



The bridge to possible\*  
(\*Et vos ambitions prennent vie)



# Rapport 2022 sur les tendances mondiales des réseaux

Édition spéciale : le point sur l'architecture  
SASE et l'essor du réseau en tant que  
service (NaaS)





Édition spéciale :  
le point sur  
l'architecture SASE



# Sommaire

Introduction .....	04
Défis IT .....	05
La relation entre le SD-WAN et le modèle SASE.....	07
Les caractéristiques souhaitées pour une architecture SASE .....	09
L'importance de l'intégration.....	12
Les tendances de l'adoption du modèle SASE .....	15
Les modèles de consommation SASE.....	17
Conclusion .....	18

# Adopter une stratégie SASE

Pour fournir une expérience exceptionnelle et homogène aux utilisateurs dans le cadre du travail hybride, il faut adopter une stratégie SASE cohérente.

Étant donné la hausse de l'intérêt pour le modèle SASE sur le marché, ainsi que pour éviter toute confusion, nous avons ajouté cette annexe à notre [Rapport 2022 sur les tendances mondiales des réseaux : l'essor du réseau en tant que service \(NaaS\)](#).

Avec la généralisation du télétravail et du cloud hybride, le modèle SASE (prononcer « sassi ») fournit une connectivité sécurisée et fluide à toutes les applications, quels que soient le réseau, l'emplacement et le terminal.

L'architecture SASE intègre des fonctions de réseau et de sécurité dans une solution ou un service cloud-natifs unifiés.

Contrairement aux solutions de sécurité classiques, elle rapproche les politiques de sécurité des utilisateurs et applications de plus en plus distribués. Elle s'appuie sur une approche zero-trust et évite les allers-retours des données au data center, ce qui réduit les charges réseau et les goulots d'étranglement, tout en optimisant l'expérience de l'utilisateur.



Elle remplace la pile de sécurité classique et fournit des accès sécurisés sur l'ensemble du réseau, y compris pour le data center, les sites distants et les utilisateurs en déplacement.

Cette annexe présente les dernières tendances et informations sur le modèle SASE, en se basant sur plusieurs études et témoignages d'analystes et experts du secteur. Nous espérons que ces informations vous aideront à mieux comprendre les bénéfices et incidences de l'architecture SASE pour votre stratégie de réseau, de sécurité et de cloud.

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



« Le modèle SASE n'est pas encore très bien défini sur le marché. Toutefois, nous ne sommes pas les seuls à estimer qu'il ne s'agit pas vraiment d'une nouvelle technologie, mais plutôt de l'intégration de technologies réseaux, telles que le SD-WAN, et de technologies de sécurité, comme les passerelles web sécurisées (SWG), dans une solution de connectivité sécurisée. »

– Dell'Oro Group<sup>1</sup>




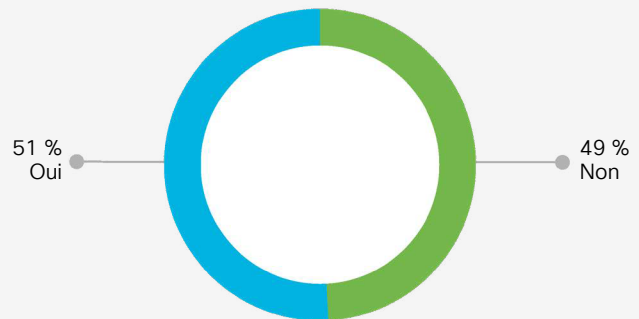
## Défis IT : fournir une expérience de travail hybride sécurisée dans le cloud

Les deux principales tendances qui occupent les équipes IT sont indéniablement la transition continue vers des applications multicloud et l'adoption de modes de travail hybrides. Aujourd'hui, les utilisateurs et les applications sont plus distribués que jamais, ce qui complexifie considérablement leur connexion et leur sécurisation.

La répartition des applications sur différents clouds privés et publics est désormais amplifiée par la tendance au travail hybride, qui provoque l'éparpillement des collaborateurs et des espaces de travail. Dans ces conditions, difficile d'assurer une expérience utilisateur inclusive et de qualité comme avant, avec des environnements on-premise entièrement sous contrôle.

**Dans les sondages récents, 76 % des équipes IT indiquent que les collaborateurs travaillant à distance sont plus difficiles à sécuriser<sup>2</sup> et 51 % des entreprises disent avoir eu du mal à connecter les équipes à leurs ressources au cours des 18 derniers mois<sup>3</sup>.**

 Est-ce que vous ou votre entreprise avez eu du mal à connecter vos collaborateurs au cours de ces 18 derniers mois ?



La transition d'applications centrées sur le data center vers un modèle axé sur le cloud compatible avec Internet a poussé les équipes IT à repenser entièrement leur stratégie réseau. En parallèle, les équipes de sécurité peinent à fournir une expérience à la fois fluide et sécurisée quand les utilisateurs et les applications se trouvent hors site, plus exposés aux potentiels incidents volontaires ou non.

Rien d'étonnant donc à ce que le niveau d'intérêt pour le modèle SASE dans le cloud ait augmenté, puisqu'il allie des solutions réseau, telles que le SD-WAN, et des solutions de sécurité dans le cloud, comme les services de sécurité en périphérie (SSE) et l'accès réseau zero-trust (ZTNA).

L'architecture SASE est conçue pour connecter et protéger les utilisateurs et applications où qu'ils se trouvent, améliorant ainsi la cohérence et la sécurité de l'expérience pour l'utilisateur. Elle promet également une réduction des coûts et de la complexité IT, ainsi qu'une amélioration de la flexibilité et des performances du réseau, et, en fin de compte, de l'expérience applicative.



« En 2020, au plus fort de la pandémie, le nombre de collaborateurs en télétravail à plein temps ou occasionnellement aux États-Unis a grimpé de 450 % par rapport à la moyenne avant la crise. Si ce nombre baisse constamment depuis, nous pensons que la nouvelle référence s'établira quand même à 200 % au-dessus de celle d'avant la pandémie. »

– Dell'Oro Group<sup>4</sup>



### À retenir :

À l'avenir, les collaborateurs seront de plus en plus décentralisés et leurs modes de travail de plus en plus variés. Mise en œuvre correctement, l'architecture SASE connecte et protège les applications et les utilisateurs distribués, aligne les politiques de réseau et de sécurité et réduit la charge de travail ainsi que les risques liés à la gestion du réseau et de la sécurité.

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

Sur le marché, le flou qui règne autour du concept de SASE a soulevé de nombreuses questions sur les solutions SD-WAN. Une architecture SASE remplace-t-elle le SD-WAN ? Est-ce que les deux se complètent ? Ou s'agit-il de deux solutions distinctes répondant à des besoins différents ?

La réponse est simple : le SD-WAN représente la base de l'architecture SASE.

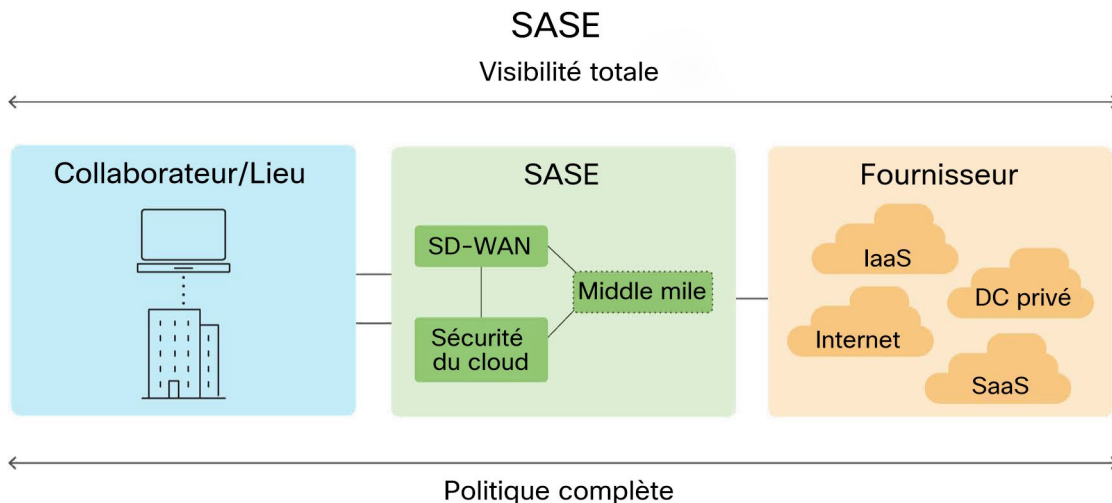
Le modèle SASE allie les capacités de sécurité natives du SD-WAN à la sécurité axée sur le cloud pour connecter et protéger les utilisateurs et les applications où qu'ils se trouvent.

L'architecture SASE est une architecture overlay et ne peut donc pas assurer une sécurité totale sans l'aide du SD-WAN qui :

- Permet de traduire les adresses réseau (NAT)
- Segmente le réseau en plusieurs sous-réseaux
- Surveille et bloque les malwares ainsi que le trafic malveillant
- Bloque les utilisateurs non autorisés
- Bloque les contenus et applications indésirables
- Stoppe le trafic entrant et VLAN-to-VLAN indésirable
- Sécurise le VPN site à site/en tunnel
- Assure le géorepérage pour les contrôles d'accès basés sur l'emplacement

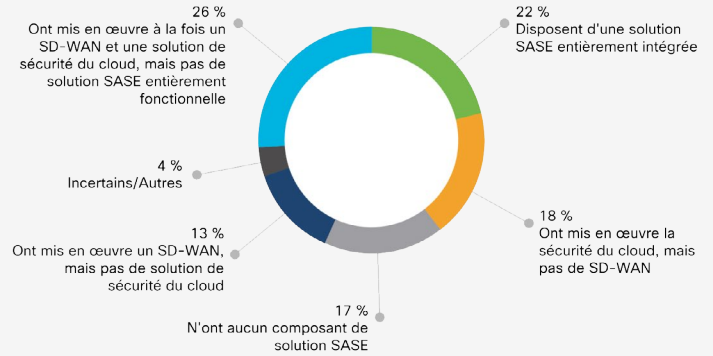
« Le modèle SASE n'a pas pour vocation de remplacer le SD-WAN. Au contraire, le SD-WAN est une composante essentielle de l'architecture SASE. Les offres SASE combinent plusieurs capacités de réseau et de sécurité en tant que service, telles que le SD-WAN, les passerelles web sécurisées (SWG), le service de sécurité pour l'accès au cloud (CASB), les pare-feu de nouvelle génération (NGFW) et l'accès réseau zero-trust (ZTNA). »

– 2021 Gartner®, Quick Answer : Does SASE Replace SD-WAN ?<sup>5</sup>





## Où en êtes-vous de votre parcours d'adoption du modèle SASE ?



Enquête Cisco 2021 sur les technologies de demain ; N = 29 506

Par quoi les départements IT doivent-ils commencer ? Le SD-WAN ou la sécurité du cloud ? Beaucoup optent pour une mise en œuvre progressive de leur architecture SASE. La plupart ont déjà bien entamé leur parcours, en investissant dans une combinaison de composants SD-WAN et de sécurité du cloud pas encore totalement intégrés ou fonctionnels.

**18 % des entreprises disposent d'une solution de sécurité du cloud, mais pas d'un SD-WAN, tandis que 13 % ont un SD-WAN, mais pas de solution de sécurité du cloud<sup>6</sup>.**



### À retenir :

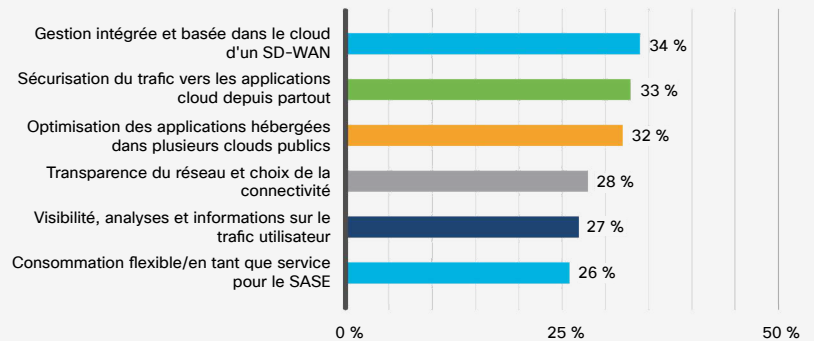
Le SD-WAN est un élément de base de l'architecture SASE, qui fonctionne de pair avec les solutions ou services de sécurité axés sur le cloud pour protéger les utilisateurs et données on-premise, dans le cloud et en périphérie.



