



The bridge to possible



# Rapport sur les tendances mondiales de mise en réseau pour 2022

Édition spéciale : l'état des service d'accès sécurisé en périphérie (SASE) et la montée en puissance du réseau sous forme de service (NaaS)





Édition spéciale :  
L'état des SASE





# Table des matières

Introduction aux SASE.....	04
Le défi informatique .....	05
La relation entre SD-WAN et SASE .....	07
Les capacités SASE souhaitées .....	09
L'importance de l'intégration.....	12
Tendances d'adoption des SASE .....	15
Modèles de consommation des SASE.....	17
Conclusion sur les SASE .....	18

# Adopter une stratégie de service d'accès sécurisé en périphérie (SASE)

Le travail hybride exige une stratégie SASE cohésive pour offrir une expérience utilisateur cohérente et exceptionnelle en tout lieu.

Pour aborder l'intérêt croissant et la confusion sur le marché autour des services d'accès sécurisé en périphérie (SASE), nous avons créé cette annexe spéciale au [rapport de 2022 sur les tendances mondiales en matière de mise en réseau : L'essor du réseau sous forme de service \(NaaS\)](#).

Le service d'accès sécurisé en périphérie, qui est porté par la forte augmentation du travail à distance et l'adoption du nuage hybride, offre une connectivité sécurisée et transparente à n'importe quelle application, sur n'importe quel réseau, à partir de n'importe quel endroit ou appareil.

Le SASE intègre les fonctions de mise en réseau et de sécurité dans une solution ou un service unifié infonuagique.

Contrairement aux solutions de sécurité habituelles, il rapproche les politiques de sécurité et leur application des utilisateurs finaux et des applications qui sont de plus en plus distribuées. Il s'appuie sur la vérification systématique et élimine la nécessité de renvoyer constamment les données vers un centre de données, réduisant ainsi efficacement les charges et les goulots d'étranglement du réseau et offrant une meilleure expérience de l'utilisateur.



En tant que solution de rechange à une pile conventionnelle de sécurité, il fournit un accès sécurisé de bout en bout, y compris le centre de données, les bureaux à distance, les utilisateurs itinérants et bien plus encore.

Cette annexe met en avant les dernières tendances et observations concernant le SASE. Les données proviennent de plusieurs études de marché et de perspectives recueillies auprès d'éminents analystes et experts de l'industrie. Nous espérons que ces renseignements vous aideront à mieux comprendre les avantages et les répercussions du SASE lorsque vous formulerez vos stratégies en matière de réseau, de sécurité et de nuage.

– Omri Guelfand, vice-président, Services réseau, Cisco

« La confusion quant à la notion de SASE est toujours aussi présente sur le marché. Cependant, le consensus émergent s'aligne bien sur notre vision actuelle selon laquelle le SASE n'est pas une technologie entièrement nouvelle mais une intégration de technologies de réseau existantes, comme le réseau WAN défini par logiciel (SD-WAN), et de technologies de sécurité, comme les passerelles Web sécurisées (SWG), dans une solution de connectivité sécurisée infonuagique. »

– Dell'Oro Group<sup>1</sup>




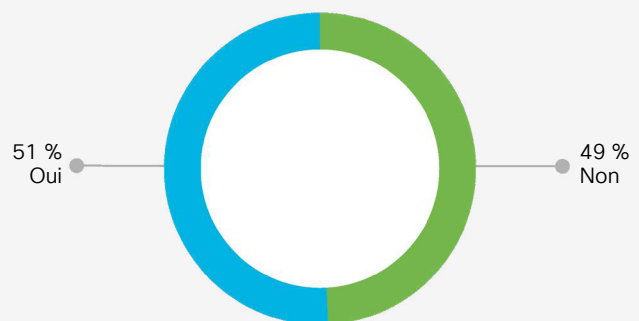
## Le défi informatique : offrir une expérience de travail hybride sécurisée et infonuagique

Les deux plus grandes tendances auxquelles les équipes informatiques sont confrontées aujourd'hui sont indéniablement la transition continue vers une stratégie d'applications à nuages multiples et l'adoption de modèles de travail hybrides. Comme les utilisateurs et les applications sont plus que jamais distribués, leur connexion et leur protection sont devenues de plus en plus complexes.

La répartition des applications sur de nuages multiples, privés et publics, est désormais amplifiée par la répartition intense des travailleurs et des espaces de travail qui découle du travail hybride. Avec cette hyperdistribution, le défi d'essayer de maintenir une expérience de l'utilisateur inclusive et de haute qualité diffère considérablement de l'environnement d'entreprise sur place, autrefois très maîtrisable.

**Les résultats de récents sondages révèlent que 76 % des équipes informatiques ont déclaré que les travailleurs à distance sont plus difficiles à sécuriser<sup>2</sup>, et 51 % des organisations ont déclaré avoir eu des problèmes pour connecter les travailleurs aux ressources de l'entreprise au cours des 18 derniers mois<sup>3</sup>.**

 Est-ce que vous ou votre entreprise avez eu des difficultés à maintenir les employés connectés au cours des 18 derniers mois?



La transition en cours d'un modèle d'application axé sur le centre de données vers un modèle axé sur le nuage activé par Internet a obligé les équipes informatiques à repenser radicalement leur stratégie de mise en réseau. De même, les équipes de sécurité s'efforcent de fournir une expérience de l'utilisateur sûre et transparente lorsque les utilisateurs et les applications sont situés hors site, où ils sont plus susceptibles d'être exposés accidentellement ou de subir des attaques intentionnelles.

Cela contribue à expliquer le haut niveau d'intérêt porté à un modèle SASE infonuagique, qui réunit des solutions de mise en réseau comme le réseau SD-WAN et des solutions de sécurité infonuagiques comme le security service edge (SSE) et l'accès réseau Zero Trust (zero-trust network access, ZTNA).

Le SASE vise à connecter et à protéger les utilisateurs et les applications, où qu'ils se trouvent ou soient hébergés, pour finalement offrir une meilleure expérience de l'utilisateur, plus cohérente et plus sûre. Il promet également de réduire le coût et la complexité du système informatique et d'améliorer la flexibilité et les performances du réseau et, en fin de compte, l'expérience des applications.



« La pandémie, à son apogée en 2020, a entraîné une augmentation de 450 % du nombre d'employés américains travaillant à distance à temps plein ou occasionnellement par rapport à la base de référence avant la pandémie. Bien que les taux aient commencé à baisser, nous prévoyons que les taux de travail à distance à long terme se stabilisent à 200 % au-dessus de la base de référence avant la pandémie. »

– Dell'Oro Group<sup>4</sup>



### Autrement dit :

Une main-d'œuvre de plus en plus distribuée et diversifiée va devenir une réalité. Le SASE, s'il est correctement implémenté, permet de connecter et de protéger les utilisateurs et les applications distribués, d'aligner les politiques de réseau et de sécurité, et de réduire la charge et le risque de la gestion du réseau et de la sécurité.

# La relation entre le réseau SD-WAN et le SASE

La confusion du marché autour du SASE a engendré un certain nombre de questions concernant les solutions de réseau SD-WAN existantes. Le SASE remplace-t-il le réseau SD-WAN? Se complètent-ils? Ou s'agit-il de solutions tout à fait différentes pour des besoins différents?

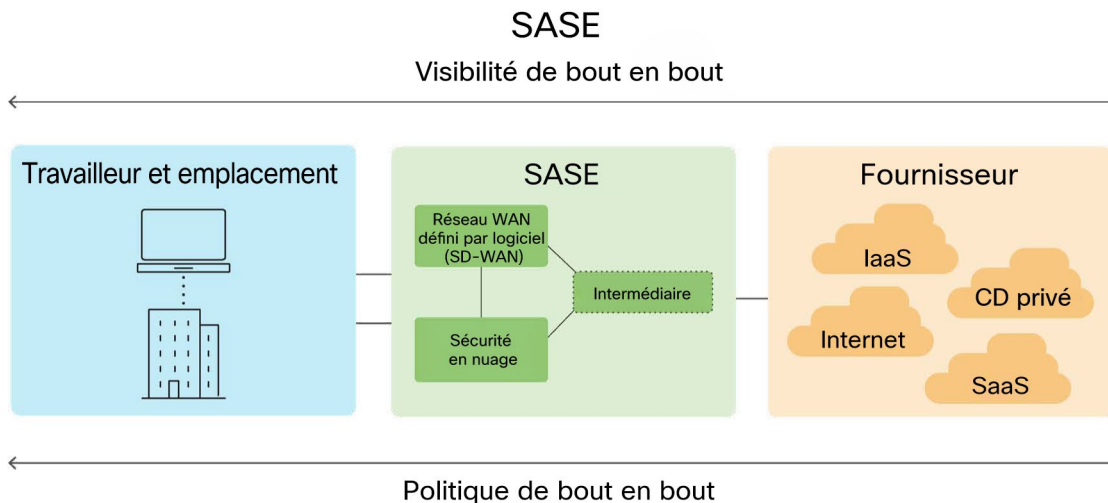
La réponse est simple : le réseau SD-WAN est la base du SASE.

et le SASE combine les capacités de sécurité natives du réseau SD-WAN avec une sécurité centrée sur le nuage pour connecter et protéger les utilisateurs et les applications, quel que soit leur emplacement ou leur hébergement. En tant qu'architecture superposée, SASE ne peut pas offrir une sécurité omniprésente sans les garanties fournies par le réseau SD-WAN, notamment :

- Activer la traduction d'adresses réseau (NAT)
- Segmenter le réseau en plusieurs sous-réseaux
- Surveiller et bloquer les logiciels et le trafic malveillants
- Restreindre les utilisateurs non autorisés
- Prévenir les contenus ou applications indésirables
- Coupe-feu du trafic entrant indésirable et du trafic de VLAN à VLAN
- Sécuriser le RPV site-à-site/dans le tunnel
- Géorepérage pour le contrôle d'accès basé sur la localisation

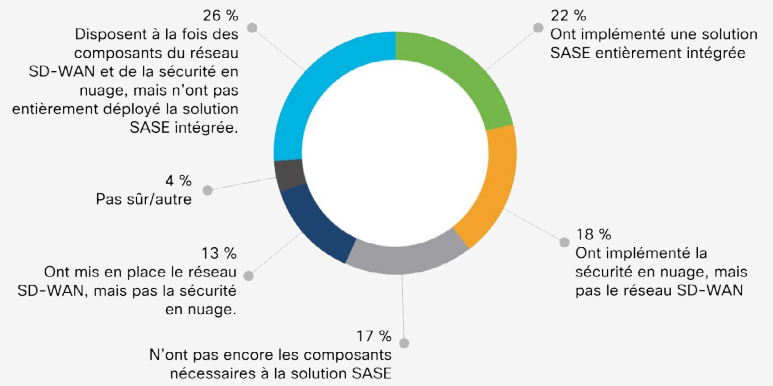
« Le SASE ne rend pas le réseau SD-WAN obsolète. Au contraire, le réseau SD-WAN est un élément fondamental du SASE. Les offres SASE font converger plusieurs capacités de réseau et de sécurité sous forme de service, comme le réseau SD-WAN, la passerelle Web sécurisée (SWG), le contrôle d'accès de sécurité infonuagique (CASB), le NGFW et l'accès au réseau Zero Trust (ZTNA). »

– 2021 Gartner®, Quick Answer: Does SASE Replace SD-WAN?





## À quelle étape en êtes-vous dans votre trajectoire d'adoption de SASE?



Cisco, Sondage sur l'avenir de la technologie 2021, N 29 506

Les organisations informatiques doivent-elles commencer par le réseau SD-WAN ou la sécurité en nuage? Beaucoup adoptent une approche progressive de l'implémentation de SASE. La plupart sont au milieu de leur trajectoire SASE, avec une combinaison de composants de réseau SD-WAN et de sécurité en nuage qui n'ont pas encore été entièrement intégrés ou opérationnalisés.

**18 % des entreprises disposent de la sécurité en nuage mais pas de réseau SD-WAN, et 13 % ont un réseau SD-WAN mais pas de sécurité en nuage<sup>6</sup>.**



### Autrement dit :

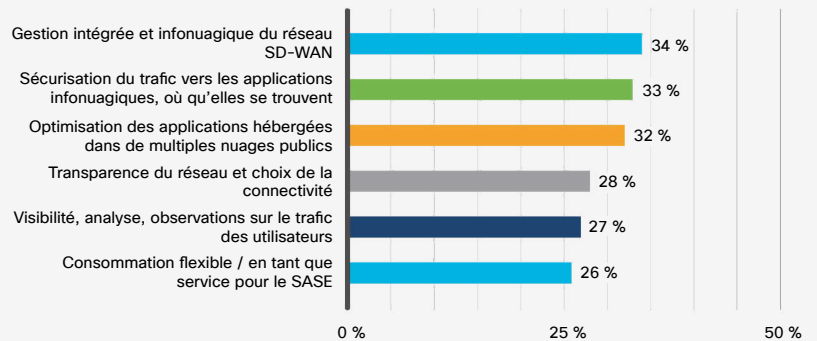
Le réseau SD-WAN est un élément fondamental du SASE qui fonctionne conjointement avec des solutions ou services de sécurité centrés sur le nuage pour protéger les utilisateurs et les données dans les domaines sur place, dans le nuage et en périphérie.



