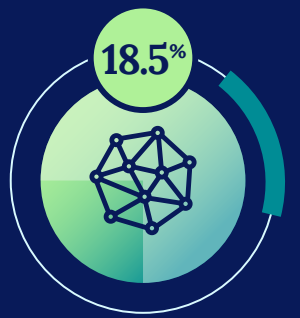
La plupart de ceux qui utilisent la sécurité dans le cloud ont déjà réduit leurs dépenses dans certains des domaines escomptés : 25% économisent sur le matériel et 23% sur la bande passante. Par ailleurs, 21% ont réduit leurs coûts grâce à la consolidation des fournisseurs et 21% ont réduit leurs dépenses de pare-feu en déployant des solutions dans le cloud. Ces chiffres sont conformes aux études mondiales. Par exemple, une étude de Secure Data suggère qu'une entreprise de 500 employés réduira ses dépenses de pare-feu de 37% et économisera en moyenne 139 000 USD.[5]

Cependant, étant donné que la plupart des entreprises sont encore en cours de transformation numérique, il est légitime de considérer ces économies comme des données préliminaires ou, du moins, qu'il conviendra de réévaluer régulièrement. Par exemple, dans notre étude, 30% des répondants à l'enquête anticipent une réduction des coûts grâce à l'introduction de technologies Firewall-as-a-Service (FWaaS), mais seuls 22% déclarent avoir réalisé ces économies jusqu'à présent.

La sécurité est considérée comme le principal avantage du cloud computing par 60 % des cadres supérieurs dans le monde[6]

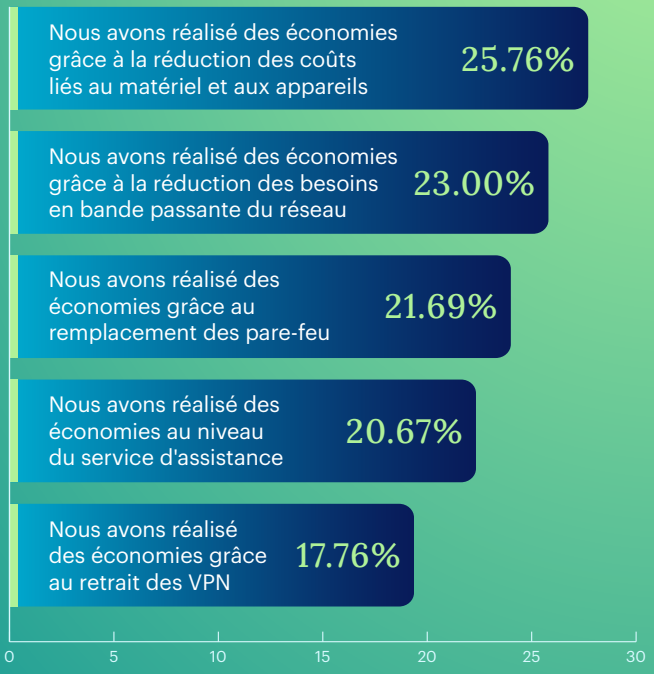
La sécurité représentera 6 % des dépenses liées au cloud en 2023[7]

98% des DSI/RSSI européens ont transféré au moins quelques ressources vers le cloud



Seuls 18,5 % ont transféré plus des trois quarts de leur infrastructure de sécurité

Laquelle de ces affirmations, le cas échéant, est vraie pour vous et votre organisation, suite à la migration de la sécurité vers le cloud ?



Les points clés à retenir

La transition vers le cloud est un chantier en cours ; on peut donc s'attendre à ce que les économies réalisées grâce au cloud et aux SASE augmentent au fil du temps. Les organisations se concentrent sur des projets à court terme tels que le remplacement des VPN et la consolidation des fournisseurs, car ce sont les meilleures sources d'économies pour les deux ans à venir.

[3] Karthik Ramachandran et David Linthicum, « Why organizations are moving to the cloud: Security, data modernization, and cost among top drivers for cloud migration », Deloitte, 5 mars 2020.

[4] « 55 Cloud Computing Statistics That Will Blow Your Mind », CloudZero, 21 octobre 2022.