# Les caractéristiques souhaitées pour une architecture SASE

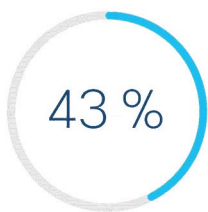
L'architecture SASE intègre à la fois des capacités de réseau et de sécurité, et 34 % des entreprises se tournent en priorité vers les solutions et services qui fournissent une gestion intégrée du SD-WAN dans le cloud. Parmi les autres priorités les plus citées figurent la sécurisation du trafic vers les applications cloud (33 %), l'optimisation des applications hébergées dans plusieurs clouds (32 %) et l'amélioration de la transparence et de la flexibilité du réseau (28 %).

À votre avis, quelles sont les capacités SASE les plus importantes pour votre entreprise ?



Enquête mondiale de Cisco 2021 sur les tendances réseau ; N = 1 534

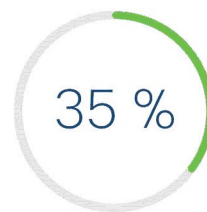
Pour connecter les collaborateurs travaillant à distance :



43 % des entreprises prévoient d'utiliser un VPN en tant que service.



36 % pensent adopter des capacités d'accès réseau zero-trust et d'authentification multifacteur.



35 % s'intéressent aux clients unifiés basés sur l'hôte.



35 % cherchent à étendre leur SD-WAN aux utilisateurs mobiles et travaillant depuis la maison.

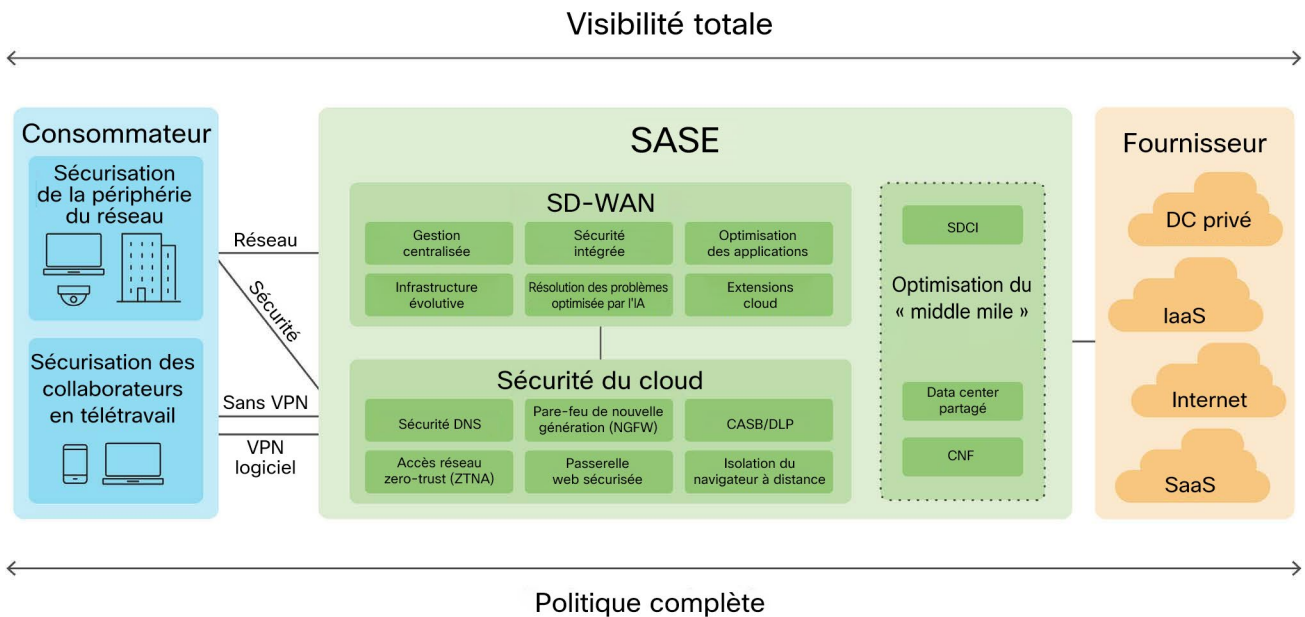
Bien que leur évolution se poursuive, les architectures, solutions et services SASE incluent toujours tout ou partie des composants de base offertes par le SD-WAN et la sécurité du cloud :

SD-WAN	Sécurité du cloud
<p><b>Gestion centralisée</b> Tableau de bord centralisé et clair qui simplifie la configuration des équipements, la gestion du réseau, la surveillance et l'automatisation. Inclut l'allocation de ressources sans intervention en périphérie du réseau.</p>	<p><b>Accès réseau zero-trust (ZTNA)</b> Cadre de sécurité qui bloque les accès non autorisés, maîtrise les failles et réduit les mouvements latéraux des hackers sur le réseau. Il est conseillé d'associer l'accès réseau zero-trust à une gestion renforcée des accès et des identités, afin de vérifier l'identité des utilisateurs et de déterminer la fiabilité des terminaux avant de leur accorder un accès aux applications autorisées.</p>
<p><b>Extension du réseau cloud et optimisation du « middle mile »</b> Intégrations Cloud OnRamp étendues pour une connectivité fluide et automatisée, quelle que soit la configuration site à site ou site à cloud. Inclut une connectivité « middle mile » optimisée à l'aide d'intégrations SDCI et dans les data centers partagés.</p>	<p><b>Passerelle web sécurisée (SWG)</b> Une passerelle qui consigne et inspecte le trafic web pour fournir un haut niveau de visibilité, de filtrage des URL, de protection contre les malwares et de contrôle des applications.</p>
<p><b>Expérience applicative</b> La capacité de surveiller et valider l'utilisabilité et les performances des applications web. Les mesures et diagrammes en cascade illustrent l'extraction et le chargement séquentiels des composants web pour identifier les erreurs et goulots d'étranglement, et comprendre leurs répercussions sur les performances applicatives.</p>	<p><b>Pare-feu cloud avec système de prévention des intrusions (IPS)</b> Services logiciels dans le cloud pour la gestion et l'inspection du trafic réseau.</p>
<p><b>Infrastructure flexible et évolutive</b> Grand choix de plateformes physiques et virtuelles haute disponibilité et haut débit, ports multigigabits, liaisons cellulaires 5G et puissantes capacités de chiffrement. Optimise le trafic WAN en sélectionnant les liaisons WAN les plus efficaces qui satisfont aux critères de niveau de service.</p>	<p><b>Service de sécurité pour l'accès au cloud (CASB)</b> Logiciel qui détecte les applications cloud en cours d'utilisation sur un réseau et génère des rapports pour signaler le recours éventuel au « shadow IT » et bloquer les applications SaaS à risque ainsi que les actions telles que les publications et les téléchargements.</p>
<p><b>Résolution des problèmes optimisée par l'IA</b> IA/ML robuste pour optimiser les performances du réseau, automatiser les tâches manuelles de routine et accélérer la résolution des problèmes. Fournit des alertes intelligentes, ainsi que des fonctions d'autoréparation et de redirection Internet prédictives.</p>	<p><b>Prévention des pertes de données (DLP)</b> Logiciel qui analyse les données en coupure et offre visibilité et contrôle sur les données sensibles transférées à l'intérieur et vers l'extérieur du réseau ou du cloud de l'entreprise.</p>
<p><b>Sécurité intégrée</b> Capacités de sécurité robustes qui s'associent au système de sécurité dans le cloud pour protéger les sites distants, les utilisateurs travaillant à la maison et les applications cloud contre les infiltrations.</p>	<p><b>Isolation du navigateur à distance</b> Logiciel qui isole le trafic web des terminaux de l'utilisateur afin de limiter les risques de menaces véhiculées par le navigateur.</p>
<p><b>Gestion des politiques basée sur l'identité</b> Microsegmentation et gestion des politiques basée sur l'identité dans plusieurs emplacements et domaines.</p>	<p><b>Sécurité de la couche DNS</b> Logiciel qui agit en tant que première ligne de défense contre les cybermenaces et bloque les requêtes DNS malveillantes avant qu'une connexion à une adresse IP puisse être établie. Un système de sécurité DNS efficace réduit considérablement le nombre de menaces de sécurité à trier au quotidien.</p>
<p><b>Informations avancées</b> Visibilité accrue sur les applications, Internet, le cloud et les environnements SaaS grâce à des analyses saut par saut complètes. Permet l'isolation des domaines à l'origine des défaillances et fournit des informations exploitables pour accélérer la résolution des problèmes et minimiser, voire neutraliser, les répercussions sur les utilisateurs.</p>	<p><b>Threat Intelligence</b> Chercheurs en vulnérabilités, ingénieurs et spécialistes des données qui utilisent la télémétrie ainsi que des systèmes sophistiqués pour créer une Threat Intelligence précise, rapide et exploitable permettant d'identifier les menaces émergentes, de découvrir de nouvelles vulnérabilités, de bloquer les menaces avant qu'elles ne s'étendent, à l'aide d'ensembles de règles qui prennent en charge les outils de votre pile de sécurité.</p>

En plus d'intégrer des capacités SD-WAN et de sécurité du cloud, les modèles SASE vous aident à éliminer les silos opérationnels et favorisent l'alignement entre les équipes chargées du réseau et de la sécurité. Grâce aux politiques standardisées, à la télémétrie partagée et aux alertes coordonnées sur l'ensemble des composants de sécurité et de réseau, le modèle SASE permet aux équipes NetOps et SecOps d'améliorer l'efficacité, la visibilité et la protection dans l'environnement IT.

C'est pourquoi les entreprises doivent établir une stratégie SASE complète qui tient compte des objectifs des équipes NetOps et SecOps, s'aligne sur les opérations et prend en charge les besoins futurs.

## SASE : Détails



« D'ici 2024, 30 % des entreprises auront adopté une passerelle web sécurisée (SWG) dans le cloud, un service de sécurité pour l'accès au cloud (CASB), l'accès réseau zero-trust (ZTNA) et le pare-feu en tant que service (FWaaS) pour leurs sites distants, le tout provenant d'un fournisseur unique, contre moins de 5 % en 2020. »

– Gartner<sup>7</sup>



### À retenir :

Les entreprises évaluent actuellement les offres et stratégies SASE. Elles cherchent des solutions et services qui incluent les capacités de base du SD-WAN et de la sécurité du cloud afin de répondre à leurs besoins actuels et futurs.



# L'importance de l'intégration

Les entreprises modernes s'appuient sur plusieurs environnements réseau (data center, réseaux locaux, réseaux étendus) et solutions de sécurité (pare-feu, passerelles et contrôles d'accès pour les systèmes on-premise et cloud). Les intégrations de technologies et services des architectures SASE assurent la visibilité, l'orchestration des politiques et la protection dans tous ces environnements.

En plus de sécuriser les connexions des utilisateurs et des applications partout, ces intégrations offrent aussi les avantages suivants :

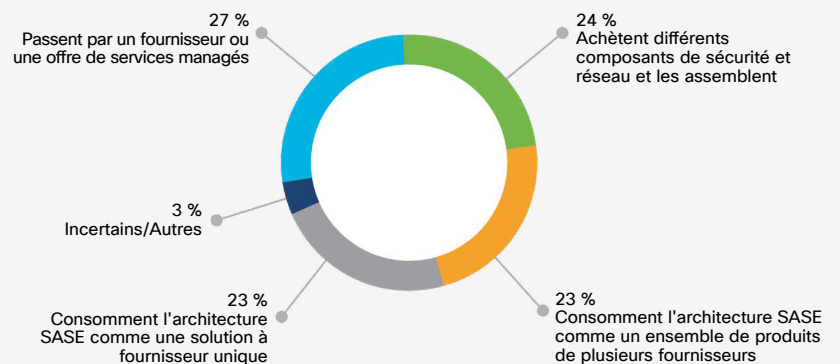
- Réduction du nombre d'incidents liés à la sécurité.
- Accélération de la recherche et de la résolution des problèmes.
- Simplification de la gestion et de la surveillance du système.
- Amélioration de la standardisation et de l'application des politiques.
- Respect des exigences relatives à la conformité et aux données.
- Réduction des CapEx et des OpEx.