# Capacités SASE souhaitées

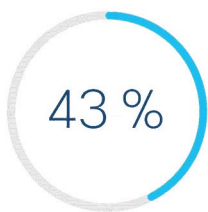
Comme le SASE représente l'intégration des capacités de réseau et de sécurité, 34 % des organisations donnent la priorité aux solutions et services qui offrent une gestion intégrée et infonuagique du réseau SD-WAN. La sécurisation du trafic vers les applications infonuagiques (33 %), l'optimisation des applications hébergées dans de multiples nuages publics (32 %) et l'amélioration de la transparence et de la flexibilité du réseau (28 %) ont également été citées comme des priorités principales.

À votre avis, quelles capacités de SASE seraient prioritaires pour votre organisation?



Cisco, Sondage sur les tendances mondiales de mise en réseau 2021 ; N 1534

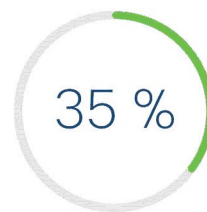
## Connecter les travailleurs à distance :



43 % des organisations prévoient d'utiliser le RPV en tant que service.



36 % cherchent à adopter un accès réseau Zero Trust et des capacités d'authentification multifactorielle.



35 % sont intéressés par les clients unifiés basés sur l'hôte.



35 % cherchent à étendre leur réseau SD-WAN aux utilisateurs mobiles et à domicile.

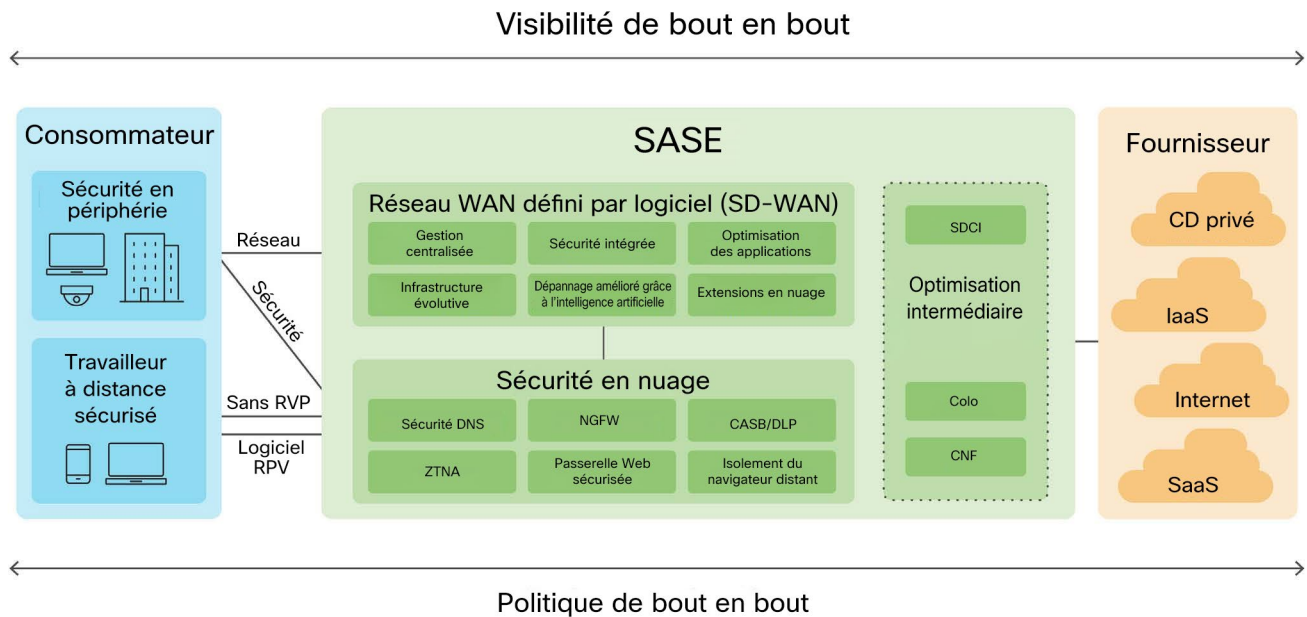
Bien que les architectures, solutions et services SASE continuent d'évoluer, ils sont fondamentalement conçus pour réunir certaines ou toutes les capacités de base fournies par le réseau SD-WAN et la sécurité en nuage :

Réseau WAN défini par logiciel (SD-WAN)	Sécurité en nuage
<p><b>Gestion centralisée</b></p> <p>Un tableau de bord centralisé et très visuel qui facilite la configuration du périphérique, la gestion du réseau, la surveillance et l'automatisation. Comprend l'approvisionnement libre-service à la périphérie du réseau.</p>	<p><b>Accès réseau Zero Trust (ZTNA)</b></p> <p>Un cadre de sécurité qui atténue les accès non autorisés, limite les brèches et réduit les mouvements latéraux des attaquants sur le réseau. Le ZTNA doit être couplé à une solide gestion des identités et des accès afin de vérifier l'identité des utilisateurs et de déterminer la confiance dans les appareils avant d'accorder l'accès aux applications autorisées.</p>
<p><b>Extension du réseau en nuage et optimisation intermédiaire</b></p> <p>Intégrations étendues de la rampe d'accès au nuage pour permettre une connectivité transparente et automatisée avec toute configuration site à nuage et site à site. Comprend une connectivité intermédiaire optimisée grâce à l'interconnexion des nuages définie par logiciel (SDCI) et aux intégrations de colocalisation.</p>	<p><b>Passerelle Web sécurisée (SWG)</b></p> <p>Une passerelle qui enregistre et inspecte le trafic Web pour offrir une totale visibilité, un filtrage des URL, un contrôle des applications et une protection contre les logiciels malveillants.</p>
<p><b>Expérience d'application</b></p> <p>La capacité de surveiller et de valider la convivialité et les performances des applications Web. Les indicateurs détaillés montrent l'extraction et le chargement séquentiels des composants Web afin d'identifier les erreurs et les goulots d'étranglement et de comprendre l'incidence sur les performances de l'application.</p>	<p><b>Pare-feu en nuage avec système de prévention des intrusions (IPS)</b></p> <p>Services basés sur des logiciels, déployés dans le nuage, qui aident à gérer et à inspecter le trafic réseau.</p>
<p><b>Infrastructure souple et évolutive</b></p> <p>Un large éventail de plateformes physiques et virtuelles qui offrent une disponibilité et un débit élevés, des options de port multigigabit, des liaisons cellulaires 5G et de puissantes capacités de chiffrement. Optimise le trafic WAN en sélectionnant dynamiquement les liens WAN les plus efficaces qui répondent aux exigences de niveau de service.</p>	<p><b>Contrôle d'accès de sécurité infonuagique (CASB)</b></p> <p>Logiciel qui détecte et signale les applications en nuage utilisées sur un réseau, ce qui permet d'exposer le service informatique parallèle et de bloquer les applications SaaS à risque et des actions précises, comme les publications et les téléversements.</p>
<p><b>Dépannage amélioré grâce à l'intelligence artificielle</b></p> <p>Une intelligence artificielle et un apprentissage automatique robustes pour optimiser les performances du réseau, automatiser les tâches manuelles de routine et accélérer le dépannage. Fournit des capacités d'alerte intelligente, d'autoréparation et de redirection prédictive de l'Internet.</p>	<p><b>Protection contre la perte de données</b></p> <p>Logiciel qui analyse les données en ligne pour fournir une visibilité et un contrôle sur les données sensibles qui sont poussées ou tirées au-delà du réseau ou du nuage de l'organisation.</p>
<p><b>Sécurité intégrée</b></p> <p>Des capacités de sécurité robustes qui fonctionnent en synergie avec la sécurité en nuage pour protéger les succursales, les utilisateurs à domicile et les applications en nuage contre l'infiltration.</p>	<p><b>Isolation du navigateur à distance (RBI)</b></p> <p>Logiciel qui isole le trafic Web des appareils de l'utilisateur pour atténuer le risque de menaces transmises par le navigateur.</p>
<p><b>Gestion des politiques basées sur l'identité</b></p> <p>Microsegmentation et gestion des politiques basées sur l'identité sur plusieurs emplacements et domaines.</p>	<p><b>Sécurité de couche DNS</b></p> <p>Logiciel qui agit comme première ligne de défense contre les menaces sur Internet, en bloquant les requêtes DNS malveillantes avant même qu'une connexion à une adresse IP soit établie. Une forte sécurité DNS peut réduire considérablement le nombre de menaces qu'une équipe de sécurité doit trier quotidiennement.</p>
<p><b>Observations détaillées</b></p> <p>Meilleure visibilité des applications, de l'Internet, des nuages et des environnements SaaS grâce à une analyse bond par bond exhaustive. Permet d'isoler les domaines de défaillance et fournit des observations pratiques pour accélérer le dépannage et minimiser ou éliminer l'incidence sur les utilisateurs.</p>	<p><b>Renseignements sur les menaces</b></p> <p>Les chercheurs en vulnérabilités, les ingénieurs et les scientifiques des données qui utilisent la télémétrie et les systèmes sophistiqués pour créer des renseignements précis, rapides et pratiques sur les menaces afin d'identifier les menaces émergentes, de découvrir de nouvelles vulnérabilités et d'interdire les menaces dans les environnements avant qu'elles ne se propagent, avec des ensembles de règles qui prennent en charge les outils de votre pile de sécurité.</p>

En plus d'intégrer les capacités du réseau SD-WAN et de la sécurité en nuage, les modèles SASE peuvent aider à briser les cloisons opérationnelles et à favoriser un meilleur alignement entre les équipes de réseau et de sécurité. Grâce à des politiques normalisées, à une télémétrie partagée et à des alertes coordonnées sur tous les composants de sécurité et de réseau, le SASE permet aux équipes NetOps et SecOps d'améliorer l'efficacité, la visibilité et la protection du système informatique.

Dans cette perspective, il est important que les organisations disposent d'une stratégie SASE globale qui tienne compte à la fois des objectifs NetOps et SecOps, renforce l'alignement opérationnel et soit capable de répondre aux besoins de l'organisation dans un avenir prévisible.

## SASE : détail



« D'ici 2024, 30 % des entreprises adopteront les fonctionnalités de passerelle Web sécurisée (SWG), de contrôle d'accès de sécurité infonuagique (CASB), d'accès réseau Zero Trust (ZTNA) et de pare-feu de succursale sous forme de service (FWaaS) fournies par le même fournisseur, contre moins de 5 % en 2020. »

– Gartner<sup>7</sup>



### Autrement dit :

Dans leur évaluation des stratégies et des offres SASE, les organisations recherchent des solutions et des services qui offrent les capacités fondamentales à la fois du réseau SD-WAN et de la sécurité en nuage pour répondre à leurs besoins actuels et évolutifs.



# L'importance de l'intégration

Les entreprises modernes s'appuient sur un certain nombre d'environnements réseau (réseaux de centres de données, réseaux locaux, réseaux étendus) et de solutions de sécurité (pare-feu, passerelles et contrôle d'accès pour les systèmes sur place et dans le nuage). Grâce à des intégrations de technologies et de services, le SASE peut fournir une visibilité, une harmonisation des politiques et une protection pour tous ces éléments.

L'objectif principal étant de connecter en toute sécurité les utilisateurs et les applications, où qu'ils soient situés ou hébergés, ces intégrations permettent également de faire ce qui suit :

- Réduire le volume des incidents de sécurité.
- Accélérer le dépannage et la résolution des problèmes.
- Simplifier la surveillance et la gestion des systèmes.
- Améliorer la normalisation et l'application des politiques.
- Soutenir les exigences régionales en matière de conformité et de données.
- Réduire les coûts d'investissement et d'exploitation.

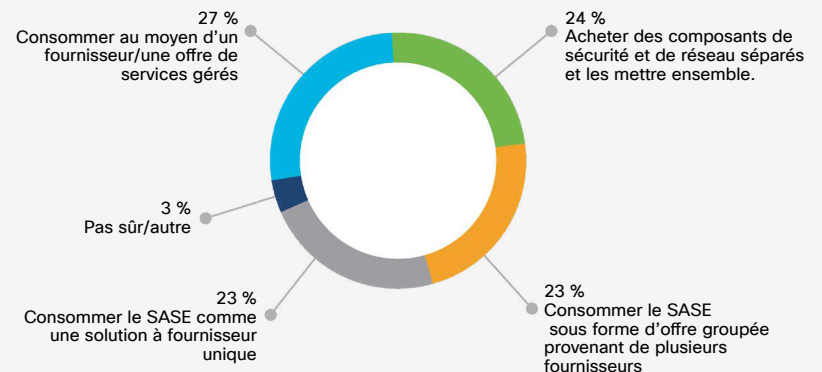


« Il existe deux grands types d'implémentation SASE sur le marché : unifiée et désagrégée. L'implémentation unifiée consiste en des plateformes SASE à fournisseur unique, étroitement intégrées. L'implémentation désagrégée est une implémentation multi-fournisseur ou multi-produit avec moins d'intégration par rapport à l'implémentation unifiée. »

– Dell'Oro Group<sup>9</sup>



Comment allez-vous déployer et rendre opérationnelle votre solution SASE?