[5] Abdul Moiz, « 12 Reasons to Choose Firewall as a Service for your Business », ExterNetworks, 8 décembre 2022.

[6] « 55 Cloud Computing Statistics That Will Blow Your Mind », CloudZero, 21 octobre 2022.

[7] Matt Ashare, « Security to take an outsized role in IT spending in 2023 », CIO Dive, 4 octobre 2022.

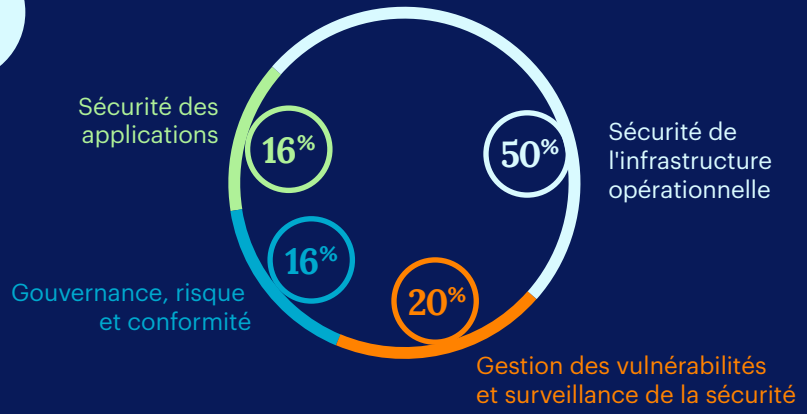
Convergence des réseaux et de la sécurité

L'unification des fonctions de sécurité et réseau est une bonne pratique pour le parcours cloud de l'entreprise. En outre, la raison invoquée par les personnes interrogées dans le cadre de l'enquête Netskope pour justifier cette convergence est tout à fait logique : environ un tiers des DSI et des RSSI pensent que la séparation des équipes n'est pas utile pour la gestion des ressources cloud.

Cependant, nous avons constaté qu'une grande majorité des entreprises qui fusionnent les objectifs de sécurité et réseau maintiennent la séparation de leurs budgets. Seuls 8 % des répondants à l'enquête ont déclaré avoir l'intention de combiner les budgets consacrés à la sécurité et aux réseaux. Même quand les deux équipes sont placées sous l'autorité du DSI (environ deux tiers de ces équipes informatiques sont placés sous l'autorité du DSI et du RSSI, soit directement, soit dans le cadre d'un partage de responsabilités), elles risquent de se retrouver en concurrence concernant les ressources et la propriété des technologies cloud ; 28 % des personnes interrogées anticipent exactement cette situation.

Cette interrogation quant à la meilleure approche à adopter en matière de stratégie cloud se double d'une incertitude plus vaste concernant la meilleure façon d'aborder la sécurité au sommet de la hiérarchie de l'entreprise. Selon une étude mondiale de l'Economist Intelligence Unit, près de 40 % des cadres estiment que le conseil d'administration de l'entreprise devrait superviser la cybersécurité, contre 24 % qui pensent que ce rôle devrait revenir à un comité spécialisé dans la cybersécurité.[8]

Allocation du budget de cybersécurité dans les entreprises[9]



