Rapport d’étude



L’impact de l’intelligence artificielle agentique sur les opérations réseau

Rapport d’étude 2026 de Cisco et d’Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Table des matières

01 Synopsis

02 Les TI ne peuvent plus résoudre leurs problèmes de personnel par le seul recrutement

03 Le réseau comporte plus d'angles morts que vous ne le pensez

04 Le consensus sur l'autonomie est déjà acquis

05 Les conditions de la confiance

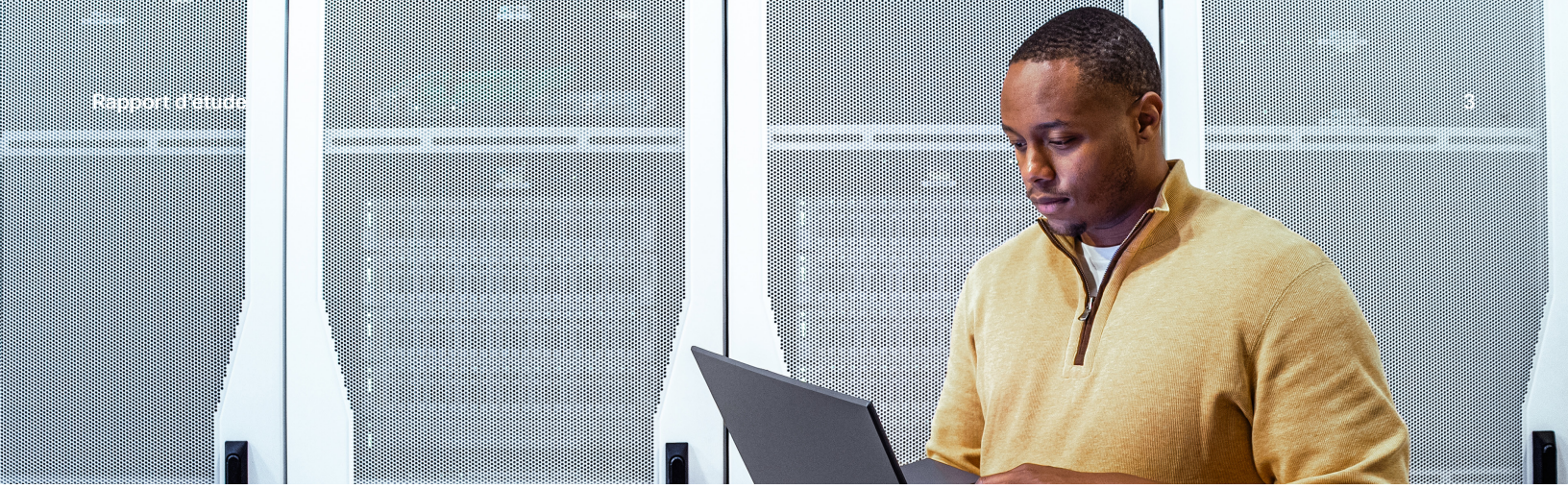
06 L'écart organisationnel qui pourrait freiner son adoption

07 Les premiers résultats confirment son efficacité

08 Les douze mois décisifs

09 À propos de cette étude

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



01 Synopsis

Le débat sur le rôle de l'intelligence artificielle dans l'exploitation des réseaux est désormais pratiquement clos.

Dès qu'il est question d'intelligence artificielle agentique dans les opérations réseau, la discussion revient presque toujours au même point : la confiance. Les entreprises céderont-elles réellement le contrôle? Une étude indépendante d'Omdia, appuyée par une analyse de données agrégées de télémétrie réseau menée par Cisco, laisse entendre que cette question est déjà dépassée.

Selon 1 000 responsables des opérations informatiques et réseau, cette transition est déjà bien amorcée. Les trois quarts des organisations ont déjà déployé l'intelligence artificielle pour les opérations réseau. La moitié exploitent déjà en production des systèmes d'intelligence artificielle agentique qui ne se contentent pas de conseiller, mais passent à l'action. 84 % prévoient adopter un modèle d'exploitation piloté par l'intelligence artificielle d'ici douze mois, délaissant les AIOps traditionnelles au profit d'opérations assurées par des agents, aussi appelées AgenticOps.

Parmi les utilisateurs de l'intelligence artificielle

75 %

ont déjà déployé l'intelligence artificielle pour les opérations réseau

51 %

exploitent déjà en production une intelligence artificielle agentique qui ne se contente pas de conseiller, mais passe à l'action

84 %

prévoient adopter un modèle d'exploitation piloté par l'intelligence artificielle d'ici douze mois

Source : Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Il ne s'agit pas d'aspirations déconnectées de la réalité. Il s'agit d'une réponse réponse rationnelle à un problème structurel : le réseau moderne a atteint un niveau de complexité qui dépasse les capacités humaines d'exploitation. Le volume des alertes, le rythme des changements et la complexité entre les domaines ont atteint un niveau qu'aucune augmentation des effectifs ne peut absorber. Les entreprises ont fait leurs calculs : les opérations autonomes ne sont pas un risque à gérer, mais une nécessité à laquelle il faut apporter une réponse technique.

Les principaux enseignements de l'étude sont les suivants :

