netskope

Gérer le changement : l'impact opérationnel de la transformation du réseau et de la sécurité

Budgets, personnel et division des responsabilités à l'ère du SASE

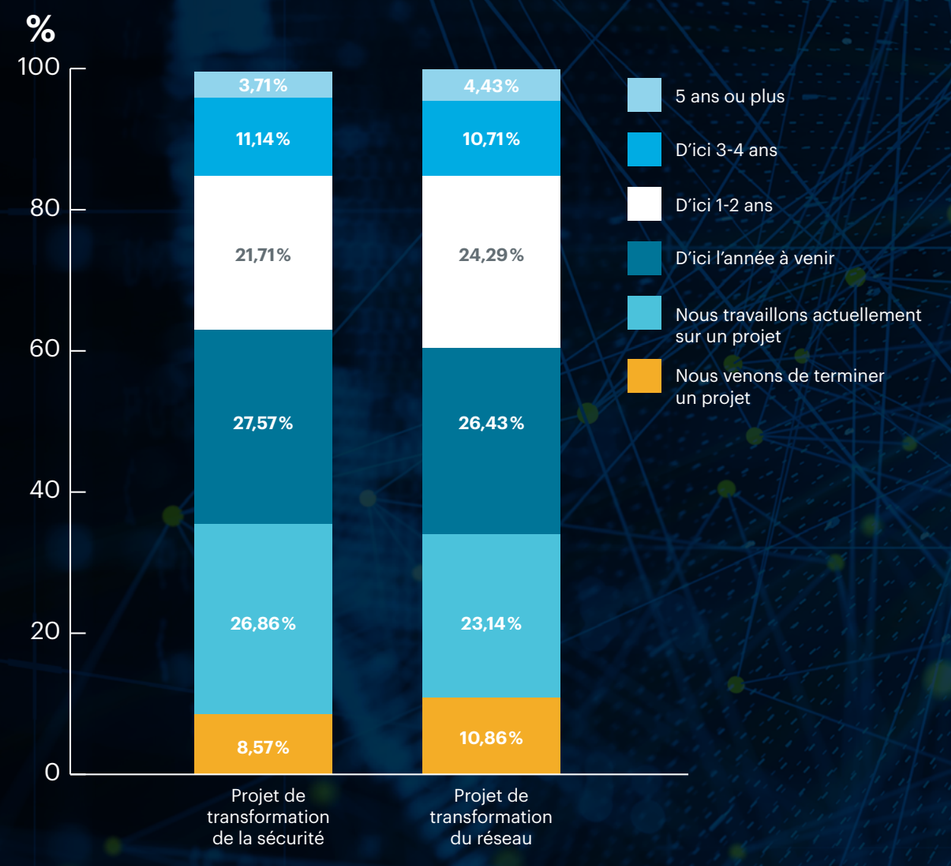
Comme d'autres entreprises du monde entier, les entreprises européennes déplacent de plus en plus de ressources opérationnelles dans le Cloud dans le cadre de leur transformation digitale. La réussite de celle-ci nécessite l'adoption de nouvelles approches en matière de réseau et de sécurité, et plus de 99,5 % des équipes IT d'Europe ont déjà mis en place (ou prévoient de lancer) des projets de transformation dans ces domaines. Mais il n'existe toujours pas de consensus sur la démarche à suivre, aussi bien sur le plan des budgets que de la gestion du changement ou de la rationalisation des technologies.

Afin d'identifier les bonnes pratiques parmi des stratégies de transformation fortement divergentes, Netskope a commandité une étude auprès de Censuswide. L'objectif : évaluer les stratégies réseau et sécurité basées dans le Cloud et comprendre comment les leaders IT des entreprises européennes abordent cette transformation.

Nous sommes entrés dans l'ère des architectures SASE, qui font converger le réseau et la sécurité au niveau des équipes comme des solutions. Or notre étude montre que les entreprises empruntent des chemins différents pour gérer cette transformation. Dans la plupart des entreprises, les équipes réseau et sécurité ont toujours des budgets et des responsabilités distincts. Et bien souvent, il est difficile de savoir exactement quelle équipe est en charge d'importants projets ou stratégies cloud.

Dans cet eBook, nous identifions certains des principaux défis mis au jour par notre étude et vous guidons dans la quête d'une approche plus collaborative et efficace. Celle-ci vous aidera à mettre en place des opérations cloud sécurisées et à rationaliser vos équipes, vos processus et vos technologies pour vous préparer au SASE.