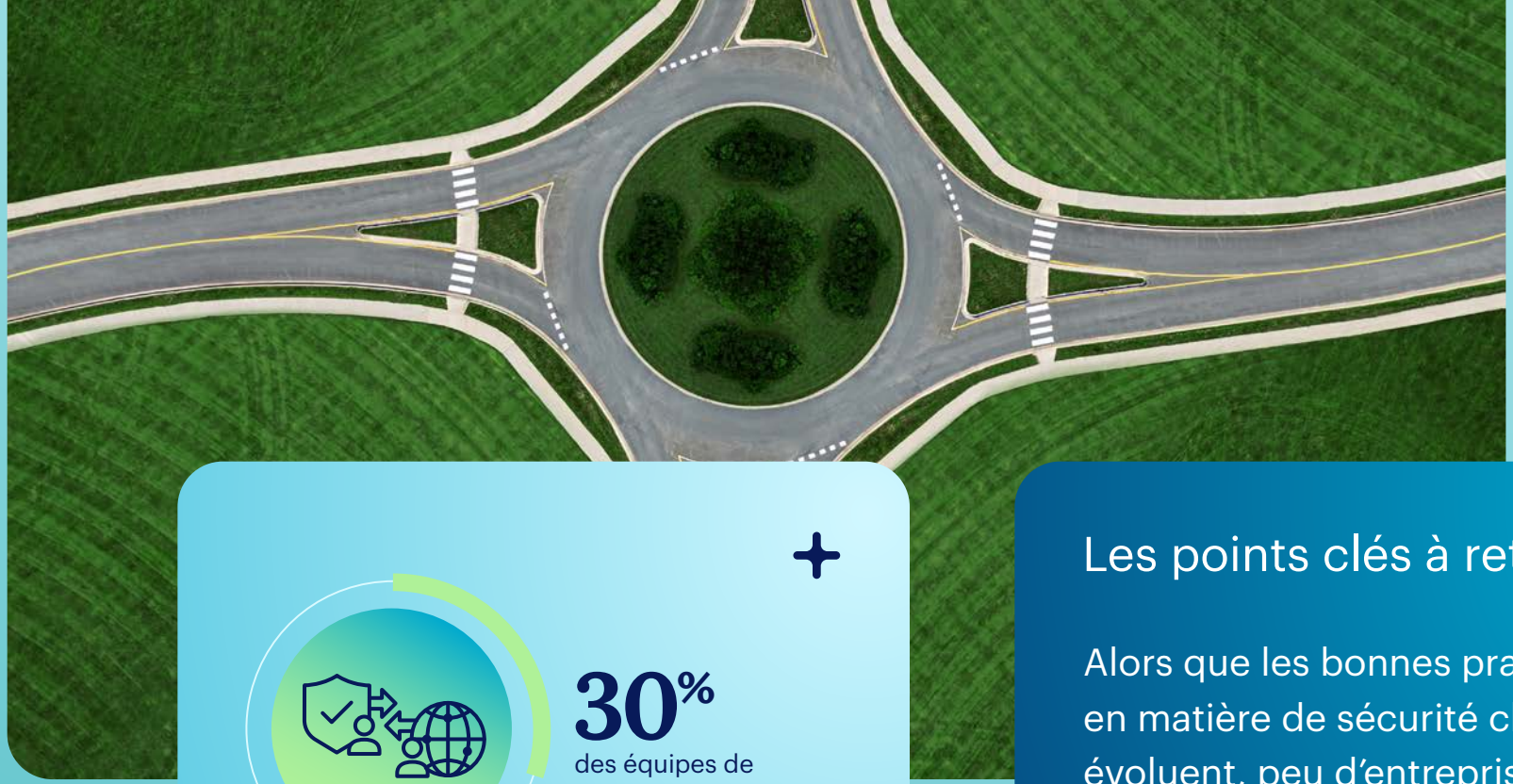
Hypothèses de planification des investissements dans les réseaux pour 2025[10]

50% des achats de SD-WAN s'inscriront dans une offre SASE d'un fournisseur unique

10% des entreprises utiliseront la 5G comme connectivité sans fil fixe principale ou de secours dans leur WAN

25% des entreprises automatiseront plus de la moitié de leurs activités réseau

15% de l'ensemble des entreprises adopteront une solution NaaS (Network-as-a-Service) sur site



30%
des équipes de sécurité et réseau ont déjà, ou vont, converger

mais seulement
8%
prévoient de fusionner les budgets de sécurité et réseau

Les points clés à retenir

Alors que les bonnes pratiques en matière de sécurité cloud évoluent, peu d'entreprises optent pour l'approche optimale qui consiste à faire converger les aspects sécurité et réseau, tant du point de vue de la dotation en personnel que de celui du budget.

[8] Nick Ismail, « Who is responsible for cyber security in the enterprise? » Information Age, 25 octobre 2022.