« Il y a deux principaux types de mises en œuvre SASE sur le marché : unifiée et dispersée. La mise en œuvre unifiée s'appuie sur des plateformes SASE étroitement intégrées provenant d'un seul et même fournisseur. tandis que la mise en œuvre dispersée associe plusieurs produits de plusieurs fournisseurs, avec moins d'intégration. »

– Dell'Oro Group<sup>9</sup>



Comment pensez-vous déployer et mettre en œuvre votre solution SASE ?



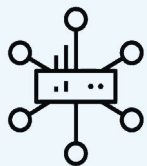
Enquête Cisco 2021 sur les technologies de demain ; N = 29 506

Avec l'émergence de solutions et services à fournisseur unique ou à plusieurs fournisseurs, et des architectures personnalisables qui associent plusieurs solutions ponctuelles, les entreprises disposent aujourd'hui d'un vaste choix pour le déploiement et la mise en œuvre de leur stratégie SASE.

Étant donné que la création et l'intégration de solutions personnalisées et la mise en œuvre d'offres SASE à plusieurs fournisseurs engendrent potentiellement de la complexité, des problèmes d'exploitation et des vulnérabilités de sécurité, la moitié des entreprises préfèrent opter pour une solution unifiée et/ou managée à un seul fournisseur.

- 70 % trouvent qu'il est de plus en plus difficile de gérer efficacement une pile de sécurité et de réseau à plusieurs fournisseurs (d'accord ou tout à fait d'accord).
- 26 % disposent à la fois de capacités SD-WAN et de sécurité du cloud, sans les avoir mises en œuvre ou intégrées dans un modèle SASE complet<sup>10</sup>.

Quelle que soit leur configuration (architecture personnalisée, offre à plusieurs fournisseurs, service managé à fournisseur unique ou autres), toutes les solutions SASE devraient assurer un meilleur alignement et une meilleure intégration entre :



#### Le SD-WAN et la sécurité du cloud

- Automatiser le routage du trafic entre le périphérique SD-WAN et les points de présence (PoP) de sécurité du cloud
- Rediriger le trafic automatiquement vers un PoP pour assurer la résilience en cas de problème de performance
- Exploiter des analyses prédictives basées sur l'IA pour rediriger automatiquement le trafic vers d'autres PoP avant que l'expérience de l'utilisateur ne se dégrade



#### Les équipes NetOps et SecOps

- Partager en permanence des politiques de sécurité (autorisations d'accès, segmentation, etc.) entre le SD-WAN et les instances de sécurité du cloud
- Échanger des données entre les plateformes SD-WAN et de gestion de la sécurité du cloud pour fournir une visibilité cohérente sur les politiques et événements
- Étendre et propager les structures réseau de l'entreprise (VPN ou balises de groupe de sécurité, par exemple) ainsi que les politiques dans des plateformes de sécurité du cloud
- Utiliser l'authentification unique pour l'administration sur les plateformes SD-WAN et de gestion de la sécurité du cloud



#### Les utilisateurs finaux et les applications

- Établir une connectivité directe entre le SD-WAN, le « middle mile » (SDI par exemple), le multicloud et les services SaaS
- Surveiller et optimiser l'expérience de l'utilisateur avec des analyses et une visibilité complète sur le SD-WAN, les PoP de sécurité du cloud et les connexions IaaS/SaaS



« Impossible d'assurer la qualité d'un réseau sans intégrer la sécurité. Il faut l'envisager de manière globale, du terminal à l'application et tout le long du chemin sur le réseau. Avec le NaaS, le fournisseur est responsable du réseau et de la sécurité. Mais s'il ne s'occupe que du réseau, j'ai besoin d'un niveau de visibilité et de contrôle suffisant pour assurer la protection et une gestion rapide des menaces. Dans l'idéal, le fournisseur devrait se charger efficacement de ces deux aspects. »

– DSI, entreprise internationale de produits de consommation



### À retenir :

Qu'ils soient personnalisés ou fournis par un ou plusieurs fournisseurs, les solutions et services SASE doivent assurer une intégration étroite entre les systèmes SD-WAN et de sécurité du cloud afin d'optimiser l'expérience de l'utilisateur et de simplifier la collaboration entre les équipes NetOps et SecOps.

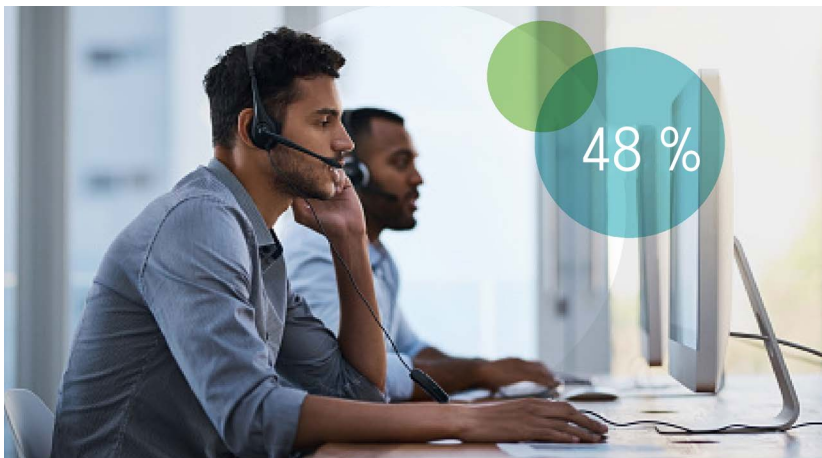
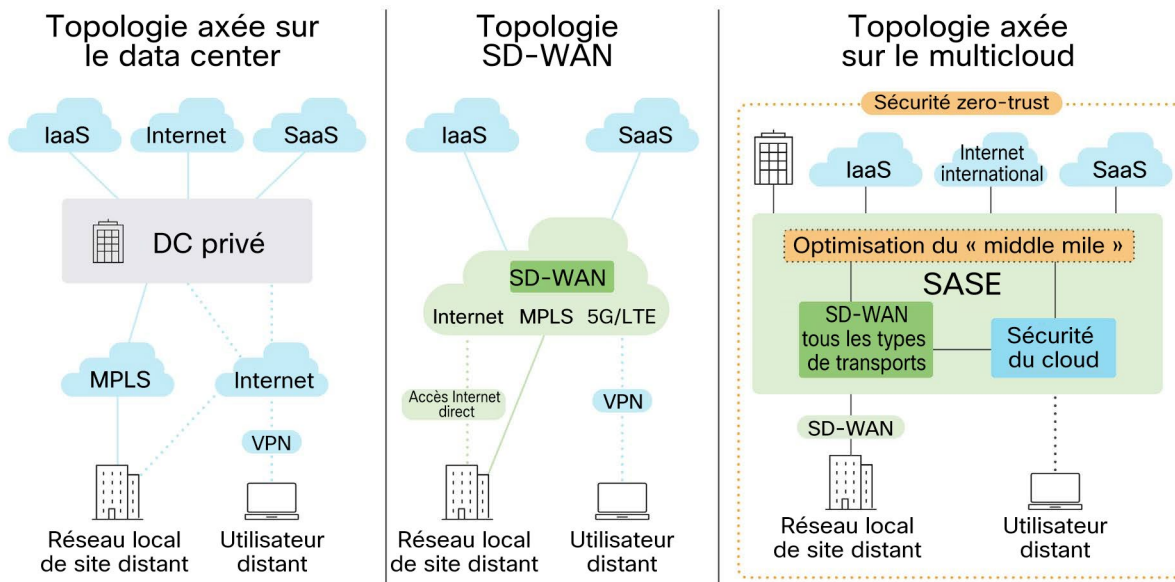


# Tendances en matière d'adoption du modèle SASE

Il n'existe pas de modèle SASE ou d'approche de déploiement idéaux. Comme toutes décisions relatives aux technologies, ces choix varient d'une entreprise à l'autre. Il est toutefois important de tenir compte des solutions de sécurité et de réseau déjà en place, ainsi que des stratégies opérationnelles et priorités métier générales. Autres facteurs à ne pas négliger : les initiatives stratégiques, les exigences réglementaires, les contraintes liées aux fusions et acquisitions, la chaîne d'approvisionnement et les besoins en matière de résilience de l'activité.

Les entreprises qui passent d'un modèle d'application axé sur le data center à un modèle axé sur le cloud ou le multicloud peuvent entamer leur migration SASE par un SD-WAN, par exemple, suivi par l'optimisation du « middle mile » et l'intégration de la sécurité du cloud.

## D'une topologie axée sur le data center à une topologie axée sur le multicloud

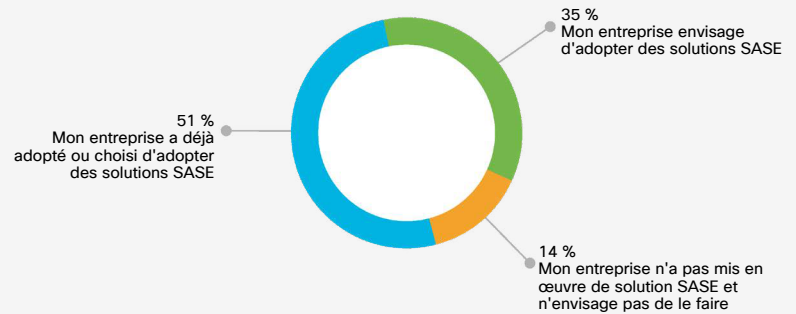


48 % des entreprises intéressées par le modèle SASE prévoient d'investir d'abord dans la sécurité, 31 % dans le réseau et 21 % dans les deux en même temps.<sup>8</sup>

De nombreuses entreprises indiquent avoir déjà bien entamé l'adoption du SASE (tous modèles et approches de déploiement confondus) : 86 % prévoient d'adopter une solution SASE ou en ont déjà adopté une.<sup>11</sup>



Votre entreprise a-t-elle déjà adopté des solutions SASE ou prévoit-elle de le faire ?



Enquête Cisco 2021 sur les technologies de demain ; N = 34 351



« D'ici 2025, au moins 60 % des entreprises auront établi des stratégies et un calendrier pour l'adoption de solutions SASE couvrant les utilisateurs, les sites distants et la périphérie du réseau. Cela représente 10 % de plus qu'en 2020. »

– Gartner<sup>12</sup>



### À retenir :

Les approches de déploiement SASE dépendent du cycle de vie des infrastructures déjà en place, des politiques d'exploitation et des initiatives métier. Les équipes IT doivent adopter une approche stratégique de la planification et avancer progressivement vers une architecture SASE complète.

# Modèles de consommation SASE

Il existe trois principaux modèles de consommation des solutions et services SASE. Tous permettent d'éliminer les silos classiques, chacun a une influence différente sur les équipes et l'exploitation. Ainsi, le modèle SASE peut améliorer l'alignement et l'efficacité opérationnels.

## En tant que service



Déploiement rapide, impact minimal sur le personnel et l'exploitation, réduction des risques liés aux SLA : le SASE en tant que service fournit un ensemble de capacités cloud entièrement intégrées avec un tableau de bord unique et la prise en charge complète du cycle de vie. 26 % des entreprises ont désigné le SASE en tant que service comme leur modèle de consommation préféré.

## Hybride ou co-managé



Les entreprises qui ne sont pas encore prêtes à adopter un modèle « en tant que service » complet ou qui souhaitent des services encore plus personnalisés peuvent opter pour une approche hybride. Elles peuvent intégrer des capacités de sécurité du cloud à une solution SD-WAN déjà en place et/ou partager la responsabilité du réseau et de la sécurité avec un fournisseur de services managés. Une approche hybride offre davantage de sécurité et une meilleure prise en charge. Elle permet en outre aux équipes IT de conserver un bon niveau de contrôle et de visibilité tout en déléguant une partie de la gestion du cycle de vie global.

## Personnalisé ou « fait maison »



Les entreprises qui souhaitent personnaliser entièrement leurs solutions réseau et sécurité et en conserver le contrôle total peuvent créer, intégrer et gérer leurs propres capacités SASE. Toutefois, ce haut niveau de personnalisation et de contrôle nuit à la rapidité et à l'agilité, augmente la charge de gestion du cycle de vie du matériel, des logiciels et des licences et nécessite l'embauche de spécialistes en sécurité et conformité. Il s'agit d'une option intéressante pour les entreprises aux demandes très spécifiques qui disposent déjà du personnel et du réseau nécessaires à prendre en charge les exigences architecturale et opérationnelle du modèle SASE.

Lisez notre [Étude de cas de déploiement Cisco SASE](#) pour découvrir les leçons que nous en avons tirées.



