The bridge to possible
(Et vos ambitions prennent vie)

# Rapport sur les tendances mondiales des réseaux en 2023

Simplifier la connectivité multicloud sécurisée pour les collaborateurs dispersés géographiquement

The bridge to possible
(Et vos ambitions prennent vie)

# Rapport sur les tendances mondiales des réseaux en 2023

## Simplifier la connectivité multicloud sécurisée pour les collaborateurs dispersés géographiquement

## Sommaire

# Bienvenue

Le rapport annuel de Cisco sur les tendances mondiales des réseaux met en avant les stratégies et les technologies essentielles pour le cloud et les réseaux d'entreprises. Ce rapport combine les résultats d'études primaires et sectorielles avec le point de vue et les analyses de dirigeants pour identifier les dernières tendances technologiques et fournir des conseils aux équipes IT qui cherchent à faire évoluer leurs modèles réseau pour répondre aux besoins dynamiques de leur entreprise.

Dans cette édition 2023, nous analysons la manière dont les entreprises déploient et font évoluer leurs réseaux pour prendre en charge la connectivité sécurisée des applications, des personnes, des sites et des objets dispersés géographiquement. Nous avons interrogé plus de 2 500 responsables IT dans 13 pays en Amérique du Nord, en Amérique latine, en Asie-Pacifique et en Europe occidentale.

The bridge to possible
(Et vos ambitions prennent vie)

# Principaux enseignements : l'état du réseau pour la connectivité multicloud

## Le travail hybride complique encore la mise en place d'une connectivité sécurisée.

À l'ère du travail hybride, les entreprises doivent adopter de nouvelles approches pour connecter en toute sécurité les collaborateurs qui travaillent à distance aux données et aux ressources dispersées dans les environnements multicloud.

- Bien qu'ils soient encouragés à retourner au bureau, plus de 40 % des collaborateurs continuent le télétravail à temps plein ou quelques jours par semaine.
- La transition vers des applications déployées sur plusieurs clouds et des effectifs très dispersés rend les modèles de sécurité classiques obsolètes et représente un casse-tête pour les professionnels de l'IT. Plus de la moitié d'entre eux (51 %) font état de risques pour la sécurité dans le cloud et 39 % déclarent que l'augmentation du nombre de collaborateurs en télétravail constitue un défi majeur.

## La transition vers le cloud et le multicloud s'accélère.

Lorsque l'agilité de l'entreprise est en jeu, beaucoup considèrent le cloud comme la solution.

- Les entreprises continuent d'adopter des plateformes cloud : 78 % des personnes interrogées, contre 63 % à l'heure actuelle, déclarent que leur entreprise prévoit d'héberger plus de 40 % des workloads dans le cloud d'ici 2025.
- L'adoption du multicloud est également en hausse : 42 % des professionnels du cloud et du réseau déclarent que le développement plus agile et évolutif des applications est l'un des principaux motifs de l'adoption de plusieurs clouds.

## En 2023, sécuriser l'accès des utilisateurs aux applications cloud est le principal enjeu des réseaux.

Les professionnels de l'IT doivent également trouver des solutions pour maintenir une visibilité de bout en bout sur toute la chaîne de distribution de services numériques (par exemple, entre l'utilisateur et le cloud) et assurer une expérience homogène des applications.

- Pour 41 % des professionnels des réseaux, fournir un accès sécurisé aux applications réparties sur plusieurs clouds constitue un défi majeur.
- Le second défi, cité par 37 % des personnes interrogées, est de bénéficier d'une visibilité de bout en bout sur les performances et la sécurité du réseau, compte tenu de l'augmentation du trafic qui provient ou aboutit au-delà du périmètre du réseau de l'entreprise.

The bridge to possible
(Et vos ambitions prennent vie)

# Conseils essentiels : les stratégies réseau efficaces pour sécuriser l'accès aux applications cloud

## Faire converger le réseau et la sécurité

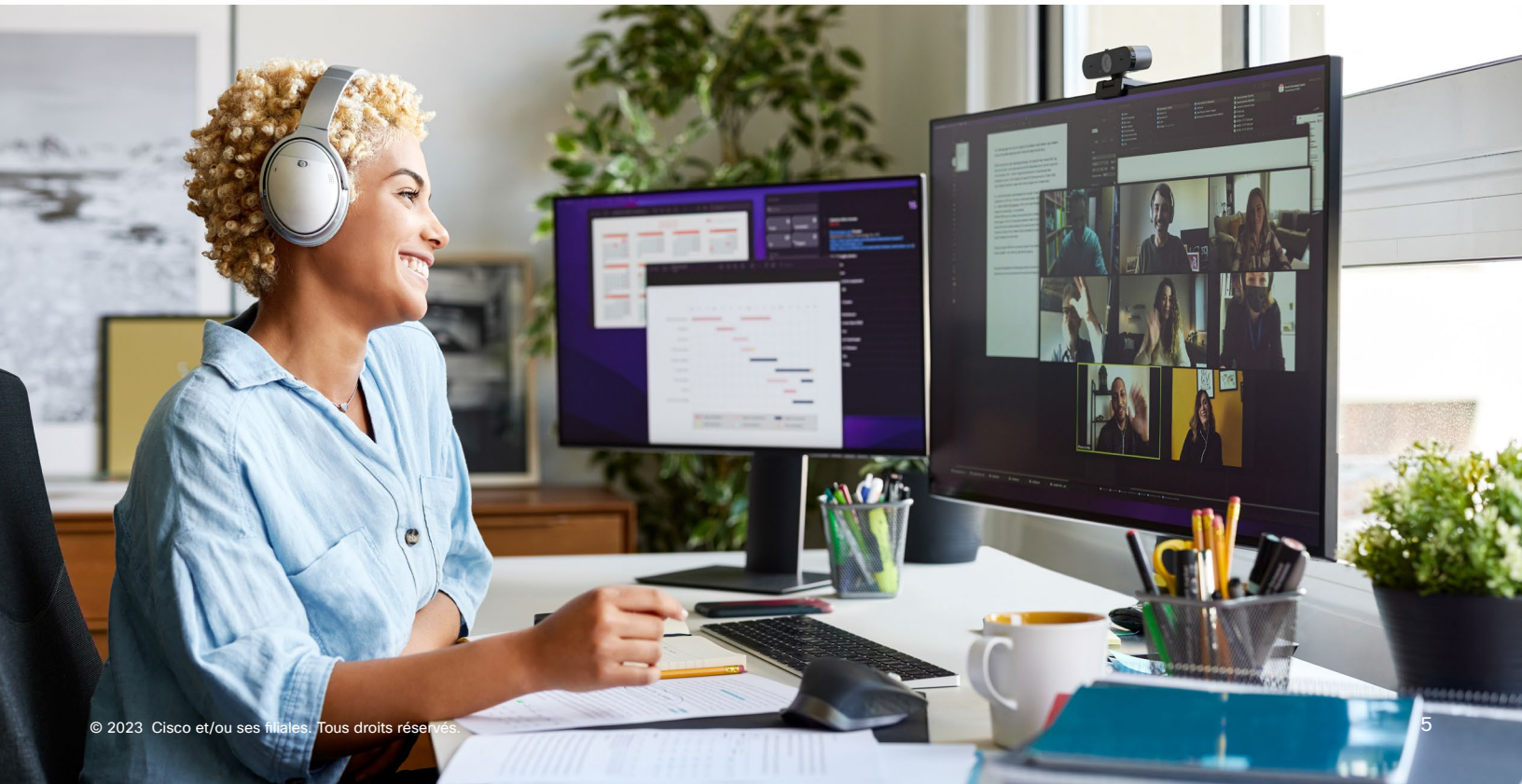
**Améliorez la collaboration entre les équipes IT pour simplifier les opérations, du réseau d'accès jusqu'au cloud.**

Les services cloisonnés et les modèles classiques de connectivité ne répondent plus aux besoins de sécurité dynamique des applications, des personnes, des lieux et des objets dispersés géographiquement.

- Avec des politiques standardisées, une télémétrie partagée et des workflows rationalisés sur l'ensemble des opérations de sécurité, réseau et cloud, les équipes IT obtiendront plus vite de meilleurs résultats IT et commerciaux qu'avec les technologies cloisonnées de leurs environnements actuels.
- Pour 40 % des personnes interrogées, les opérations cloisonnées compliquent la fourniture d'un accès sécurisé entre les sites distribués et les applications réparties dans plusieurs clouds.
- Selon les professionnels du cloud, les opérations réseau doivent être mieux alignées sur les opérations du cloud : 38 % souhaitent une intégration plus étroite avec les équipes réseau et 34 % ont pour principal objectif la cohérence opérationnelle.