- **Les TI ne peuvent plus résoudre leurs problèmes de personnel par le seul recrutement.** La demande imposée aux réseaux atteint un niveau sans précédent. Pourtant, 95 % des répondants affirment que les outils non agentiques existants (AIOps) ne parviennent pas à suivre le rythme dans au moins un domaine. Les organisations qui n'utilisent pas AgenticOps auraient besoin d'une équipe d'environ 100 spécialistes pour résorber manuellement l'arriéré d'alertes réseau.
- **Le réseau comporte plus d'angles morts que vous ne le pensez.** Alors que 92 % des répondants indiquent que les problèmes touchent fréquemment plusieurs domaines et que les équipes utilisent au moins dix outils distincts pour assurer la visibilité, la fragmentation est devenue une faiblesse structurelle.
- **Le consensus sur l'autonomie est déjà acquis.** Face à un volume de travail impossible à absorber par le recrutement et à une fragmentation qui échappe aux corrélations manuelles, 51 % des organisations utilisent déjà l'intelligence artificielle agentique en production. De plus, 84 % prévoient adopter un modèle d'exploitation entièrement piloté par l'intelligence artificielle d'ici douze mois.
- **Les conditions de la confiance sont claires.** Les entreprises ne veulent pas réduire l'automatisation. Elles veulent pouvoir se fier aux agents qui la pilotent. La transparence est indispensable : 69 % des répondants exigent une traçabilité détaillée des causes et des effets des actions de l'intelligence artificielle agentique. Pour 86 % des répondants, la voie la plus efficace repose sur une plateforme intégrée unique, plutôt que sur un nouvel outil spécialisé.
- **Le principal obstacle n'est peut-être pas technologique. Il tient plutôt à la capacité des organisations à se préparer au changement.** Les spécialistes des opérations réseau sont presque deux fois plus susceptibles que les dirigeants des secteurs d'activité de reconnaître la transition vers AgenticOps. Ce décalage entre les équipes et la direction pourrait freiner l'adoption de l'intelligence artificielle et retarder la transformation des opérations.
- **Les organisations les plus avancées en intelligence artificielle creusent déjà l'écart.** Les organisations qui ont le plus largement adopté l'intelligence artificielle dans leurs opérations réseau affichent une productivité par employé supérieure de près de 30 %. Elles sont également 3,2 fois plus susceptibles d'obtenir une visibilité complète de bout en bout que les organisations moins avancées. Ces résultats laissent entrevoir une évolution majeure : la maîtrise de l'intelligence artificielle devient un avantage concurrentiel, et non plus seulement un moyen d'améliorer les opérations.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



02 Capacité

Les TI ne peuvent plus résoudre leurs problèmes de personnel par le seul recrutement

Pendant vingt ans, les organisations ont répondu à la complexité croissante des opérations en multipliant les effectifs, les outils et les processus. Mais les opérations fondées sur les AIOps ne suivent plus le rythme. Ce modèle a atteint ses limites.

Le volume des alertes dépasse désormais les capacités de traitement.

Une organisation génère aujourd'hui en moyenne quelque 4 100 alertes et événements de surveillance par jour. Un peu plus de la moitié (51 %) concernent le réseau. Un spécialiste peut généralement examiner, analyser et résoudre environ 21 alertes réseau par jour. Pour résorber manuellement l'arriéré quotidien, il faudrait une équipe d'environ 100 spécialistes. Or, la plupart des équipes d'exploitation réseau disposent d'effectifs bien inférieurs.

Le volume des alertes en chiffres

4 100
alertes et événements par jour, par organisation

51 %
sont liés au réseau (~2 100/jour)

21
alertes qu'un seul spécialiste peut traiter en une journée

~100
spécialistes nécessaires pour résorber manuellement l'arriéré d'alertes réseau

Source : Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Les conséquences sont prévisibles et préoccupantes

46 % des alertes réseau sont fermées sans enquête ou mises de côté, faute de personnel ou en raison d'alertes parasites récurrentes ou de faux positifs.

45 % du temps d'enquête est consacré à vérifier des faux positifs, sans résoudre de problème ni créer de valeur.

65 % des dirigeants considèrent que la fatigue liée aux alertes contribue fortement à l'insatisfaction des employés. Par ailleurs, 67 % affirment que le volume d'alertes empêche leurs équipes d'accomplir d'autres tâches essentielles.

Source : Omdia

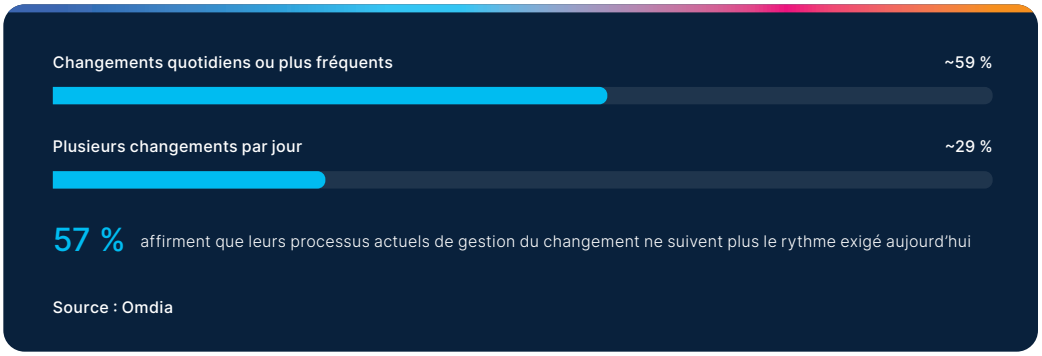
Le recrutement ne suffit plus à résoudre le manque d'effectifs. Le déséquilibre est structurel : les environnements produisent davantage d'informations que les équipes ne peuvent en traiter.

Les changements sont désormais constants

Près des trois cinquièmes des organisations modifient les environnements de leurs réseaux de production au moins une fois par jour. La moitié d'entre elles effectuent plusieurs changements par jour. Pour une proportion non négligeable, ces changements surviennent même plusieurs fois par heure. Selon 57 % des répondants, leurs processus actuels de gestion du changement ne permettent plus de suivre le rythme des mises à jour nécessaires. Le réseau n'est plus un système stable que l'on modifie ponctuellement, mais un système en mouvement constant, et le modèle d'exploitation doit suivre ce mouvement.

Fréquence des changements dans les réseaux de production

Les changements ne sont plus occasionnels. Pour la plupart des équipes, ils surviennent chaque jour, souvent même plusieurs fois par heure.



© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

L'intelligence artificielle accentue elle-même cette pression.

C'est l'un des grands paradoxes de cette étude : les technologies censées alléger la charge opérationnelle contribuent aussi à l'alourdir. Les deux tiers des répondants (67 %) affirment que l'essor de l'intelligence artificielle générative a considérablement accru la complexité des réseaux. Et pour 70 %, son adoption a alourdi, plutôt qu'allégé, la charge de travail des équipes NetOps. Autre constat révélateur : 95 % des organisations signalent des lacunes importantes dans leurs outils non agentiques actuels (AIOps). Ces outils exigent notamment trop d'interprétation humaine et n'offrent pas une visibilité suffisante entre les différents domaines.