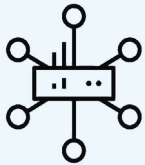
Cisco, Sondage sur l'avenir de la technologie 2021; N 29 506

Avec l'émergence de solutions et de services à fournisseur unique et à fournisseurs multiples, ainsi que la possibilité d'architectures personnalisées qui assemblent un certain nombre de solutions individuelles, les organisations disposent d'un certain nombre d'options pour déployer le SASE et le rendre opérationnel.

Parce que l'élaboration et l'intégration d'une solution personnalisée ou l'opérationnalisation d'un ensemble SASE à fournisseurs multiples peuvent introduire des complexités indésirables, des défis opérationnels et des vulnérabilités en matière de sécurité, beaucoup (50 %) recherchent une solution unifiée et/ou gérée par un seul partenaire.

- 70 % sont d'accord ou tout à fait d'accord pour dire qu'il est devenu de plus en plus complexe de gérer efficacement une pile de réseaux et de sécurité à fournisseurs multiples.
- 26 % disposent à la fois de capacités de sécurité en nuage et de réseau SD-WAN, mais ne les ont pas pleinement opérationnalisées et intégrées dans un modèle SASE global.<sup>10</sup>

Qu'il s'agisse d'une architecture sur mesure, d'une offre groupée de plusieurs fournisseurs, d'un service entièrement géré par un seul fournisseur ou d'une variation de ces éléments, chaque solution SASE devrait permettre un meilleur alignement et une meilleure intégration entre :



### Le réseau SD-WAN et la sécurité en nuage

- Automatiser le routage du trafic entre le dispositif de réseau SD-WAN et les points de présence (PoP) de sécurité infonuagique.
- Rediriger automatiquement le trafic vers un autre PoP pour assurer la résilience en cas de problème de performance.
- Utiliser l'analyse prédictive basée sur l'intelligence artificielle pour rediriger automatiquement le trafic vers d'autres PoP avant que l'expérience de l'utilisateur ne soit compromise.



### Les équipes NetOps et SecOps

- Devenir capable de partager en permanence les politiques de sécurité (comme les autorisations d'accès et la segmentation) entre les implémentations du réseau SD-WAN et de la sécurité en nuage.
- Permettre l'échange de données entre les plateformes de gestion du réseau SD-WAN et de la sécurité en nuage afin de fournir une visibilité cohérente des politiques et des événements.
- Étendre et propager les configurations et les politiques des réseaux pour grandes entreprises (telles que les RPV et les étiquettes de groupe de sécurité) dans les plateformes de sécurité infonuagique.
- Utilisez l'authentification administrative à connexion unique (SSO) sur les plateformes de gestion du réseau SD-WAN et de la sécurité en nuage.



### Les utilisateurs finaux et les applications

- Permettre une connectivité directe entre le réseau SD-WAN, les services intermédiaires (tels que SDCI), les services à nuages multiples et le SaaS.
- Surveiller et optimiser l'expérience de l'utilisateur avec une visibilité et des analyses intégrales sur le réseau SD-WAN, les PoP de sécurité infonuagique et les connexions IaaS/SaaS.



« Il est impossible de réussir une mise en réseau sans intégrer la sécurité. Je dois envisager la sécurité de manière globale, du point d'extrémité à l'application en passant par le réseau. Avec le réseau sous forme de service, j'ai besoin que le fournisseur prenne la responsabilité à la fois du réseau et de la sécurité. S'ils se chargent uniquement du réseau, j'ai besoin de la visibilité et du contrôle nécessaires pour assurer une protection intégrale et une atténuation rapide des menaces. Dans une situation optimale, le fournisseur s'occuperait très bien à la fois de la mise en réseau et de la sécurité. »

– Directeur de l'infrastructure de TI, société internationale de biens de consommation



### Autrement dit :

Qu'ils soient conçus sur mesure ou fournis par un ou plusieurs fournisseurs, les solutions et services SASE doivent permettre une intégration étroite entre le réseau SD-WAN et les systèmes de sécurité en nuage, afin d'optimiser une expérience de l'utilisateur sécurisée et de rationaliser la collaboration entre NetOps et SecOps.

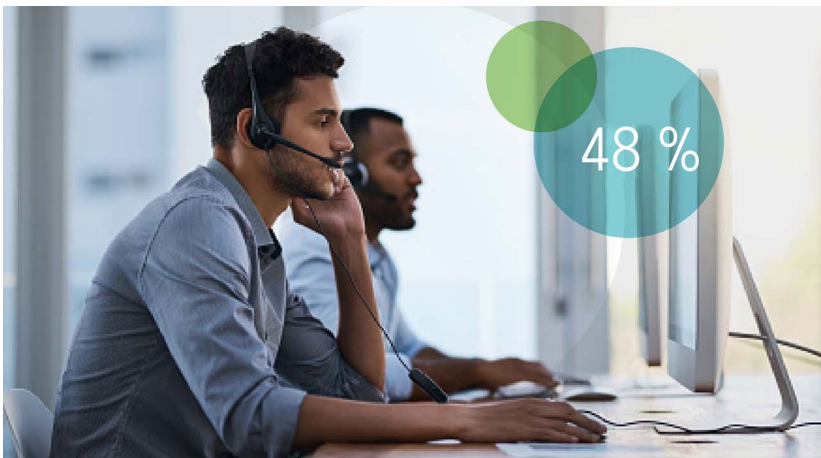
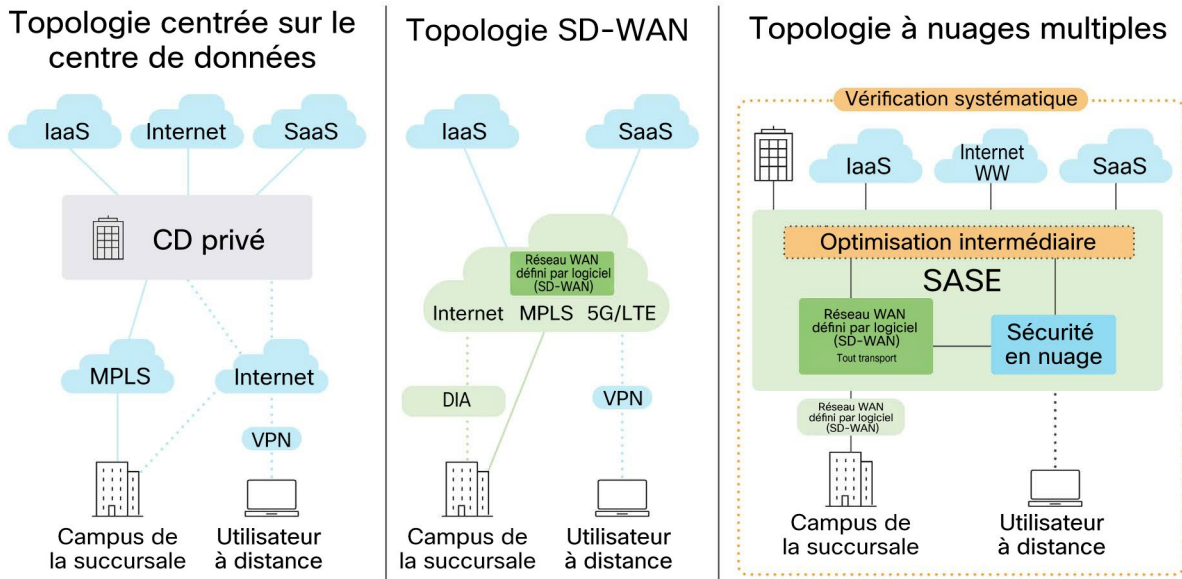


# Tendances d'adoption du SASE

Comme c'est le cas pour toute décision technologique, chaque organisation a besoin d'un modèle SASE et d'une approche de déploiement qui lui sont adaptés. Les solutions de réseau et de sécurité déjà en place, ainsi que les stratégies opérationnelles globales et les priorités de l'entreprise, doivent être des facteurs déterminants dans toute décision en matière de SASE. Les initiatives cruciales, les exigences réglementaires, les fusions et acquisitions, les opérations de la chaîne d'approvisionnement et les exigences de résilience de l'entreprise doivent également être prises en compte.

Les organisations qui passent d'un modèle d'application centré sur le centre de données à un modèle centré sur le nuage ou à nuages multiples peuvent commencer leur trajectoire SASE avec le réseau SD-WAN, par exemple, suivi de l'optimisation intermédiaire et de l'intégration de la sécurité infonuagique.

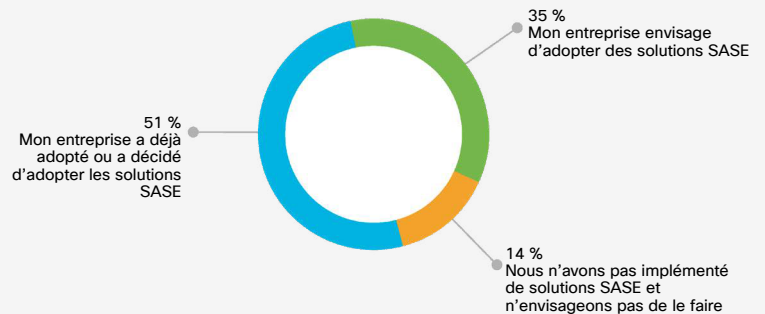
## De la topologie centrée sur le CD à la topologie à nuages multiples



48 % des entreprises intéressées par le SASE commenceront par la sécurité, 31 % par le réseau et 21 % prévoient d'aborder simultanément la sécurité et le réseau<sup>8</sup>.

Indépendamment du modèle particulier ou de l'approche de déploiement, de nombreuses entreprises disent être déjà bien engagées dans l'adoption du SASE : 86 % des organisations envisagent d'adopter le SASE ou l'ont déjà adopté<sup>11</sup>.

Votre entreprise a-t-elle adopté, décidé d'adopter ou envisagé d'adopter des solutions SASE?



Cisco, Sondage sur l'avenir de la technologie 2021; N 34 351

« D'ici 2025, au moins 60 % des entreprises auront des stratégies et des calendriers précis pour l'adoption du SASE qui couvrent l'accès des utilisateurs, des succursales et de la périphérie, contre 10 % en 2020. »

– Gartner<sup>12</sup>

**Autrement dit :**  
Les approches de déploiement de SASE sont déterminées par les cycles de vie des infrastructures existantes, les priorités opérationnelles et les initiatives commerciales. Les équipes informatiques devraient adopter une approche de planification stratégique qui vise à élaborer progressivement une architecture SASE intégrale.

# Modèles de consommation SASE

Il existe trois principaux modèles de consommation pour les solutions et services SASE. Bien que ces modèles de consommation aient des incidences variables sur les équipes et les opérations internes, ils brisent tous les silos traditionnels de mise en réseau et de sécurité. Par conséquent, le SASE peut être une fonction de forçage qui améliore l'alignement opérationnel et l'efficacité.



## Sous forme de service

Pour ceux qui veulent un déploiement rapide, une incidence minimale sur les opérations et le personnel, et le risque réduit qui va de pair avec les accords de niveau de service, SASE en tant que service offre un éventail de capacités infonuagiques entièrement intégrées, avec un tableau de bord unique et un soutien tout au long du cycle de vie. 26 % des organisations citent le SASE en tant que service comme leur modèle de consommation préféré.



## Hybride ou cogéré

Les organisations qui ne sont pas encore prêtes pour un modèle en tant que service intégral ou qui veulent plus de personnalisation que ce que ces services offrent peuvent adopter une approche hybride. Cela implique l'intégration de capacités de sécurité basées sur le nuage à une solution de réseau SD-WAN existante et/ou le partage des responsabilités en matière de réseau et de sécurité avec un fournisseur de services gérés. Ces approches hybrides offrent une sécurité et un soutien supplémentaires et permettent aux équipes informatiques de conserver une certaine visibilité et un certain contrôle tout en réduisant les demandes de gestion du cycle de vie global.



## Hautement personnalisé ou sur mesure

Les organisations qui veulent une personnalisation et un contrôle intégraux de leur réseau et de leur empreinte de sécurité peuvent élaborer, intégrer et gérer elles-mêmes les capacités de SASE. Ce niveau de personnalisation et de contrôle se fait généralement au détriment de la rapidité et de l'agilité, exige une gestion supplémentaire du cycle de vie du matériel, des logiciels et des licences, et nécessite des spécialistes supplémentaires en matière de sécurité et de conformité. Il s'agit d'une bonne option pour les organisations qui présentent des exigences très particulières et dont le réseau et le personnel existants peuvent répondre aux exigences architecturales et opérationnelles du SASE.

Découvrez les leçons tirées de notre expérience dans cette [étude de cas de Cisco sur le déploiement du service d'accès sécurisé en périphérie \(SASE\)](#).