**Opérez une transition vers un modèle de convergence du réseau et de la sécurité avec une architecture SASE.**

La sécurité au niveau des points d'accès (SASE) répond aux exigences de l'accès multicloud et du travail hybride en simplifiant les opérations et en fournissant des performances et une sécurité homogènes.



- Les entreprises font converger le SD-WAN (WAN sous forme logicielle) et la sécurité cloud pour déployer une architecture SASE.
- D'ici deux ans, 47 % des personnes interrogées prévoient de connecter leurs sites et leurs clients distants en étendant leurs environnements SD-WAN à une architecture SASE complète.

## Adopter un réseau et une sécurité axés sur le cloud

**Étendez la connectivité SD-WAN de façon homogène sur plusieurs clouds pour simplifier la gestion IT et améliorer l'expérience des applications.**

Appliquez des politiques de façon homogène dans tous les clouds pour automatiser la connectivité, quel que soit le cloud, afin de sécuriser et optimiser l'expérience des applications.

- En étendant la visibilité, le contrôle et l'accès Zero Trust aux fournisseurs cloud, SaaS et « middle-mile », les équipes IT peuvent fournir des expériences utilisateur de meilleure qualité et plus sécurisées.
- Plus de la moitié des personnes interrogées (53 %) vont donner la priorité à l'intégration avec les fournisseurs de services cloud pour améliorer la connectivité aux applications cloud à partir de tous les sites au cours des deux prochaines années.

**Évoluez vers une sécurité axée sur le cloud pour des opérations et des politiques cohérentes.**

En combinant les fonctions de sécurité dans une plateforme cloud, vous bénéficiez d'une visibilité, d'une gestion des politiques et d'un contrôle plus complets, plus simples et plus efficaces.

- Pour 59 % des personnes interrogées, la centralisation de la sécurité dans le cloud sera à mettre en place en priorité dans leur réseau d'accès cloud au cours des deux prochaines années, compte tenu de l'importance d'appliquer des politiques cohérentes pour tous les utilisateurs et les équipements, où qu'ils se trouvent.

## Passer à une approche proactive

**Offrez une expérience utilisateur homogène d'un bout à l'autre de la chaîne de distribution de services numériques de plus en plus complexe grâce à une visibilité totale sur le réseau.**

En l'absence d'une visibilité couvrant à la fois leur réseau, Internet et les environnements cloud, les équipes IT ne peuvent pas fournir une expérience d'utilisation des applications et des services cloud cohérente et de qualité.

- 51 % des personnes interrogées considèrent que la télémétrie et la visibilité complète sur le réseau sont indispensables pour détecter et résoudre les problèmes de façon proactive.
- La visibilité sur le trafic Internet et cloud est particulièrement importante lorsque la majorité des transactions des utilisateurs et des équipements transite au-delà du périmètre de l'entreprise.

**Passez d'une approche réactive à une approche prédictive pour améliorer la disponibilité et les niveaux de performance.**

L'analyse prédictive est de plus en plus reconnue comme un élément essentiel de l'intelligence artificielle pour les opérations IT (AIOps) et contribue à simplifier, accélérer et optimiser les opérations IT globales.

- Soucieuses d'éviter la dégradation des performances sur le réseau plutôt que de résoudre les pannes qui se produisent, 47 % des personnes interrogées vont donner la priorité aux analyses prédictives du réseau au cours des deux prochaines années.

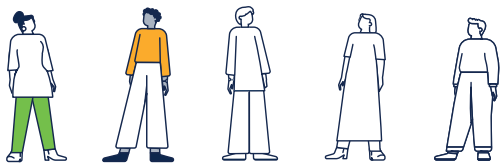
# Introduction : les tendances en matière d'accès multicloud

« Le réseau informatique pourrait un jour être organisé comme un service public, tout comme le réseau téléphonique est un service public, chaque abonné n'ayant à payer que pour la capacité qu'il utilise réellement. »[1] Ce discours prémonitoire a été prononcé par le professeur John McCarthy devant un auditoire du MIT en 1961.

Plus de six décennies plus tard, cette vision d'un réseau informatique partagé à la demande s'est non seulement concrétisée, mais elle est devenue l'un des principaux moteurs de la révolution numérique mondiale.

### La migration vers le multicloud se poursuit

Aujourd'hui, la plupart des entreprises ont adopté le multicloud. Le rapport Cisco 2023 sur les tendances mondiales des réseaux révèle que deux tiers des entreprises ont déjà réparti plus de 40 % de leurs workloads dans plusieurs clouds. Par ailleurs, la plupart des entreprises utilisent plus de deux fournisseurs de cloud et ont en majorité plus de cinq fournisseurs SaaS (voir la Figure 1).



**Deux personnes sur cinq travaillent à distance au moins une partie de la semaine.**

### Le travail hybride n'est pas prêt de disparaître

Les applications ne sont pas les seules à être très dispersées. Avec l'adoption globale du travail hybride, les personnes et les objets sont plus dispersés que jamais.

Selon une étude récente, même si 59 % des personnes sont retournées au bureau à temps plein, une grande partie continue à travailler à distance : 28 % en mode hybride et les 13 % restants en télétravail à plein temps.[2] Ces chiffres varient considérablement selon le secteur d'activité et la fonction.

Dans le même temps, l'adoption rapide de la technologie IoT et de l'edge computing multiplie le nombre de connexions et les milliers de milliards de données à gérer et protéger chaque jour.

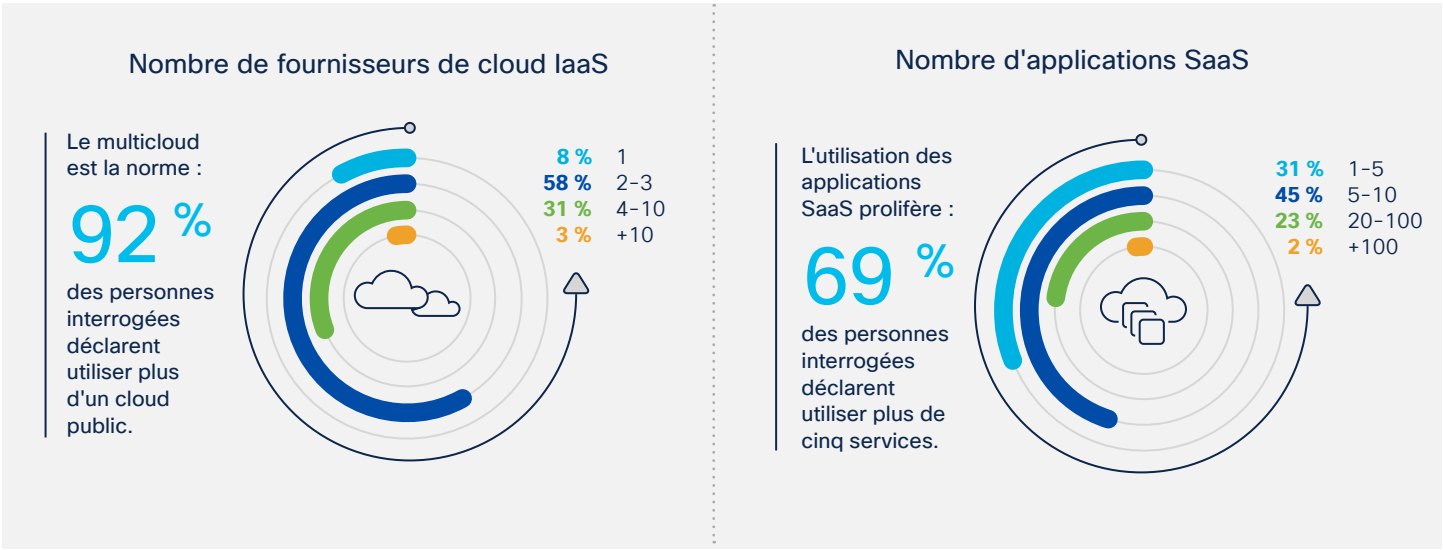



**Figure 1. L'utilisation de plusieurs fournisseurs de cloud et SaaS est devenue la norme.**

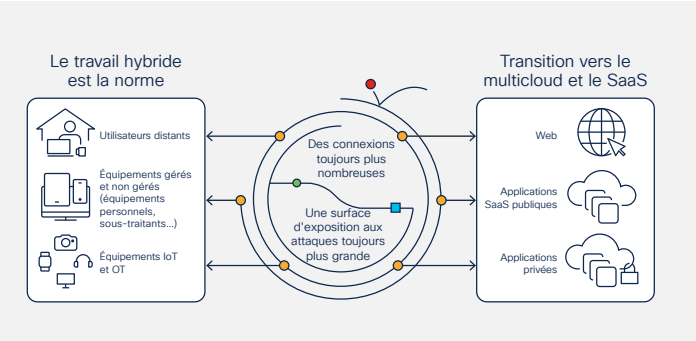



**Figure 2. Avec le travail hybride et la transition vers le cloud et le SaaS, la capacité humaine seule ne suffit plus à relever les défis liés à la sécurité du réseau.**

La dispersion des effectifs et la multiplication de l'IoT et de l'edge computing exigent la mise en place d'une connectivité et d'un accès sécurisés et évolutifs aux applications multicloud et aux services hébergés dans le monde entier, sur tous les réseaux (Figure 2). Les professionnels des réseaux considèrent qu'il s'agit du principal défi en 2023.