[9] Toby Shackleton, « Cyber Security Budget Trends in 2022 », Six Degrees, 17 août 2021.

[10] « The top 5 trends in enterprise networking and why they matter: A Gartner® trend insight report », DE-CIX Management GmbH, 22 septembre 2022.

Une question de responsabilité

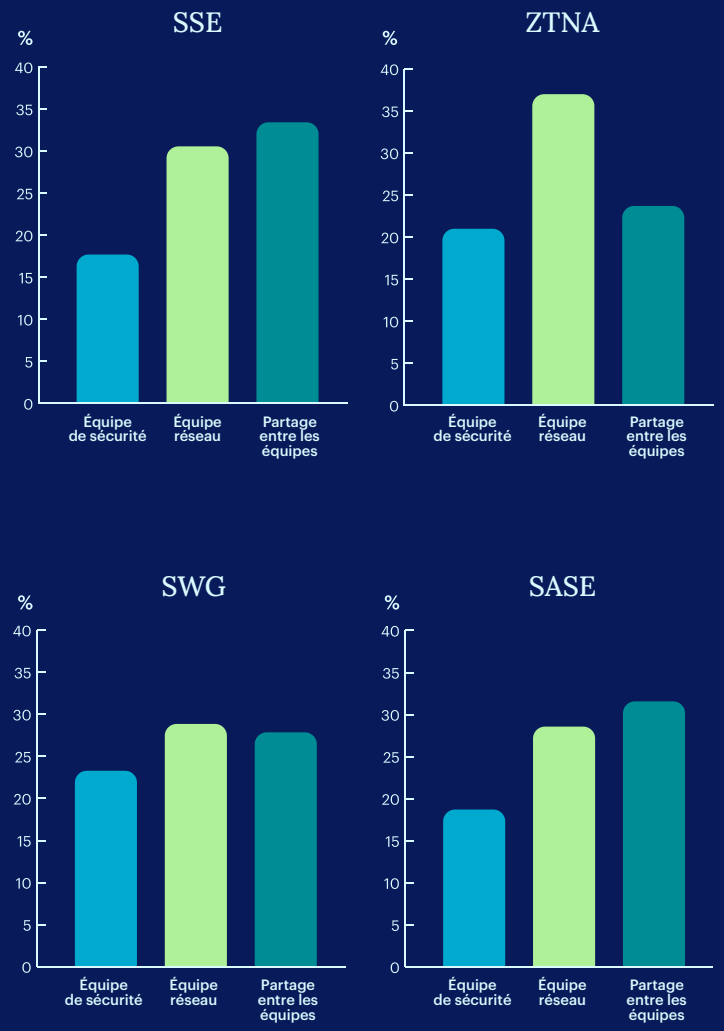
Les technologies et cadres de sécurité transformationnels, notamment SASE, SSE, ZTNA et SWG, sont dans le collimateur des DSI et des RSSI du monde entier. Par exemple, les dépenses mondiales consacrées au SASE devraient augmenter à un TCAC de 26,4 % pour atteindre 4,1 milliards de dollars d'ici 2026.[11] De même, les dépenses mondiales totales consacrées aux logiciels et solutions de sécurité zero trust devraient passer de 27,4 milliards de dollars en 2022 à 60,7 milliards de dollars d'ici 2027, à un TCAC de 17,3 %.[12]