L'incidence de l'intelligence artificielle ne se limite pas aux outils et aux charges de travail. Elle transforme en profondeur l'utilisation des réseaux et les façons de travailler. Selon une analyse de Cisco, le volume quotidien moyen du trafic réseau directement destiné aux systèmes d'intelligence artificielle devrait doubler tous les six mois. Cette projection s'appuie sur des données concrètes : la même analyse révèle une hausse de 54 % de ce trafic par client. Cette accélération s'explique probablement par la complexité croissante des tâches d'intelligence artificielle, qui nécessitent davantage d'échanges de données qu'une simple requête.

Pourtant, ces chiffres ne représentent qu'une fraction du trafic réellement généré par l'intelligence artificielle. Ils excluent notamment le trafic produit par l'intelligence artificielle intégrée à des plateformes comme Copilot et Search. Ils ne tiennent pas non plus compte de l'augmentation inévitable du trafic continu entre machines généré par les agents. Les recherches de Cisco montrent d'ailleurs que les agents d'intelligence artificielle sollicitent intensivement les réseaux : ils fonctionnent à la vitesse des logiciels, et non à celle des humains. Des tests empiriques montrent qu'une tâche exécutée par un agent peut générer jusqu'à 450 % de trafic total supplémentaire.

La part de l'intelligence artificielle dans le trafic réseau

Tous les 6 mois

Le trafic lié à l'intelligence artificielle double, puis double encore et encore.



Source : Cisco

Ce n'est pas encore le volume du trafic lié à l'intelligence artificielle qui bouleverse les réseaux. C'est sa croissance cumulative et son comportement, auxquels les réseaux et les modèles d'exploitation actuels ne sont pas préparés.

Le constat est sans équivoque : le modèle d'exploitation traditionnel fondé sur les AIOps subit des pressions sur tous les fronts. Les alertes se multiplient, les changements s'accélèrent et une vague massive de trafic lié à l'intelligence artificielle se profile.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



03 Fragmentation

Le réseau comporte plus d'angles morts que vous ne le pensez

Si le volume constitue le premier problème structurel, la fragmentation est le deuxième.

Les défaillances des réseaux modernes ne s'arrêtent pas aux frontières des organisations. Selon 92 % des organisations, les problèmes de performance touchent fréquemment plusieurs domaines à la fois : l'infonuagique, la sécurité, les applications et les terminaux. Un problème prend rarement naissance là où ses premiers symptômes apparaissent. Un problème de latence peut provenir d'une mauvaise configuration du réseau dans le nuage, ralentir une application et déclencher une alerte dans un outil de sécurité, le tout simultanément.

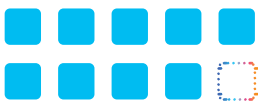
Pourtant, les outils de diagnostic restent largement cloisonnés. Les organisations utilisent en moyenne près de dix outils distincts pour assurer une visibilité de bout en bout sur leurs réseaux. Chacun n'offre qu'une vue partielle. Aucun ne permet de voir l'ensemble. Les équipes doivent donc diagnostiquer des problèmes sans en avoir une vue complète, mettre manuellement en corrélation les journaux et les événements, puis transférer les incidents d'une équipe spécialisée à l'autre.

Fragmentation des outils et de la visibilité

92 % des problèmes de performance touchent plusieurs domaines à la fois — et prennent rarement naissance là où ils se manifestent

- Nuage
- Sécurité
- Applications
- Terminaux
- API tierces
- WAN

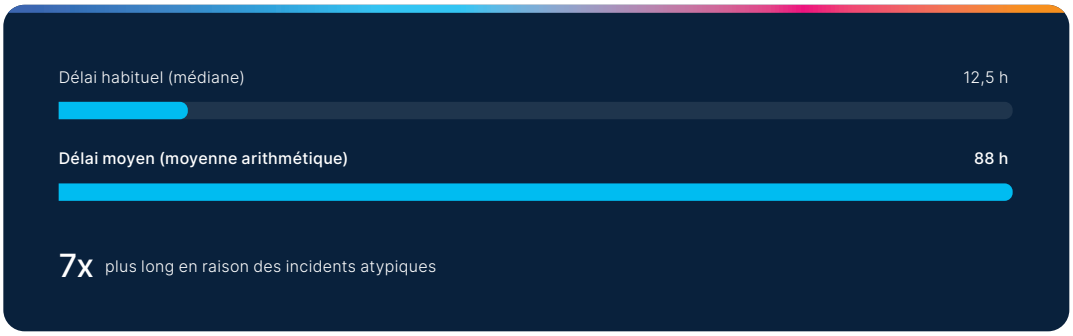
~10 outils distincts pour assurer une visibilité de bout en bout — chacun n'offre qu'une vue partielle, jamais complète



Source : Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Délai de résolution d’un incident



46 %

des organisations indiquent que la résolution des incidents prend généralement plus d’une journée

1 sur 10

indique que la résolution des incidents prend généralement plus d’une semaine

Source : Omdia

C’est dans les délais de résolution que les conséquences de cette fragmentation sont les plus visibles. Il faut en moyenne 88 heures pour résoudre un incident réseau. C’est sept fois plus que le délai médian de 12,5 heures. Cet écart est révélateur. Si de nombreuses organisations parviennent à résoudre leurs problèmes dans des délais raisonnables, une proportion importante reste régulièrement aux prises avec des incidents complexes dont la résolution s’étend sur plusieurs jours, voire plusieurs semaines. Près de la moitié des répondants (46 %) indiquent que la résolution des incidents prend généralement plus d’une journée. Un sur dix affirme qu’elle nécessite plus d’une semaine. Quelques incidents atypiques suffisent à paralyser les organisations. Ces incidents majeurs, particulièrement difficiles à résoudre, plombent les délais de résolution et empêchent les équipes NetOps d’atteindre la rapidité d’intervention exigée par l’entreprise.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



04 Autonomie

Le consensus sur l'autonomie est déjà acquis

Face à un volume de travail que les effectifs ne peuvent absorber et à une fragmentation qui rend les corrélations manuelles impraticables, les entreprises s'accordent sur un point : la solution ne consiste pas à multiplier les effectifs ou les tableaux de bord, mais à adopter des opérations autonomes pilotées par des agents.