### À retenir :

Il existe plusieurs modèles de consommation SASE et chacun a des répercussions différentes sur l'exploitation. Pour choisir le modèle qui lui convient le mieux, une entreprise doit tenir compte de multiples facteurs, notamment la taille, les compétences et la disponibilité de son équipe IT, ses besoins métier prioritaires ainsi que ses exigences en matière de rapidité, agilité, visibilité et contrôle.





## Conclusion

Les architectures, solutions et services SASE assurent une connectivité sécurisée entre un utilisateur et une application, où qu'ils se trouvent. Toutefois, le parcours d'adoption de chaque entreprise sera différent. Le modèle et l'approche idéaux dépendent des technologies déjà en place, ainsi que des priorités métier.

Cisco et son écosystème de partenaires peuvent vous aider à répondre à vos exigences particulières en matière de réseau et de sécurité, avec la solution SASE la plus complète, flexible et résiliente sur le marché.

Notre gamme SASE combine des produits réseau, de connectivité client et de sécurité de pointe, ainsi que des capacités d'observabilité Internet inégalées afin de vous assurer les résultats que vous attendez. Nous proposons également plusieurs modèles de consommation et de déploiement SASE simples et flexibles qui répondent à divers besoins et cas d'usage.

Hautement disponible, notre infrastructure de sécurité du cloud mondiale fournit un accès sécurisé où que se trouvent les utilisateurs et les applications. Nos solutions SD-WAN leaders sur le marché offrent le niveau d'agilité et les fonctionnalités nécessaires pour assurer la cohérence et la qualité de l'expérience de l'utilisateur. Ensemble, nos solutions SD-WAN et de sécurité du cloud fournissent les capacités SASE les plus complètes et intégrées disponibles sur le marché.

Nous prévoyons d'accélérer l'innovation SASE via des intégrations continues et l'amélioration de nos fonctions. Nous faisons évoluer nos offres pour vous offrir les services SASE les plus flexibles et faciles à consommer.

Pour en savoir plus, rendez-vous sur le [centre des ressources SASE de Cisco](#).

Cisco a été nommé leader dans le Magic Quadrant™ de Gartner pour l'infrastructure WAN Edge pour sa capacité d'exécution et l'exhaustivité de sa vision<sup>13</sup>.



## Ressources supplémentaires et assistance

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

[Trouver un partenaire Cisco >](#)

[Contacter un commercial Cisco >](#)

Gartner ne fait la promotion d'aucun fournisseur, produit ou service présenté dans ses rapports d'étude et ne conseille pas aux utilisateurs de ne choisir que les fournisseurs les mieux notés. Les études publiées par Gartner reflètent uniquement les opinions des rédacteurs de son entité de recherche et de conseil, et ne sont en aucun cas à considérer comme des faits irréfutables. Gartner exclut toute garantie, explicite ou implicite, concernant cette étude, notamment toute garantie de qualité marchande ou d'adéquation à un usage particulier. GARTNER et le MAGIC QUADRANT sont des marques commerciales et des marques de services de Gartner Inc. et/ou de ses sociétés affiliées, et sont utilisées ici avec son 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. « Les technologies de demain », 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. « Rapport Cisco 2022 sur les tendances réseau dans le monde : l'essor du réseau en tant que service (NaaS) », Cisco, octobre 2021.
7. « Feuille de route 2021 pour la convergence SASE », Gartner, mars 2021.
8. « SASE Trends : Plans Coalesce but Convergence Will Be Phased », rapport ESG Research, décembre 2021.
9. « Advanced Research Report : SASE Market Forecast, Vol. 2, No. 1 », Dell'Oro Group, septembre 2021.
10. « Rapport Cisco 2022 sur les tendances réseau dans le monde : l'essor du réseau en tant que service (NaaS) », Cisco, octobre 2021.
11. « Les technologies de demain », Cisco, novembre 2021.
12. « Feuille de route 2021 pour la convergence SASE », Gartner, mars 2021.
13. « Magic Quadrant pour l'infrastructure WAN », Gartner, septembre 2021.



•• L'essor du réseau en tant que service (NaaS)



# Sommaire

Bienvenue .....	22
Principaux résultats .....	23
Un modèle réseau différent .....	25
Répondre aux enjeux, apporter de la valeur.....	27
Comment le NaaS transforme-t-il les opérations réseau ? .....	29
Rôles, responsabilités et compétences.....	31
Préoccupations et hésitations.....	33
Tendances en matière d'adoption.....	35
Choisir un fournisseur NaaS.....	36
La technologie SASE et les différents aspects du NaaS.....	38
Conclusion .....	40
Ressources supplémentaires et assistance.....	40
À propos de ce rapport .....	41
Autorisation d'utiliser ce rapport.....	42



# Bienvenue

## Bienvenue dans le *rapport 2022 sur les tendances mondiales des réseaux : l'essor du réseau en tant que service (NaaS)*.

Nous vivons une époque incroyable, autant humainement qu'en tant que professionnels du réseau. L'année dernière, les responsables IT et les professionnels du réseau ont dû faciliter le travail à distance, protéger les données dans un environnement informatique de plus en plus décentralisé et déployer de nouveaux services pour leurs utilisateurs, clients et partenaires. Beaucoup d'entreprises ont accéléré leur transformation numérique pour s'adapter à ces nouveaux besoins, en tirant parti du cloud et des logiciels en tant que service (SaaS) pour gagner en souplesse, en agilité et en rapidité.

Dans notre [Rapport 2021 sur les tendances mondiales des réseaux](#), nous avons mis en avant le rôle des technologies réseau pour favoriser la résilience des entreprises dans toutes les situations.

Dans le rapport de cette année, nous présentons une nouvelle tendance qui aura de grandes répercussions à l'avenir : le réseau en tant que service.

Dans la lignée de modèles « en tant que service » (aaS) de plus en plus populaires, comme ceux des logiciels SaaS et de l'infrastructure IaaS, le NaaS va radicalement transformer la manière dont les entreprises acquièrent, distribuent et gèrent leurs fonctionnalités réseau. Pour en savoir plus, nous avons discuté avec 20 responsables IT et interrogé 1 534 professionnels de l'informatique dans 13 pays différents afin de connaître leur avis sur le NaaS, ses atouts et ses limites, ainsi que leur intention ou non d'adopter ce nouveau modèle de consommation des services réseau.

Nous espérons que les données, les points de vue et les conseils présentés dans ce rapport vous permettront de mieux comprendre les bénéfices et les implications du NaaS pour l'évolution de vos stratégies réseau.

— James Mobley, vice-président, Services réseau, Cisco



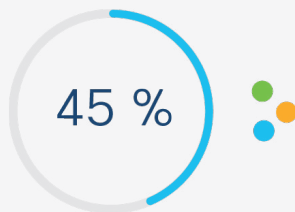


# Principaux résultats

Il n'est pas simple de transformer complètement la manière dont vous consommez et exploitez vos services réseau. Pour faire la transition vers un modèle en tant que service, il faut avoir de solides besoins métiers et technologiques. Il faut aussi pouvoir s'appuyer sur des partenaires fiables pour assurer la continuité de l'activité. Malgré tout, beaucoup d'entreprises sont prêtes à franchir le pas. Voici les principaux résultats de notre étude 2022 sur le NaaS :

## Résultat n° 1 : les problématiques

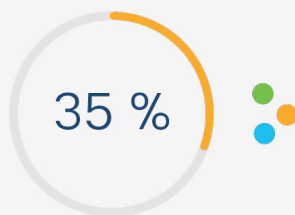
Pour beaucoup, le NaaS est la réponse aux enjeux en matière de résilience et d'agilité.



- En 2021, les principaux défis réseau sont de « faire face aux perturbations » (45 %) et de « s'adapter aux nouveaux besoins de l'entreprise » (40 %).
- Les équipes IT reconnaissent également que le principal bénéfice du NaaS est de laisser plus de temps pour innover et apporter une valeur ajoutée à l'entreprise (46 %). 40 % des personnes interrogées déclarent par ailleurs que le NaaS permet de mieux répondre aux perturbations, et 34 % qu'il améliore l'agilité du réseau.

## Résultat n° 2 : les bénéfices

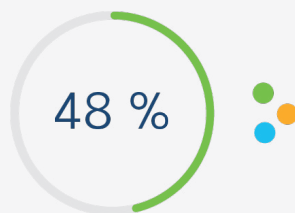
Les attentes sont grandes, puisque l'objectif final est de pouvoir accéder rapidement aux toutes dernières technologies.



- Les technologies évoluent plus rapidement que les entreprises ne peuvent les adopter. 35 % des participants déclarent que leur volonté de transition vers le NaaS est principalement motivée par la nécessité de déployer constamment les technologies réseau les plus récentes, comme le Wi-Fi 6, le SD-WAN (Software-Defined WAN), la sécurité au niveau des points d'accès (SASE), la 5G, l'IA, etc.

## Résultat n° 3 : les opérations

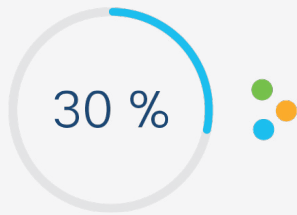
Le NaaS est une excellente solution s'il permet à l'équipe réseau de respecter les contrats de niveau de service (SLA).



- Les principaux services attendus des fournisseurs NaaS sont la gestion du cycle de vie du réseau (48 %), la résilience du réseau (42 %) ainsi que la supervision et le dépannage pour respecter les contrats de qualité de service (38 %).

## Résultat n° 4 : les préoccupations

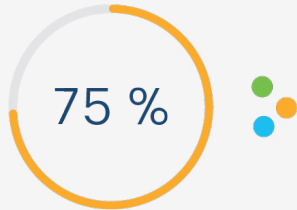
Mais tout n'est pas simple pour autant : les personnes interrogées s'inquiètent de la perte de contrôle et de l'incertitude au niveau des coûts.



- Les préoccupations vont de la capacité du NaaS à prendre en charge les besoins inédits (30 %) à la perte de contrôle sur la sécurité (26 %).
- Les coûts et les perturbations liés à la transition figurent aussi parmi les principales préoccupations (28 %).

## Résultat n° 5 : les rôles

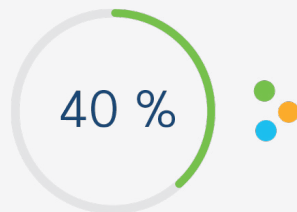
Le NaaS ouvre de nouveaux horizons pour les professionnels de l'IT qui seront capables de relever le défi.



- Plus de 75 % des entreprises sont d'accord ou tout à fait d'accord sur le fait que le NaaS donne aux équipes IT l'opportunité de développer leurs compétences.
- Cependant, actuellement seule 1 entreprise sur 4 se fie davantage à son équipe IT qu'à un intégrateur de systèmes, un fournisseur de services managés ou un fournisseur de services NaaS pour traduire les besoins de l'entreprise en politiques techniques.

## Résultat n° 6 : l'adoption

Il existe plusieurs façons de déployer le NaaS, et l'une d'entre elles est la technologie SASE.



- L'accès multicloud (40 %) et la sécurité (34 %) sont cités par les entreprises comme des motifs d'adoption de services NaaS. La technologie SASE offre donc un point d'entrée potentiel pour le NaaS.
- 45 % des entreprises prévoient de déployer le NaaS durant un cycle de mise à niveau ou d'actualisation, et 34 % déclarent vouloir le faire en adaptant un site existant.