### Autrement dit :

Il existe plusieurs modèles de consommation de SASE dont l'incidence opérationnelle varie. Le bon modèle pour chaque organisation dépend d'un certain nombre de facteurs, notamment de la taille, des compétences et de la bande passante de l'équipe informatique interne et de la priorité accordée aux besoins spécialisés, à la vitesse, à l'agilité, à la visibilité et au contrôle.





## Conclusion sur les SASE

Les architectures, solutions et services SASE offrent une connectivité sécurisée entre tout utilisateur et toute application, quel que soit l'endroit où ils se trouvent ou sont hébergés. Mais le trajectoire vers le SASE est propre à chaque organisation. Le modèle et l'approche adéquats dépendront des investissements technologiques existants ainsi que des professionnels de l'informatique et des priorités opérationnelles.

Cisco et notre écosystème de partenaires peuvent vous aider à répondre à vos besoins uniques en matière de réseau et de sécurité avec la solution SASE la plus exhaustive, souple et résiliente du marché.

Vous pouvez choisir parmi notre vaste gamme de services SASE qui réunit la meilleure mise en réseau, la meilleure connectivité client, la meilleure sécurité et des capacités uniques en matière de surveillance de l'Internet pour obtenir les résultats dont vous avez besoin. Vous pouvez également choisir parmi une gamme de modèles de déploiement et de consommation SASE simples et flexibles qui répondent à une variété de situations et d'exigences.

Notre infrastructure de sécurité infonuagique hautement disponible au niveau mondial fournit un accès sécurisé quel que soit l'endroit où se trouvent les utilisateurs et les applications. Et nos solutions SD-WAN, à la pointe du marché, offrent l'agilité et les fonctionnalités nécessaires pour offrir à vos utilisateurs des expériences de qualité constante. Ensemble, nos solutions de sécurité en nuage et de réseau SD-WAN offrent les capacités de SASE les plus exhaustives et les plus intégrées de l'industrie.

Pour l'avenir, Cisco innove autour de SASE à un rythme accéléré par des intégrations continues et des améliorations continues des fonctionnalités. Nous faisons évoluer nos offres pour fournir les services SASE les plus souples et les plus facilement consommables en fonction de vos conditions.

Pour en savoir plus, visitez le [Centre de ressources SASE de Cisco](#).

Cisco est reconnue comme un Chef de file dans le Magic Quadrant™ de Gartner consacré à l'infrastructure de périphérie du réseau élargie pour sa capacité d'exécution et l'exhaustivité de sa vision<sup>13</sup>.



## Ressources et aide supplémentaire

[Lien vers la feuille de route SASE >](#)


[Trouver un partenaire Cisco >](#)

[Communiquer avec le service commercial de Cisco >](#)

Gartner n'approuve aucun fournisseur, produit ou service défini dans ses publications de recherche, et n'incite pas les utilisateurs de technologie à choisir uniquement les fournisseurs qui ont la meilleure cote ou une autre nomination. Les publications de recherche de Gartner présentent l'opinion du cabinet d'études et de conseil de Gartner et ne doivent pas être interprétées comme des constats. Gartner exclut toute garantie explicite ou implicite concernant cette recherche, y compris toute garantie de qualité marchande et d'adéquation à un usage particulier. GARTNER et MAGIC QUADRANT sont des marques de commerce et des marques de service de Gartner, Inc. et/ou de ses sociétés affiliées et sont utilisées ici avec autorisation. Tous droits réservés.

### Sources SASE

1. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, septembre 2021.
2. The State of Security 2021, Splunk, février 2021.
3. Future of Technology, Cisco, novembre 2021.
4. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, septembre 2021.
5. Gartner Quick Answer: Does SASE Replace SD-WAN?, Andrew Lerner, Neil MacDonald, décembre 2021.
6. 2022 Cisco Global Networking Trends Report: The Rise of Network as a Service, Cisco, octobre 2021.
7. Gartner 2021 Strategic Roadmap for SASE Convergence, mars 2021.
8. SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG Research Report, décembre 2021.
9. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, septembre 2021.
10. 2022 Cisco Global Networking Trends Report: The Rise of Network as a Service, Cisco, octobre 2021.
11. Future of Technology, Cisco, novembre 2021.
12. 2021 Strategic Roadmap for SASE Convergence, Gartner, mars 2021.
13. Gartner Magic Quadrant for WAN Edge Infrastructure, septembre 2021.



Rapport sur l'avènement  
du réseau sous forme de  
service (NaaS)





# Table des matières

Bienvenue .....	22
Principaux constats .....	23
Un modèle de mise en réseau différent .....	25
Gérer les enjeux et tirer profit des avantages .....	27
Comment le réseau sous forme de service modifie l'exploitation du réseau .....	29
Rôles, responsabilités et compétences .....	31
Inquiétudes et hésitations .....	33
Tendances d'adoption .....	35
Choix d'un prestataire de réseau sous forme de service .....	36
Le service d'accès sécurisé en périphérie et les différentes sortes de réseau sous forme de service .....	38
Conclusion .....	40
Ressources et aide supplémentaires .....	40
À propos de ce rapport .....	41
Autorisations pour l'utilisation de ce rapport .....	42



# Bienvenue

## Bienvenue dans le Rapport sur les tendances mondiales de mise en réseau pour 2022 : *L'avènement du réseau sous forme de service (NaaS).*

Quelle époque remarquable nous vivons, à la fois en tant que personnes et que professionnels des réseaux. Au cours de la dernière année, on a demandé aux responsables des TI et aux professionnels des réseaux de prendre en charge les télétravailleurs, de protéger les données dans un environnement de TI plus distribué et d'offrir de nouveaux services aux utilisateurs, aux clients et aux partenaires. Beaucoup d'entreprises ont accéléré leurs efforts de transformation numérique pour répondre à ces nouvelles exigences et tiré parti de l'infonuagique et du logiciel sous forme de service pour accroître leur souplesse, leur agilité et leur rapidité.

Dans notre [Rapport sur les tendances mondiales de mise en réseau pour 2021](#), nous avons expliqué comment les technologies de réseau sont utilisées pour accroître la résilience des affaires, quelles que soient les circonstances.

Cette année, nous abordons une tendance émergente qui aura de grandes répercussions sur l'avenir : le réseau sous forme de service.

Dans la foulée des modèles sous forme de service dont la popularité ne cesse de croître, comme le logiciel sous forme de service (SaaS) et l'infrastructure sous forme de service (IaaS), le réseau sous forme de service changera inévitablement la façon pour les entreprises d'acquiescer, d'offrir et de gérer leurs capacités de réseau. Pour en savoir plus, nous nous sommes entretenus avec 20 responsables des TI et nous avons effectué un sondage auprès de 1 534 professionnels des TI de 13 pays pour connaître leur point de vue sur le réseau sous forme de service, ses forces et ses limites ainsi que pour savoir s'ils prévoient adopter le nouveau modèle de consommation de réseau.

Nous espérons que les données, les points de vue et les conseils contenus dans ce rapport vous aideront à mieux comprendre les avantages et les implications du réseau sous forme de service afin d'améliorer vos stratégies de mise en réseau.

– James Mobley, vice-président directeur, Services de réseau de Cisco



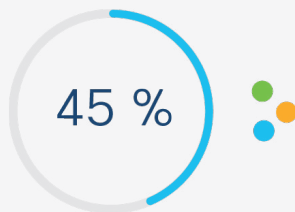


# Principaux constats

Le projet de transformer complètement votre façon de consommer et d'exploiter votre réseau n'est pas une mince affaire. Vous devez avoir de bonnes raisons professionnelles et technologiques d'effectuer cette transition vers un modèle sous forme de service. Vous avez également besoin de partenaires de confiance sur lesquels vous pouvez vous fier pour que vos activités se poursuivent sans heurts. Et pourtant, bon nombre d'entreprises sont très motivées à faire le saut. Voici certains des principaux constats de notre recherche sur les réseaux sous forme de service pour 2022 :

## Principal constat 1 : Enjeux

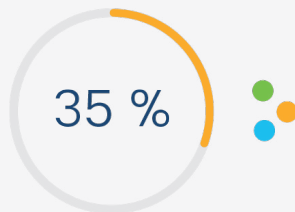
Lorsqu'il est question de résilience et d'agilité, le réseau sous forme de service est souvent la réponse.



- Les réactions en cas de perturbations (45 %) et la prise en charge des nouveaux besoins d'affaires (40 %) étaient les principaux enjeux des réseaux mentionnés en 2021.
- Parallèlement, les équipes de TI reconnaissent que le principal avantage du réseau sous forme de service est qu'il libère les équipes de TI, qui ont ainsi plus de temps à consacrer à l'innovation et à la création de valeur commerciale (46 %). De plus, 40 % des répondants conviennent que le réseau sous forme de service améliore les réactions en cas de perturbations, et 34 % indiquent qu'il augmente l'agilité du réseau.

## Principal constat 2 : Avantages

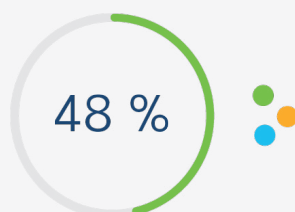
Grandes attentes : un accès rapide aux dernières technologies est le grand prix.



- Les technologies continuent d'évoluer plus vite que les entreprises n'arrivent à les adopter. Dans notre sondage, 35 % des répondants reconnaissent que le besoin de continuellement déployer les dernières technologies de mise en réseau comme le Wi-Fi 6, le réseau WAN défini par logiciel (SD-WAN), le service d'accès sécurisé en périphérie (SASE), la 5G, intelligence artificielle, etc., est leur principale motivation pour adopter le réseau sous forme de service.

## Principal constat 3 : Opérations

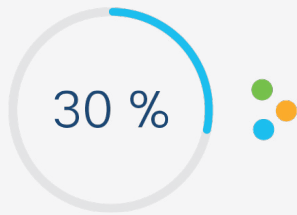
Le réseau sous forme de service est fantastique, mais seulement s'il aide l'équipe responsable de la mise en réseau à respecter les contrats de niveau de service.



- Les principales tâches qu'on demande aux prestataires de réseaux sous forme de service d'effectuer sont la gestion du cycle de vie des réseaux (48 %), la résilience des réseaux (42 %) ainsi que la surveillance et le dépannage pour respecter les contrats de niveau de service (38 %).

## Principal constat 4 : Inquiétudes

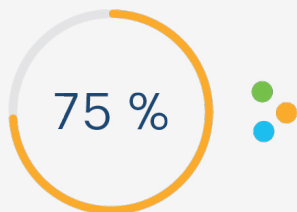
Mais tout ne se passe pas toujours sans heurts. Certaines inquiétudes se posent quant aux coûts et à l'abandon d'un certain niveau de contrôle.



- On se demande notamment si le réseau sous forme de service peut prendre en charge les nouvelles exigences imprévues (30 %) et si son adoption nécessite de sacrifier le contrôle de la sécurité (26 %).
- Le coût et les perturbations occasionnés par la transition sont également des inquiétudes souvent mentionnées (28 %).

## Principal constat 5 : Rôles

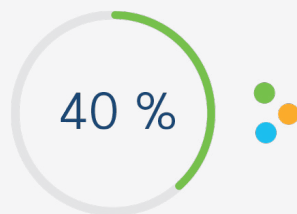
Le réseau sous forme de service ouvre de nouveaux horizons aux professionnels des TI, mais ceux-ci devront améliorer leurs façons de faire.



- Plus de 75 % des entreprises sont d'accord ou fortement d'accord pour dire que le réseau sous forme de service offrira aux équipes de TI des possibilités d'améliorer leurs compétences.
- Aujourd'hui cependant, seulement 1 entreprise sur 4 est susceptible de faire davantage confiance à son équipe de TI qu'à un intégrateur de système, à un prestataire de services gérés ou à un prestataire de réseau sous forme de service pour transposer ses besoins dans des politiques techniques.

## Principal constat 6 : Adoption

Il existe plusieurs façons de mettre en route le réseau sous forme de service. L'une d'entre elles est le service d'accès sécurisé en périphérie (SASE).



- Le SASE est une option de point d'entrée vers le réseau sous forme de service, puisque les entreprises ont cité l'accès multinuage (40 %) et la sécurité (34 %) comme étant des éléments qui se prêteraient bien à ce type de réseau.
- Au total, 49 % des entreprises prévoient mettre en route le réseau sous forme de service lors d'un cycle d'actualisation ou de mise à jour, et 34 % des répondants ont affirmé qu'ils commenceraient par adapter un site existant.