Les données qui étayent cette conclusion sont particulièrement explicites :

75 % des organisations ont déployé des technologies d'intelligence artificielle, des AIOps à AgenticOps, pour leurs opérations réseau.

51 % exploitent déjà en production des systèmes d'intelligence artificielle agentique capables de passer à l'action.

80 % sont favorables à ce que l'intelligence artificielle joue un rôle largement ou entièrement autonome : 56 % avec une approbation humaine avant chaque action et 24 % sans aucune supervision humaine.

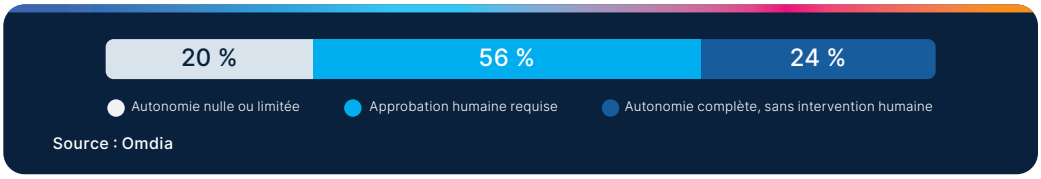
82 % sont prêtes à laisser l'intelligence artificielle modifier leurs réseaux de production sans autorisation humaine préalable, du moins pour certaines catégories d'actions.

Source : Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Les différents degrés d'autonomie

Répartition des 80 % de répondants favorables à un rôle largement ou entièrement autonome de l'intelligence artificielle.

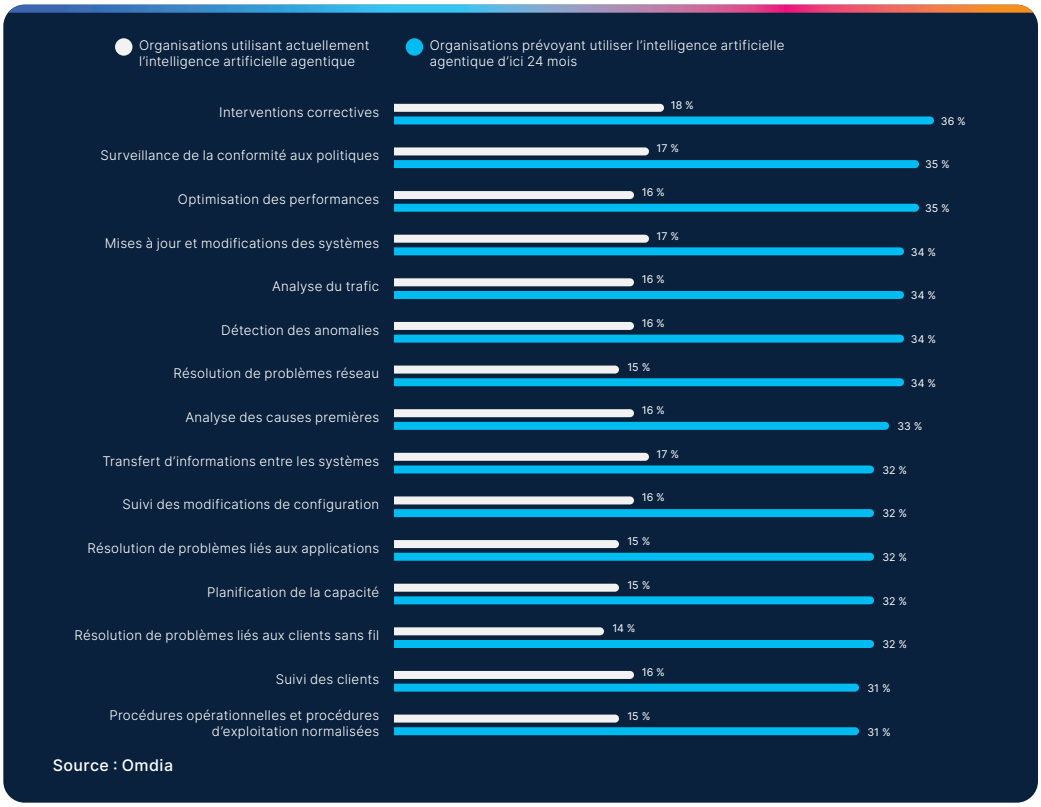


La grande majorité des organisations (85 %) estiment que les agents d'intelligence artificielle géreront de façon autonome la plupart des tâches opérationnelles d'ici cinq ans. Dès aujourd'hui, 80 % des organisations sont favorables à ce que l'intelligence artificielle assume un rôle largement ou entièrement autonome dans les opérations réseau. Par ailleurs, 82 % sont prêtes à laisser l'intelligence artificielle modifier leurs réseaux de production sans autorisation humaine préalable pour certaines catégories d'actions. Ces interventions comprennent notamment le réacheminement du trafic, l'ajustement des paramètres sans fil, l'isolement des terminaux suspects et la résolution des incidents de bout en bout.

Il ne s'agit pas d'une simple hypothèse. Cette évolution est déjà bien engagée. D'ici douze mois, 84 % des organisations prévoient adopter un modèle d'exploitation entièrement piloté par l'intelligence artificielle. Sur la même période, l'adoption de l'intelligence artificielle agentique devrait presque doubler dans certains processus NetOps.