La connectivité sur Internet complique tout, puisqu'une partie de l'infrastructure échappe à la visibilité et au contrôle des professionnels du réseau et de la sécurité. Or, ils restent responsables de l'expérience numérique et de la protection de leurs collaborateurs, clients et partenaires.

### L'importance croissante de la vitesse et de l'agilité

Aujourd'hui, l'agilité est devenue un enjeu majeur pour la plupart des entreprises. Les résultats de l'enquête montrent que le principal motif de migration vers plusieurs clouds n'est pas le coût, comme l'avait prédit John McCarthy, mais le besoin d'agilité et d'innovation, et la nécessité de déployer rapidement de nouvelles applications et de nouveaux services de qualité. Suite à la pandémie, aux perturbations géopolitiques et économiques et aux problèmes rencontrés par le secteur logistique, la capacité à tirer rapidement parti des tendances du marché est devenue prioritaire.

Les entreprises ont compris que, dans l'environnement actuel, les technologies et les modèles d'exploitation cloisonnés sont trop contraignants et ne suffisent plus à répondre à leurs besoins. Elles doivent utiliser de nouveaux outils et processus. Les problématiques de connectivité et de sécurité exigent l'adoption d'une approche globale, favorisant la mise en place d'une infrastructure réseau et d'un modèle d'exploitation plus simples, plus sécurisés et plus souples.

« Les gens ne veulent pas attendre des semaines ou des mois pour atteindre leurs objectifs professionnels. Les entreprises doivent être en mesure de fournir des résultats immédiats et éliminer les goulots d'étranglement classiques. »

**– DSI, secteur du commerce de détail**

La prochaine partie de ce rapport traite de ces problématiques et fournit des conseils sur les bonnes pratiques à adopter pour déployer une connectivité flexible et sécurisée. Elle explique également comment et pourquoi les équipes en charge du réseau et de la sécurité doivent s'associer pour fournir aux collaborateurs, aux partenaires et aux clients, où qu'ils se trouvent, des expériences cloud fiables, sécurisées et robustes.

1 https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative

2 https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf

# Conseils essentiels : six bonnes pratiques pour fournir un accès sécurisé à plusieurs clouds

## Conseil essentiel nº 1 : améliorez la collaboration entre les équipes IT pour simplifier les opérations IT, du réseau d'accès jusqu'au cloud.

Les services cloisonnés et les modèles classiques de connectivité ne répondent plus aux besoins de sécurité dynamique des applications, des personnes, des lieux et des objets dispersés géographiquement.

Pour faire face à la complexité accrue et à l'augmentation de la surface d'exposition aux menaces, les responsables IT doivent améliorer la collaboration entre les équipes. Ils pourront ainsi répondre plus rapidement, plus efficacement et en toute sécurité à l'évolution rapide des besoins de l'entreprise.

La sécurité est au cœur de quatre des cinq principaux défis à relever pour fournir un accès aux applications multicloud (infrastructure en tant que service [IaaS] ou logiciel en tant que service [SaaS], par exemple) à partir de sites distribués. Pour 40 % des entreprises interrogées, les opérations cloisonnées, que ce soit au niveau du cloud, du réseau ou de la sécurité, compliquent la fourniture d'un accès sécurisé entre les sites distribués et les applications réparties dans plusieurs clouds.

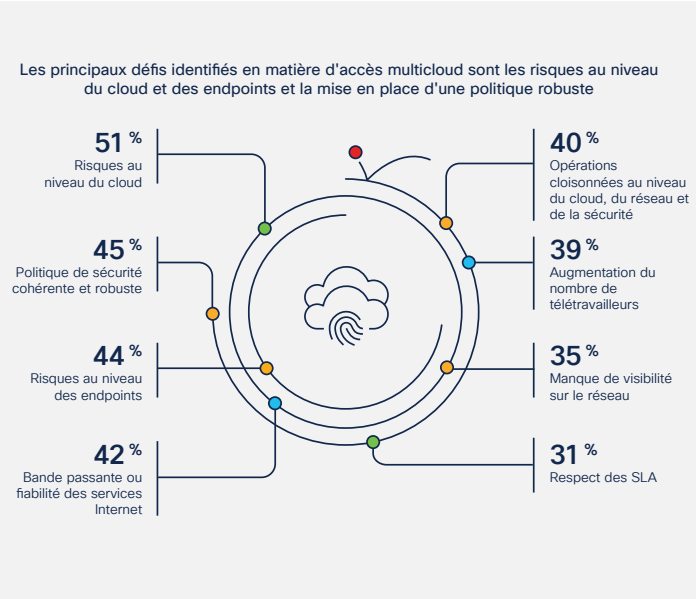



**Figure 3. Défis inhérents à la fourniture d'un accès sécurisé aux applications multicloud à partir de sites distants.**

La plupart de services IT s'appuient sur des équipes réseau et sécurité qui planifient et fonctionnent séparément. Pourtant, les responsables IT ne peuvent relever les défis actuels en matière de sécurité qu'en éliminant les silos technologiques et opérationnels et en réduisant le nombre d'intégrations ponctuelles de systèmes.

Pour aligner les équipes, les outils et les processus et rationaliser les opérations, ils doivent améliorer la

# 38 % des professionnels du cloud considèrent l'amélioration de l'intégration avec le réseau comme un défi opérationnel majeur.

cohérence de leurs modèles d'exploitation. Selon une étude Cisco, 86 % des DSI et des responsables IT reconnaissent la nécessité de développer un modèle d'exploitation plus cohérent couvrant les systèmes on-premise, SaaS, des clouds privés et des clouds publics.[3] Les principes du modèle d'exploitation cloud sont largement reconnus. Ils ont fait leurs preuves auprès des équipes DevOps et CloudOps en termes de simplification des opérations et de gain d'agilité. Les équipes IT peuvent bénéficier d'avantages similaires en adoptant les principes d'un modèle d'exploitation cloud. C'est ce que confirment les données de cette enquête : 38 % des professionnels du cloud déclarent que leur principal défi est d'améliorer l'intégration avec le réseau et 34 % qu'il est de préserver la cohérence opérationnelle entre le cloud et le réseau.

En appliquant les principes du modèle d'exploitation du cloud au réseau et à l'ensemble de la pile IT du cloud/réseau, les équipes IT peuvent accélérer l'innovation, améliorer la sécurité et éliminer les risques liés aux opérations cloud. Elles peuvent réduire la complexité et la fragmentation qui entravent la collaboration entre les équipes de sécurité, réseau et cloud, et ainsi répondre aux besoins dynamiques de leur entreprise.

### À retenir

En faisant converger le réseau et la sécurité sur la base d'un modèle d'exploitation cloud permettant de couvrir l'ensemble des politiques, des technologies, des outils et des workflows opérationnels, les entreprises peuvent utiliser des outils communs et mettre en place une connectivité sécurisée permanente, tout en augmentant l'efficacité et en réduisant les risques.

3 https://ebooks.cisco.com/story/accelerating-digital-agility-2021/page/7/1

## L'avis des experts

**L'alignement solide des équipes contribue à améliorer la sécurité, la simplicité et les performances.**

« Autrefois, l'équipe chargée des opérations connaissait chaque couche et chaque système, du câblage aux applications, et elle gérait tout globalement. Nous devons revenir à ce modèle.

Certes, le réseau cloud est différent du réseau on-premise et l'entreprise ne contrôle plus tous les équipements et logiciels de l'écosystème, mais le besoin de sécurité reste le même. Pour sécuriser l'accès aux applications cloud partout où l'utilisateur se trouve et quel que soit l'équipement, nous avons surtout besoin de politiques cohérentes, qui contribueront à combiner la conception, les opérations et l'architecture.

À l'avenir, les équipes en charge du réseau et de la sécurité seront plus nombreuses à collaborer sur une infrastructure de bout en bout, en se basant sur des principes de sécurité et de simplicité, et pas seulement sur les performances opérationnelles, pour atteindre le même objectif. »

**Wendy Nather**
Responsable des services de conseil RSSI, Cisco

## Conseil essentiel nº 2 : opérez une transition vers un modèle de convergence du réseau et de la sécurité avec une architecture SASE.