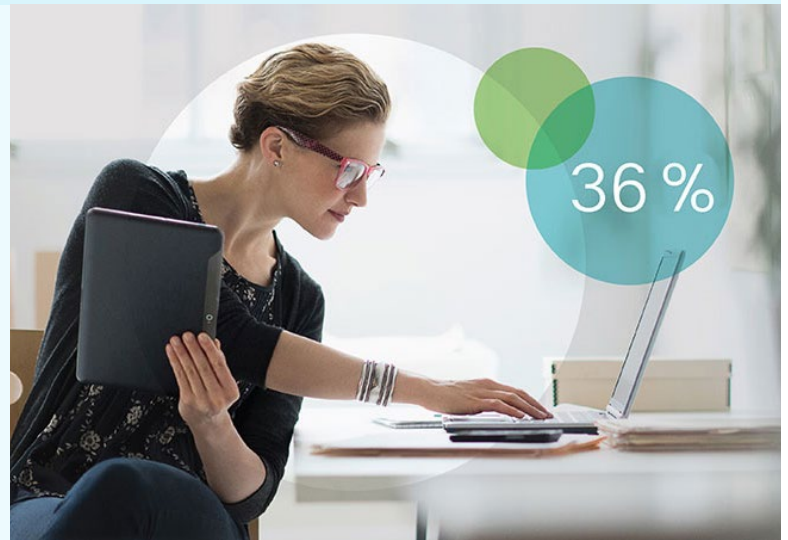
## Un modèle de mise en réseau différent

Après plus de 18 mois de perturbations et d'adaptation, le rôle des technologies de réseau dans la survie et la réussite des entreprises n'a jamais été aussi clair, ou essentiel. On demande maintenant aux réseaux, qui étaient déjà un facteur clé dans le télétravail, de prendre en charge des milieux de travail plus sûrs, des modèles de travail hybrides et des tâches opérationnelles en constante évolution. Pour ce faire, ils doivent fonctionner

de façon harmonieuse dans les environnements de périphérie, multinuages et sur site. Ils doivent offrir une expérience sûre et cohérente à tous les utilisateurs, quel que soit leur emplacement, leur périphérique ou leur méthode de connectivité. Et ils doivent prendre en charge les applications traditionnelles et modernes orientées vers les microservices.

Puisque les ressources et la bande passante sont souvent limitées, bon nombre de responsables des TI et des réseaux envisagent d'utiliser le réseau sous forme de service comme solution pour gérer ces enjeux. Mais en quoi consiste le réseau sous forme de service exactement?

Lorsque nous avons demandé aux responsables des TI de nous donner une définition, nous avons rapidement constaté que ce terme peut désigner plusieurs choses. En fait, nous avons été surpris d'apprendre que 36 % des répondants à notre sondage affirment déjà posséder un réseau sous forme de service. Bien que ce chiffre puisse sembler élevé pour une nouvelle technologie, nous avons compris pendant nos entretiens que beaucoup de gens considèrent avoir un réseau sous forme de service si une partie de leur réseau est gérée par un prestataire tiers. Nous croyons que cette définition est beaucoup trop large et doit être précisée.



**Le réseau sous forme de service est un modèle de consommation fondé sur l'utilisation et adapté au nuage qui permet aux utilisateurs d'acquérir ou de gérer des capacités de réseau sans avoir à détenir, à construire ou à maintenir leur propre infrastructure.**

« Les entreprises tentent de trouver l'équilibre parfait entre les ressources internes et celles fournies par des partenaires. Bon nombre d'entre elles choisissent d'investir dans leurs employés, les analyses, l'observabilité et l'automatisation et réfléchissent sérieusement aux façons de tirer parti des prestataires stratégiques pour déléguer la gestion et la maintenance de l'infrastructure. »

– Mary Turner, vice-présidente, Recherche, IDC

Le réseau sous forme de service peut représenter un modèle de consommation différent pour une variété d'éléments de réseau comme les LAN avec et sans fil, les WAN, les VPN ainsi que les environnements infonuagiques, hybrides, multilingues, de périphérie, de centre de données et de succursale. Il peut servir à créer de nouveaux modèles de réseau comme le service d'accès sécurisé en périphérie. Il peut permettre de changer les modèles organisationnels, par exemple de passer à un milieu de travail hybride. Et en tant que service à la demande, le réseau sous forme de service peut permettre aux équipes de TI de procéder à une mise à l'échelle ou à une réduction plus faciles, de déployer rapidement de nouveaux services et d'optimiser l'équilibre entre les dépenses d'immobilisation et les dépenses d'exploitation.

Pour certains responsables des TI avec lesquels nous nous sommes entretenus, le réseau sous forme de service représente une forme de mise en réseau nouvelle et améliorée dont ils ont grandement besoin.

Ils reconnaissent qu'ils prennent du retard et perdent la confiance de leurs utilisateurs. Et ils croient que le réseau sous forme de service peut les aider à obtenir les dernières technologies, à répondre à des exigences de plus en plus nombreuses et à suivre le rythme toujours plus rapide des affaires.



« Étant donné le niveau de complexité de la mise en réseau, la vitesse à laquelle les entreprises doivent réagir aux changements du marché et la grande portée des réseaux modernes, beaucoup de gens se rendent compte qu'ils n'y arrivent plus et qu'ils ont besoin d'aide. »

– Mark Leary, directeur de la recherche, Analyses de réseau, IDC

### Autrement dit :

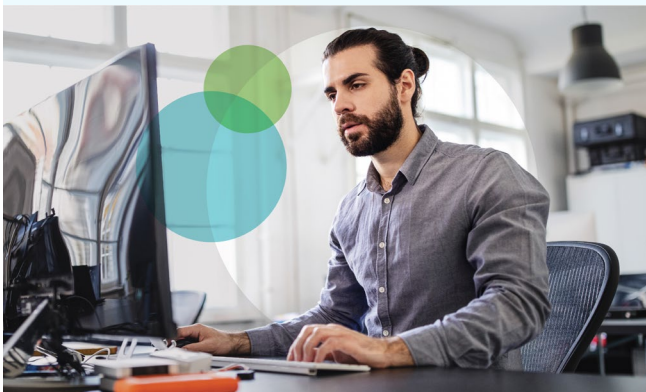
De 2021 à 2027, on s'attend à ce que le taux de croissance annuel composé de l'adoption du réseau sous forme de service soit de 40,7 %<sup>1</sup>.

# Gérer les enjeux et tirer profit des avantages

Le choix d'adopter ou non un réseau sous forme de service dépend en fin de compte des enjeux commerciaux et technologiques qu'il doit gérer ainsi que des avantages qu'il offre.

La priorité des entreprises que nous avons sondées demeurait l'agilité. Lorsque nous leur avons demandé quels étaient les plus gros enjeux commerciaux de leur réseau, près de 50 % des professionnels des TI ont indiqué les réactions aux perturbations, et 40 % ont mentionné la prise en charge de nouvelles applications commerciales et des nouveaux projets de l'entreprise. Plus du tiers des répondants ont nommé le besoin d'agilité du réseau comme une des principales raisons d'adopter le réseau sous forme de service, et la moitié d'entre eux ont souligné qu'ils croyaient que le réseau sous forme de service leur permettrait d'accroître leur innovation et leur valeur commerciale.

Dans le cadre de leurs efforts pour augmenter leur agilité, beaucoup d'équipes de TI transfèrent leurs applications et leurs services sur le nuage, ce qui peut créer des enjeux de sécurité, de gouvernance et de conformité.

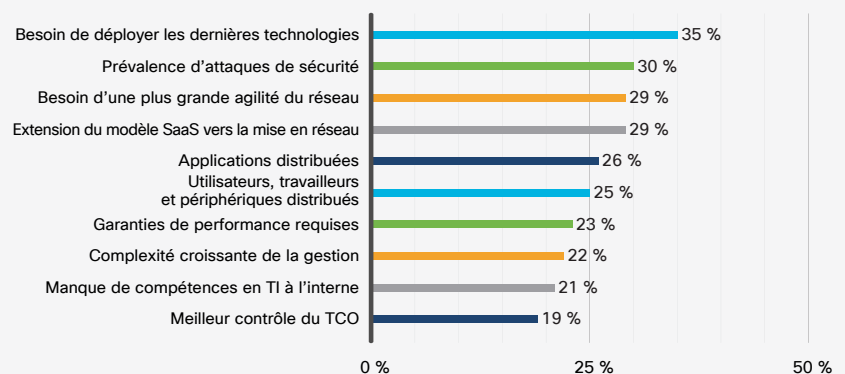


Selon les professionnels des TI que nous avons interrogés, les plus gros enjeux technologiques actuels dans la gestion des réseaux sont la connexion au multinuage (36 %), la sécurisation des réseaux, des utilisateurs et des applications (34 %) ainsi que la définition des causes premières des problèmes de sécurité ou de performance et leur résolution rapide (31 %).

Parallèlement, le tiers des répondants a indiqué que le besoin de constamment déployer les dernières technologies de mise en réseau (p. ex., Wi-Fi 6, SD-WAN, SASE, 5G et intelligence artificielle) était l'une des principales motivations pour passer au réseau sous forme de service, tandis qu'un autre tiers a mentionné la capacité à se défendre contre les menaces de sécurité, de plus en plus fréquentes et complexes.



Quelles seraient les raisons les plus susceptibles de convaincre votre entreprise de passer au réseau sous forme de service?







« Pour nos dirigeants, le fait que mon personnel configure les périphériques ou exploite l'infrastructure ne crée aucune valeur. Ils veulent que l'équipe des TI se penche sur les objectifs commerciaux. En ayant recours à des services externes pour les activités de base, je permets à mon personnel de s'occuper davantage des résultats commerciaux. »

– Directeur de l'infrastructure de TI, société internationale de biens de consommation

Lorsque nous avons demandé aux décideurs les principaux avantages que les professionnels des TI attendaient du réseau sous forme de service, ils ont mentionné la capacité de se concentrer sur la création de valeur commerciale plutôt que sur la gestion de l'infrastructure au quotidien.

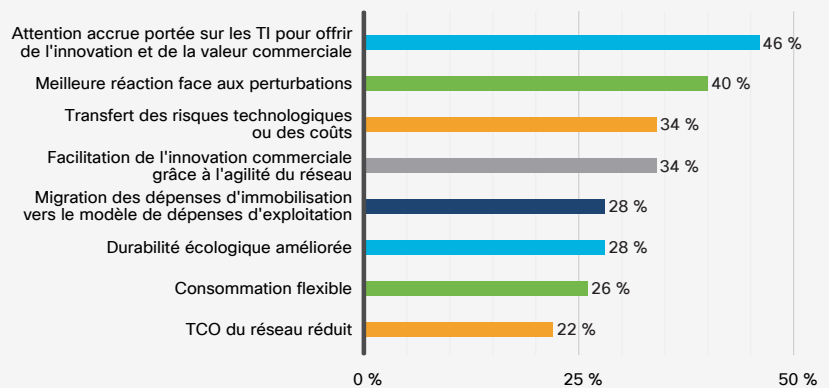
L'amélioration des réactions aux perturbations du réseau et de la sécurité est un autre avantage régulièrement mentionné du réseau sous forme de service (par 45 % des professionnels des réseaux et 40 % des principaux décideurs). Bien que nous n'ayons pas été surpris d'apprendre que l'amélioration de la sécurité était une priorité, nous avons trouvé intéressant de savoir que plus de 25 % des professionnels des réseaux et 33 % des principaux décideurs croient que l'amélioration de la durabilité écologique est un des grands avantages du réseau sous forme de service.

## Ce qui nous a encore plus surpris a été la faible importance accordée aux avantages financiers de cette solution.

Avec un modèle de consommation flexible et une tarification par abonnement, le réseau sous forme de service permet aux équipes de TI d'effectuer moins de dépenses d'immobilisation et plus de dépenses d'exploitation et d'éviter les investissements importants et récurrents dans l'infrastructure réseau. Ainsi, les dépenses deviennent plus constantes et prévisibles et les entreprises paient uniquement pour les ressources qu'elles utilisent. Et pourtant, ces avantages financiers ont été jugés beaucoup moins importants par les responsables des TI et les professionnels des réseaux que les avantages en matière d'agilité, d'innovation et d'allègement de la gestion offerts par le réseau sous forme de service.



Selon vous, quels sont les trois principaux avantages pour les entreprises d'utiliser un réseau sous forme de service ?



### Autrement dit :

En matière de réseau sous forme de service, le coût total de possession vient au bas de la liste des priorités parce que les entreprises s'intéressent beaucoup plus à la création de valeur commerciale et aux réactions rapides aux perturbations. Soixante-six pour cent des responsables des TI sont d'accord ou fortement d'accord pour dire que le réseau sous forme de service allégera la gestion du réseau au quotidien pour leurs équipes, ce qui donnera plus de temps à ces dernières pour se concentrer sur l'innovation et la valeur commerciale.

# Comment le réseau sous forme de service modifie l'exploitation du réseau (NetOps)

Une préoccupation courante à propos du réseau sous forme de service est qu'il nécessite un transfert de toutes les tâches d'exploitation du réseau : l'ensemble des responsabilités incombe ainsi au prestataire du réseau sous forme de service et l'équipe responsable des opérations de réseau de l'entreprise se retrouve sans tâches. En fait, ce n'est pas tout ou rien en matière de responsabilités opérationnelles.