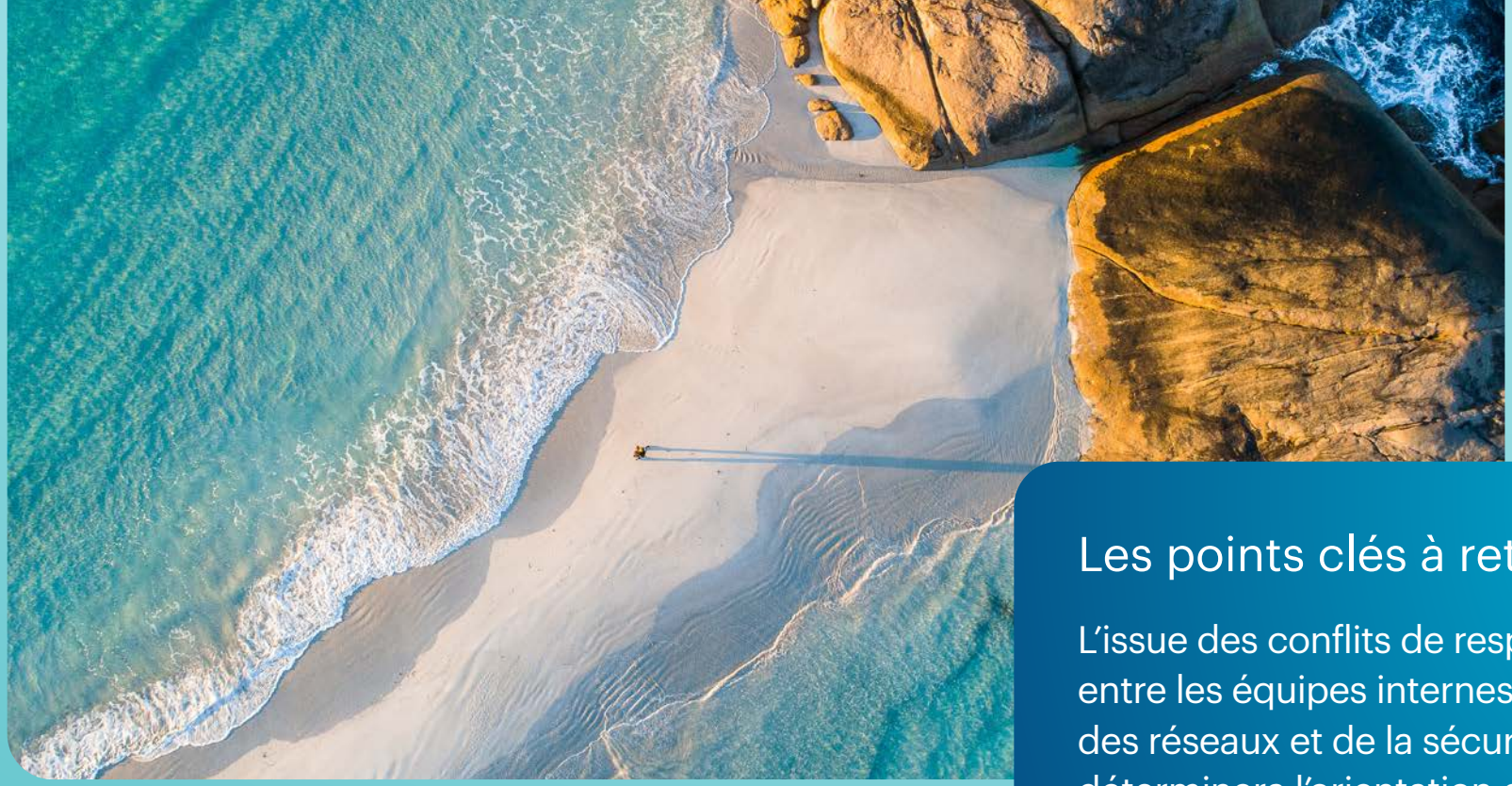
Cependant, l'intérêt commun pour ces technologies ne se traduit pas par un accord concernant la responsabilité de tel ou tel groupe vis-à-vis des produits ou des projets de transformation. Notre enquête a révélé que 28 % des entreprises confient la responsabilité de leurs projets SASE à leurs équipes réseau et 18 % à leur organisation de sécurité. Parallèlement, dans 31 % des entreprises européennes, la responsabilité SASE est partagée entre les deux équipes.

Bien que le terme SSE soit relativement nouveau et qu'il soit considéré comme englobant les services de sécurité qui font partie du SASE, nous avons trouvé des répartitions de responsabilité très similaires entre les deux. Quant à la responsabilité des solutions SSE, elle relève de l'équipe réseau pour 31% des répondants, de l'équipe sécurité pour 18 %, et est partagée pour 33 %.