La sécurité au niveau des points d'accès (SASE) répond aux exigences de l'accès multicloud et du travail hybride en simplifiant les opérations et en fournissant des performances et une sécurité homogènes.

Pour cela, elle fait converger le réseau et la sécurité, fournissant le cadre indispensable à la connexion sécurisée et fluide des utilisateurs aux applications dans des environnements complexes et très distribués.

L'architecture SASE est en passe de devenir l'architecture de convergence de prédilection pour l'accès multicloud sécurisé. Dans les deux ans à venir, 47 % des personnes interrogées prévoient de connecter leurs sites et leurs clients distants principalement à l'aide d'un modèle SASE.

Cependant, beaucoup d'entreprises peinent à exploiter le plein potentiel de l'architecture SASE, car leurs solutions n'intègrent pas certaines fonctionnalités ou ne permettent pas de faire totalement converger le réseau et la sécurité.

La convergence SASE repose sur un réseau SD-WAN robuste combiné à une solution de sécurité cloud ou SSE (Security Service Edge) avancée (Figure 4). Les équipes IT ne peuvent tirer pleinement parti des bénéfices du modèle SASE que lorsque ces architectures sont entièrement convergées. Ces bénéfices incluent un modèle d'exploitation rationalisé qui améliore la cohérence et simplifie au maximum la visibilité, la gestion et le contrôle de la connexion sécurisée des utilisateurs, où qu'ils se trouvent.

Grâce aux politiques standardisées, à la télémétrie partagée et aux alertes coordonnées sur l'ensemble des composants de sécurité et de réseau, la solution SASE unifiée permet aux équipes NetOps et SecOps d'améliorer l'efficacité, la performance et la protection de l'environnement IT. L'amélioration de l'efficacité et de la cohérence du modèle d'exploitation et des workflows entre les équipes NetOps et SecOps contribue invariablement à optimiser l'expérience utilisateur.

Les implémentations SASE complètes améliorent l'efficacité opérationnelle, optimisent les expériences

« La sécurité au niveau des points d'accès (SASE) offre des fonctionnalités convergées de réseau et de sécurité en tant que service : SD-WAN, SWG, CASB, pare-feu de nouvelle génération et accès réseau Zero Trust (ZTNA). Le modèle SASE prend en charge les cas d'usage des sites distants, des télétravailleurs et des accès sécurisés sur site. Le modèle SASE est déployé en tant que service et fournit un accès Zero Trust basé sur l'identité de l'équipement ou de l'entité, combiné à un contexte en temps réel et à des politiques de sécurité et de conformité. »

**– Glossaire IT de Gartner, Secure Access Service Edge (SASE), version du 2 mai 2023.**

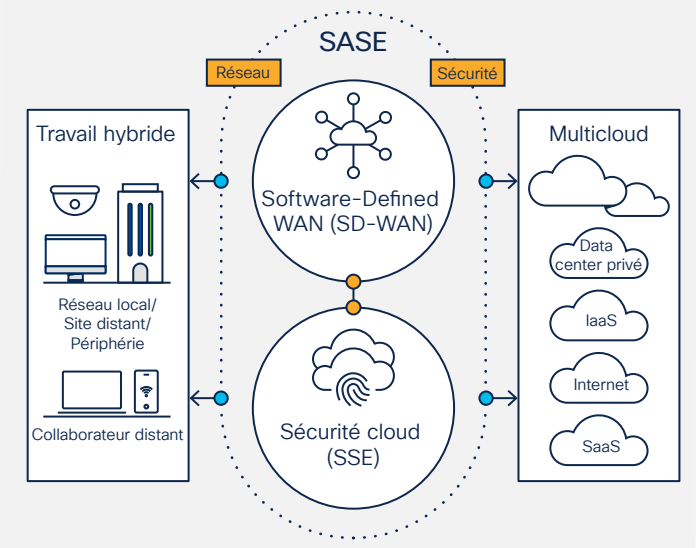



**Figure 4. La convergence des opérations et des technologies de réseau et de sécurité offre un nouveau modèle de connectivité sécurisée : la sécurité au niveau des points d'accès.**

The bridge to possible
(Et vos ambitions prennent vie)

Selon les prévisions de Gartner®, d'ici 2025, 50 % des achats de réseau SD-WAN feront partie d'une offre SASE contractée auprès d'un seul fournisseur, contre moins de 10 % en 2021.[4]

utilisateur et renforcent la protection. Voici quelques exemples de ces bénéfices :

- L'équipe IT interne de Cisco fait état d'une réduction de 40 % des dépenses d'exploitation grâce au modèle SASE.
- L'évaluation rigoureuse des performances par une société de test indépendante a révélé qu'Umbrella (un composant central de Cisco SASE) associé à des politiques de sécurité permettait d'obtenir d'aussi bons résultats (voire meilleurs) que l'accès non sécurisé aux applications SaaS via Internet.
- L'étude client menée par TechValidate montre que 85 % des clients de Cisco réduisent de 50 % les infections par malwares grâce à la mise en place d'une architecture SASE.

Deux approches élémentaires permettent d'atteindre les résultats souhaités.

La première repose sur des produits réseau et de sécurité/SSE distincts, généralement fournis par un ou deux fournisseurs, qui peuvent être intégrés dans une solution SASE complète. Cette approche peut être utilisée par les entreprises qui ont déjà déployé un SSE ou un SD-WAN, et nécessitent davantage de personnalisation et de souplesse.

La deuxième est une approche unifiée qui déploie tous les composants réseau et de sécurité sous la forme d'un service cloud clé en main unique avec une gestion unifiée. Une solution SASE unifiée et bien conçue permet de gagner en rapidité et en simplicité et d'accélérer la rentabilisation.

4 Feuille de route stratégique pour la convergence SASE en 2022, Gartner, Neil MacDonald, Andrew Lerner, John Watts, juin 2022. GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses filiales aux États-Unis et dans le reste du monde, et est utilisée ici avec son autorisation. Tous droits réservés.

## L'avis des experts

**Une solution SASE répond à des critères précis.**

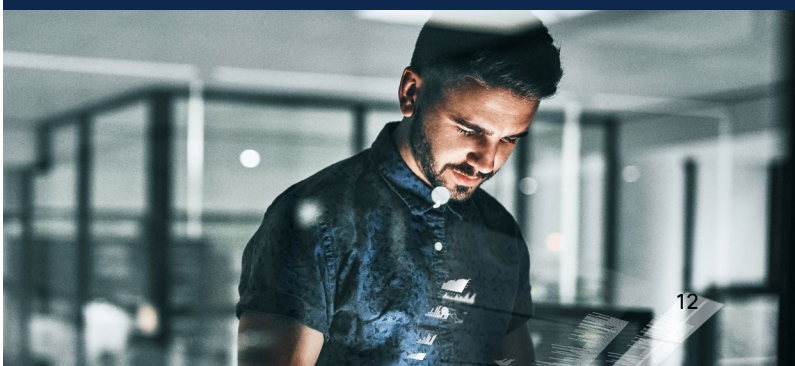
« Chaque entreprise peut être tentée d'ajouter simplement les fonctionnalités SASE manquantes à sa base technologique installée existante. Toutefois, il faut savoir que le modèle SASE est un choix stratégique à long terme et que le simple déploiement de tous les composants d'un modèle SASE sans un niveau élevé d'intégration ne constitue pas une solution SASE entièrement fonctionnelle et ne permet pas d'atteindre les résultats souhaités.

En fonction de leurs priorités, les responsables du réseau et de la sécurité doivent opter pour une solution SASE bien intégrée ou pour un service unifié clé en main.

En optant pour un service cloud unifié clé en main, les équipes NetOps et SecOps bénéficient d'une gestion centralisée avec mise en application distribuée intelligente, ainsi que de contrôles et d'une visibilité sur les endpoints, la périphérie du réseau de l'entreprise et la périphérie du cloud. Elles peuvent ainsi déployer une solution complète plus sécurisée, qui améliore sensiblement l'expérience utilisateur.

« Quelles que soient les technologies et architectures mises en place pour mieux répondre à vos besoins, votre fournisseur doit s'engager sur le long terme à combiner tous les composants dans un système intégré ou unifié. »

**Omri Guelfand**
Vice-président de la gestion des produits, NaaS/SASE
Cisco Meraki



### À retenir

Contrairement aux solutions de sécurité classiques, l'architecture unifiée et centrée sur le cloud du modèle SASE permet de centraliser la gestion des politiques de sécurité et de les appliquer aux utilisateurs et aux applications, fournissant une connectivité souple, fluide et sécurisée.

[En savoir plus sur le modèle SASE](#)

## Conseil essentiel nº 3 : étendez la connectivité SD-WAN de façon homogène sur plusieurs clouds pour simplifier l'expérience IT et améliorer l'expérience des applications.

