

Cisco AgenticOps :

Repenser la résilience à l'échelle mondiale grâce au réseau autonome et à l'intelligence multi-domaine



MARS 2026

Auteur :

Ron Westewall

Vice-président et responsable
de l'infrastructure et du réseau



Synthèse

Les opérations réseau de l'entreprise (NetOps) évoluent, passant de la simple gestion des équipements à la supervision d'un ensemble de fonctionnalités distribuées et optimisées par l'intelligence artificielle (IA). Les cadres opérationnels existants ne suivent pas, car ils ont été conçus pour les environnements statiques et la croissance linéaire. De plus, les NetOps sont de plus en plus complexes. Les opérations s'étendent désormais à des millions d'entités cloud éphémères et à des milliards d'équipements OT/IT en périphérie, générant des volumes de télémétrie qui dépassent les capacités d'analyse humaine. Une cellule de crise où des ingénieurs analysent manuellement les journaux ne permet plus d'identifier et de résoudre les problèmes assez rapidement, ni d'éviter une dégradation ou une interruption des services. Une logique opérant à la vitesse de la machine est désormais nécessaire pour gérer la stabilité du réseau, le routage du trafic et la neutralisation des menaces. Pour s'adapter à cette évolution, les entreprises doivent passer d'une surveillance passive à un système disposant du contexte nécessaire pour s'auto-corriger avant même qu'une intervention humaine ne soit possible. Ce système, c'est AgenticOps de Cisco.

Cisco AgenticOps est un cadre qui permet de gérer et de faire évoluer des équipes d'agents IA autonomes avec différents niveaux d'autonomie dans une entreprise. Il assure la discipline opérationnelle nécessaire au déploiement, à la gestion, à la supervision et à l'administration des agents IA autonomes dans les environnements IT. Ce cadre permet aux agents d'observer l'infrastructure, d'analyser les problèmes et de prendre des mesures correctives avec une intervention humaine minimale. AgenticOps couvre l'ensemble du cycle de vie des agents et fournit une infrastructure qui assure leur fiabilité, leur sécurité et leur responsabilité. Il fournit également des mécanismes de gouvernance, de transparence et de contrôle qui permettent de superviser l'autonomie et l'exécution des agents.

Cisco AgenticOps représente la nouvelle évolution des opérations IT (AIOps). Cette solution associe des actions autonomes conçues spécifiquement pour les agents à des mécanismes de supervision, au sein d'un environnement unifié où humains et agents collaborent. L'approche agentic va au-delà de l'AIOps sur plusieurs points essentiels :

- L'AIOps s'appuie sur l'IA générative et l'apprentissage automatique pour détecter les anomalies et mettre en corrélation les événements. Les opérateurs humains doivent interpréter les recommandations, rédiger des scripts d'automatisation et approuver ou exécuter manuellement les actions correctives.
- La solution AgenticOps va plus loin en permettant aux entreprises de déployer, de manière fiable et sécurisée, des agents IA capables d'analyser les problèmes de façon autonome et d'exécuter, à la vitesse de la machine, des tâches complexes en plusieurs étapes sur différentes plateformes logicielles et matérielles. AgenticOps apporte de l'autonomie dans les opérations IT, découple les capacités et l'expertise humaines, et transforme le réseau d'un système réactif en un système proactif et auto-optimisé grâce à la combinaison du raisonnement, de la simulation et de l'exécution en boucle fermée.

Au quotidien, cela signifie sortir d'un modèle reposant sur une multitude de tableaux de bord et un acheminement manuel des demandes d'assistance. Avec AgenticOps, les agents analysent en continu l'ensemble des dépendances et raisonnent à leur sujet avant même qu'un ingénieur ne soit alerté d'un goulot d'étranglement sur le réseau et puisse en identifier l'origine. Des équipements locaux jusqu'au cloud, les agents détectent et exécutent les correctifs instantanément. AgenticOps décloisonne les différents domaines opérationnels afin d'optimiser l'expérience de service dans son ensemble.