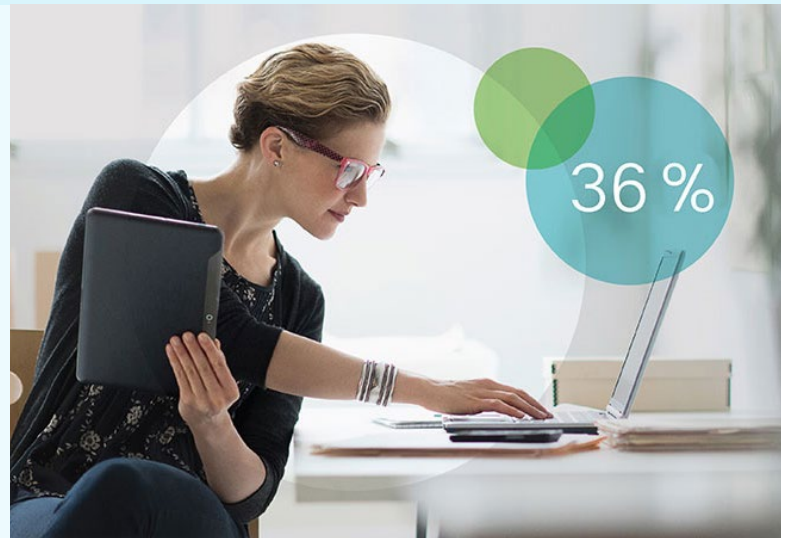
## Un modèle réseau différent

Après plus de 18 mois de bouleversement et d'adaptation, l'importance du rôle des technologies réseau dans la survie et la réussite des entreprises n'est plus à démontrer. En plus de faciliter le travail à distance, les réseaux doivent maintenant permettre de sécuriser les lieux de travail, de mettre en place des modèles de travail hybrides et de prendre en charge l'évolution des opérations de l'entreprise. Pour cela, ils doivent fonctionner simplement

quel que soit le type d'environnement : sur site, en multcloud et au niveau des points d'accès. Ils doivent fournir une expérience cohérente et sécurisée à tous les utilisateurs, où qu'ils soient et quels que soient leur l'équipement ou leur méthode de connexion. Enfin, ils doivent prendre en charge les applications classiques et modernes axées sur les microservices.

Les ressources et la bande passante étant souvent limitées, beaucoup de responsables IT et réseau envisagent le NaaS comme une solution pour résoudre ces problématiques. Mais de quoi s'agit-il exactement ?

Lorsque nous avons demandé aux responsables IT quelle était leur définition du NaaS, il nous est apparu que le sens n'était pas le même pour tous. Nous avons d'ailleurs été surpris par les 36 % de participants déclarant utiliser déjà un réseau NaaS. Cela nous paraissait beaucoup pour une technologie si récente, mais il s'avère que la plupart des entreprises déclarent utiliser le NaaS dès qu'un fournisseur tiers gère une partie de leur réseau. Selon nous, cette définition est trop large et doit être plus spécifique.



**Le NaaS est un modèle de consommation basé sur l'utilisation et géré dans le cloud qui permet d'acquérir et d'orchestrer des fonctionnalités réseau sans posséder, construire, ni entretenir sa propre infrastructure.**

« Les entreprises tentent de trouver le bon équilibre entre ressources internes et ressources fournies par les partenaires. Beaucoup choisissent d'investir dans leurs collaborateurs, l'analytique, l'observabilité et l'automatisation, et se demandent comment s'appuyer sur des partenaires stratégiques pour se décharger d'une partie de la gestion et de la maintenance de l'infrastructure. »

– Mary Turner, vice-présidente de la recherche, IDC

Le NaaS fournit un modèle de consommation alternatif pour un grand nombre d'éléments réseau, y compris les LAN filaires et sans fil, les WAN et les VPN, mais aussi pour tout type d'environnement (site distant, data center, points d'accès, multicloud et cloud hybride). Il peut être utilisé pour déployer de nouveaux modèles réseau, comme l'architecture SASE. Il simplifie l'évolution des modèles organisationnels, comme la transition vers le travail hybride. Par ailleurs, en tant que service à la demande, il permet aux équipes IT d'adapter facilement l'échelle de l'infrastructure, de déployer rapidement de nouveaux services et de mieux équilibrer CapEx et OpEx.

Pour certains des responsables IT interrogés, le NaaS est une nouvelle forme de réseau améliorée dont ils ont grandement besoin.

Ils reconnaissent leur retard et la perte de confiance progressive de leurs utilisateurs. Ils pensent que le NaaS peut les aider à intégrer les nouvelles technologies, à satisfaire un nombre croissant d'exigences et à s'adapter à l'évolution rapide de l'entreprise.



« Compte tenu du niveau de complexité et de l'étendue des réseaux modernes, ainsi que de la rapidité avec laquelle les entreprises doivent s'adapter aux évolutions du marché, beaucoup réalisent qu'ils ne peuvent plus s'en sortir seuls, sans rien changer. »

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

### Résultat :

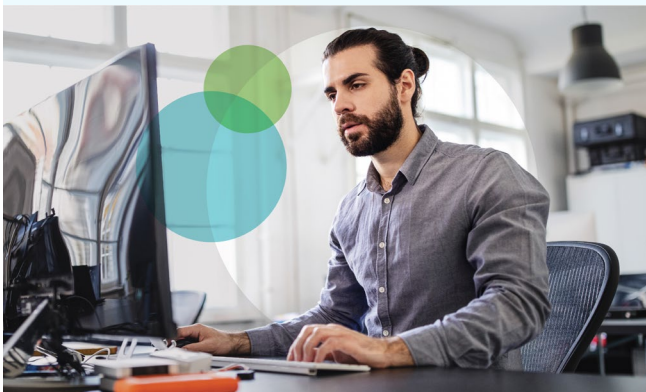
Selon les estimations, l'adoption du NaaS devrait connaître un taux de croissance annuel cumulé de 40,7 % entre 2021 et 2027<sup>1</sup>.

## Répondre aux enjeux, apporter de la valeur

Le choix de l'adoption ou non d'un modèle NaaS dépend des problématiques métiers et technologiques à résoudre, et des bénéfices recherchés.

Pour les entreprises sondées, l'agilité reste la priorité. Les professionnels de l'IT interrogés sur la principale problématique métier devant être résolue par leur réseau sont près de 50 % à citer la réponse aux perturbations et 40 % l'intégration de nouvelles applications et de nouveaux projets métiers. Plus d'un tiers des participants identifient le besoin d'agilité réseau comme une raison majeure d'adopter un modèle NaaS, et la moitié déclarent qu'ils s'attendent à ce que le NaaS les aide à innover et à créer de la valeur.

Dans le cadre de leurs efforts pour gagner en agilité, beaucoup de départements IT migrent leurs applications et leurs services dans le cloud, ce qui peut introduire de nouvelles problématiques de sécurité, de gouvernance et de conformité.

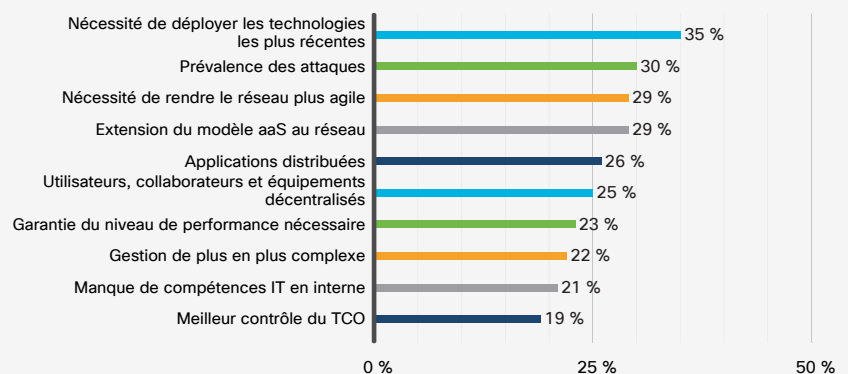


Selon les professionnels de l'IT sondés, les principales problématiques technologiques auxquelles ils sont confrontés en matière de gestion du réseau sont la connexion à plusieurs clouds (36 %), la sécurisation du réseau, des utilisateurs et des applications (34 %), et l'identification des causes premières ainsi que la résolution rapide des problèmes de sécurité et de performance (31 %).

Dans le même temps, un tiers des participants identifient la nécessité de déployer constamment les technologies réseau les plus récentes (Wi-Fi 6, SD-WAN, SASE, 5G, IA, etc.) comme principale motivation de la transition vers le NaaS, et un tiers citent la capacité à se protéger contre les menaces, qui sont de plus en plus fréquentes et sophistiquées.



Qu'est-ce qui motiverait le plus votre entreprise à migrer vers un modèle NaaS ?





« Notre équipe dirigeante ne voit pas l'intérêt de se charger en interne de configurer les équipements et d'exploiter l'infrastructure. Pour elle, le département IT doit se concentrer sur les objectifs de l'entreprise. En s'appuyant sur des services externes pour effectuer les opérations de base, nos collaborateurs se recentrent sur les objectifs métiers. »

– Directeur de l'infrastructure IT, entreprise internationale de produits de consommation

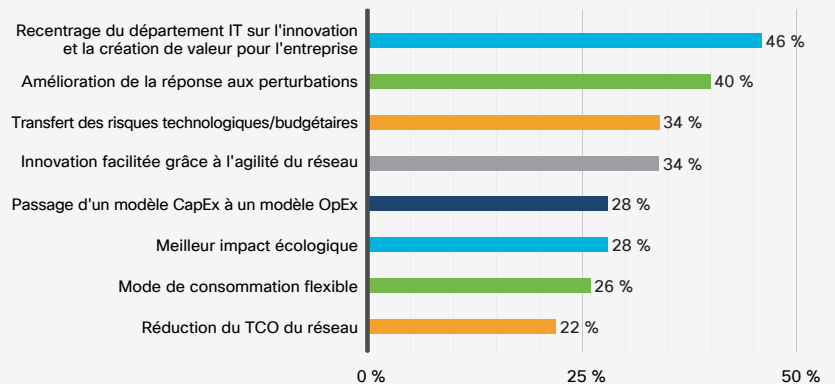
Interrogés sur les principaux bénéfices attendus du NaaS par les professionnels de l'IT, les décideurs citent la capacité de se focaliser sur la création de valeur plutôt que sur la gestion quotidienne de l'infrastructure.

L'amélioration de la réponse aux problèmes de sécurité et aux perturbations du réseau est l'un des autres bénéfices les plus appréciés du NaaS, comme le confirment 45 % des professionnels des réseaux et 40 % des décideurs. Le fait que l'amélioration de la sécurité soit jugée comme prioritaire ne nous surprend pas. En revanche, il est intéressant de noter que plus de 25 % des professionnels du réseau et 33 % des décideurs identifient l'impact écologique comme l'un des grands bénéfices du NaaS.

## Encore plus surprenant, les bénéfices financiers du NaaS ne figurent pas en tête de liste.

Avec un modèle de consommation souple et une tarification par abonnement, le NaaS permet aux équipes IT de transformer les CapEx en OpEx et d'éviter des investissements massifs récurrents dans l'infrastructure réseau. Les dépenses deviennent plus homogènes et prévisibles, et les entreprises paient seulement pour les ressources utilisées. Pourtant, ces bénéfices sont beaucoup moins bien classés par les responsables IT et les professionnels du réseau que l'agilité, l'innovation et l'allègement de la gestion offerts par le NaaS.

● ● ●  
Selon vous, quels sont les 3 principaux bénéfices offerts par l'utilisation d'un modèle NaaS ?



● ● ●  
**Résultat :**  
Le coût total de possession (TCO) apparaît en bas de la liste des priorités associées au NaaS, car les entreprises sont bien plus soucieuses de créer de la valeur et de faire rapidement face aux perturbations. 68 % des responsables IT sont d'accord ou tout à fait d'accord sur le fait que le NaaS réduit la gestion quotidienne du réseau, laissant plus de temps aux équipes pour se focaliser sur l'innovation et la création de valeur.

# Comment le NaaS transforme-t-il les opérations réseau (NetOps) ?

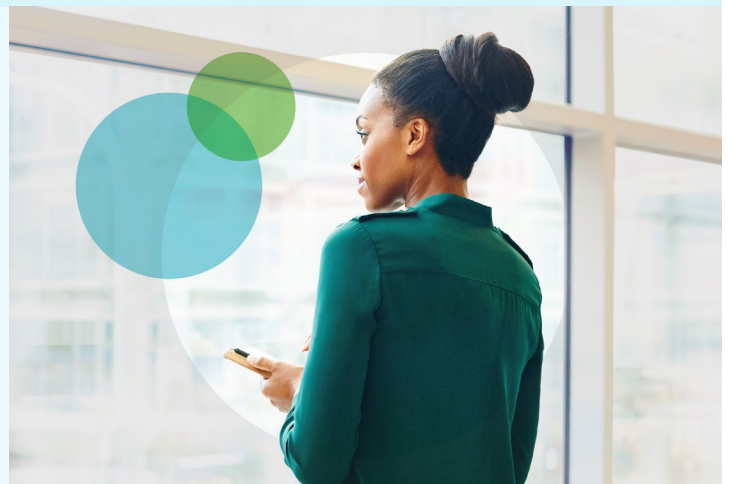
L'une des préoccupations récurrentes concernant les services NaaS est le transfert complet de la responsabilité des opérations réseau au fournisseur NaaS, ne laissant plus rien à faire à l'équipe d'exploitation réseau de l'entreprise. En réalité, le NaaS ne vous oblige pas à choisir entre tout ou rien en matière de responsabilité opérationnelle.