Appliquez des politiques de façon homogène dans tous les clouds pour automatiser la connectivité, quel que soit le cloud, afin de sécuriser et optimiser l'expérience des applications.

Le cloud est devenu une extension du réseau de l'entreprise. Pour beaucoup, le SD-WAN est devenu le tremplin vers une implémentation SASE complète. En automatisant l'extension de la fabric SD-WAN avec les principaux fournisseurs IaaS, SaaS et « middle-mile », les équipes IT bénéficient d'un meilleur contrôle opérationnel pour déployer une expérience utilisateur optimale.

L'optimisation du contrôle de l'expérience de l'utilisateur est une priorité claire des équipes réseau : 53 % des personnes interrogées déclarent donner la priorité à l'intégration avec les fournisseurs de services cloud pour améliorer la connectivité aux applications cloud à partir de sites distribués. Les équipes réseau prennent des mesures : 49 % des personnes interrogées déclarent qu'elles vont donner la priorité aux intégrations SD-WAN et multicloud au cours des 24 prochains mois.

Les intégrations multicloud SD-WAN permettent aux équipes réseau et cloud d'accélérer et d'automatiser les extensions des sites de l'entreprise vers les différents fournisseurs cloud et les autres sites de l'entreprise via Internet, les interconnexions ou la colocation et les réseaux des fournisseurs cloud (Figure 5). Ces intégrations permettent aux administrateurs d'optimiser l'expérience des applications et de créer une expérience opérationnelle plus cohérente sur tous les sites cloud et on-premise. En outre, les équipes IT peuvent fournir un accès

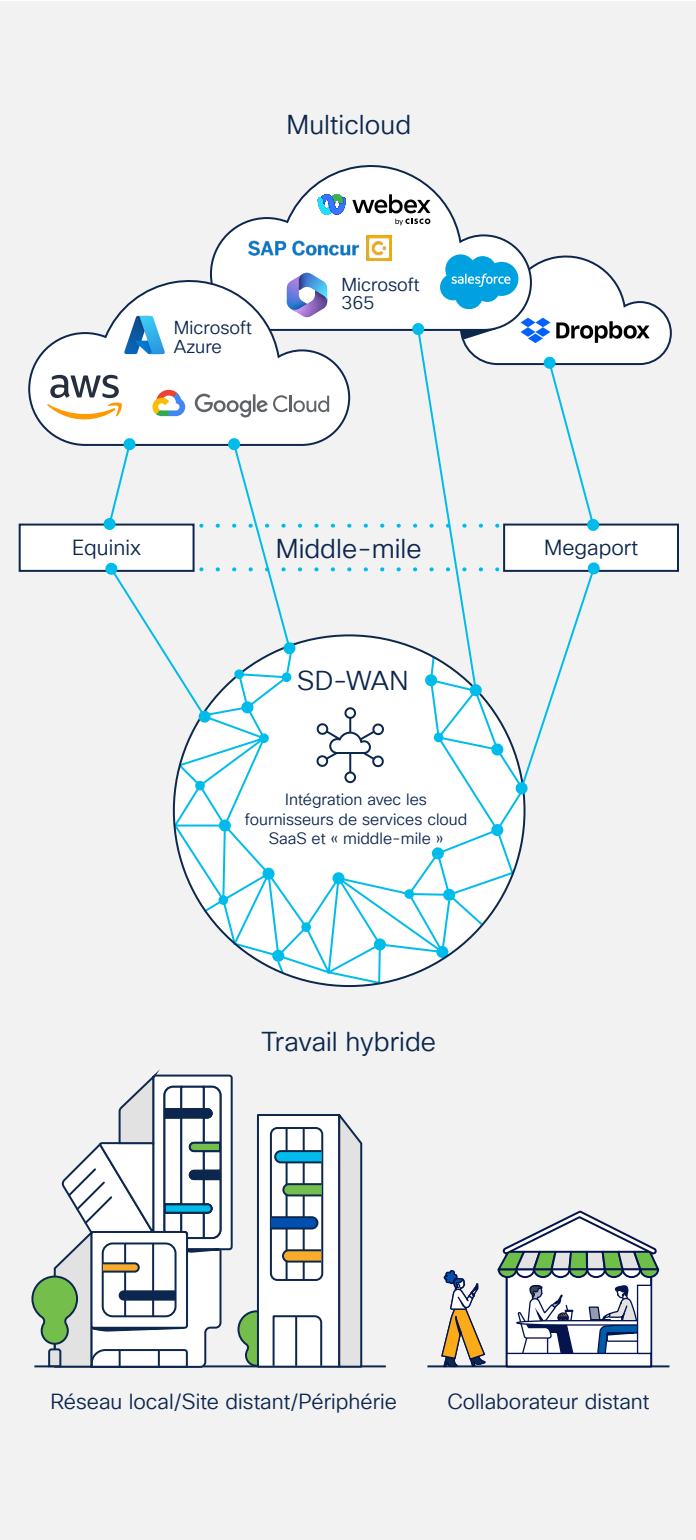



**Figure 5. Les intégrations du SD-WAN avec les fournisseurs IaaS, SaaS et « middle-mile » sont essentielles pour améliorer l'expérience IT et utilisateur.**

sécurisé et évolutif aux applications et points de présence cloud via l'intégration avec des fournisseurs mondiaux d'interconnexion réseau, tels qu'Equinix et Megaport. Ces intégrations permettent aux équipes IT de créer un réseau mondial de façon simple et automatisée en quelques minutes.

**À retenir**

Les intégrations multicloud pour le SD-WAN sont essentielles pour toute équipe IT qui souhaite accélérer et simplifier les extensions de l'entreprise à un ou plusieurs cloud, optimiser l'expérience des applications de l'utilisateur et mieux sécuriser les applications cloud grâce à l'accès Zero Trust.

En savoir plus sur Cisco SD-WAN

## L'avis des experts

**Nous ne pouvons pas ignorer la complexité et les risques de la connectivité multicloud.**

« Dans un monde axé sur le cloud, il est inimaginable de déployer une solution SD-WAN ne prévoyant pas des intégrations étroites avec les principaux fournisseurs cloud, SaaS et « middle-mile ». Les clients peuvent accélérer leur transition vers le cloud en automatisant l'extension de la fabric SD-WAN entre leurs sites mondiaux et leurs workloads cloud. Ils profitent ainsi d'opérations réseau simplifiées, du chiffrement de bout en bout et de la souplesse nécessaire pour accélérer l'innovation.

Par ailleurs, compte tenu de l'évolution et de l'augmentation des menaces associées à l'utilisation d'applications cloud et SaaS distribuées, les réseaux doivent répondre à une approche « Zero Trust » et adopter ses principes fondamentaux : « ne jamais faire confiance d'emblée, toujours vérifier et appliquer le principe du moindre privilège ». En intégrant le SD-WAN avec une approche Zero Trust, les entreprises peuvent déployer une stratégie de sécurité qui contrôle les accès aux services cloud, automatiser le contrôle de la sécurité du trafic admis, assurer la mise en œuvre continue des politiques et s'adapter immédiatement aux changements d'état de la sécurité. »

**JL Valente**
Vice-président, gestion des produits, routage d'entreprise, réseau SD-WAN et cloud
Cisco

## Conseil essentiel nº 4 : évoluez vers une sécurité axée sur le cloud pour des opérations et des politiques cohérentes.

En combinant les fonctions de sécurité dans une plateforme cloud, vous bénéficiez d'une visibilité, d'une gestion des politiques et d'un contrôle plus complets, plus simples et plus efficaces.

Le travail hybride se généralisant, les utilisateurs utilisent à la fois des équipements professionnels et personnels. Par ailleurs, ils accèdent à un nombre croissant d'applications sur des réseaux gérés et non gérés, à l'intérieur et à l'extérieur du périmètre du réseau de l'entreprise. La protection classique du périmètre ne suffit plus. Par conséquent, la priorité des équipes IT est d'assurer la protection globale des endpoints, des applications et des données.

Traditionnellement, les politiques de sécurité appliquées aux collaborateurs en télétravail étaient différentes de celles appliquées aux équipes qui travaillent sur site. Les politiques de sécurité à distance ont différents niveaux de confiance et sont gérées par des outils de sécurité distincts. La prise en charge de politiques disparates augmente la charge de travail de l'équipe IT et peut être source de frustration pour les utilisateurs. Selon cette étude, 45 % des personnes interrogées considèrent qu'une politique de sécurité robuste et cohérente est indispensable pour fournir un accès multicloud sécurisé à partir de sites distribués.