Quand votre organisation prévoit-elle d'entreprendre un projet de transformation lié à la sécurité et/ou au réseau ?



79 % des DSI et des RSSI ont déjà constaté des économies en déplaçant leur sécurité dans le Cloud.

La grande majorité des DSI et des RSSI européens (98 %) ont déplacé au moins quelques ressources vers le Cloud, même si moins d'1 sur 5 (18,5 %) a effectué la transition pour plus des trois-quarts de son infrastructure de sécurité. La plupart de ceux qui ont adopté la sécurité cloud ont déjà réduit leurs dépenses dans certains des domaines prévus : 25 % réalisent des économies en coûts d'équipements et 23 % en frais de bande passante. En parallèle, 21 % ont réduit leurs coûts en diminuant le nombre de leurs fournisseurs, et 21 % ont réduit leurs dépenses en équipements de pare-feu en les remplaçant par des alternatives dans le Cloud.

Comme la grande majorité des personnes interrogées n'ont pas terminé leur transformation digitale, ces économies doivent être considérées comme préliminaires. Elles méritent en tous cas d'être analysées régulièrement. Un exemple : 30 % des sondés pensent réduire leurs coûts en déployant des technologies Firewall-as-a-Service (FWaaS), mais seuls 22 % déclarent avoir atteint cet objectif pour le moment.

98%

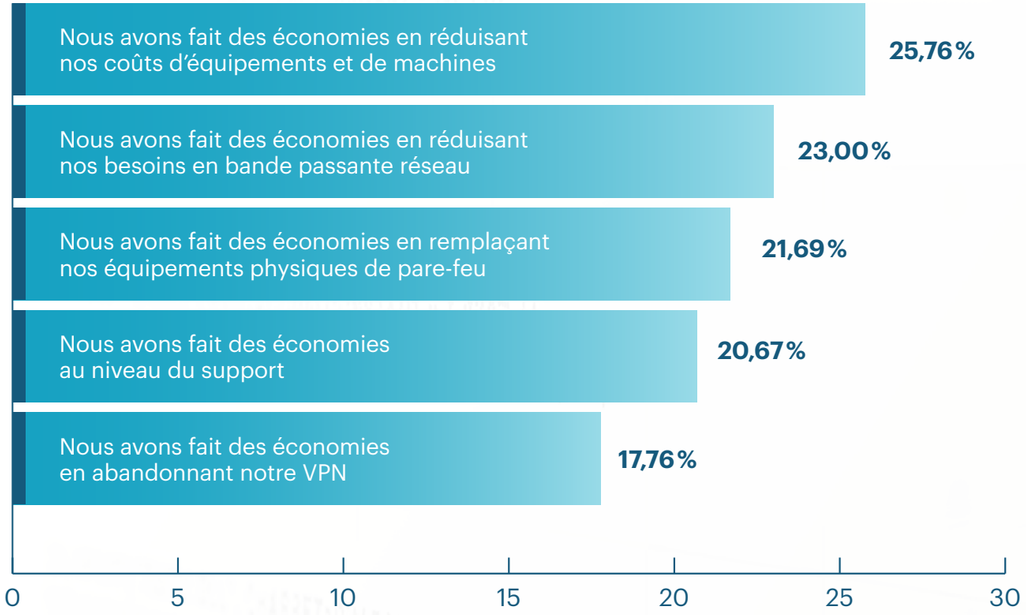
des DSI/RSSI européens ont déplacé au moins certaines ressources dans le Cloud

mais seuls

18,5%

ont déplacé plus des trois quarts de leur infrastructure de sécurité

PARMI CES AFFIRMATIONS, LESQUELLES SONT VRAIES POUR VOTRE ORGANISATION ET VOUS CONCERNANT LA TRANSITION DE VOTRE SÉCURITÉ VERS LE CLOUD ?



Point à retenir

La transition vers le Cloud est un chantier en cours : les économies générées par le Cloud et le SASE augmenteront probablement au fil du temps. Les entreprises se focalisent sur des projets à court terme, comme le remplacement des VPN et le regroupement de leurs fournisseurs, qu'elles considèrent comme les meilleures sources d'économies d'ici deux ans.

Un DSI/RSSI sur trois compte faire converger ses équipes réseau et sécurité, mais très peu prévoient de combiner les budgets respectifs de ces équipes.