Avec un réseau sous forme de service, le prestataire est responsable de tous les aspects de la gestion du cycle de vie du

réseau, notamment le déploiement, l'intégration, le contrôle, les mises à jour, la surveillance et la réparation de tous les éléments de l'infrastructure réseau (et de l'équipement sur site du client, le cas échéant) requis pour livrer les résultats prévus au contrat. Il peut notamment s'agir du nombre d'utilisateurs connectés, de sites, de prestataires de services infonuagiques et d'applications ainsi que des niveaux de service convenus, de la bande passante, de la performance des applications, des dispositions de sécurité, de la conformité et de toute autre exigence.

Alors que reste-t-il à gérer? L'équipe responsable des opérations de réseau du client pourra se consacrer davantage aux activités essentielles ou à valeur ajoutée,

comme définir et surveiller les résultats attendus du réseau, par exemple les politiques d'accès des utilisateurs et des applications et les niveaux de performance des applications. En surveillant les renseignements sur le réseau et sa performance, l'équipe responsable des opérations de réseau du client peut adapter et optimiser continuellement les politiques de réseau et les comportements connexes dans tous les domaines.

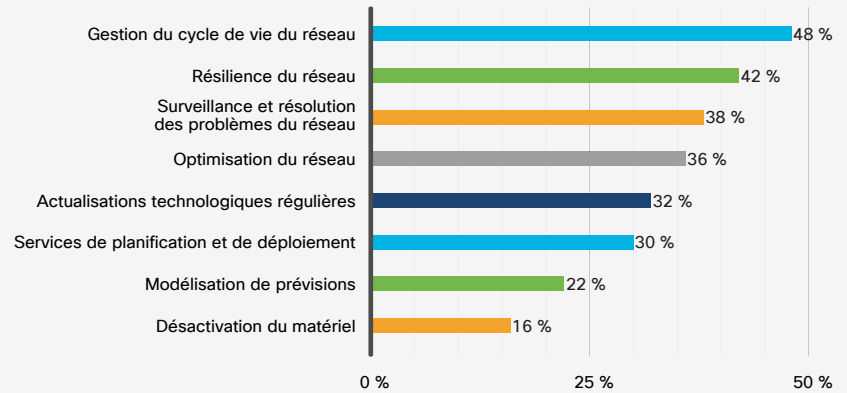


À l'aide d'API, l'équipe responsable des opérations de réseau du client peut également gérer les intégrations du réseau sous forme de service et des systèmes existants afin d'harmoniser les flux de travail et les processus de TI. Et elle voudra probablement travailler en étroite collaboration avec le prestataire de réseau sous forme de service pour respecter les contrats et les objectifs de niveaux de service. Quelles que soient les responsabilités opérationnelles et les tâches transférées, les professionnels des TI souhaitent manifestement réduire le fardeau de la gestion de l'infrastructure.

Au total, 48 % des professionnels des TI interrogés ont indiqué que la gestion du cycle de vie du réseau était le service le plus important à inclure dans un modèle de réseau sous forme de service. La résilience du réseau (42 %) et la surveillance et le dépannage du réseau (38 %) complètent le palmarès des trois services les plus importants. Ces résultats confirment que la gestion d'une combinaison de plus en plus distribuée et complexe d'emplacements, d'utilisateurs, de périphériques, d'applications et de ressources infonuagiques laisse trop peu de temps pour gérer l'innovation et les activités à valeur ajoutée.



Selon vous, parmi les services suivants, lequel serait-il le plus important d'inclure dans un modèle de réseau sous forme de service?



« Le prestataire gère les détails au quotidien. L'équipe interne peut alors se concentrer sur l'ajout de valeur au réseau en gérant les nouvelles exigences qui se présentent. Nos ingénieurs et nos techniciens n'ont pas besoin d'interrompre leurs activités pour gérer des problèmes. Ils peuvent se concentrer sur de nouveaux projets. »

– Ingénieur réseau principal, société internationale d'experts-conseils



### Autrement dit :

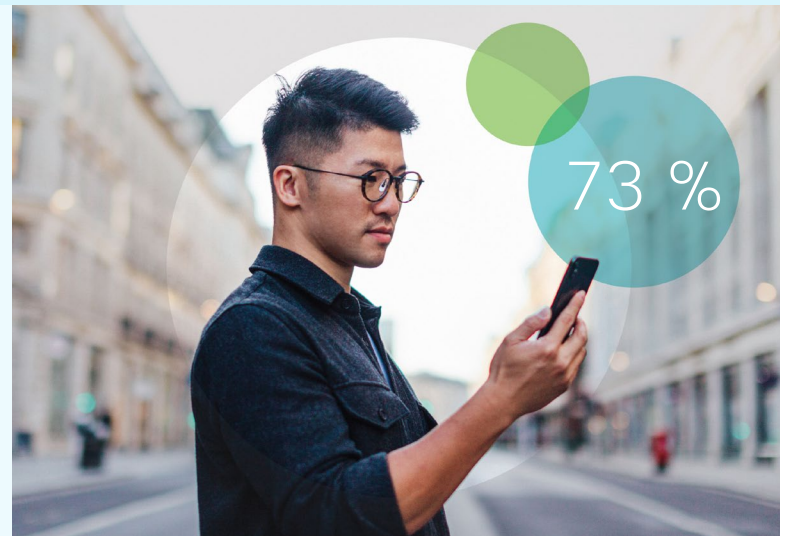
Avec un réseau sous forme de service, les responsabilités opérationnelles sont partagées. Le fardeau de la gestion du cycle de vie du réseau est transféré au prestataire pour que l'équipe de TI du client puisse se concentrer davantage sur les activités opérationnelles qui créent de la valeur commerciale.

## Rôles, responsabilités et compétences

En transférant les responsabilités d'entretien de l'infrastructure et de gestion du cycle de vie au prestataire, le réseau sous forme de service libère beaucoup de temps, ce qui permet à l'équipe responsable des opérations de réseau du client de se concentrer sur les résultats attendus du réseau plutôt que sur les aspects opérationnels et technologiques liés à l'entretien de l'infrastructure.

Autrement dit, au lieu de « piloter l'avion », les ingénieurs réseau « gèrent les activités depuis la tour de contrôle ». Mais de quels types d'activités parle-t-on ici ?

Au total, 27 % de nos répondants croient que leur personnel de TI utiliserait son savoir-faire technique (et le tableau de bord du réseau sous forme de service) pour traduire les besoins commerciaux en politiques de réseau. À notre surprise, 73 % des répondants ont affirmé qu'ils préféreraient que des prestataires tiers jouent ce rôle essentiel à la mission, ce qui dénote peut-être une absence de compétences à l'interne ou un manque de confiance envers ces compétences.

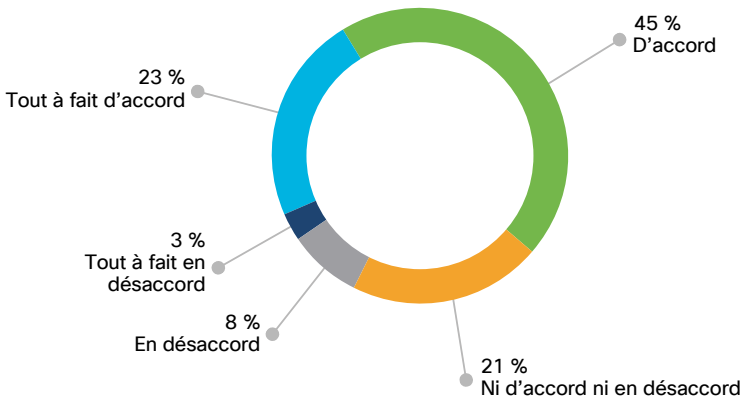
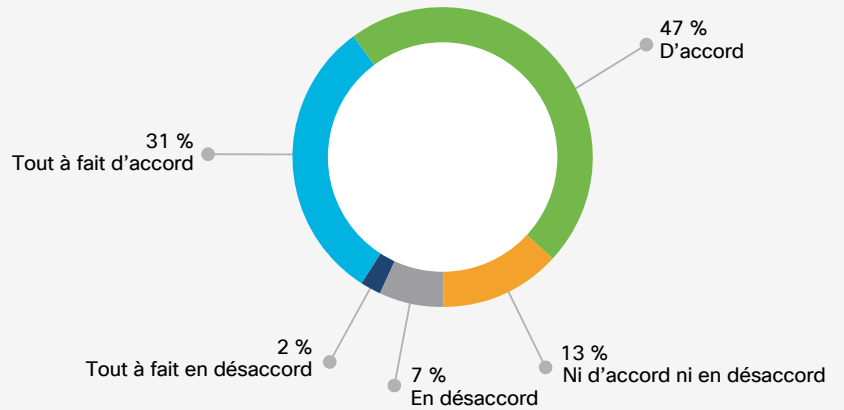


« Puisque la majeure partie des tâches quotidiennes serait transférée au prestataire de réseau sous forme de service, l'équipe responsable des opérations de réseau du client s'occuperait vraisemblablement davantage des compétences de mise en réseau et de sécurité générales ainsi que de compétences en conception qui transposent les intentions commerciales dans ces concepts généraux de mise en réseau. L'équipe devra travailler en étroite collaboration avec le prestataire de réseau sous forme de service pour optimiser la conception, les politiques et la performance des réseaux ainsi que les contrats de niveaux de service. De plus, de solides compétences en sciences des données seront nécessaires pour définir et gérer ces changements. »

– Joe Clarke, expert éminent en ingénierie de Cisco



L'adoption d'un réseau sous forme de service offrirait aux membres de l'équipe responsable de notre réseau des occasions d'améliorer leurs compétences et de créer plus de valeur pour l'entreprise.



Le réseau sous forme de service libérera mon équipe de mise en réseau, qui pourra se concentrer sur les tâches qui génèrent des innovations en TI et de la valeur commerciale plutôt que sur la gestion du réseau au quotidien.



### Autrement dit :

Plus de 75 % des entreprises sont d'accord ou fortement d'accord pour dire que le réseau sous forme de service offrira à leurs équipes la possibilité d'améliorer leurs compétences et de créer plus de valeur.



## Inquiétudes et hésitations

Le réseau sous forme de service a des répercussions sur plusieurs secteurs pour une équipe de TI. Il nécessite de nouveaux modèles d'exploitation, de nouvelles intégrations avec des technologies et des processus existants, un changement des rôles et des compétences et, du point de vue financier, un passage des dépenses d'immobilisation aux dépenses d'exploitation. Avec ces différentes conséquences en tête, les professionnels des TI auxquels nous avons parlé ont réagi différemment au réseau sous forme de service. La plupart d'entre eux se situaient aux extrémités du spectre : ils étaient soit très chauds, soit très frileux à l'idée d'adopter le réseau sous forme de service.

Les points de vue des responsables des TI sur le réseau sous forme de service semblaient refléter leur philosophie de mise en réseau globale. Ces philosophies peuvent principalement être regroupées en deux camps : « contrôle des TI » et « TI allégées ». Ceux qui adhèrent à la première philosophie disposent d'une main-d'œuvre hautement qualifiée et croient fermement que leurs équipes devraient détenir et gérer entièrement la pile réseau. À l'opposé, le deuxième groupe cherche à consolider ses TI, à réévaluer les tâches de routine et à valeur ajoutée et à trouver des façons de déléguer la maintenance de l'infrastructure. Sans surprise, les entreprises ayant une philosophie de « TI allégées » ont déjà transféré certaines de leurs ressources informatiques dans le nuage et sont très ouvertes aux solutions de réseau sous forme de service.

« Nous tirons de la patte en matière de réseau sous forme de service parce que nous croyons que le réseau ne serait pas traité avec les égards et l'importance qu'il mérite et que ce ne serait pas la solution parfaite pour notre environnement. »

– Gestionnaire des TI, mise en réseau, agence militaire américaine

Certains responsables des TI à qui nous avons parlé ont indiqué que leurs réseaux et leurs processus étaient tout à fait uniques et qu'ils ne croyaient pas que le réseau sous forme de service pouvait gérer leurs complexités et leurs enjeux hors du commun.

D'autres ont réellement peur que le réseau sous forme de service bouleverse leur équipe de TI.

Si les responsables des TI partagent bon nombre de préoccupations, la plus importante est la perte de contrôle perçue. Trente pour cent des répondants se demandent s'ils pourront répondre à la demande future s'ils adoptent le réseau sous forme de service. D'autres répondants s'inquiètent des effets de la perte de contrôle sur la sécurité (26 %) et les performances (20 %). Dans les faits, le réseau sous forme de service est conçu pour offrir une plus grande évolutivité sur demande et une prise en charge plus rapide des dernières technologies. De plus, c'est l'équipe des TI, et non le prestataire, qui demeure responsable des décisions relatives à la sécurité et à la performance et des autres décisions de contrôle importantes.