En plus de gérer la protection constante contre les cybermenaces, les équipes de sécurité doivent régulièrement mettre à jour les politiques de sécurité des applications pour l'ensemble des collaborateurs dispersés, ce qui incite fortement à centraliser la sécurité pour l'ensemble des utilisateurs géographiquement dispersés. De fait, 59 % des personnes interrogées déclarent que la centralisation de la sécurité du cloud sera leur principale priorité pour le réseau d'accès au cloud au cours des 24 prochains mois (Figure 6).

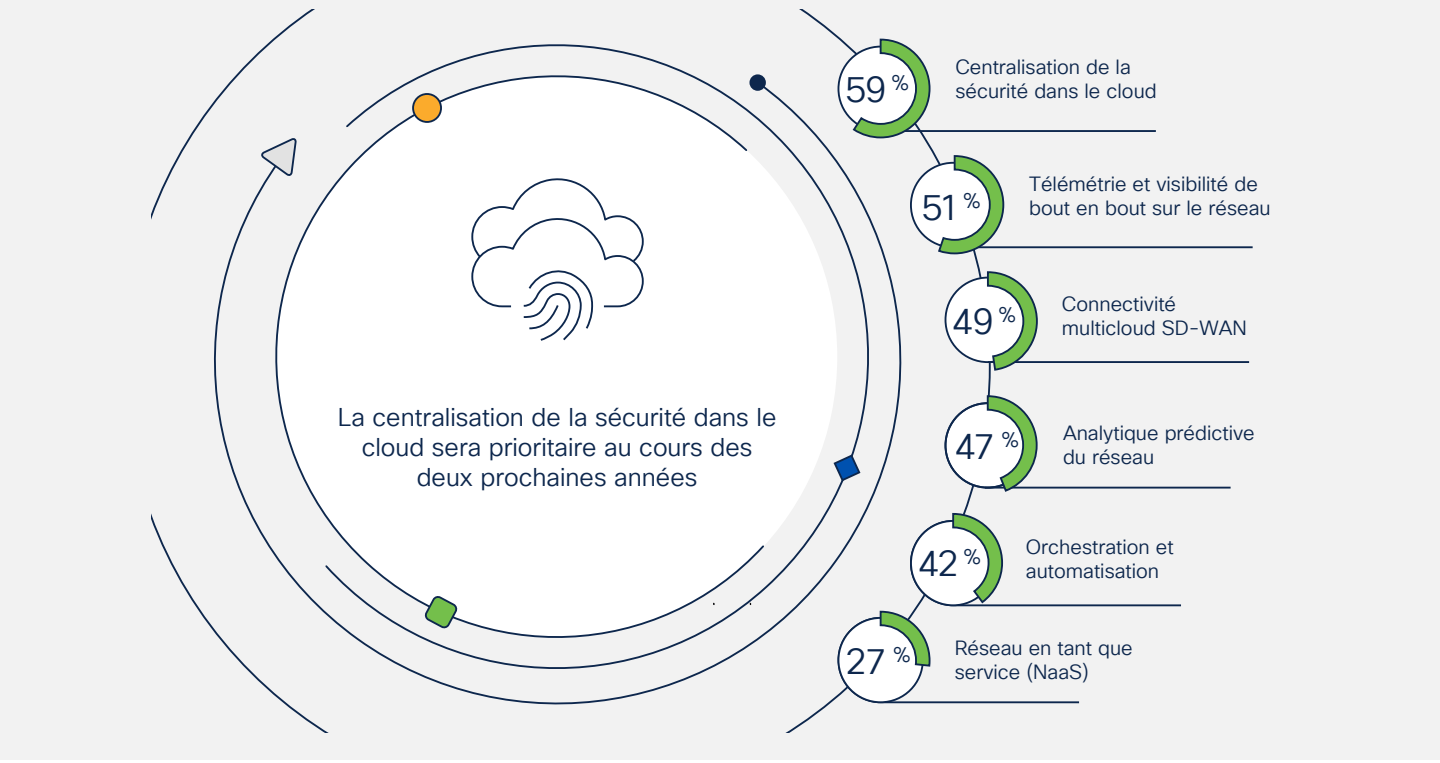



**Figure 6. Principales priorités en matière de réseau d'accès au cloud au cours des 24 prochains mois.**

Les systèmes de défense classiques ne suffisent plus à assurer une protection efficace. Pour sécuriser l'accès aux applications et aux workloads à grande échelle à l'aide de votre solution de sécurité cloud centralisée, vous avez besoin d'un système plus intelligent. C'est le rôle du SSE, pilier central de l'architecture SASE.

**À retenir**

Le travail à distance, le BYOD et la multiplication des services cloud ont rendu obsolètes les périmètres de sécurité auparavant clairement définis. Comme la plupart des applications utilisées quotidiennement résident dans le cloud, les entreprises doivent concevoir une stratégie SSE complète qui consolide plusieurs fonctionnalités de sécurité et les distribue efficacement depuis le cloud.

## L'avis des experts

**La convergence de la sécurité cloud est la clé d'un modèle centralisé et intégré.**

« Pendant des années, les entreprises ont ajouté des produits de sécurité ponctuels pour faire face aux menaces toujours plus nombreuses. Elles ont ainsi amélioré leur sécurité, mais elles sont aujourd'hui dépassées par la complexité opérationnelle croissante. Le passage à une solution SSE permet de profiter de fonctions de sécurité cloud natives, évolutives et convergées (passerelle web sécurisée, services de sécurité pour l'accès au cloud, accès réseau Zero Trust et pare-feu en tant que service) pour optimiser l'expérience utilisateur, renforcer la sécurité et réduire la charge de travail des équipes IT.

En choisissant ce type d'approche intégrée et centralisée, vous simplifiez les tâches de gestion, vous améliorez la performance à grande échelle, vous bénéficiez d'une meilleure visibilité et vous renforcez la sécurité dans toute l'entreprise. Une solution SSE convergée est essentielle dans une architecture SASE complète. »

**Jeff Scheaffer**
Vice-président, Gestion des produits, Sécurité/SSE
Cisco

## Conseil essentiel nº 5 : offrez une expérience utilisateur homogène d'un bout à l'autre de la chaîne de distribution de services numériques de plus en plus complexe grâce à une visibilité totale sur le réseau.

En l'absence d'une visibilité couvrant à la fois leur réseau, Internet et les environnements cloud, les équipes IT ne peuvent pas fournir une expérience d'utilisation des applications et des services cloud cohérente et de qualité.

L'amélioration de l'expérience utilisateur est un objectif important pour les équipes IT. Pour optimiser l'expérience, les équipes réseau ne se limitent plus aux outils classiques et adoptent des solutions qui améliorent la visibilité en temps réel sur les événements à l'intérieur et à l'extérieur de leur réseau. En mettant en corrélation ces indicateurs étendus avec les performances des applications, les équipes IT peuvent exploiter les informations obtenues pour optimiser l'expérience numérique des collaborateurs et des clients.

Les entreprises accélèrent leur adoption des solutions SaaS et cloud et utilisent de plus en plus les réseaux publics comme Internet pour fournir un accès à ces applications. Ces réseaux à sauts multiples sont par ailleurs de plus en plus complexes et il devient donc indispensable d'investir dans des solutions avancées de visibilité. Plus de la moitié des entreprises interrogées (51 %) reconnaissent qu'il s'agit d'une priorité et se concentrent sur l'amélioration de la télémétrie et de la visibilité sur le réseau de bout en bout.

Toute transaction d'application peut traverser plusieurs réseaux, segments de réseau et services (Figure 7), rendant difficile le suivi des performances et de la disponibilité d'une application spécifique. Près de la moitié (48 %) des personnes interrogées reconnaissent la nécessité de donner la priorité aux informations et à la visibilité sur Internet pour améliorer la connectivité. Les équipes IT ont donc besoin d'outils pour visualiser le chemin complet des transactions, y compris dans