Le cadre AgenticOps doit avant tout s'appuyer sur les workflows existants de l'entreprise. Les opérations autonomes ne sont pas instantanées, et ne doivent pas l'être. Les agents intégrés à ce cadre proposent des plans de remédiation précis, soumis à l'approbation des équipes, au sein d'un environnement unifié où humains et agents interagissent. Les équipes peuvent ainsi développer progressivement leur confiance dans le système et lui donner davantage d'autonomie, faisant évoluer les opérations informatiques d'un modèle fondé sur des interventions manuelles permanentes vers une supervision automatisée très fiable.

Ce résumé d'étude aborde trois points essentiels :

1. Premièrement, AgenticOps est devenu indispensable, car la complexité des infrastructures numériques modernes a atteint un point de bascule où une exécution autonome à la vitesse de la machine est essentielle pour combler l'écart entre la télémétrie en temps réel et une remédiation efficace.
2. Ensuite, le cadre AgenticOps de Cisco transforme le réseau en un environnement autonome et sans silos grâce au déploiement d'une multitude d'agents spécialisés dans le dépannage, l'optimisation et la validation, qui s'appuient sur la télémétrie multi-domaine et 40 ans d'expertise formalisée pour collaborer avec les équipes IT.
3. Enfin, nous expliquons pourquoi Cisco est le fournisseur le mieux placé pour accompagner les équipes NetOps dans l'adoption d'AgenticOps, grâce à une architecture IA unique, profondément intégrée et multicouche, qui simplifie les opérations et accélère la création de valeur grâce à une mise en œuvre complète entre les différents domaines. Nous concluons par un plan d'action concret qui aide les décideurs à transformer leur stratégie en une mise en œuvre progressive.



L'impératif stratégique : pourquoi AgenticOps est devenu indispensable

AgenticOps : pourquoi l'AIOps classique ne suffit plus

Les solutions d'AIOps classiques atteignent leurs limites. Dans un premier temps, l'apprentissage automatique a permis de détecter les anomalies et de générer des alertes. L'IA générative a ensuite permis d'expliquer les problèmes et de recommander des actions correctives. Puis sont apparues les plateformes AIOps, conçues pour collecter la télémétrie, mettre en corrélation les événements et améliorer les mécanismes d'alerte au sein de domaines fonctionnels distincts, tels que le réseau ou la sécurité. Si l'AIOps contribue à réduire le bruit, il ne transforme pas le modèle opérationnel : les humains restent au cœur de la résolution des problèmes, en assurant manuellement la coordination entre des domaines et des informations cloisonnées.

Dans les infrastructures modernes, les pannes et les baisses de performance proviennent rarement d'une seule couche. Elles résultent plutôt d'interactions complexes entre le réseau, le cloud, les mécanismes de sécurité et les couches applicatives. Comme les solutions d'AIOps classiques restent largement cloisonnées et limitées à l'observation, les problèmes multi-domaines obligent les équipes à mettre manuellement en corrélation les informations et à mobiliser des cellules de crise. L'AIOps détecte les anomalies dans le système, mais laisse aux humains le soin de les analyser. Cette dépendance à des processus de dépannage pilotés par l'humain entraîne une fatigue liée aux alertes et allonge le délai moyen de résolution (MTTR).

Par exemple, alors que l'AIOps se limite à réagir à des données structurées et à des alertes fondées sur des seuils, en signalant par exemple une hausse du trafic via une simple alerte de type « utilisation élevée du processeur », AgenticOps s'appuie sur la planification assistée par les LLM et enrichie par des outils pour parcourir l'ensemble de la pile opérationnelle avec un raisonnement proche de celui d'un humain. Au lieu de simplement alerter un ingénieur, un agent autonome peut analyser la cause première du problème en interrogeant les visualisations des workflows marketing afin d'identifier les campagnes commerciales en cours, en récupérant les runbooks de mise à l'échelle promotionnelle dans les référentiels de documentation internes, en exécutant les scripts nécessaires pour ajuster les ressources, puis en résumant l'ensemble de la procédure de résolution sur le canal de messagerie de l'équipe. Cette évolution fait passer le système d'un simple observateur de tendances passées à un acteur capable de mener des recherches sur plusieurs plateformes et d'exécuter des tâches de bout en bout. En d'autres termes, l'AIOps est un modèle qui ne peut pas évoluer pour répondre aux exigences actuelles des opérations réseau.