Le ZTNA penche en faveur de la responsabilité de l'équipe réseau réseau (37% pour l'équipe réseau contre 21% pour "l" équipe sécurité et 23 % pour le partage). La SWG est légèrement plus susceptible de relever de responsabilité de l'équipe de sécurité que les autres technologies (23 % pour "l" équipe sécurité contre 28 % pour "l" équipe réseau et 27 % pour le partage).

À quel moment votre organisation prévoit-elle d'entreprendre un projet de transformation de la sécurité et/ou des réseaux ?





Les points clés à retenir +

L'issue des conflits de responsabilité entre les équipes internes chargées des réseaux et de la sécurité déterminera l'orientation de l'organisation en matière de SASE.

En l'absence de large consensus externe concernant la répartition des initiatives entre les différentes équipes, le DSI et le RSSI doivent décider et s'entendre, puis faire preuve de clarté et de cohérence quant à l'équipe responsable de chaque domaine de transformation.

[11] « Secure Access Service Edge Market Report », MarketsandMarkets, août 2021.

[12] « Zero Trust Security Market Report », MarketsandMarkets, août 2021.

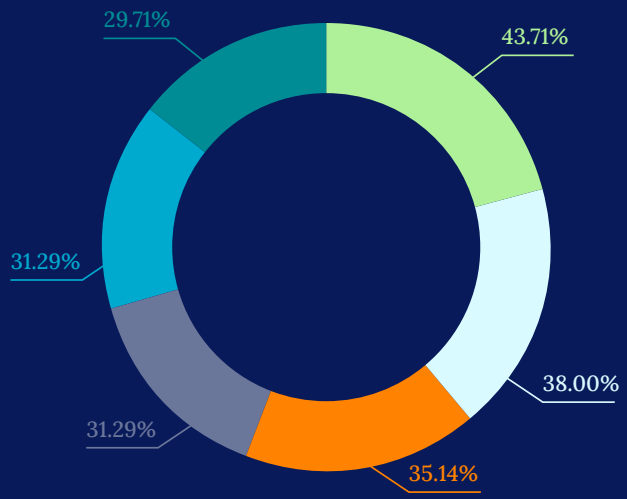
Le déficit de compétences en matière de sécurité

Selon le rapport Cost of a Data Breach 2022 d'IBM et du Ponemon Institute, 62 % des organisations estiment que leur équipe de sécurité ne dispose pas de ressources suffisantes.[13] Notre étude montre que le passage au cloud aura un impact supplémentaire sur le problème du déficit de compétences ; près d'un tiers des répondants à l'enquête augmentent actuellement, ou prévoient d'augmenter, les effectifs de leur équipe de sécurité pour une meilleure adéquation avec les attributions plus larges du groupe, à mesure que l'organisation étend ses opérations dans le cloud.

Une part importante des DSI/RSSI interrogés (29 %) a déclaré ne pas avoir rencontré de difficultés pour trouver des candidats qualifiés pour ces postes de sécurité. Cependant, un groupe encore plus important (46 %) a actuellement du mal à trouver des profils adéquats ou s'attend à rencontrer des difficultés à l'avenir. C'est peut-être en raison de ces préoccupations que 38 % des personnes interrogées envisagent de rechercher de nouveaux membres pour leur équipe de sécurité en dehors de la cybersécurité ou même de l'informatique.

Il est essentiel de combler ce déficit de compétences, car tant qu'il perdurera, les entreprises risqueront davantage d'être victimes d'une attaque. Selon le Forum économique mondial, 59 % des organisations à travers le monde auraient actuellement du mal à faire face à un incident de cybersécurité en raison de la pénurie de compétences au sein de leur équipe.[14] Cela n'est guère étonnant, étant donné que seuls 8 % des technologues mondiaux disposent de compétences et d'une expérience significatives en matière de cloud.[15] Inversement, les entreprises dont l'équipe de sécurité est suffisamment étoffée affirment que le coût moyen d'une violation de données est inférieur à la moyenne.[16]

Si vous deviez recruter pour votre équipe de sécurité, quel type de profil rechercheriez-vous ?