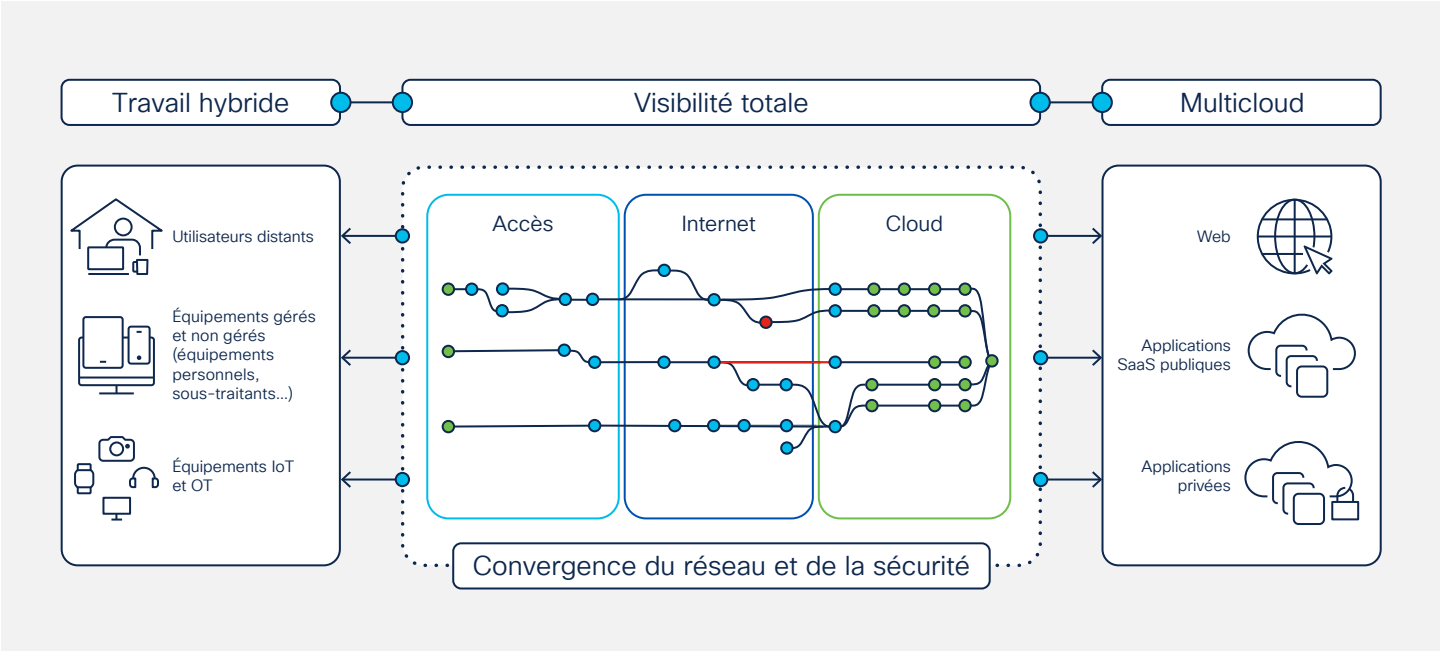



**Figure 7. La connexion des environnements distribués via Internet gagne en complexité, ce qui exige une meilleure visibilité de bout en bout.**

les réseaux et les environnements externes qu'elles ne contrôlent pas ou ne possèdent pas.

**À retenir**

Le cloud est le nouveau data center, Internet est le nouveau réseau et les offres cloud dominent les applications. En bénéficiant d'une visibilité sur l'intégrité d'Internet à l'échelle mondiale et les performances des principales applications SaaS, les équipes IT peuvent détecter et résoudre de manière proactive les problèmes réseau ou applicatifs majeurs inattendus dès qu'ils se produisent.

## L'avis des experts

**Considérez Internet comme le nouveau réseau principal de votre infrastructure.**

« Les chaînes d'approvisionnement de l'expérience numérique ont évolué, passant d'un domaine unique à des systèmes et réseaux multi-parties et collaboratifs. Les utilisateurs peuvent se trouver n'importe où. Les applications sont conçues pour être agiles et reposent sur des API et des microservices distribués. Les entreprises doivent fournir une expérience fluide sur un grand nombre de services, d'applications, de clouds et de réseaux, alors qu'elles ont moins de contrôle qu'avant.

Les expériences numériques modernes doivent donc s'appuyer sur une nouvelle approche de la visibilité et du contrôle, permettant aux équipes de détecter et diagnostiquer rapidement les perturbations et de les corréler avec les problèmes d'infrastructure et de réseau, quel que soit le domaine (domicile, bureau, cloud ou Internet). Pour cela, elles doivent avoir accès aux bonnes données au bon moment. Elles doivent pouvoir les collecter et les relier facilement en interne en couvrant l'ensemble des applications, du réseau et de l'infrastructure, avec un écosystème connecté qui intègre des fournisseurs tiers. »

**Joe Vaccaro**
Vice-président, Gestion des produits
ThousandEyes, Cisco

## Conseil essentiel nº 6 : passez d'une approche réactive à une approche prédictive pour améliorer la disponibilité et les niveaux de performance.

L'analyse prédictive est de plus en plus reconnue comme un élément essentiel de l'intelligence artificielle pour les opérations IT (AIOps) et contribue à simplifier, accélérer et optimiser les opérations IT globales.

Comme le réseau étendu est indispensable au bon fonctionnement des entreprises, toute dégradation du service ou interruption est intolérable. Les responsables IT veulent pouvoir identifier et résoudre les problèmes de façon proactive avant qu'ils ne se produisent et ne détériorent l'expérience utilisateur.

Avec l'avènement des plateformes de gestion cloud, les entreprises ont accès à des données de télémétrie historiques et en temps réel provenant d'un plus grand nombre de sources. Les modèles d'analytique prédictive ont été améliorés grâce à l'intelligence artificielle et à l'apprentissage automatique. Ils permettent désormais d'obtenir des informations exploitables basées sur toutes ces données historiques et en temps réel. Les entreprises peuvent ainsi comprendre les schémas identifiés par les données, et anticiper et résoudre efficacement les problèmes avant qu'ils n'impactent le réseau. Ces modèles deviennent de plus en plus intelligents à mesure qu'ils reçoivent les données fournies par une boucle de rétroaction continue.

47 % des personnes interrogées vont donner la priorité à l'adoption de l'analytique prédictive du réseau pour améliorer la connectivité du cloud au cours des deux prochaines années.

La proactivité des opérations IT est indispensable pour fournir des services cohérents et performants aux utilisateurs à distance qui accèdent aux applications cloud distribuées. Cette capacité est considérée comme essentielle par 47 % des personnes interrogées, qui prévoient de donner la priorité à l'adoption de l'analytique prédictive du réseau

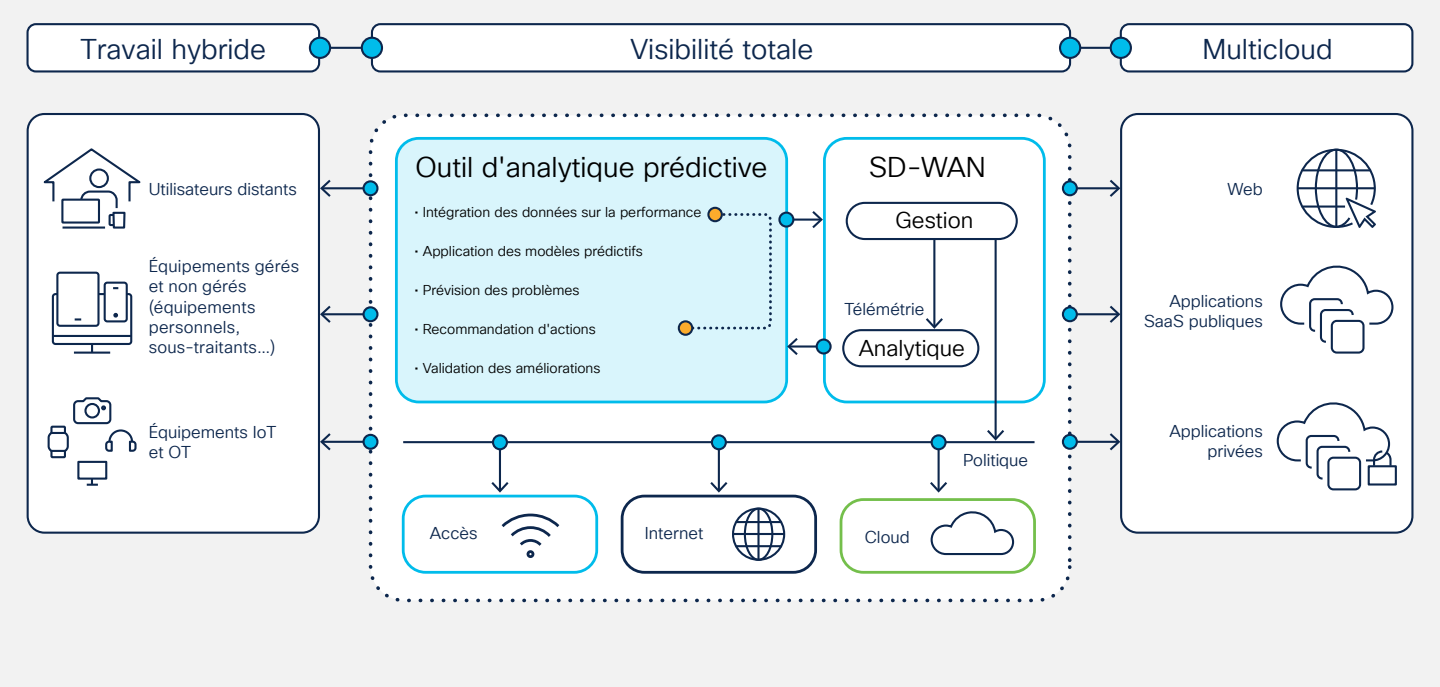



**Figure 8. Intégrer l'analytique prédictive à la gestion du SD-WAN pour identifier et empêcher la dégradation du réseau avant qu'elle ne nuise à l'expérience utilisateur.**

pour améliorer la connectivité cloud au cours des deux prochaines années.