AIOps et AgenticOps : les principales différences en matière d'impact opérationnel

Activité NetOps	AIOps classique	AgenticOps
Surveillance et supervision	Les ingénieurs supervisent les tableaux de bord et répondent aux alertes manuellement.	Les agents surveillent le système en continu, tandis que les humains assurent sa supervision.
Gestion du changement	Les modifications du système nécessitent une exécution manuelle et une supervision humaine.	Les agents planifient, simulent et exécutent les modifications de manière autonome, dans le respect de paramètres de sécurité définis.
Résolution des problèmes	Les ingénieurs analysent les journaux pour identifier la cause première.	Diagnostic piloté par les agents, qui identifient les problèmes, analysent les solutions et prennent les mesures appropriées, avec ou sans validation humaine.

Source : HyperFRAME Research

AgenticOps marque une rupture nette en donnant la priorité à l'action intelligente. Il concrétise le concept d'environnement auto-réparateur en s'appuyant sur l'IA agentique pour anticiper les pannes et déclencher des mesures correctives avant qu'une dégradation des performances, ou pire, ne se propage à l'ensemble du réseau. En passant d'une surveillance passive à une exécution à la vitesse de la machine, les entreprises peuvent donner la priorité à la résorption de la dette d'infrastructure et réduire, voire éliminer, les arrêts de service qui surviennent lorsque les cellules de crise pilotées par des humains ne suivent plus le rythme des perturbations et des défaillances numériques.

Pour se préparer à l'adoption d'AgenticOps, les entreprises doivent d'abord :

1. Mettre en place un cadre de gouvernance définissant des mécanismes clairs de responsabilité, d'auditabilité et de supervision humaine pour les agents autonomes.
2. Privilégier une architecture modulaire pilotée par les données, selon une approche progressive, afin de garantir une fabric de données de haute qualité et une intégration à faible latence avec les workflows et systèmes existants.
3. Adopter un cadre AgenticOps complet qui associe une intelligence spécialisée par domaine à une télémétrie multi-domaine unifiée, ainsi qu'à une gouvernance avec supervision humaine, afin d'assurer la préparation de l'entreprise, de répondre aux pénuries de compétences et de faciliter l'adoption.



De l'outil au coéquipier : l'émergence de la main-d'œuvre agentique de Cisco

AgenticOps fait évoluer l'IA vers une véritable équipe d'agents numériques autonomes capables de travailler aux côtés des équipes humaines. En intégrant à la plateforme une logique spécialement conçue et fondée sur une expertise de niveau CCIE, Cisco fournit des fonctionnalités disponibles en permanence qui vont au-delà de l'automatisation pour entrer dans une logique de collaboration active. Ses fonctionnalités agentiques s'appuient sur une intelligence opérationnelle approfondie pour gérer le réseau de manière proactive, avec des niveaux d'autonomie flexibles allant d'investigations déclenchées par les équipes à des analyses continues et approfondies

de l'environnement. Cette évolution marque une transition majeure vers une IA qui agit comme un partenaire collaboratif aux côtés des opérateurs humains, donnant naissance à un partenariat agentique où l'IA et l'expertise humaine se conjuguent pour orchestrer le réseau.

Cisco a récemment dévoilé la nouvelle évolution de son cadre AgenticOps, qui met l'accent sur la simplification des opérations et sur des solutions pilotées par l'IA afin d'accélérer la transition vers un réseau autonome et sans silos. Au cœur de cette évolution figurent de nouvelles fonctionnalités agentiques dédiées au dépannage, à l'optimisation et à la validation, conçues pour exploiter les environnements réseau avec un minimum d'intervention manuelle. Ces fonctionnalités agentiques, associées à de nouvelles fonctionnalités d'IA, sont intégrées aux interfaces IT couramment utilisées, notamment AI Assistant de Cisco, les workflows agentiques, la plateforme Cisco Cloud Control, AI Canvas (à venir), ainsi qu'à des applications tierces.