Évolution prévue de l'adoption des agents par processus NetOps

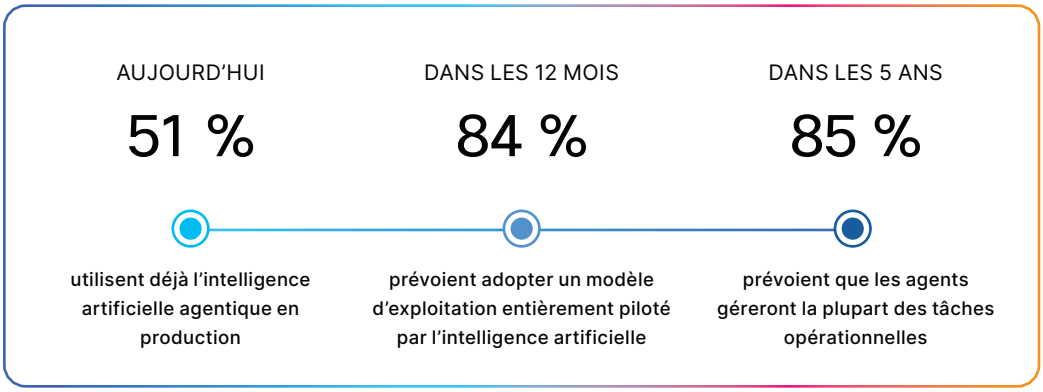
Adoption prévue de l'intelligence artificielle agentique au cours des 24 prochains mois, par processus (environ deux fois les niveaux actuels dans tous les domaines).



© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

La progression de l'adoption

Trois résultats distincts de l'étude, issus de trois questions différentes, convergent vers une même conclusion.

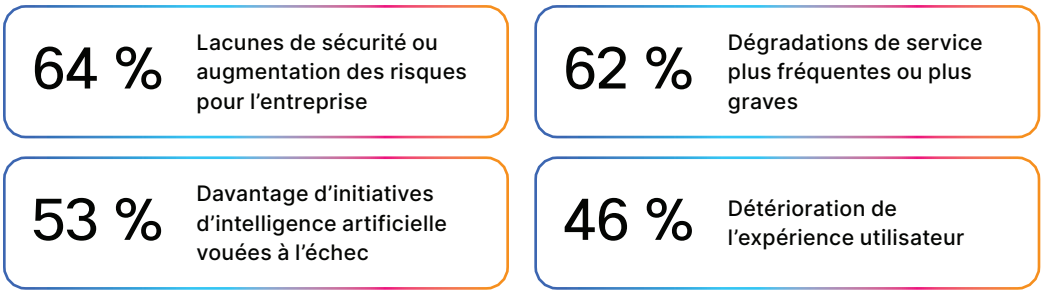


Source : Omdia

Les motivations sont avant tout pragmatiques. Les principaux moteurs de l'adoption de l'intelligence artificielle agentique dans les opérations réseau sont le renforcement de la sécurité et de la détection des menaces, la maîtrise de la complexité des réseaux et l'amélioration de l'expérience des utilisateurs finaux. Les entreprises n'adoptent pas AgenticOps pour suivre une tendance. Elles l'adoptent parce que ne pas automatiser aurait des conséquences qu'elles jugent inacceptables : 64 % anticipent des lacunes de sécurité ou une augmentation des risques pour l'entreprise, 62 % prévoient des dégradations de service plus fréquentes ou plus graves, 53 % craignent une multiplication des initiatives d'intelligence artificielle vouées à l'échec et 46 % s'attendent à une détérioration de l'expérience utilisateur.

Le coût de l'inaction

Pour les dirigeants, ne rien faire n'est pas sans conséquence. La plupart s'attendent à en payer le prix sur plusieurs fronts.



Source : Omdia

Le secteur ne se demande plus si l'intelligence artificielle prendra en charge l'exploitation des réseaux. Il cherche désormais à déterminer comment.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



05 Confiance

Les conditions de la confiance

Les entreprises ne sont pas prêtes à céder le contrôle les yeux fermés. Les dirigeants favorables à AgenticOps définissent clairement les conditions auxquelles ils sont prêts à lui faire confiance. Et ces conditions font largement consensus.

La transparence est indispensable.

Malgré le fort intérêt pour AgenticOps, la confiance repose sur la visibilité et la transparence de son raisonnement. Ainsi, 69 % des organisations exigent des explications détaillées sur les actions pilotées par des agents. Le groupe le plus important (36 %) considère qu'une observabilité complète constitue le minimum acceptable : traçabilité détaillée, synthèse des motifs justifiant les décisions et vérification après chaque action.

Le constat est clair : sans transparence, pas de confiance.

Les entreprises privilégient une architecture intégrée.

Impossible de faire confiance à ce que l'on ne peut pas voir. La fragmentation répartit la visibilité entre des outils distincts, créant des angles morts qui minent la confiance. Les entreprises en sont conscientes. Pour 86 % d'entre elles, la solution passe par une plateforme intégrée unique couvrant le calcul, la sécurité, les applications et la mise en réseau. Pas par l'ajout d'un outil spécialisé à ceux déjà en place.

La voie à suivre

86 % **estiment que la solution la plus efficace repose sur une plateforme intégrée unique couvrant le calcul, le stockage, les applications et la mise en réseau.**

Source : Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Ces garde-fous forment un ensemble indissociable.

Invités à désigner les garde-fous essentiels, les répondants en ont retenu en moyenne trois sur six, sans qu'aucun ne se démarque nettement :

Garde-fous indispensables

99 %

des organisations refusent de laisser l'intelligence artificielle agir sans ces garde-fous. Seul 1 % des organisations accepterait de s'en passer entièrement.

Source : Omdia

Tous ont été jugés essentiels. Aucun ne peut être considéré comme facultatif :

- Explication des actions de l'intelligence artificielle
- Approbation humaine des actions
- Limites opérationnelles définies par des stratégies
- Mécanismes de reprise de contrôle en cas d'urgence
- Contrôle d'accès fondé sur les rôles
- Pistes d'audit immuables

Pour les organisations, ces garde-fous ne sont pas des options parmi lesquelles choisir, mais des exigences à satisfaire ensemble.