**À retenir**

La vitesse, le coût et la qualité des expériences numériques sont menacés par l'évolution continue d'Internet. Pour améliorer la flexibilité et la résilience de l'infrastructure, les entreprises doivent adopter des modes de fonctionnement prédictifs et des workflows opérationnels proactifs optimisés progressivement par des boucles de rétroaction continues de données.

## L'avis des experts

**L'analytique prédictive, rendue possible par la technologie, est devenue un outil indispensable pour les équipes IT.**

« Les modes opérationnels réactifs classiques redirigent le trafic vers d'autres chemins, mais seulement après avoir détecté un problème (souvent causé par une connectivité défaillante ou une dégradation des services). L'analytique prédictive permet d'utiliser la télémétrie, les données statistiques et les modèles informatiques basés sur l'intelligence artificielle et l'apprentissage automatique pour prévoir les problèmes potentiels avant qu'ils ne se produisent. Les environnements axés sur le cloud sont par nature imprévisibles. La recommandation automatique d'actions ou la redirection proactive du trafic sont des capacités essentielles pour optimiser les performances et limiter les risques d'interruption du système. Elles permettent aux entreprises d'améliorer l'expérience utilisateur et aux équipes IT de se concentrer sur les initiatives stratégiques au lieu de réagir aux problèmes. »

**Murtaza Doctor**
Vice-président, Ingénierie
ThousandEyes, Cisco

# Conclusion

Le télétravail et le travail hybride ne sont pas prêts de disparaître. L'adoption du multicloud s'accélère. Pourtant, il est encore compliqué de fournir une connectivité sécurisée et cohérente aux collaborateurs, aux équipements et aux applications très dispersés en raison de l'accroissement des menaces et de la complexité des outils et techniques utilisés par les équipes chargées du réseau, du cloud et de la sécurité.

Seules, ces équipes ne peuvent pas résoudre ces problématiques de connectivité et de sécurité ni offrir les expériences numériques et l'agilité dont les entreprises ont besoin pour rester compétitives. La plupart des responsables IT le savent. C'est pourquoi ils regroupent leurs technologies réseaux, cloud et de sécurité, et testent des modèles d'exploitation innovants pour répondre à ces besoins en constante évolution.

La migration vers un modèle SASE est l'une des approches privilégiées : près de la moitié des entreprises interrogées prévoient de déployer une architecture SASE bien intégrée pour connecter leurs sites et leurs clients distants d'ici deux ans. Le modèle SASE promet de simplifier et de sécuriser davantage l'expérience IT, grâce à une solution simple et souple de connexion des collaborateurs et des clients dispersés aux applications cloud à grande échelle. En combinant des plateformes réseau et de sécurité qui prennent en charge l'automatisation dans le cloud et les analyses du réseau, il améliore l'intégration des workflows et la collaboration entre les équipes NetOps et SecOps.

Un modèle SASE axé sur le cloud s'appuie sur les données pour fournir des fonctionnalités essentielles au déploiement d'une expérience utilisateur cohérente (comme la visibilité de bout en bout et l'analytique prédictive).

Vous pouvez entamer votre transition vers un modèle SASE de plusieurs manières en fonction de vos priorités commerciales et technologiques.

Apprenez-en plus sur le modèle SASE et découvrez comment Cisco peut vous aider à réaliser votre transition.

The bridge to possible
(Et vos ambitions prennent vie)

## À propos de ce rapport

Le rapport sur les tendances mondiales des réseaux a été compilé en février 2023 sur la base d'enquêtes menées dans 13 pays d'Amérique du Nord, d'Amérique latine, d'Asie-Pacifique et d'Europe occidentale.

Cette année, le rapport s'appuie sur des données recueillies auprès de professionnels des opérations réseau au sein d'entreprises utilisant des services cloud. Ces données fournissent des informations sur la façon dont les environnements multicloud influencent les priorités, les préférences et les choix en matière de technologie et d'exploitation du réseau.

Les données présentées dans ce rapport ont été commandées par Cisco, collectées par 451 Research, qui fait partie de S&P Global Market Intelligence, et analysées par Cisco. Elles font partie d'une enquête indépendante menée sur le web auprès de plus de 2 500 décisionnaires IT et professionnels du cloud computing, du DevOps et des réseaux d'entreprises à travers le monde.

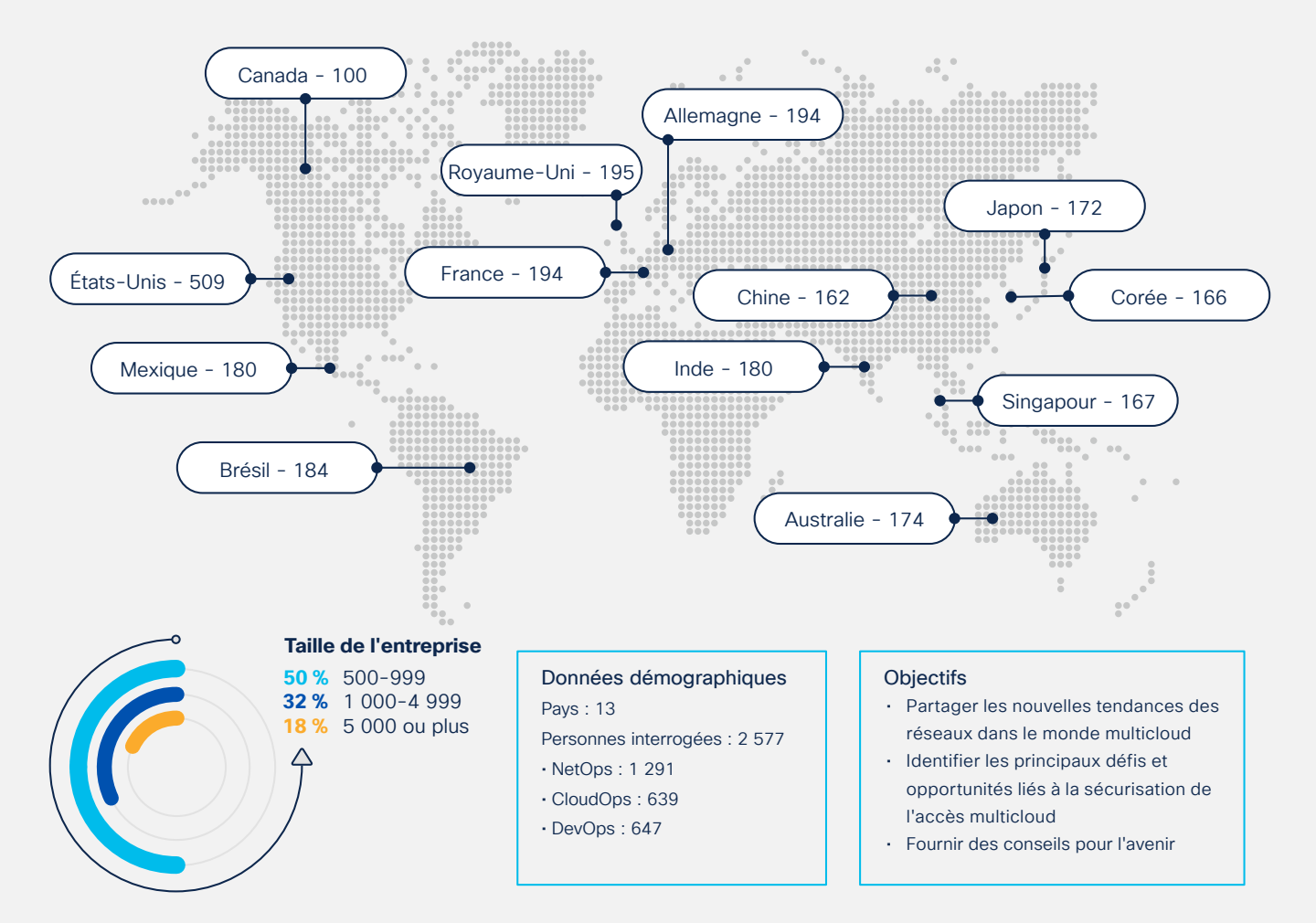



**Figure 9. Méthodologie et objectifs de l'étude de Cisco sur les tendances mondiales des réseaux en 2023.**