Agents IA de Cisco : fonctionnalités agentiques

Fonctionnalité agentique	Mission principale	Fonctionnalité clé	Outils avancés
Résolution autonome des problèmes	Prise en charge des incidents (de la détection à la résolution)	Appliquer un raisonnement fondé sur la télémétrie pour remonter jusqu'à la cause première, valider plusieurs hypothèses simultanément et exécuter des actions correctives déterministes avec une précision de niveau CCIE.	Capture de paquets d'IA (mise en corrélation de milliers de signaux en temps réel)
Optimisation en continu	Amélioration continue (de la performance et de l'efficacité)	Maintenir en permanence la qualité de l'expérience utilisateur en ajustant de manière autonome les paramètres RF, la qualité de service, les chemins réseau et les plans de contrôle, grâce à une compréhension en temps réel de l'état du réseau de bout en bout.	Recommandations de configuration basées sur l'IA (optimisation proactive pour garantir des performances prévisibles)
Validation fiable	Validation des changements (de l'intention au résultat)	Valider les changements réseau en tenant compte des risques à partir de la topologie, de la configuration et de la télémétrie en temps réel, tout en évaluant leur impact et leur périmètre d'impact.	Modélisation de l'impact (analyse de la propagation des changements dans le système)

Source : HyperFRAME Research

La première de ces fonctionnalités agentiques est le dépannage autonome, dont la mission principale consiste à prendre en charge les incidents, de leur détection jusqu'à leur résolution. Ces fonctionnalités analysent et résolvent les problèmes entre les différents domaines en mettant en corrélation en temps réel la télémétrie issue des couches réseau, sécurité et Internet. Au lieu de s'appuyer sur des hypothèses, elles analysent les signaux à grande échelle afin d'identifier les causes premières et de recommander ou d'exécuter les actions correctives appropriées. Cette fonctionnalité repose sur de nouveaux outils tels que la capture de paquets d'IA, qui permettent à l'agent de traiter simultanément des milliers de signaux et de fournir des preuves et des explications fiables en quelques minutes.

Pour préserver la santé du réseau, Cisco propose également des fonctionnalités agentiques d'optimisation continue, véritables opérateurs numériques dédiés à l'amélioration permanente des performances et de l'efficacité. Ces fonctionnalités agentiques agissent de manière proactive en détectant les dérives de configuration et en anticipant les baisses de performance dans les environnements sans fil, de commutation et WAN avant qu'elles n'affectent les utilisateurs. Au lieu d'attendre l'ouverture d'une demande d'assistance, elles identifient les risques émergents et ajustent l'environnement dans le respect des garde-fous définis. Ces fonctionnalités s'enrichissent de nouvelles compétences, notamment avec les recommandations de configuration basées sur l'IA, conçues pour garantir de manière proactive des performances réseau prévisibles.