Dans un modèle NaaS, le fournisseur est responsable de tous les aspects de la gestion du cycle de vie du réseau.

Cela inclut le déploiement, l'intégration, le contrôle, la mise à jour, la surveillance et la réparation de tous les éléments de l'infrastructure réseau (y compris des équipements sur site des clients) requis pour atteindre les objectifs contractuels. Ces objectifs peuvent inclure le nombre d'utilisateurs connectés, de sites, de fournisseurs cloud et d'applications, ainsi que les niveaux de service, la bande passante, la performance des applications, le provisionnement de sécurité, la conformité et d'autres exigences.

Alors que reste-t-il à gérer ? L'équipe d'exploitation réseau du client des services NaaS peut consacrer plus de temps à des activités clés et créatrices de valeur.

Cela peut inclure, par exemple, la définition et la surveillance des objectifs réseau, comme les politiques d'accès des utilisateurs et des applications, et les niveaux de performance des applications. En surveillant les insights et les performances du réseau, l'équipe d'exploitation réseau du client peut continuellement s'adapter et optimiser les politiques et comportements réseau sur l'ensemble des domaines.

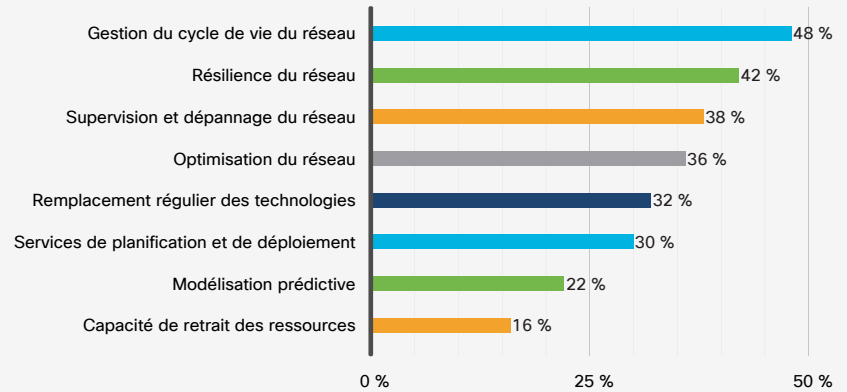


À l'aide d'API, l'équipe d'exploitation réseau du client gère également les intégrations entre le NaaS et les systèmes existants pour rationaliser les workflows et les processus IT. Elle peut aussi travailler en étroite collaboration avec le fournisseur NaaS pour s'assurer du respect des contrats de niveau de service (SLA) et des objectifs de niveau de service (SLO). Indépendamment des responsabilités opérationnelles et de leur transfert, ce qui ressort de cette recherche, c'est la volonté des professionnels de l'IT de réduire la charge de gestion de l'infrastructure.

48 % des professionnels de l'IT interrogés déclarent que la gestion du cycle de vie du réseau est le service le plus important à inclure dans un modèle NaaS. La résilience du réseau (42 %) ainsi que la supervision et la résolution des problèmes réseau (38 %) complètent le trio de tête. Cela confirme que la gestion d'un ensemble de sites, d'utilisateurs, d'équipements, d'applications et de ressources cloud de plus en plus distribués et complexes ne laisse que peu de temps pour les activités à valeur ajoutée et l'innovation.



Selon vous, lequel des services suivants doit être inclus en priorité dans un modèle NaaS ?



« Le fournisseur s'occupe des détails quotidiens. L'équipe interne se concentre sur la création de valeur par l'intermédiaire du réseau en s'adaptant aux nouveaux besoins. Nos ingénieurs et techniciens n'ont pas besoin de s'interrompre pour résoudre les problèmes. Ils peuvent se focaliser sur les nouveaux projets. »

– Ingénieur réseau, société de conseil internationale



### Résultat :

Dans un modèle NaaS, les responsabilités opérationnelles sont partagées. La charge de la gestion du cycle de vie du réseau est transférée au fournisseur, ce qui permet à l'équipe IT du client de se recentrer sur les activités opérationnelles qui créent de la valeur.

## Rôles, responsabilités et compétences

En transférant la maintenance de l'infrastructure et la gestion du cycle de vie à un partenaire externe, le NaaS libère beaucoup de temps en interne. Il permet aussi à l'équipe d'exploitation réseau du client de se focaliser sur ses objectifs pour le réseau, plutôt que sur les aspects opérationnels et technologiques de la maintenance de l'infrastructure.

En d'autres termes, les ingénieurs réseau passent du statut de « pilotes d'avion » à celui de « contrôleurs aériens ». Mais quels types de décisions doivent-ils prendre ?

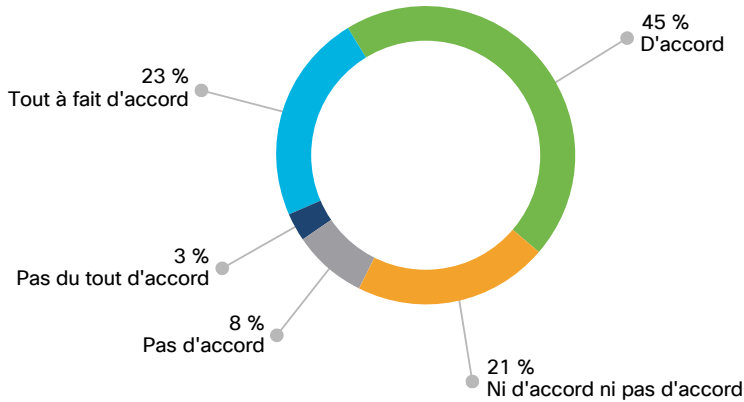
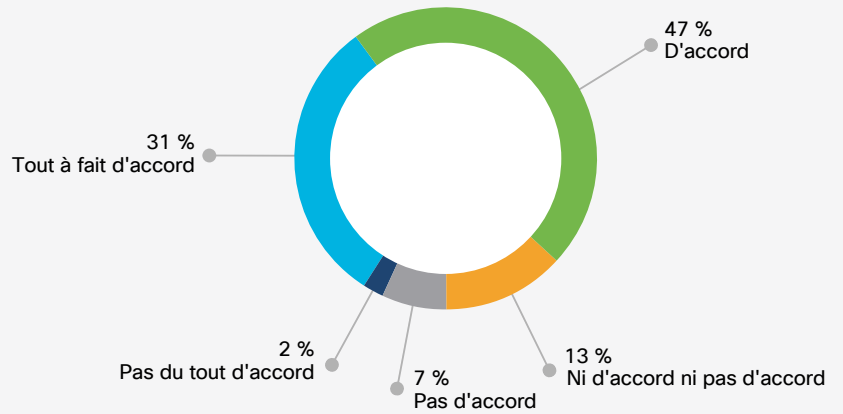
27 % des participants pensent que leurs équipes IT peuvent s'appuyer sur leur expertise technique et un tableau de bord NaaS pour traduire les besoins de l'entreprise en politiques réseau. De façon assez surprenante, 73 % des participants préfèrent que des fournisseurs tiers endossent ce rôle critique, révélant une possible pénurie de compétences ou un manque de confiance dans les compétences internes.



« La plus grande part des tâches quotidiennes étant transférée au fournisseur NaaS, l'équipe d'exploitation réseau du client se recentrera sans doute sur des compétences générales en matière de réseau et de sécurité, ainsi que sur des compétences en conception permettant de traduire les objectifs de l'entreprise en concepts réseau globaux. Elle doit travailler en étroite collaboration avec le fournisseur NaaS pour optimiser les conceptions, les politiques, les performances et les SLA du réseau. Et elle doit aussi pouvoir compter sur de fortes compétences en science des données pour identifier et orchestrer ces changements. »

– Joe Clarke, ingénieur expert, Cisco

L'adoption d'un modèle NaaS permettra aux membres de l'équipe réseau de monter en compétences et de créer de la valeur pour l'entreprise.



Le NaaS permettra à l'équipe réseau de consacrer plus de temps aux tâches de création de valeur et d'innovation IT plutôt qu'à la gestion quotidienne du réseau.



Résultat :

Plus de 75 % des entreprises sont d'accord ou tout à fait d'accord sur le fait que les modèles NaaS donneront à leurs équipes l'opportunité de monter en compétences et de créer plus de valeur.



## Préoccupations et hésitations

Le NaaS a des répercussions sur de nombreux domaines du département IT. Il nécessite de nouveaux modèles d'exploitation, de nouvelles intégrations avec les technologies et processus existants, des changements de rôles et de compétences, et une transition des CapEx vers les OpEx. Compte tenu de ces nombreuses implications, les professionnels de l'IT interrogés ont des réactions mitigées à l'égard des services NaaS. La plupart d'entre eux se situent aux extrémités du spectre : ils sont soit enthousiastes, soit réticents.

Les points de vue des responsables IT sur le NaaS reflètent leur philosophie en matière de réseau. Or,

ces philosophies sont principalement divisées en deux camps : celui du « contrôle IT » et celui de l'« IT agile ». Ceux qui suivent la première philosophie ont des équipes hautement qualifiées et sont fermement convaincus que ces dernières doivent posséder et contrôler entièrement la pile réseau. À l'inverse, le second groupe cherche à consolider son environnement IT, à réévaluer les tâches routinières par rapport aux tâches à valeur ajoutée, et à trouver des solutions pour se décharger d'une partie de la maintenance de l'infrastructure. Sans surprise, les entreprises œuvrant pour un environnement IT agile qui ont déjà migré une partie de leurs ressources IT vers le cloud sont très ouvertes aux solutions NaaS.

« Nous tardons à adopter le NaaS car nous pensons que le réseau ne recevra pas suffisamment d'attention et ne sera pas priorisé comme il le mérite, ce qui ne convient pas à notre environnement. »

– Responsable IT, réseaux, agence militaire américaine

Certains responsables IT avec lesquels nous nous sommes entretenus considèrent que leurs réseaux et processus sont uniques, et que le NaaS ne pourra pas résoudre leurs problématiques spécifiques.

D'autres s'inquiètent que le NaaS puisse bouleverser leur département IT.

Si les responsables IT partagent de nombreuses préoccupations, la perte de contrôle figure parmi les principales. 30 % des participants se demandent s'ils seront en mesure de répondre aux besoins futurs en adoptant un modèle NaaS. D'autres participants se préoccupent de la perte de contrôle au niveau de la sécurité (26 %) et de la performance (20 %). En réalité, le NaaS est conçu pour offrir une plus grande évolutivité à la demande et une prise en charge accélérée des nouvelles technologies. La sécurité, les performances et d'autres décisions importantes en matière de contrôle relèvent toujours de l'équipe IT, et non du fournisseur NaaS.

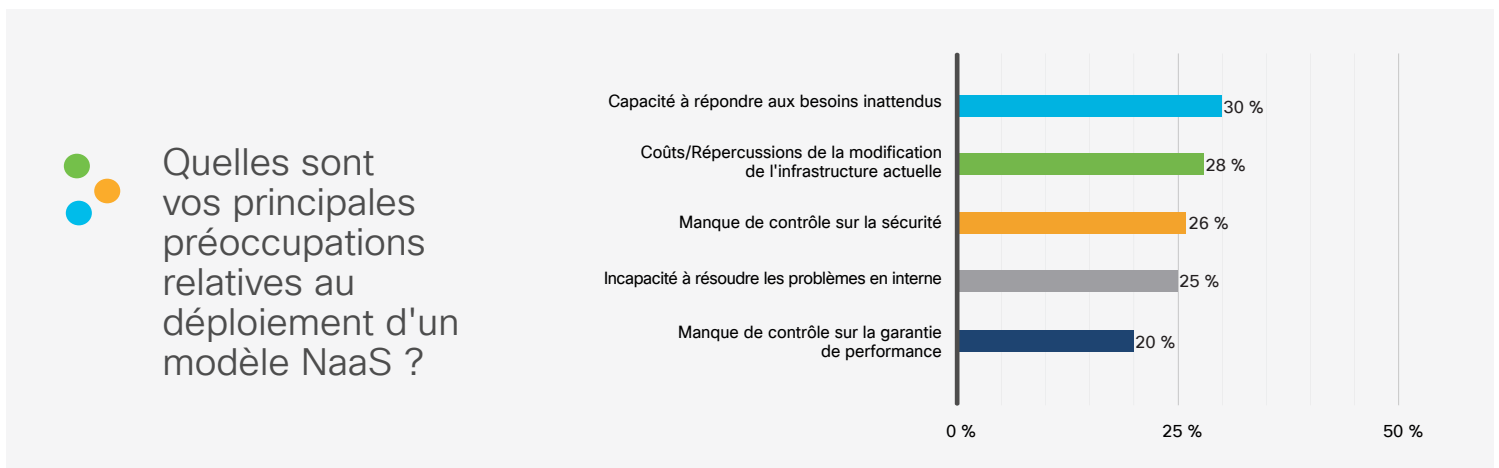




« Le fournisseur doit s'adapter à nos directives de sécurité et suivre nos instructions. C'est un facteur clé de différenciation du NaaS. »

– Architecte en chef, société technologique internationale

28 % des participants déclarent que le coût et les perturbations liés au changement de leur infrastructure et de leurs opérations existantes constituent des obstacles. Naturellement, les entreprises disposent d'une multitude de technologies et d'investissements, dont beaucoup relèvent de différents plans d'amortissement. Certaines disposent également de technologies et d'applications existantes qui ne sont pas forcément adaptées au NaaS. Et certaines ne veulent tout simplement pas confier à quelqu'un d'autre la gestion quotidienne de leur infrastructure.