Unifier la sécurité et le réseau est une bonne pratique du parcours cloud des entreprises. Par ailleurs, la raison donnée par les sondés pour expliquer cette convergence est parfaitement logique : environ un tiers des DSI et RSSI pensent que la division des équipes empêche la gestion optimale des ressources cloud.

Nous avons cependant remarqué que la vaste majorité des entreprises européennes qui fusionnent leurs équipes réseau et sécurité maintiennent des budgets séparés. Seules 8 % des personnes interrogées ont l'intention d'unifier les budgets du réseau et de la sécurité. Même si les deux équipes sont sous la responsabilité du DSI – environ deux tiers des équipes IT européennes seront sous la double responsabilité du DSI et du RSSI, directement ou indirectement –, elles pourraient se retrouver en concurrence face aux ressources et à la propriété des technologies cloud. C'est précisément ce que redoutent 28 % des sondés.

Ces préoccupations sont renforcées par une absence de consensus, parmi les personnes interrogées, concernant la bonne stratégie cloud à adopter. Nous avons identifié que 27 % des organisations transfèrent la responsabilité et le financement de leur sécurité réseau à leur équipe sécurité, avec l'espoir que ce budget supplémentaire favorisera des projets de transformation comme l'adoption du ZTNA et du SASE. En parallèle, 27 % des sondés transfèrent les budgets de sécurité à leurs équipes réseau et infrastructure afin de financer une approche de la sécurité dès la conception.

30 %

des équipes réseau et sécurité se sont déjà rapprochées ou comptent le faire

mais seules

8 %

prévoient d'unifier leurs budgets respectifs

Point à retenir

Alors qu'évoluent les bonnes pratiques en matière de sécurité cloud, peu d'entreprises adoptent une approche parfaitement efficace : faire converger la sécurité et le réseau sur le plan du personnel comme des budgets.

La forte divergence de points de vue concernant la responsabilité des technologies de sécurité essentielles ouvre la porte à des conflits de propriété.

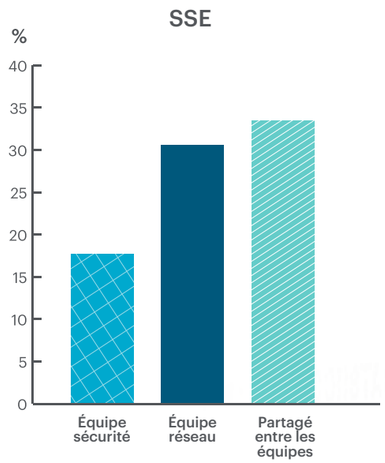
Les technologies et environnements de sécurité transformationnels – y compris le SASE, le SSE, le ZTNA et le SWG – ont attiré l'intérêt de nombreux DSI et RSSI européens. Néanmoins, un intérêt commun pour ces technologies n'aboutit pas forcément à un accord concernant la propriété de tels produits ou projets de transformation.

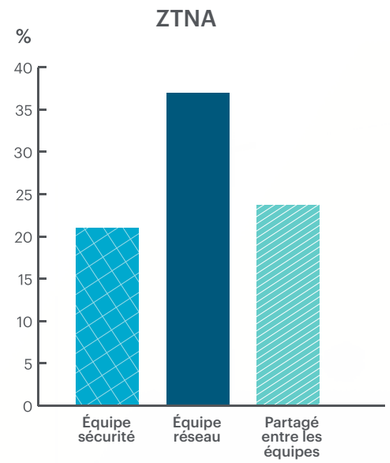
Notre sondage a déterminé que 28 % des entreprises attribuent la propriété de leurs projets SASE à leurs équipes réseau et 18 % à leurs équipes sécurité. Parallèlement à cela, dans 31 % des entreprises européennes, les deux équipes se partagent la responsabilité du SASE.

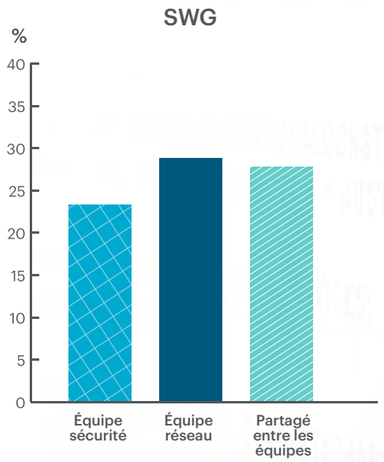
Bien que SSE soit un terme relativement nouveau et englobe les services de sécurité entrant dans la composition du SASE, nous avons relevé que la propriété de ces deux technologies était divisée de manière très similaire. La responsabilité des solutions SSE revient à l'équipe réseau dans 30 % des entreprises et à l'équipe sécurité dans 18 % des entreprises. Dans 33 % des entreprises, les deux équipes se la partagent.