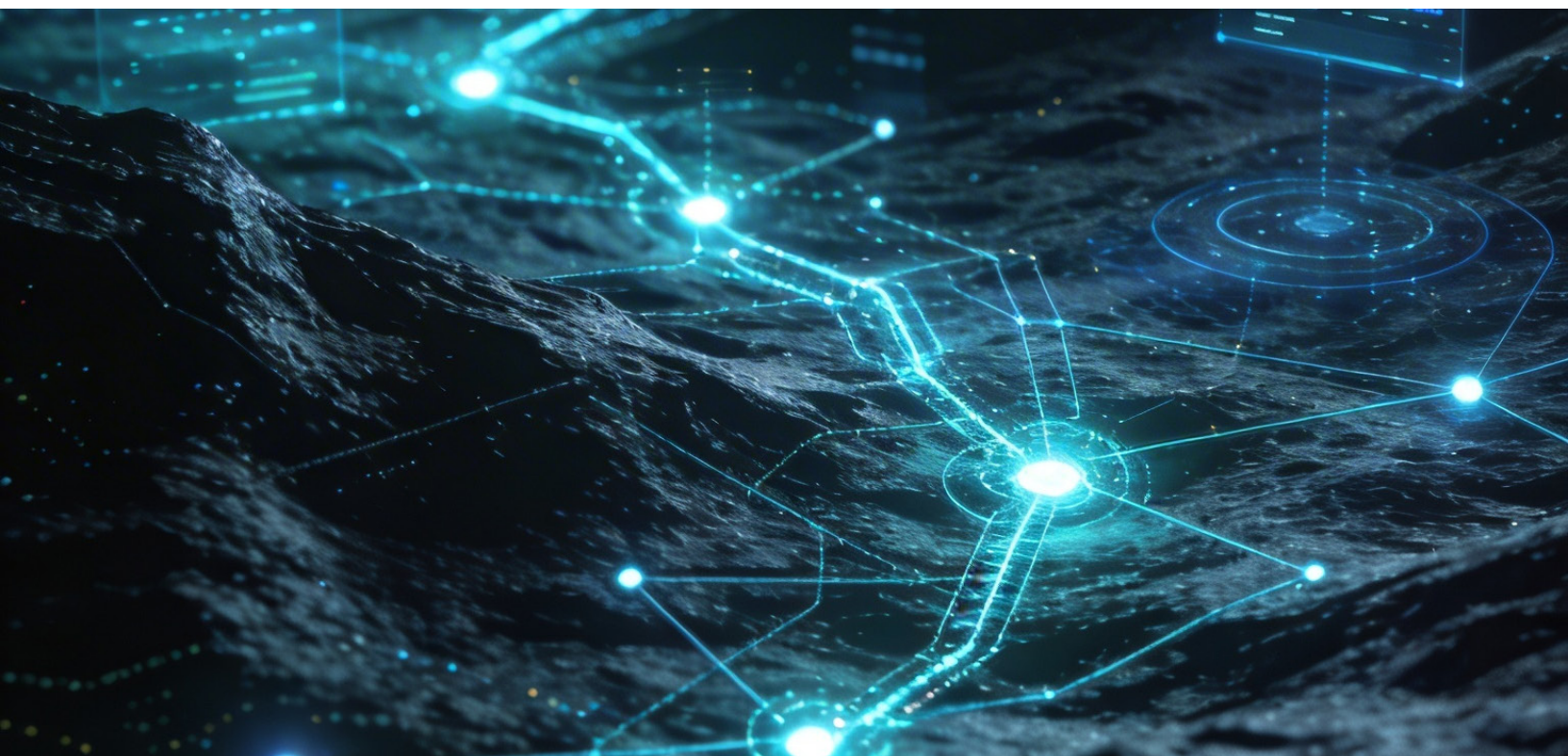
Les autres acteurs de cette équipe agentique sont les fonctionnalités de validation de confiance, dont la mission consiste à rendre les modifications du réseau plus sûres et plus prévisibles. Ces fonctionnalités modélisent l'impact potentiel et le périmètre d'impact

d'une modification avant sa mise en œuvre, afin de révéler les dépendances cachées et les risques en aval. Une fois la modification mise en œuvre, les agents vérifient automatiquement le résultat et tirent des enseignements des observations effectuées afin d'améliorer leurs actions futures. En analysant la manière dont les modifications se propagent dans le système, ces fonctionnalités garantissent que chaque mise à jour rapproche le réseau de son état cible, sans conséquences imprévues.

Les fonctionnalités agentiques de Cisco sont conçues pour offrir une grande flexibilité et fonctionner selon différents modes, en fonction du niveau d'autonomie requis :

1. Les fonctionnalités à la demande sont déclenchées par les équipes et visent des objectifs précis, comme la résolution d'un problème rencontré par un client.
2. Les fonctionnalités agentiques ambiantes fonctionnent en continu et poursuivent des objectifs permanents, tels que l'optimisation du wifi ou la correction des dérives de configuration.
3. Le mode de raisonnement approfondi traite des objectifs complexes et de longue durée, comme les validations à l'échelle de l'environnement ou la planification de grande envergure.