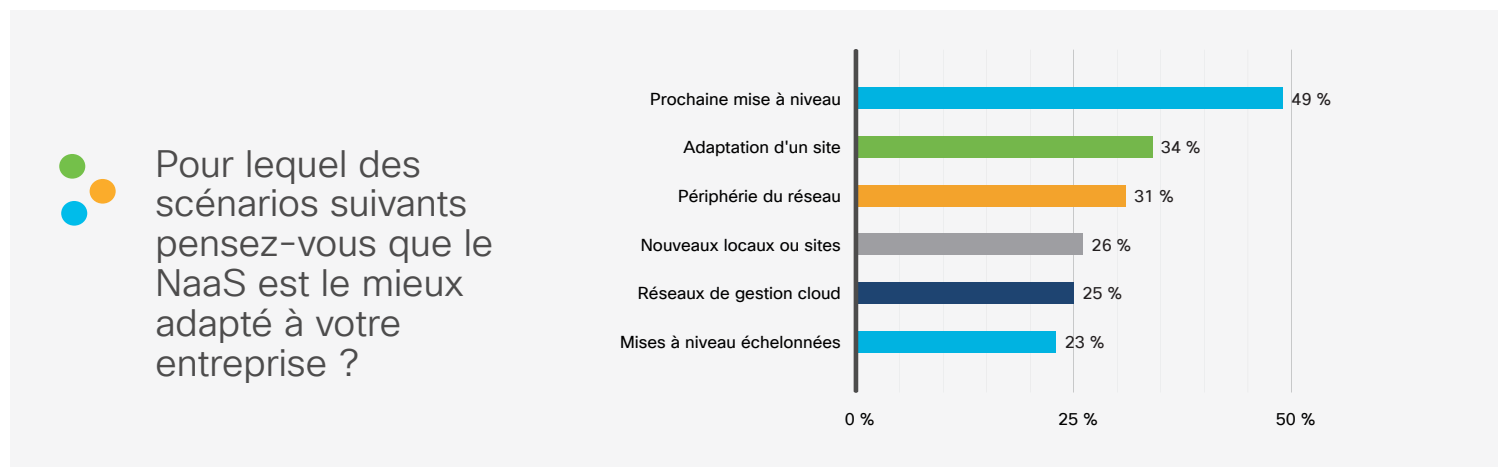
Face à ces préoccupations et hésitations, les entreprises peuvent choisir de tester le modèle NaaS en commençant petit, avec un seul domaine. Cela leur permet de mieux comprendre les fonctionnalités et les points de contrôle du NaaS sans modifier sensiblement leur infrastructure et leurs opérations réseau. Elles peuvent ainsi expérimenter et optimiser la répartition des responsabilités entre le fournisseur et leur équipe interne, et apprendre à collaborer pour optimiser les résultats. Une fois qu'elles connaissent et maîtrisent parfaitement les rôles, les responsabilités et les points de contrôle, elles peuvent aller plus loin et s'attaquer à d'autres domaines au fil du temps, en tirant parti des informations et des bonnes pratiques acquises au fur et à mesure.

**Résultat :**  
Tout modèle transformationnel soulève des inquiétudes. Les responsables IT peuvent commencer petit pour évaluer les risques et les bénéfices associés au NaaS et déterminer s'il est adapté pour leur entreprise.

## Tendances en matière d'adoption

En raison de ses répercussions sur les opérations réseau et de la diversité de ses possibilités d'exploitation, le NaaS n'est pas adopté de la même façon par chaque entreprise. L'évaluation du niveau de préparation au NaaS et la feuille de route de déploiement réduisent les complications potentielles et optimisent les chances de réussite.

49 % des responsables IT et 57 % des professionnels du réseau considèrent que la mise à niveau ou l'actualisation de l'infrastructure réseau, c'est-à-dire l'intégration d'une nouvelle technologie (automatisation, 100 Gigabit Ethernet, Wi-Fi 6, 5G, SD-WAN, SASE, etc.), constituent le meilleur moment pour adopter le NaaS. Pour 34 % des participants, l'adaptation d'un site sur lequel la technologie réseau a déjà été déployée constitue le scénario idéal pour l'adoption du NaaS. Il est intéressant de noter qu'ils sont seulement 26 % à penser qu'un nouveau site constitue le meilleur environnement pour déployer le NaaS. Ils sont seulement 23 % à déclarer qu'une approche progressive, où les domaines sont mis à niveau un par un avec le NaaS, constitue le meilleur scénario pour leur entreprise.



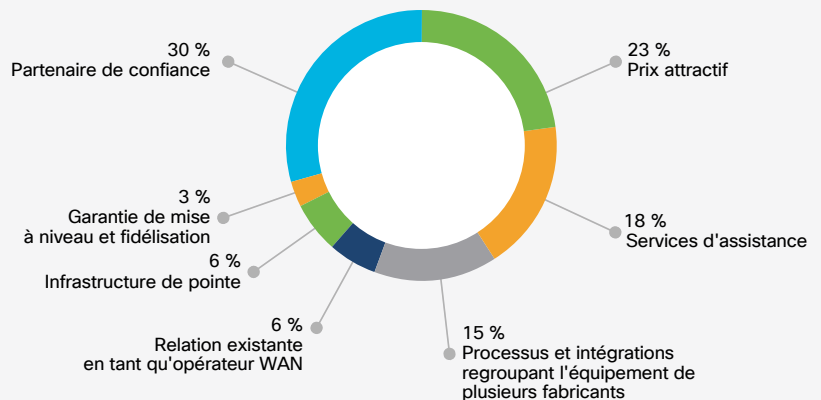
**Résultat :**  
La méthode, le moment et le motif de déploiement du NaaS varient pour chaque entreprise.

## Choisir un fournisseur NaaS

Le réseau étant un acteur essentiel de la productivité des équipes, des interactions clients et des opérations de l'entreprise, le choix d'un fournisseur de NaaS approprié n'est pas une tâche aisée. Certains responsables IT avec lesquels nous nous sommes entretenus sont très inquiets à l'idée de perdre le contrôle sur leur réseau. Toutefois, ils sont prêts à céder un peu de ce contrôle si, et seulement si, il est placé entre les mains d'un partenaire de confiance. Qu'il s'agisse de travailler avec un intégrateur système, un fournisseur de services managés ou un revendeur à valeur ajoutée, leur volonté est de pouvoir compter sur des partenaires établis qui connaissent déjà parfaitement leur environnement réseau, leurs objectifs métiers et les besoins d'assistance.

Pour leurs déploiements NaaS, près d'un tiers des professionnels IT interrogés considèrent que recourir à des intégrateurs de systèmes est plus fiable et plus abordable que de se tourner vers les opérateurs réseau. Ils nous disent également qu'une « expertise fiable » est beaucoup plus importante qu'une « infrastructure de pointe ».

Quelle est la raison principale pour laquelle vous préférez travailler avec un partenaire plutôt que directement avec un opérateur réseau pour votre déploiement NaaS ?

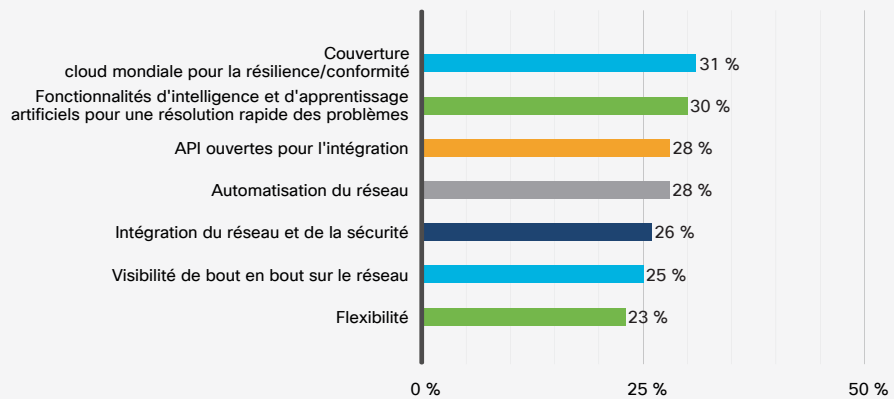


Lorsqu'il s'agit de traduire les besoins de l'entreprise en politiques techniques, les professionnels de l'IT sont deux à trois fois plus susceptibles de faire confiance à des intégrateurs de systèmes ou à leur équipe IT interne qu'à un fournisseur de services NaaS. Cela souligne le fait que les entreprises ne cherchent pas seulement une solution NaaS, mais aussi les conseils et l'assistance d'un expert de confiance qui les connaît bien.

Concernant les attributs techniques des fournisseurs et des solutions NaaS, les participants donnent la priorité aux partenaires bénéficiant d'une couverture cloud mondiale pour la fiabilité, la performance et la conformité aux règles locales (31 %), ainsi qu'aux fonctionnalités de machine learning (ML) et d'intelligence artificielle qui facilitent l'optimisation continue du service NaaS (30 %). Les API, l'automatisation, la sécurité intégrée, la visibilité et la flexibilité du réseau figurent également parmi leurs priorités.



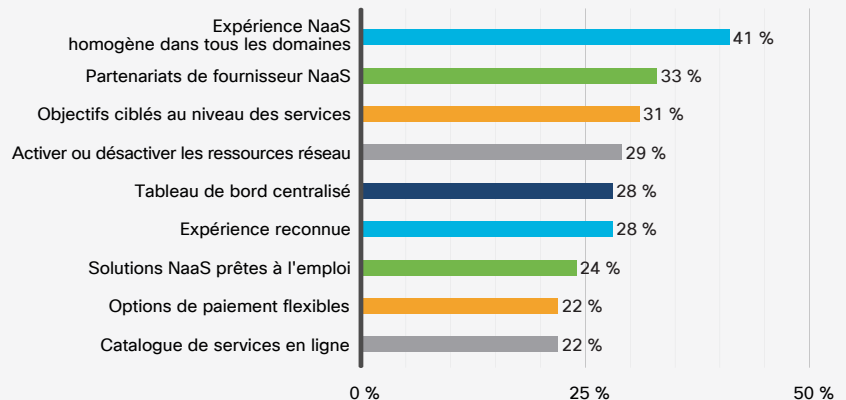
Selon vous, quels sont les 2 attributs techniques les plus importants d'une offre NaaS ?



41 % des participants déclarent qu'il est important qu'un fournisseur NaaS offre une plateforme cohérente sur l'ensemble des domaines réseau (accès, WAN, data center, cloud, etc.). Alors que de nombreuses équipes IT doivent jongler entre plusieurs environnements, jeux d'outils et modèles d'exploitation, le NaaS fournit une opportunité de consolider les ressources, les politiques et les opérations réseau.



Lequel des éléments suivants serait selon vous indispensable pour déployer la solution NaaS d'un fournisseur ?