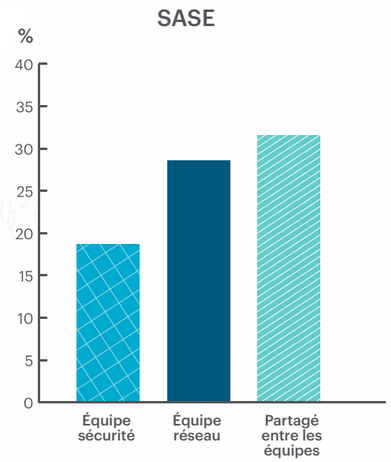
La responsabilité du ZTNA est fortement orientée vers l'équipe réseau (37 %, contre 21 % pour l'équipe sécurité et 23 % en responsabilité partagée). Le SWG est la technologie la plus susceptible d'être à la charge de l'équipe sécurité (23 %, contre 28 % pour l'équipe réseau et 27 % en responsabilité partagée).

À QUELLE ÉQUIPE EST ATTRIBUÉ LE BUDGET DES TECHNOLOGIES / INITIATIVES SUIVANTES ?









Point à retenir

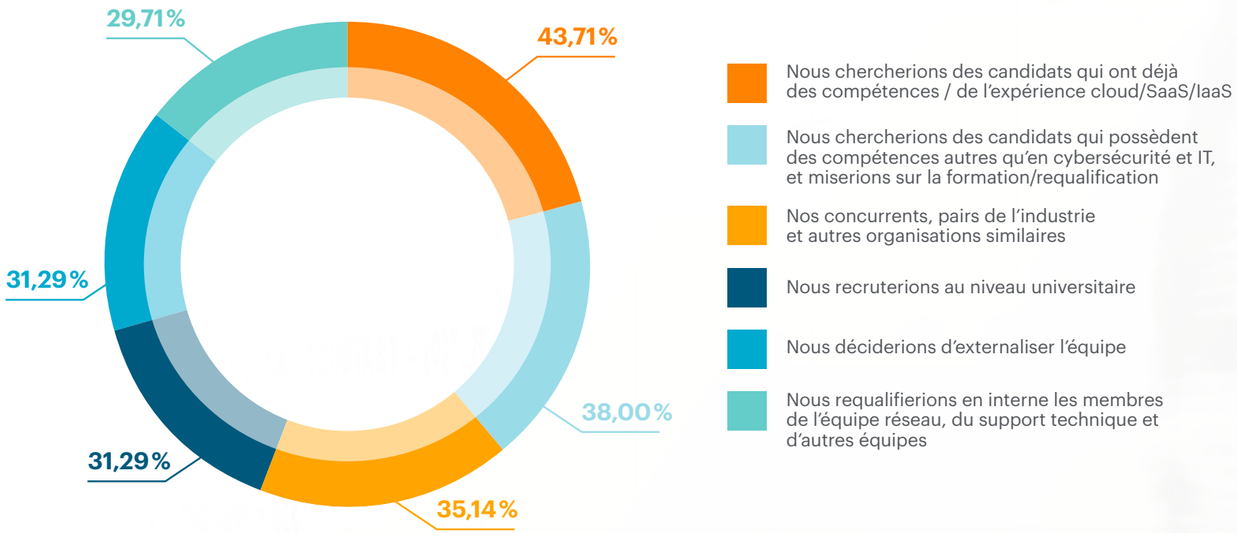
Les conflits de propriété entre les équipes réseau et sécurité pourraient avoir un impact négatif sur les résultats et les bénéfices. Comme la responsabilité de telles initiatives par telle équipe fait débat, il revient au DSI et au RSSI de trouver un accord, et de communiquer de manière claire et cohérente sur la responsabilité de chacune des équipes pour chaque domaine lié à la transformation.

46 % des entreprises font face à des difficultés de recrutement lorsqu'elles veulent embaucher de nouveaux membres pour leur équipe sécurité.