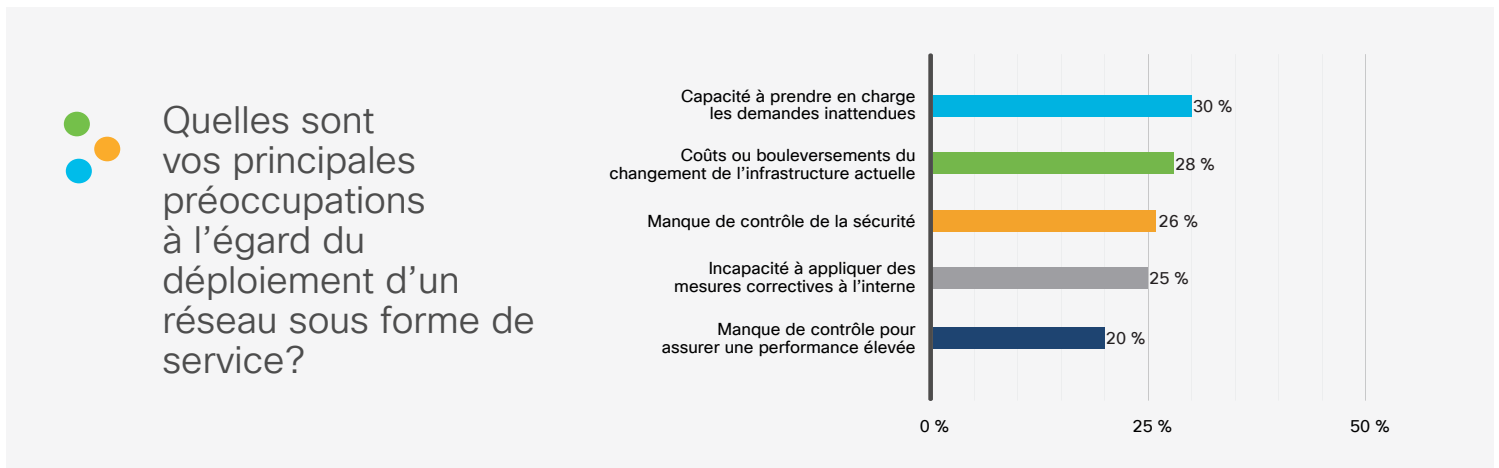




« Le prestataire doit s'adapter à nos directives de sécurité et suivre nos instructions. C'est un des principaux éléments qui distingue le réseau sous forme de service. »

– Architecte principal, entreprise internationale spécialisée en technologies

Vingt-huit pour cent des répondants ont indiqué que les perturbations et les coûts associés au changement de leur infrastructure et de leurs opérations existantes étaient des freins. On le comprend aisément, puisque les entreprises ont plusieurs technologies et investissements qui n'ont pas tous le même calendrier de dépréciation. D'autres entreprises utilisent des technologies et des applications existantes qui pourraient ne pas être compatibles avec le réseau sous forme de service. Et d'autres encore ne veulent tout simplement pas déléguer la gestion de leur infrastructure au quotidien.



Pour apaiser certaines de ces inquiétudes et hésitations, les entreprises peuvent commencer simplement par un seul domaine pour mettre à l'essai le réseau sous forme de service. Cette stratégie leur permet de mieux comprendre les capacités et les points de contrôle du réseau sous forme de service sans trop modifier leurs opérations ou leur infrastructure de réseau. Elles peuvent tester et optimiser la division des responsabilités entre le prestataire et leur équipe interne et apprendre comment collaborer pour atteindre les meilleurs résultats. Lorsqu'elles sont à l'aise avec les rôles, les responsabilités et les points de contrôle et qu'elles les comprennent bien, elles peuvent élargir la portée à d'autres domaines au fil du temps en mettant à profit les connaissances et les pratiques exemplaires acquises en cours de route.

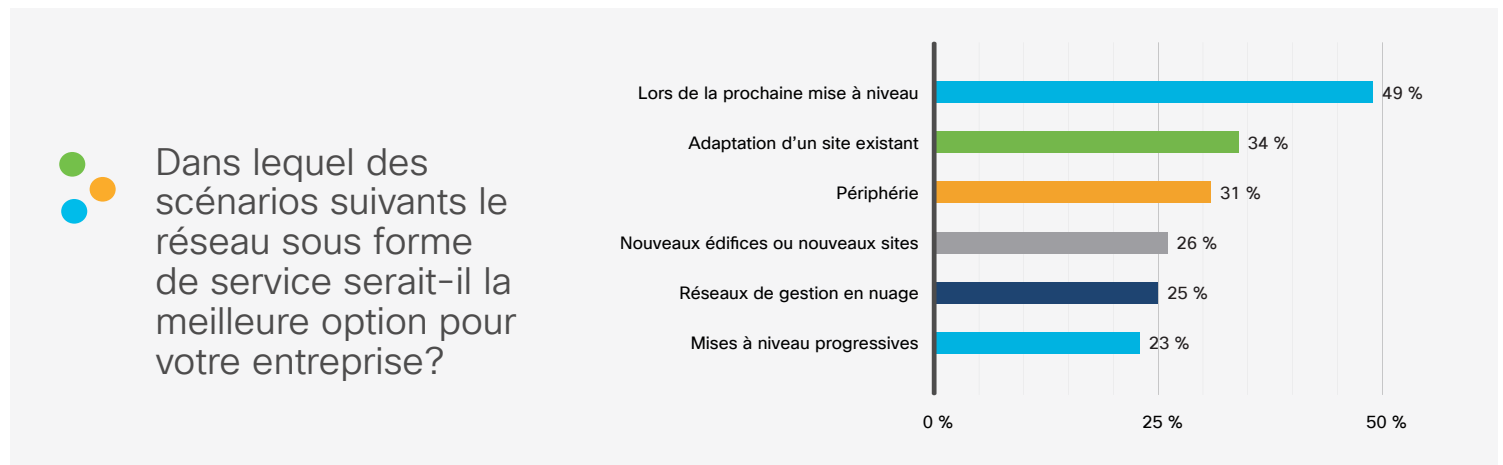


**Autrement dit :**  
Des inquiétudes sont à prévoir avec tout modèle transformationnel. Les responsables des TI peuvent commencer simplement pour évaluer les risques et les avantages associés au réseau sous forme de service afin de déterminer si cette solution convient à leur entreprise.

# Tendances d'adoption

En raison de ses répercussions sur l'exploitation du réseau et des différentes façons de l'utiliser, l'adoption du réseau sous forme de service différera pour chaque entreprise. Une évaluation de l'état de préparation et une feuille de route du déploiement peuvent réduire au minimum les complications et maximiser les réussites.

Selon notre sondage, 49 % des responsables des TI et 57 % des professionnels des réseaux croient que le meilleur moment pour adopter un réseau sous forme de service est lors d'une actualisation ou d'une mise à niveau de l'infrastructure réseau, lorsqu'ils cherchent à accéder à de nouvelles technologies (automatisation, Ethernet 100 gigabits, Wi-Fi 6, 5G, SD-WAN, SASE, etc.). Trente-quatre pour cent des répondants ont indiqué que l'adaptation d'un site existant où des technologies de mise en réseau sont déjà déployées était le meilleur scénario pour l'adoption du réseau sous forme de service. À noter que seulement 26 % des répondants ont indiqué que de nouvelles installations seraient la meilleure option pour adopter un réseau sous forme de service. Et à peine 23 % ont mentionné qu'une approche progressive, dans le cadre de laquelle les domaines seraient mis à niveau un par un, serait le meilleur scénario d'adoption du réseau sous forme de service pour leur entreprise.



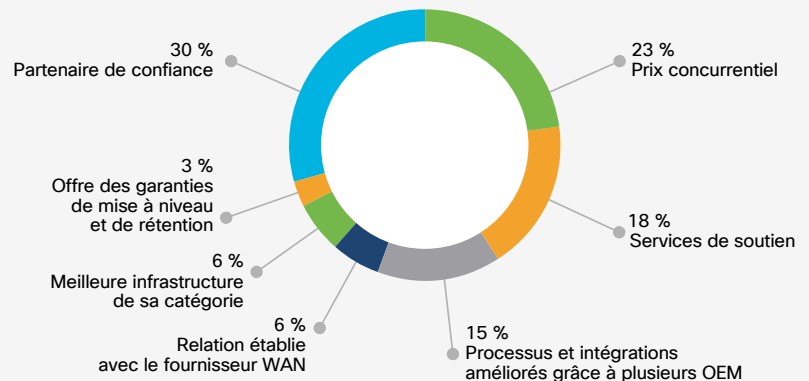
Autrement dit :  
Le moment, la façon et la raison de déployer le réseau sous forme de service seront différents pour chaque entreprise.

## Choix d'un prestataire de réseau sous forme de service

Comme le réseau est un des facteurs essentiels pour favoriser la productivité des employés, les échanges avec les clients et les tâches opérationnelles, le choix du bon prestataire de réseau sous forme de service n'est pas à prendre à la légère. Certains des responsables des TI auxquels nous avons parlé ont réellement peur de perdre le contrôle. Mais ils sont prêts à céder une partie de ce contrôle si, et seulement si, c'est à un partenaire de confiance. Que cela signifie de collaborer avec un intégrateur de système, un prestataire de services gérés ou un revendeur à valeur ajoutée, ces personnes sont plus à l'aise de travailler avec des partenaires établis qui comprennent déjà bien leur environnement réseau, leurs objectifs commerciaux et leurs besoins en matière de soutien.

Pour les déploiements de réseau sous forme de service, près du tiers des professionnels des TI sondés croient que les intégrateurs de systèmes sont plus fiables et offrent des prix plus concurrentiels que les prestataires de réseau. Ils nous ont également indiqué qu'un « savoir-faire fiable » était beaucoup plus important que la « meilleure infrastructure de sa catégorie ».

Quelle est la principale raison pour laquelle vous préféreriez travailler avec un partenaire plutôt que directement avec un prestataire de réseau pour le déploiement de votre réseau sous forme de service?

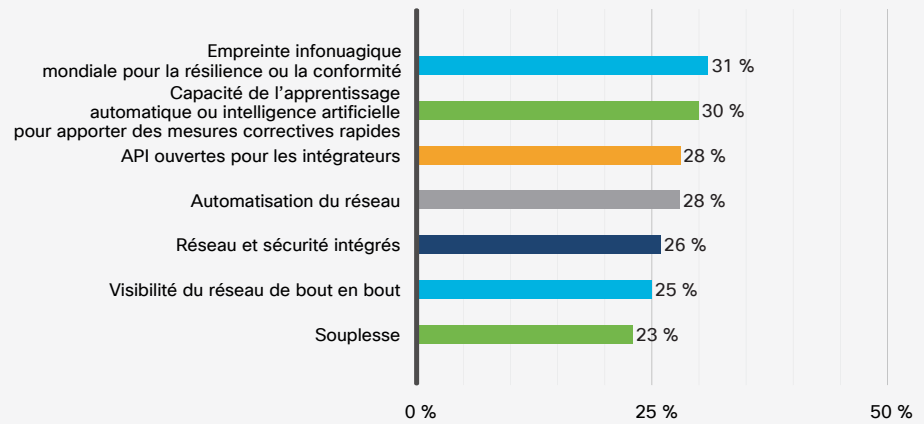


Et au moment de traduire les besoins commerciaux en politiques techniques, les professionnels des TI sont deux à trois fois plus susceptibles de faire confiance à un intégrateur de système ou à leur personnel de TI à l'interne qu'à un prestataire de réseau sous forme de service. Cette statistique prouve qu'en matière de réseau sous forme de service, les entreprises cherchent non seulement une solution, mais aussi l'aide et les conseils d'un conseiller de confiance qui les connaît bien.

À la question sur les attributs techniques des solutions et des prestataires de réseau sous forme de service, nos répondants ont préféré une présence internationale des services en nuage pour une meilleure fiabilité, performance et conformité régionale (31 %) ainsi que des capacités d'apprentissage automatique et d'intelligence artificielle qui permettent d'optimiser de façon continue le réseau sous forme de service (30 %). Les API, l'automatisation, la sécurité intégrée, la visibilité sur le réseau et la souplesse du réseau sont également souvent ressortis.



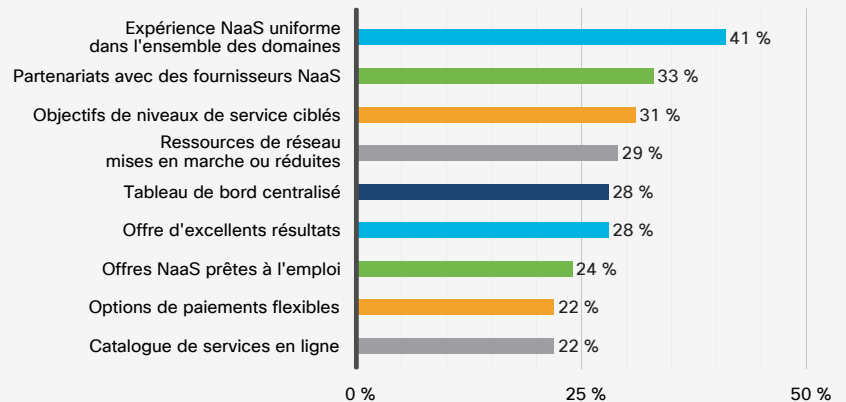
À votre avis, quels sont les deux attributs techniques les plus importants d'un réseau sous forme de service ?