- Candidats ayant déjà des compétences/de l'expérience en matière de cloud/SaaS/IaaS
- Candidats en dehors des marchés des cybercompétences ou des technologies de l'information et de la formation/du perfectionnement
- Candidats chez les concurrents, chez nos pairs du secteur ou dans d'autres organisations similaires
- Candidats diplômés
- Sous-traitance
- Formation en interne pour les membres des équipes réseau, d'assistance et autres

40%

des organisations mondiales reconnaissent que la sécurité constitue la principale lacune en matière de compétences.[17]

28%

ont déjà apporté des changements à la structure ou au personnel de l'équipe réseau.

26%

ont apporté des changements à l'équipe de sécurité.

Les points clés à retenir

La volonté des entreprises de rechercher des candidats qui n'ont pas encore de compétences et d'expérience en matière de sécurité cloud témoigne d'un niveau de créativité rassurant. Cependant, cette approche n'est pas seulement créative, elle est aussi nécessaire compte tenu de la difficulté des organisations à trouver des talents. Les DSI et RSSI qui sont ouverts à la formation de nouveaux membres pour leur équipe de sécurité sont beaucoup moins susceptibles d'être confrontés à une pénurie de talents, d'autant plus s'ils sont prêts à dénicher des compétences adéquates ou des talents prêts à se former dans des lieux non traditionnels.

[13] « Cost of a Data Breach Report 2022 », Ponemon Institute et IBM Security, juillet 2022.

[14] « What you need to know about cybersecurity in 2022 », Forum économique mondial, 18 janvier 2022.

[15] « State of Cloud: The cloud skills vs. expectation gap », Pluralsight, 2022.

[16] « Cost of a Data Breach Report 2022 », Ponemon Institute et IBM Security, juillet 2022.

[17] « State of Cloud: The cloud skills vs. expectation gap », Pluralsight, 2022.

Budgets, dotation en personnel et répartition des responsabilités à l'ère du SASE

Le déplacement des activités de l'entreprise vers le cloud représente un véritable changement générationnel pour les organisations informatiques et leurs DSI/RSSI. Comme tout changement important, la transformation numérique peut être source de désagréments, mais il s'agit d'une priorité pour les organisations. Ce faisant, ces dernières transforment également les réseaux et la sécurité en déplaçant des systèmes clés dans le cloud.

De nombreuses organisations tâtonnent encore pour trouver les bonnes pratiques. Certaines passent au cloud en utilisant les structures de gestion qui fonctionnaient bien sur site et espèrent que tout ira pour le mieux. Cette approche est risquée. Il est absurde de s'attendre à ce que les compétences et les stratégies budgétaires existantes fonctionnent aussi bien dans le cloud que dans le datacenter de l'entreprise.

Les dirigeants les mieux préparés à la transformation numérique redéfinissent leurs budgets, refondent leurs équipes et revoient leurs pratiques de recrutement pratiques de recrutement. Ces organisations seront bien placées pour tirer parti des opportunités offertes par l'avènement de l'entreprise SASE-first.

À propos de Netskope

Netskope est un leader du Secure Access Service Edge qui redéfinit la sécurité du cloud, des données et du réseau et aide les organisations à appliquer les principes zero trust. La plateforme Netskope Intelligent Security Service Edge (SSE) est rapide, facile à utiliser et protège les personnes, les appareils et les données où qu'ils se trouvent. Netskope aide les entreprises à réduire les risques, à accroître leur efficacité et à obtenir une visibilité inégalée sur toutes les activités des applications cloud, Web et personnelles.

Des milliers de clients, dont plus de 25 entreprises du classement Fortune 100, font confiance à Netskope et à son puissant réseau NewEdge pour atténuer les menaces et faire face aux changements technologiques, organisationnels, réglementaires, ainsi qu'à l'évolution des réseaux.

Méthodologie

Étude réalisée en octobre 2021 par Censuswide pour le compte de Netskope, auprès de 700 professionnels de l'informatique en Allemagne et au Royaume-Uni. Les participants sont tous des DSI, des RSSI ou des directeurs informatiques d'organisations comptant plus de 5 000 utilisateurs informatiques.

netskope