Parmi les organisations européennes ayant déplacé certaines activités de sécurité dans le Cloud, 28 % ont déjà modifié la composition ou la taille de leur équipe réseau, et 26 % ont effectué des changements au niveau de leur équipe sécurité. Près d'un tiers des sondés renforcent ou prévoient de renforcer leur équipe sécurité pour refléter sa responsabilité plus large à mesure que leurs entreprises étendent leurs opérations dans le Cloud.

Un nombre non négligeable de DSI/RSSI interrogés (29 %) affirment ne pas avoir eu de mal à trouver des candidats qualifiés pour ces postes de sécurité. Cependant, ils sont encore plus nombreux (46 %) à rencontrer des difficultés pour trouver des candidats appropriés, ou à penser qu'ils en rencontreront à l'avenir. Ces préoccupations expliquent peut-être le fait que 38 % des sondés prévoient de compléter leur équipe sécurité par des membres non spécialisés en cybersécurité ou même en informatique.

SI VOUS AVIEZ BESOIN DE RENFORCER VOTRE ÉQUIPE SÉCURITÉ, OÙ CHERCHERIEZ-VOUS DE NOUVEAUX MEMBRES ?



28 % ont déjà modifié la structure ou la composition de leur **équipe réseau**.

26 % ont modifié leur **équipe sécurité**.

Point à retenir

La volonté des entreprises européennes de chercher des candidats qui ne possèdent pas encore de compétences et d'expérience cloud traduit un niveau de créativité rassurant. Mais cette créativité est nécessaire : les chiffres du sondage montrent que plus des deux tiers des équipes ont du mal à trouver des talents. Les DSI et les RSSI ouverts à l'idée de former de nouveaux membres pour leur équipe sécurité – et prêts à trouver des candidats qui possèdent les compétences voulues ou capables d'apprendre – sont bien moins susceptibles de faire face à une pénurie de talents.

Ce que vous pouvez faire dès aujourd'hui

Pour les entreprises IT et leurs DSI et RSSI, déplacer les opérations dans le Cloud représente un véritable changement de paradigme, tel qu'on n'en vit qu'une fois par génération. Tout comme n'importe quel changement important, la transformation digitale est certainement inconfortable, mais les entreprises en font une priorité. Plus de la moitié de nos sondés pensent lancer leurs projets de transformation digitale au cours des deux prochaines années.

Les DSI et RSSI pour lesquels la transformation du réseau et de la sécurité suit une même chronologie font face à diverses approches contradictoires concernant la meilleure façon de procéder. Comme l'indique notre étude, la plupart des entreprises européennes tâtonnent et expérimentent dans la quête de bonnes pratiques. Certaines effectuent la transition dans le Cloud en utilisant des structures de gestion qui ont bien fonctionné sur site, et croisent les doigts.

Cette approche n'est pas sans risque. Il n'est pas raisonnable d'attendre des compétences et des stratégies budgétaires traditionnelles qu'elles fonctionnent aussi bien dans le Cloud que dans le datacenter de l'entreprise. Les leaders susceptibles de mieux gérer la transformation numérique sont ceux qui se préparent pour ces projets en réalignant les budgets, en repensant les ressources de leurs équipes et en réexaminant leurs méthodes de recrutement.

À propos de Netskope

Avec Netskope, le leader du SASE, les utilisateurs sont connectés directement à Internet, à toutes leurs applications et à leur infrastructure, rapidement et en toute sécurité, depuis n'importe quel appareil, dans ou hors du réseau. Grâce à notre technologie brevetée ainsi qu'au CASB, au Cloud Firewall, au proxy et au ZTNA intégrés au sein d'une seule plateforme, Netskope Security Cloud donne le contexte le plus spécifique. Il fournit un accès conditionnel et favorise la sensibilisation des utilisateurs tout en appliquant les principes du Zero Trust aux solutions de protection des données et de prévention des menaces et ce à tous les niveaux. Contrairement à d'autres solutions qui font des compromis entre sécurité et réseau, le Cloud privé et global de sécurité de Netskope permet des capacités de calcul complètes, même en périphérie du réseau.

La solution Netskope est rapide partout, centrée sur les données et adaptée au Cloud. Elle favorise une bonne citoyenneté numérique et la réduction du coût total de possession.

netskope.com

Méthodologie

Sondage mené en octobre 2021 par Censuswide pour le compte de Netskope, et pour lequel ont été interrogés 700 professionnels de l'IT en Allemagne et au Royaume-Uni. Les participants au sondage sont tous des DSI, RSSI ou directeurs IT d'entreprises comptant plus de 5 000 utilisateurs.