Quarante et un pour cent des répondants affirment qu'il est important pour les prestataires de réseau sous forme de service d'offrir une plateforme cohérente dans tous les domaines de réseau (accès, WAN, centre de données, nuage, etc.). Bon nombre d'équipes de TI ont de la difficulté à gérer plusieurs environnements, trousse d'outils et modèles d'exploitation. Le réseau sous forme de service leur donne l'occasion de regrouper les opérations, les politiques et les ressources des réseaux.



Lequel des éléments suivants serait le plus important si vous deviez étudier l'offre d'un prestataire de réseau sous forme de service ?



« Ce que je recherche, c'est quelqu'un qui peut gérer les activités de gestion de routine dans l'ensemble de notre réseau et de nos systèmes, comme les modifications, les configurations et les mises à niveau des micrologiciels. Ainsi, mon équipe peut se concentrer sur les améliorations, la création et la mise en œuvre de stratégies. Et ça peut varier. Peut-être que ce mois-ci je prendrai en charge le gros du travail, puis je demanderai de l'aide pendant deux mois pour effectuer certaines tâches et élargir cette utilisation. »

– Vice-président des technologies et de la sécurité, organisme sans but lucratif américain de 100 M\$



Autrement dit :

Les intégrateurs de systèmes sont perçus comme des partenaires plus fiables, plus orientés vers le service et aux tarifs plus concurrentiels que les prestataires de réseau sous forme de service. Quel que soit le prestataire, les clients veulent un service et une expérience opérationnelle dans tous les domaines de réseau.

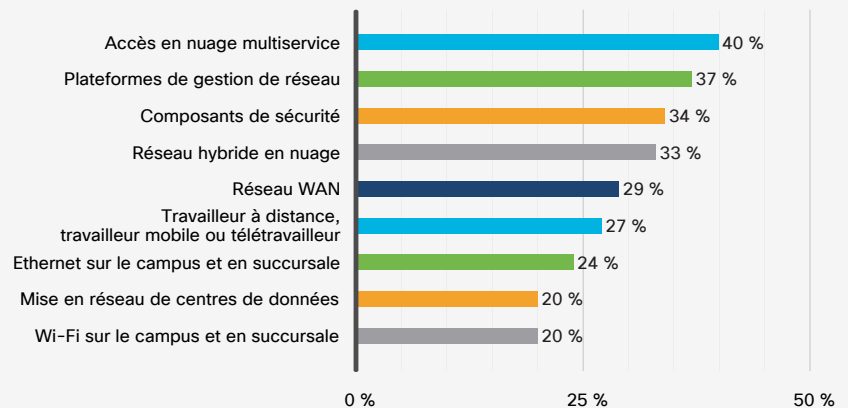


# Le service d'accès sécurisé en périphérie et les différentes sortes de réseau sous forme de service

On dénombre de plus en plus d'offres de réseau sous forme de service, y compris les LAN avec et sans fil, les VPN, les WAN, la sécurité des réseaux, l'accès à distance ou à domicile, les réseaux de centres de données et les réseaux infonuagiques. Selon nos recherches, les modèles de réseaux sous forme de service qui comprennent un accès multinuage et des fonctions de sécurité sont les plus recherchés. Cela signifie que le service d'accès sécurisé en périphérie (SASE), qui offre un accès multinuage sécurisé de partout, serait une offre sous forme de service populaire auprès de nombreuses équipes de TI.

Étant donné les enjeux associés à la connexion à plusieurs nuages disparates, il n'est pas surprenant que l'accès multinuage ait été désigné comme étant la priorité absolue (40 %) pour le réseau sous forme de service. En proposant des services SD-WAN, les prestataires de réseau sous forme de service peuvent offrir une façon cohérente et optimisée de se connecter à une panoplie d'applications infonuagiques (infrastructure et logiciel sous forme de service).

Quels aspects de l'équipement et de la gestion de votre réseau se prêteraient bien au réseau sous forme de service?



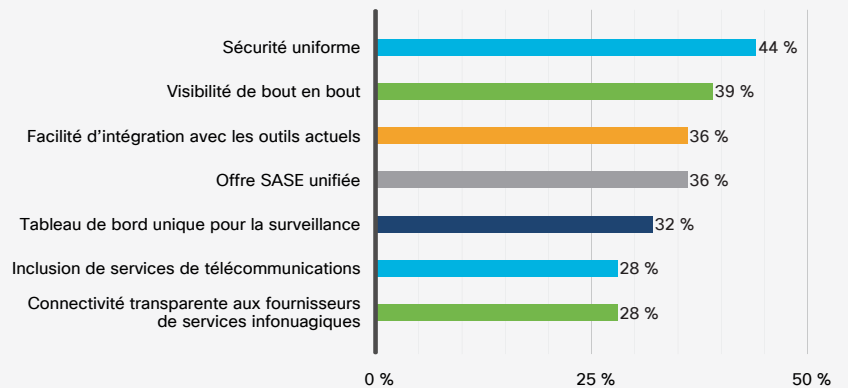
Trente-quatre pour cent des répondants privilégient les solutions de réseau sous forme de service axées sur la sécurité, y compris le VPN, les gestionnaires d'informations et d'événements de sécurité (SIEM), les passerelles Web sécurisées, les pare-feu et les services de détection et de prévention des intrusions. Ces fonctions peuvent contribuer à protéger les utilisateurs, les périphériques et les applications de façon uniforme dans divers environnements informatiques et multinuages.

Les prestataires de réseau sous forme de service qui offrent à la fois un accès multinuage et des fonctions de sécurité en périphérie sont bien placés pour répondre à la demande croissante pour des solutions de service d'accès sécurisé en périphérie.

Près de la moitié (44 %) des répondants ont mentionné des « fonctions de sécurité cohérentes, y compris la détection et la correction des menaces, pour tous les utilisateurs et les périphériques », peu importe l'origine de l'accès, comme aspect important du service d'accès sécurisé en périphérie. Étant donné l'importance accrue d'Internet pour accéder aux applications infonuagiques, plus du tiers (39 %) des répondants recherchent une « visibilité et des connaissances sur le trafic réseau dans l'ensemble des infrastructures infonuagiques et sur Internet ». Et finalement, 36 % des répondants recherchent des solutions de service d'accès sécurisé en périphérie qui s'intègrent facilement à leurs outils actuels.



Si votre entreprise décidait de déployer le SASE sous forme de service, laquelle des capacités suivantes serait la plus importante pour vous ?



### Autrement dit :

L'accès multilingue et la sécurité sont les priorités absolues pour le réseau sous forme de service. Les prestataires qui intègrent une option de service d'accès sécurisé en périphérie à leur gamme de réseaux sous forme de service peuvent répondre à la demande croissante d'harmonisation et de sécurisation des ressources infonuagiques et sur site.

# Conclusion

D'innombrables entreprises de TI ont de la difficulté à gérer la complexité des réseaux, à réagir aux perturbations, à protéger les utilisateurs et les données et à suivre le rythme toujours plus rapide des affaires. Pour gérer ces enjeux, bon nombre d'entre elles explorent de nouveaux modèles de mise en réseau comme le réseau sous forme de service.

Celui-ci offre un accès continu aux dernières technologies de mise en réseau grâce à un modèle sur demande ou par abonnement. Il transfère le fardeau de la gestion quotidienne du réseau à un prestataire tiers. Ce faisant, le réseau sous forme de service permet aux équipes de TI de se concentrer sur des activités à valeur ajoutée qui offrent plus d'agilité, de résilience et d'innovation.

Comme pour tout modèle transformationnel, il peut y avoir des inquiétudes et des hésitations au sujet du réseau sous forme de service. Mais il ne s'agit pas d'un modèle de type « tout ou rien ». Les équipes de TI peuvent travailler avec des partenaires de confiance pour essayer le réseau sous forme de service à petite échelle, évaluer les risques et les avantages et voir si cela correspond à leurs stratégies globales commerciales et technologiques.



## Ressources et aide supplémentaire

[Qu'est-ce qu'un réseau sous forme de service \(NaaS\)? >](#)

[Solutions de Cisco+ >](#)

[Trouver un partenaire Cisco >](#)

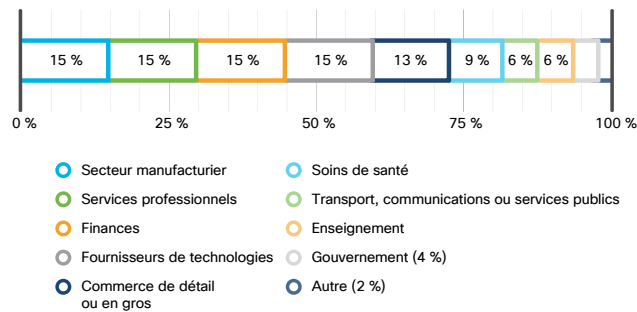
[Contacter le service des ventes de Cisco >](#)

## À propos de ce rapport

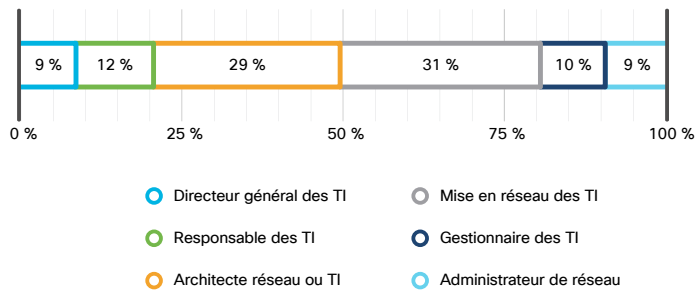
D'abord publié en 2019, le [Rapport sur les tendances mondiales de mise en réseau](#) explique les dernières stratégies et technologies au sein de l'industrie de la mise en réseau d'entreprise et de l'infonuagique. Le rapport s'appuie sur des recherches de l'industrie et il fournit des points de vue, des idées et des conseils pour aider les équipes de TI à comprendre les tendances technologiques actuelles, à faire évoluer leurs modèles de mise en réseau et à soutenir les besoins opérationnels dynamiques.

Pour le rapport de 2022, nous avons mené des entrevues auprès de 20 responsables des TI et reçu des commentaires de 1 534 professionnels des TI de 13 pays au sujet de leurs points de vue sur les réseaux sous forme de service et de la façon dont ils envisagent de les harmoniser avec leurs stratégies de mise en réseau ou de les améliorer au cours des deux prochaines années. Les répondants pouvaient sélectionner jusqu'à trois réponses par question.

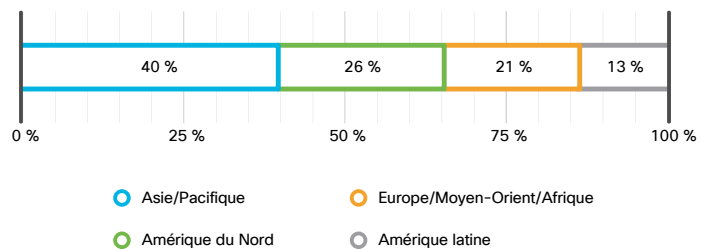
## Secteur des répondants



## Rôle des répondants



## Emplacement des répondants





## Autorisations pour l'utilisation de ce rapport

Cisco invite les médias, les analystes, les fournisseurs de services et les autres parties intéressées à utiliser les informations contenues dans ce rapport. Nous exigeons une mention appropriée des sources pour toutes les données du Rapport sur les tendances mondiales de mise en réseau pour 2022 de Cisco qui sont publiées ou partagées, soit en privé ou en public, en format imprimé ou électronique (c.-à.-d. « Source : Rapport de Cisco sur les tendances mondiales de mise en réseau pour 2022 »). Aucun consentement ni signature n'est nécessaire pour faire référence à nos livres blancs, à nos rapports ou à nos outils Web accessibles au public.

Nous sommes toujours désireux de connaître le contexte dans lequel notre contenu est utilisé. Nous sommes heureux lorsque les parties qui utilisent notre contenu peuvent partager des copies de leur travail terminé contenant des références au Rapport sur les tendances mondiales du réseautage pour 2022 de Cisco. Vous pouvez transmettre les documents contenant des références au Rapport de Cisco sur les tendances mondiales de mise en réseau pour 2022 à l'adresse [networkingtrends-inquiries@cisco.com](mailto:networkingtrends-inquiries@cisco.com).

© Cisco ou ses sociétés affiliées, 2022. Tous droits réservés. Cisco et le logo Cisco sont des marques de commerce ou des marques de commerce déposées de Cisco ou de ses filiales aux États-Unis et dans d'autres pays. Pour voir la liste des marques de commerce de Cisco, consultez la page des [page dédiée](#) sur le site Web de Cisco. Les autres marques de commerce mentionnées appartiennent à leur détenteur respectif. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et une autre entreprise. (2205R)

### Sources du rapport sur les tendances mondiales de mise en réseau pour 2022

1. Global Network-as-a-Service (NaaS) Market Industry Dynamics, Market Size, and Opportunity Forecast to 2027, Report Ocean, mars 2021.