À terme, chaque fonctionnalité agentique de l'écosystème Cisco devrait couvrir ces trois modes afin d'offrir aux équipes IT un système d'assistance complet et adaptable.



De la télémétrie à la confiance : l'architecture fondatrice de Cisco AgenticOps

Le cadre agentique de Cisco repose sur quatre piliers architecturaux stratégiques, à commencer par une base fondée sur une télémétrie unifiée entre les différents domaines. La technologie agentique de Cisco s'appuie sur l'un des ensembles de télémétrie les plus étendus du secteur, couvrant les environnements locaux, distants, WAN et de data center, ainsi que les couches de sécurité et les chemins d'application. Cette visibilité complète de bout en bout permet aux agents d'analyser les situations et d'agir à l'échelle de l'ensemble du système, en s'appuyant sur une vision globale du réseau plutôt que sur des données isolées.

Le deuxième pilier repose sur les modèles d'ensemble et l'expertise Cisco formalisée, qui transforment une IA généraliste en une intelligence opérationnelle spécialisée. En combinant des modèles fondamentaux et de pointe avec des modèles dédiés comme le Deep Network Model, Cisco ancre ses fonctionnalités agentiques dans des bases de connaissances issues de l'expertise CCIE (Cisco Certified Internetwork Expert) et dans des runbooks élaborés par des experts. Selon nous, cette combinaison de modèles permet au système de sélectionner l'outil le plus adapté à chaque situation, qu'il s'agisse de

réagir rapidement, de mener un dépannage approfondi ou de résoudre des défis architecturaux complexes.

Pour s'assurer que ces actions sont exécutées en toute sécurité, le troisième pilier intègre des outils, des garde-fous et une conception sécurisée. Les fonctionnalités agentiques de Cisco n'agissent pas à l'aveugle : elles s'appuient sur des protocoles MCP et des API pour collecter les données nécessaires, tout en respectant des garde-fous explicites et des modèles d'approbation définis par les clients. Pour garantir la transparence, chaque action s'accompagne d'un raisonnement clair, d'éléments probants et d'une piste d'audit complète. Pour Cisco, la confiance est considérée comme une propriété fondamentale du système plutôt qu'une simple fonctionnalité, ce qui permet à l'équipe IT de garder le contrôle de l'exécution automatisée.

Enfin, l'architecture est complétée par des interactions multimodales, partant du principe que les équipes techniques ont besoin de flexibilité dans leur manière d'interagir avec l'IA. Plutôt que d'imposer une interface unique, Cisco met ses fonctionnalités agentiques à disposition via divers points d'interaction, notamment les tableaux de bord déjà accessibles en disponibilité générale (GA) et AI Assistant, ainsi que des plateformes émergentes comme AI Canvas, les systèmes de messagerie et des outils tiers tels que ServiceNow. Grâce à l'intégration avec des alertes déclenchées par des événements et des interfaces tierces, le système s'adapte aux workflows des équipes IT modernes, et leur apporte son assistance là où elles sont le plus efficaces.

Les quatre piliers stratégiques du cadre agentique de Cisco pour les opérations réseau

Pilier	Objectif principal	Fonctionnalités clés	Valeur ajoutée
Télémétrie multi-domaine	Visibilité et contexte	Couvre les réseaux locaux, les sites distants, le WAN, le data center, la sécurité et les chemins d'applications.	Élimine les silos en permettant aux agents de raisonner à l'échelle du système.
Modèles d'ensemble et expertise	Informations opérationnelles	Combine des modèles de pointe avec le Deep Network Model spécialement conçu par Cisco et des bases de connaissances issues de l'expertise CCIE.	Va au-delà d'une IA généraliste pour offrir une logique de dépannage spécialisée de niveau expert.
Outils, garde-fous et confiance	Exécution sécurisée	Utilise des protocoles MCP et des API dans le respect de garde-fous explicites ; fournit des pistes de raisonnement et d'audit.	Garantit que l'IA n'agit pas « à l'aveugle » et que les opérateurs humains conservent la maîtrise des opérations.
Interaction multimodale	Intégration des workflows	Accessible via les tableaux de bord, AI Assistant, AI Canvas et les outils de messagerie.	S'adapte aux modes de travail des équipes IT sans imposer d'interface unique.