Ces résultats changent fondamentalement la nature du débat sur la confiance. Les entreprises ne cherchent pas à limiter l'automatisation. Elles veulent pouvoir s'y fier. Elles veulent suivre et comprendre les actions automatisées depuis une interface unifiée, sans devoir reconstituer leur déroulement à partir d'une multitude d'outils. Elles sont prêtes à accorder davantage d'autonomie aux agents, à condition que leurs actions soient explicables, soumises aux approbations et aux limites prévues par les stratégies, et encadrées par des mécanismes de reprise de contrôle et des pistes d'audit.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



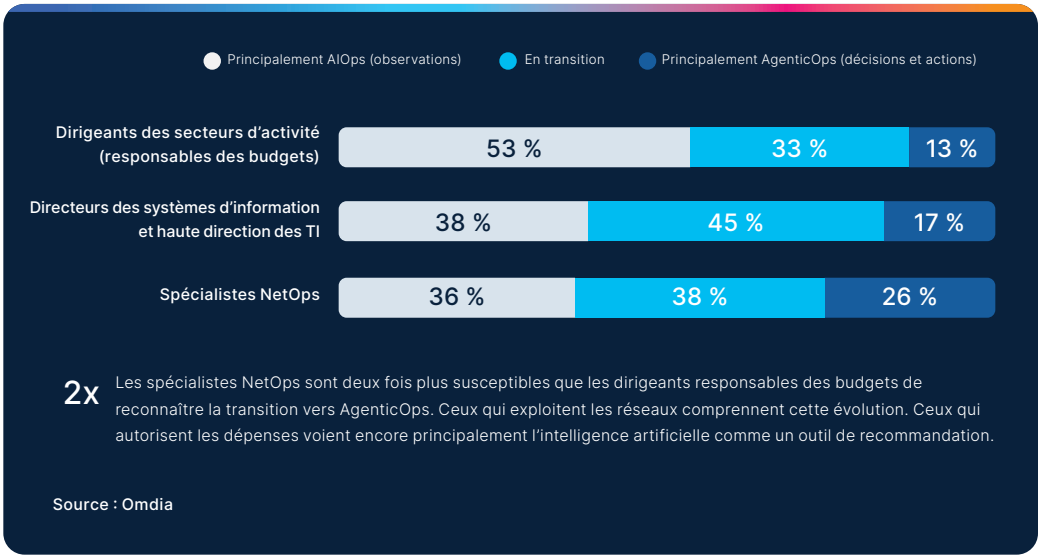
06 Préparation

L'écart organisationnel qui pourrait freiner son adoption

Le principal obstacle à l'adoption d'AgenticOps n'est peut-être pas d'ordre technique. Il pourrait être organisationnel. L'étude révèle un décalage important entre les équipes qui assurent les opérations au quotidien et les dirigeants qui contrôlent les budgets. Les spécialistes NetOps sont environ deux fois plus susceptibles que les dirigeants des secteurs d'activité de reconnaître la transition vers AgenticOps. Confrontés chaque jour aux contraintes opérationnelles, ces spécialistes perçoivent clairement cette évolution. Les dirigeants des secteurs d'activité qui influencent les décisions budgétaires continuent, pour leur part, de voir surtout l'intelligence artificielle comme un outil d'observation et de recommandation, selon le modèle traditionnel des AIOps, plutôt que comme un moyen de confier des décisions et des actions autonomes à des agents.

Perception du rôle de l'intelligence artificielle dans les opérations TI selon les fonctions

Plus les répondants sont proches des opérations quotidiennes, plus ils reconnaissent que l'intelligence artificielle passe de la recommandation à l'action.



2x Les spécialistes NetOps sont deux fois plus susceptibles que les dirigeants responsables des budgets de reconnaître la transition vers AgenticOps. Ceux qui exploitent les réseaux comprennent cette évolution. Ceux qui autorisent les dépenses voient encore principalement l'intelligence artificielle comme un outil de recommandation.

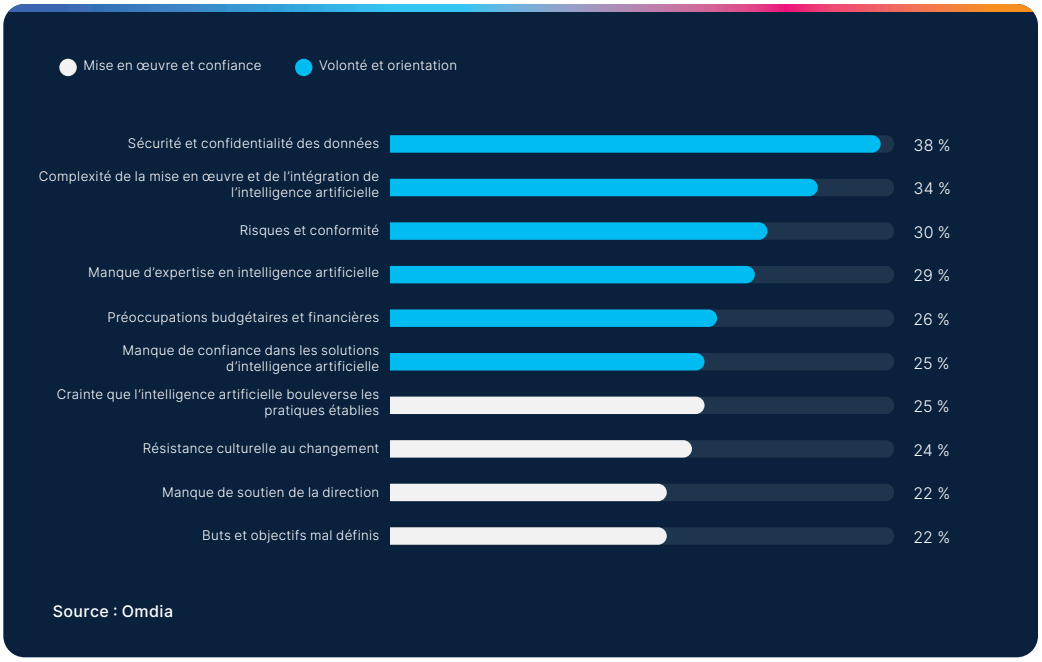
Source : Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