« Je recherche un partenaire capable d'assurer les tâches de gestion routinières sur l'ensemble de notre réseau et de nos systèmes, comme les mises à jour des micrologiciels, les configurations et les modifications de l'environnement. Ainsi, mon équipe pourra se concentrer sur les améliorations, les évolutions et les implémentations de stratégies. Mais il nous faut aussi de la souplesse. Nous pouvons, par exemple, faire un travail important nous-mêmes pendant un mois, puis pendant les deux mois qui suivent, nous faisons appel à une aide extérieure pour étendre la portée du projet. »

– Vice-président, technologie et sécurité, société américaine à but non lucratif de 100 M de dollars US



Résultat :

Les intégrateurs de systèmes sont considérés comme plus fiables, abordables et orientés service que les fournisseurs NaaS. Quel que soit le partenaire, les clients attendent une expérience opérationnelle et des services qui couvrent tous les domaines du réseau.

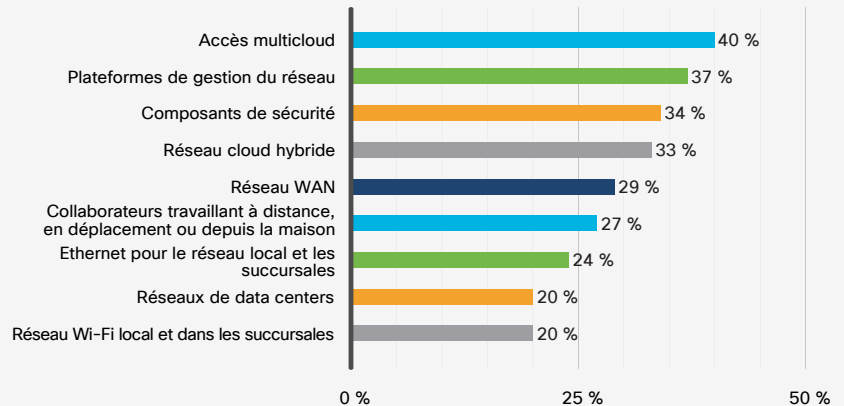


## La technologie SASE et les différents aspects du NaaS

Les offres de services NaaS sont toujours plus nombreuses : LAN filaires et sans fil, VPN, WAN, sécurité réseau, accès à distance ou en télétravail, réseaux de data center, réseaux cloud, etc. Selon notre étude, les modèles NaaS qui incluent l'accès et la sécurité multicloud sont les plus souhaitables. L'architecture SASE, qui fournit un accès multicloud sécurisé partout, est donc une offre en tant que service qui répond aux besoins de nombreux départements IT.

Compte tenu des difficultés liées aux connexions à plusieurs clouds disparates, il n'est pas surprenant que l'accès multicloud soit identifié comme une priorité (40 %) pour le NaaS. En proposant des services SD-WAN, les fournisseurs NaaS offrent une solution cohérente et optimisée de connexion à un large éventail d'applications basées dans le cloud (IaaS et SaaS).

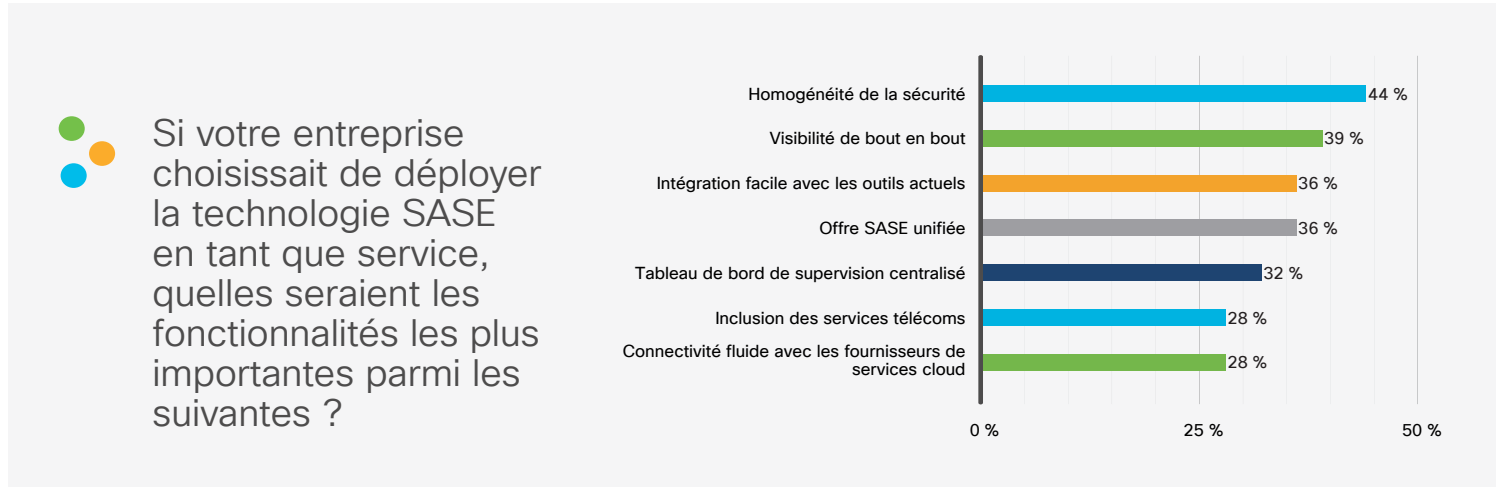
Quels aspects de l'équipement et de la gestion du réseau sont les plus adaptés au NaaS ?



34 % des participants donnent la priorité aux solutions NaaS axées sur la sécurité, comme le VPN, la gestion des informations et événements liés à la sécurité (SIEM), la passerelle web sécurisée, les pare-feu, et les services de détection et de prévention des intrusions (IPS/IDS). Ces solutions protègent les utilisateurs, les équipements et les applications de façon homogène à travers plusieurs clouds et environnements informatiques.

Les fournisseurs NaaS qui combinent l'accès multicloud et la sécurité au niveau des points d'accès sont bien placés pour répondre à la demande croissante en solutions SASE.

Près de la moitié (44 %) des participants considèrent « qu'une sécurité homogène, incluant la détection et le traitement des menaces, pour tous les utilisateurs et les équipements », quel que soit leur point d'accès, est une fonctionnalité essentielle de la technologie SASE. Compte tenu du caractère indispensable d'Internet pour l'accès aux applications cloud, plus d'un participant sur trois (39 %) cite « la visibilité et les informations sur le trafic réseau qui traverse les infrastructures Internet et cloud ». Enfin, ils sont 36 % à rechercher des solutions SASE qui s'intègrent facilement avec leurs outils actuels.



Si votre entreprise choisissait de déployer la technologie SASE en tant que service, quelles seraient les fonctionnalités les plus importantes parmi les suivantes ?



### Résultat :

L'accès multicloud et la sécurité sont des priorités pour le NaaS. Les fournisseurs qui intègrent une option SASE dans leur portefeuille NaaS sont en mesure de répondre à la demande croissante d'alignement et de sécurisation des ressources cloud et sur site.

# Conclusion

Nombreux sont les départements IT qui rencontrent des difficultés pour gérer la complexité du réseau, faire face aux perturbations, protéger les utilisateurs et les données, et s'adapter à l'accélération des activités de l'entreprise. Pour remédier à ces problématiques, ils choisissent pour la plupart d'investir dans de nouveaux modèles réseau, comme le NaaS.

Le réseau en tant que service (NaaS) fournit un accès continu aux technologies réseaux les plus récentes par le biais d'un modèle à la demande ou reposant sur des abonnements. Il transfère la charge de la gestion quotidienne du réseau à un fournisseur tiers. Ce faisant, il permet aux équipes IT de se concentrer sur des activités à valeur ajoutée qui améliorent l'agilité, la résilience et l'innovation.

Comme tout modèle révolutionnaire, le NaaS soulève des préoccupations et fait naître des hésitations. Pour autant, ce n'est pas tout ou rien. Les équipes IT peuvent travailler avec des partenaires de confiance pour tester le NaaS à petite échelle, évaluer les risques et les bénéfices, et déterminer s'il s'aligne avec leurs stratégies commerciales et technologiques globales.



## Ressources supplémentaires et assistance

[Qu'est-ce que le réseau en tant que service \(NaaS\) ? >](#)

[Solutions Cisco+ >](#)

[Rechercher un partenaire Cisco >](#)

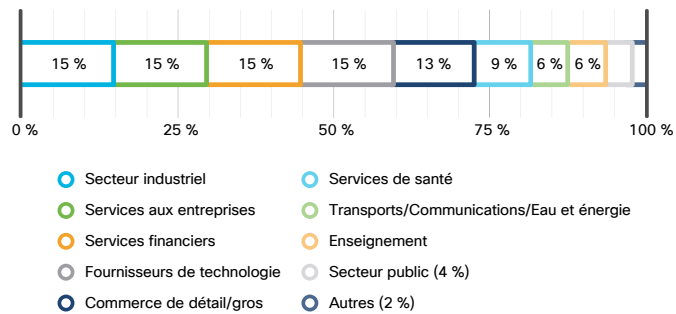
[Contacter un commercial Cisco >](#)

## À propos de ce rapport

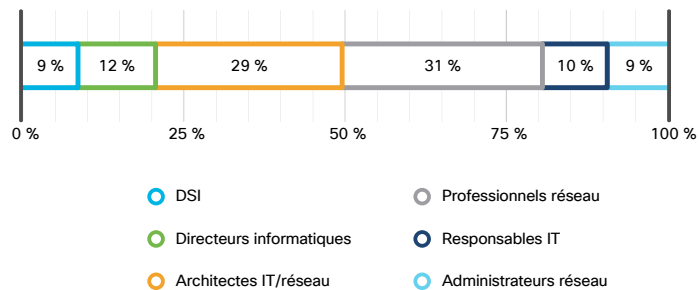
Publié pour la première fois en 2019, le [Rapport sur les tendances mondiales des réseaux](#) met en avant les toutes dernières stratégies et technologies en matière de cloud et de réseaux d'entreprises. Il s'appuie sur l'étude du secteur et fournit des perspectives, des informations et des conseils pour aider les départements IT à comprendre les tendances technologiques actuelles, à faire évoluer leurs modèles réseau et à prendre en charge les besoins dynamiques de l'entreprise.

Pour le rapport 2022, nous nous sommes entretenus avec 20 responsables IT et nous avons collecté l'avis de 1 534 professionnels de l'IT dans 13 pays sur le NaaS et son alignement potentiel avec leurs stratégies réseau, ou l'extension de ces dernières au cours des deux prochaines années. Les personnes interrogées pouvaient choisir jusqu'à trois réponses par question.

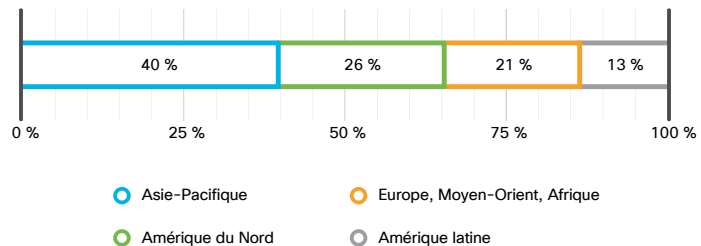
### Secteur d'activité des participants



### Rôle des participants



### Localisation des participants





## Autorisation d'utiliser ce rapport

Cisco invite et encourage la presse, les analystes, les fournisseurs de service et toutes personnes intéressées à utiliser les informations présentées dans ce rapport. Nous demandons cependant que le Rapport Cisco 2022 sur les tendances mondiales des réseaux soit mentionné lors d'une publication ou d'un partage de tout ou partie de ses données sous forme papier ou électronique – que ce soit pour un usage public ou privé (en insérant par exemple, « Source : Rapport Cisco 2022 sur les tendances mondiales des réseaux »). Aucun consentement supplémentaire n'est requis pour citer nos livres blancs, rapports et outils en ligne publics.

Nous adorons savoir dans quel contexte nos contenus sont utilisés. Lorsque notre contenu est utilisé, nous apprécions de recevoir un exemplaire des publications citant le Rapport Cisco 2022 sur les tendances mondiales des réseaux. Vous pouvez envoyer vos documents citant le Rapport Cisco 2022 sur les tendances mondiales des réseaux à l'adresse [networkingtrends-inquiries@cisco.com](mailto:networkingtrends-inquiries@cisco.com).

© 2022 Cisco et/ou ses filiales. Tous droits réservés. Cisco et le logo Cisco sont des marques commerciales ou déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, rendez-vous sur la [page dédiée](#) du site web de Cisco. Les autres marques commerciales mentionnées dans ce document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (2205R)

### Sources sur les tendances mondiales des réseaux en 2022

1. Préviation des opportunités, de la taille et de la dynamique du marché mondial du réseau en tant que service (NaaS) jusqu'en 2027, Report Ocean, mars 2021.