Source : HyperFRAME Research

L'atout de Cisco : bâtir l'avenir des réseaux autonomes avec AgenticOps

Le cadre AgenticOps de Cisco se distingue par une intelligence conçue pour répondre à des besoins clients spécifiques, notamment :

1. **Deep Network Model** : un grand modèle de langage (LLM) spécialement conçu pour le réseau, entraîné sur plus de quarante ans de propriété intellectuelle Cisco. Il interprète la logique sous-jacente des opérations réseau et fournit des informations en temps réel grâce à son intégration avec la télémétrie en direct.
2. **Portée multi-domaine** : une visibilité unifiée couvrant l'ensemble des workloads Cisco dans les domaines du réseau, de la sécurité et de la collaboration.
3. **Socle de données** : une vaste base de données alimentée par les fonctionnalités de Splunk (sécurité et journaux), ThousandEyes (visibilité sur Internet et les applications SaaS) et Meraki (réseau cloud).
4. **Intelligence agentique connectée** : l'intégration et la coordination des technologies de réseau, de sécurité et de collaboration dans les plateformes et les solutions Cisco permettent aux agents et aux outils de partager des informations de manière fluide et de travailler ensemble en temps réel.

Le modèle Deep Network Model de Cisco permet aux agents de s'exécuter avec une large visibilité opérationnelle. Alors que les solutions concurrentes restent souvent limitées à des silos, tels que le diagnostic des réseaux sans fil ou l'automatisation des data centers, les fonctionnalités agentiques de Cisco s'appuient sur une vaste base de données alimentée par les fonctionnalités de Splunk, ThousandEyes et Meraki. Cette approche permet à AgenticOps d'aller au-delà de la simple reconnaissance de schémas en s'appuyant sur une logique de niveau CCIE pour exécuter de manière autonome des actions complexes à l'échelle de l'entreprise, du matériel utilisateur aux applications cloud. Ce modèle est en outre enrichi par plus de 3 000 traces de raisonnement, c'est-à-dire des cheminements logiques issus de l'expertise humaine, qui permettent à l'IA de reproduire les étapes de diagnostic d'un professionnel plutôt que de s'appuyer sur de simples inférences statistiques.

La richesse des données issues de la plateforme Splunk constitue un atout clé d'AgenticOps face aux offres de HPE Juniper et d'Arista. Les agents Cisco s'appuient sur un contexte multi-domaine qui couvre tout le cycle de vie des paquets. Cisco combine la télémétrie en temps réel de Meraki et ThousandEyes avec les vastes données de sécurité et de journalisation de Splunk dans une matrice AI Canvas unifiée. Les agents

disposent ainsi d'une visibilité leur permettant de suivre l'expérience des utilisateurs de la connexion wifi domestique au backend des applications cloud natives en passant par l'Internet public.

Cette télémétrie permet à Cisco d'adopter une approche plus sophistiquée que les diagnostics à domaine unique de ses concurrents. Dans un environnement Cisco, un agent autonome peut établir un lien entre une baisse des performances applicatives et une mise à jour de sécurité spécifique ou une panne affectant un fournisseur d'accès Internet régional, ce qui lui permet d'identifier des causes premières qui resteraient invisibles pour des fournisseurs limités à une vision du seul réseau interne. Ce socle de données complet garantit que lorsqu'un agent Cisco agit, par exemple en réacheminant le trafic ou en ajustant des politiques de sécurité, il le fait avec une compréhension globale des impacts sur l'entreprise. Il offre ainsi un niveau d'intelligence opérationnelle couvrant l'ensemble de la pile technologique que ne peuvent égaler Arista et HPE Juniper.