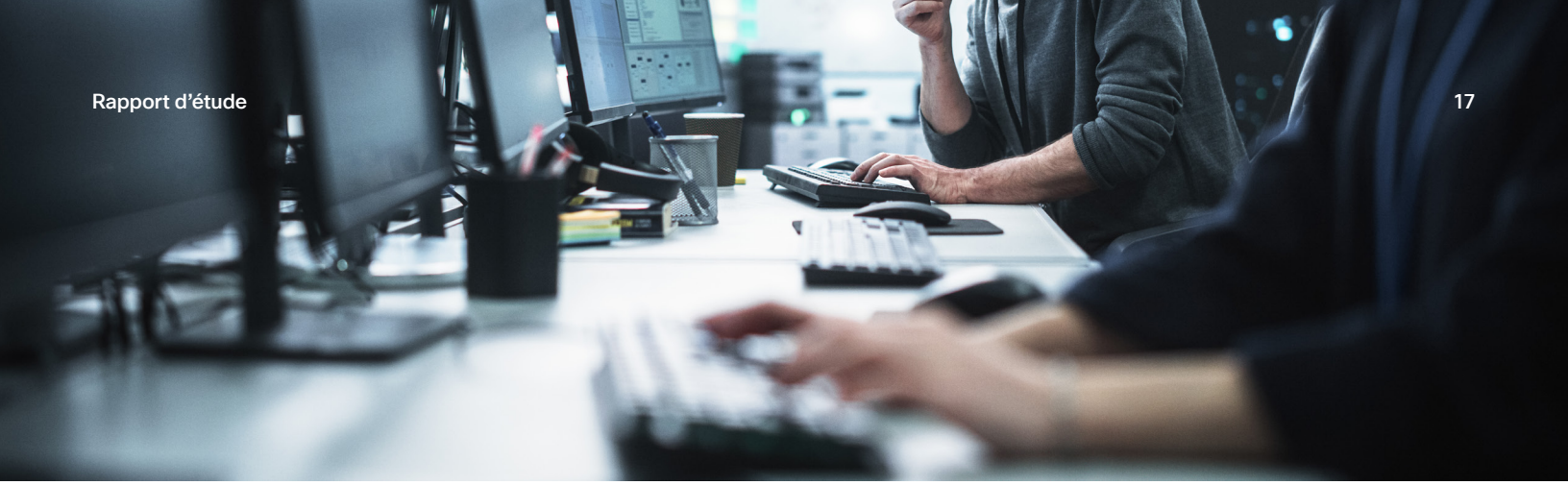
Ce décalage est déterminant : ceux qui comprennent le mieux les besoins ne sont pas toujours ceux qui autorisent les investissements. Les responsables techniques doivent donc montrer à leurs homologues des finances et des secteurs d'activité qu'AgenticOps transforme fondamentalement les opérations, plutôt que de simplement améliorer les pratiques existantes.

Les autres obstacles sont bien réels, mais moins importants qu'on pourrait le croire. Les principales préoccupations concernent la sécurité et la confidentialité des données (38 %), la complexité de la mise en œuvre et de l'intégration de l'intelligence artificielle (34 %), ainsi que les risques et la conformité (30 %). Fait révélateur, le manque de clarté des objectifs et le manque de soutien de la direction figurent parmi les obstacles les moins souvent cités. Les organisations ne manquent donc ni de motivation ni d'orientation. Les difficultés tiennent avant tout à la mise en œuvre et à la confiance, plutôt qu'à la volonté d'agir.

Principaux obstacles à l'utilisation de l'intelligence artificielle dans les opérations réseau



© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



07 Résultats

Les premiers résultats confirment son efficacité

Les investissements commencent-ils à porter leurs fruits? Les premiers résultats sont encourageants.

Les organisations qui ont le plus investi dans l'intelligence artificielle pour les opérations réseau, notamment en déployant AgenticOps, obtiennent des résultats nettement supérieurs à ceux des organisations moins avancées dans les domaines qui comptent le plus :

Les avantages d'une adoption avancée de l'intelligence artificielle dans NetOps

~ 30 %

de productivité supplémentaire par spécialiste. Les organisations les plus avancées en intelligence artificielle traitent davantage d'alertes par personne et par jour.

3,2x

plus susceptibles de disposer d'une visibilité complète sur les goulots d'étranglement de leur infrastructure en périphérie que les organisations les moins avancées en intelligence artificielle.

Source : Omdia

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

Productivité

Une productivité individuelle accrue. Dans les organisations les plus avancées en intelligence artificielle qui utilisent AgenticOps, les spécialistes sont près de 30 % plus productifs que dans les organisations les moins avancées. Ils peuvent examiner et résoudre nettement plus d’alertes par personne et par jour. À conditions égales, ce gain de productivité permettrait de résorber le même arriéré avec plusieurs dizaines de spécialistes de moins, libérant ainsi des ressources humaines limitées pour des tâches à plus forte valeur ajoutée.

Visibilité

Une meilleure visibilité. Les organisations les plus avancées dans l’adoption d’AgenticOps sont 3,2 fois plus susceptibles de disposer d’une visibilité complète de bout en bout sur les goulots d’étranglement de leur infrastructure en périphérie. Elles sont également beaucoup plus susceptibles de reconnaître que les problèmes de performance touchent plusieurs domaines à la fois, une condition préalable à leur résolution.

Capacité

Une capacité accrue et une plus grande confiance dans les moyens disponibles. Les organisations les plus avancées sont nettement plus susceptibles d’affirmer que leurs équipes parviennent à absorber leur charge de travail, plutôt que de suivre difficilement le rythme ou d’accumuler du retard.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.



08 Perspectives

Douze mois décisifs

Les résultats de ce rapport montrent qu'un tournant décisif a déjà été franchi. Confrontées à un problème structurel (des réseaux trop vastes, trop changeants et trop fragmentés pour être exploités uniquement par des humains), les entreprises ont conclu que les opérations autonomes pilotées par des agents constituent la solution. Elles ont commencé à déployer ces technologies en production, défini les conditions nécessaires pour leur faire confiance et prévoient adopter un modèle d'exploitation piloté par l'intelligence artificielle d'ici un an.

La question n'est donc plus de savoir quelle direction prendre. Il s'agit désormais de passer à l'action. Les organisations mettront-elles en place les garde-fous nécessaires pour assurer la fiabilité des opérations autonomes pilotées par des agents? Regrouperont-elles leurs outils fragmentés au sein des plateformes intégrées dont elles affirment avoir besoin? Et les responsables techniques parviendront-ils à rallier les dirigeants des secteurs d'activité à cette transformation?

Les douze prochains mois ne détermineront pas si AgenticOps prendra en charge les réseaux d'entreprise. Les entreprises interrogées ont déjà tranché cette question. Ils détermineront plutôt dans quelle mesure cette transition réussira et quelles organisations disposeront d'un modèle d'exploitation capable de prendre en charge leurs réseaux pendant la prochaine décennie.

Du chaos opérationnel à l'efficacité des opérations autonomes

Pour passer du chaos opérationnel actuel à un modèle fondé sur AgenticOps, où les agents assurent une grande partie des opérations, les dirigeants doivent prendre trois décisions stratégiques :

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

01

Remplacer le recrutement par une nouvelle architecture opérationnelle

Cessez de chercher à résoudre un problème de capacité en augmentant les effectifs. Aucun recrutement ne permettra de résorber durablement un arriéré de 4 100 alertes par jour. Et même si cela était possible, le modèle ne serait pas viable à long terme. Réorientez vos priorités et vos budgets : plutôt que d'embaucher davantage, concevez une architecture qui favorise l'autonomie. Formez vos équipes à orchestrer les agents plutôt qu'à traiter manuellement les tickets et à multiplier les vérifications de fausses alertes. L'objectif est de libérer vos meilleurs spécialistes du flot incessant d'alertes et de changements pour qu'ils se consacrent à des activités à plus forte valeur ajoutée, notamment la conception stratégique des réseaux.

02

Rapprocher les dirigeants et les équipes opérationnelles

Un décalage préoccupant persiste entre ceux qui exploitent les réseaux et ceux qui financent leur exploitation. Vos équipes NetOps savent que le modèle actuel, fondé sur les interventions humaines, a atteint ses limites. Pourtant, les dirigeants des secteurs d'activité peuvent encore considérer l'automatisation pilotée par des agents comme un simple avantage supplémentaire, plutôt que comme une nécessité stratégique. Votre rôle consiste à traduire les réalités techniques — les 4 100 alertes quotidiennes et les délais de résolution problématiques — en risques concrets pour l'entreprise. Présentez la transition vers AgenticOps non comme une simple modernisation des TI, mais comme une stratégie de réduction des risques qui protège l'entreprise contre les interruptions de service et les atteintes à la sécurité.

03

Établir un cadre de gouvernance fondé sur la confiance

N'attendez pas qu'une crise survienne pour définir les garde-fous applicables à l'intelligence artificielle et aux agents. La valeur des actions et de l'autonomie des agents dépend directement de la confiance qu'ils inspirent. Avant de déployer ces technologies à grande échelle, adoptez des solutions qui assurent la sécurité des agents, la transparence de leurs actions, leur vérifiabilité et une supervision humaine intégrée. Appuyez ces outils sur un cadre de gouvernance précis qui définit les actions autorisées pour l'intelligence artificielle et garantit que chaque décision est consignée et expliquée. C'est à cette condition que vous pourrez dissiper les craintes liées à l'inconnu. Faites de l'explicabilité de l'intelligence artificielle une exigence incontournable pour chaque fournisseur et chaque système intégré à votre environnement.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.

09 Annexe

À propos de cette étude

À mesure que l'intelligence artificielle gagne en maturité dans les opérations réseau, une terminologie commune se précise. Les définitions suivantes reflètent les distinctions que le secteur établit de plus en plus entre les différentes formes d'intelligence artificielle appliquées aux opérations TI et à NetOps.

L'intelligence artificielle (IA) désigne la capacité générale des machines à accomplir des tâches qui exigent normalement l'intelligence humaine, comme comprendre le langage, reconnaître des tendances, résoudre des problèmes et apprendre à partir de nouvelles informations. Ce terme générique englobe toutes les technologies présentées ci-dessous.

L'intelligence artificielle générative est une forme d'intelligence artificielle qui crée du contenu, comme du texte, du code, des images ou des résumés, en réponse à une instruction. Plutôt que de se limiter à la classification ou à la prédiction, elle produit du contenu original. C'est cette capacité qui alimente notamment les assistants conversationnels et les assistants de programmation.

Les AIOps sont issues de l'apprentissage automatique et de l'analytique, auxquels s'ajoute désormais l'intelligence artificielle générative. Elles permettent de détecter les problèmes, de mettre en corrélation les événements provenant de différents systèmes et de proposer des solutions. Toutefois, une intervention humaine reste généralement nécessaire pour interpréter les résultats et agir.

L'intelligence artificielle agentique va plus loin en agissant de manière autonome, dans les limites de garde-fous prédéfinis. Elle prend des décisions, exécute des actions et s'adapte aux changements pour atteindre un objectif. L'humain dirige les agents et définit leurs objectifs, sans avoir à exécuter chaque étape. L'humain définit les intentions et les objectifs; l'agent se charge de leur exécution.

Les opérations agentiques, de plus en plus souvent appelées **AgenticOps**, découlent de l'intelligence artificielle agentique. Elles reposent sur des agents dirigés par des humains, capables d'observer, de raisonner et d'agir dans plusieurs domaines. Les spécialistes définissent les objectifs et les garde-fous, tandis que les agents exécutent les tâches qui nécessiteraient autrement une intervention manuelle.

Toutes les informations présentées dans ce rapport reposent sur une étude indépendante menée par Omdia en 2026 auprès de 1 000 Responsables des opérations TI et réseau d'organisations comptant au moins 500 employés, en Amérique du Nord, en Europe occidentale et dans la région Asie-Pacifique. Le rapport comprend également des observations tirées d'une analyse de Cisco portant sur des données agrégées de télémétrie, qui a permis de suivre le trafic réseau directement destiné aux systèmes d'intelligence artificielle d'octobre 2025 à avril 2026.

© 2026 Cisco et/ou ses sociétés affiliées. Tous droits réservés.