Enfin, Cisco s'appuie sur une intelligence agentique connectée et multi-domaine, qui permet aux agents de travailler ensemble au sein des outils de réseau, de sécurité et de collaboration tels que Webex, pour résoudre les problèmes sans intervention manuelle. Ce niveau d'intégration est difficile à égaler pour des concurrents tels que HPE Juniper ou Arista, dont les gammes de solutions couvrent un périmètre plus restreint. Cette intégration horizontale permet de limiter les problèmes de performance entre les différentes équipes et les piles technologiques avant qu'elles n'impactent les utilisateurs. Par exemple, un agent réseau qui détecte une hausse de la latence peut automatiquement collaborer avec un agent Webex pour améliorer la qualité des appels ou solliciter un agent de sécurité afin d'isoler un appareil compromis, le tout sans intervention manuelle ni transfert entre les différentes équipes IT.

Cisco accorde une priorité particulière à la sécurité et à la fiabilité de l'IA grâce à une forte capacité d'explication et à des mécanismes de protection intégrés. Pour garantir la fiabilité du système, chaque action réalisée par un agent s'accompagne d'une explication transparente, ce qui permet :

- **De réduire les hallucinations de l'IA** : chaque action autonome s'accompagne d'un raisonnement détaillé expliquant les données et la logique ayant conduit à la conclusion.
- **D'automatiser les restaurations**, pour protéger le réseau contre les conséquences imprévues. Le cadre intègre des mécanismes de restauration automatique qui rétablissent immédiatement la configuration précédente lorsqu'une modification initiée par l'IA entraîne une dégradation des performances, garantissant ainsi une haute disponibilité, même lors des optimisations automatisées.

Par conséquent, Cisco est le seul fournisseur capable de faire le lien entre les plateformes de réseau, de sécurité et d'applications.

Cisco face à la concurrence

Fonctionnalité	Cisco AgenticOps	HPE Juniper/Arista
Moteur d'intelligence	Deep Network Model : entraîné à partir de plus de 40 ans de propriété intellectuelle Cisco et de l'expertise CCIE.	Modèles généralistes ou AIOps cloisonnée reposant sur la reconnaissance de schémas.
Portée des données	Approche multi-domaine : unifie le réseau, la sécurité et la collaboration (Webex).	Principalement axé sur des silos internes, tels que le réseau ou le sans-fil.
Socle de données	Splunk, Meraki et ThousandEyes : un vaste patrimoine de données couvrant les réseaux gérés par Cisco comme les réseaux tiers.	Limité à la télémétrie des équipements propriétaires ou à des outils cloud spécifiques.
Synchronisation des agents	Intégration horizontale : les agents d'un domaine peuvent solliciter ceux d'autres domaines afin de résoudre les problèmes sans transfert manuel entre les équipes.	Silos verticaux nécessitant des transferts manuels entre les différents départements IT.

Source : HyperFRAME Research

L'avantage de la gamme Cisco : ouvrir la voie à l'entreprise autonome grâce à AgenticOps

Pour nous, le principal atout de Cisco réside dans son cadre AgenticOps qui transforme la gestion du réseau de tâches manuelles en un système numérique automatisé et unifié. Cette évolution s'appuie sur un ensemble de fonctionnalités agentiques spécialisées dans le dépannage, l'optimisation et la validation. Ces agents servent d'experts CCIE numériques pour gérer aussi bien la résolution des problèmes que la sécurisation des changements. L'architecture complète repose sur les quatre piliers clés de Cisco pour AgenticOps :

1. Une télémétrie multi-domaine complète
2. Un ensemble de modèles optimisés par des experts
3. Des mécanismes de confiance rigoureux
4. Des interfaces multimodales flexibles, comme AI Assistant et AI Canvas de Cisco

Selon nous, Cisco est idéalement positionné pour accompagner les entreprises dans la mise en œuvre d'une stratégie AgenticOps efficace. Cisco associe son modèle Deep Network Model, qui assure la précision

de ses diagnostics, à l'importante fabric de données de Splunk et à la télémétrie de Meraki et ThousandEyes pour offrir une vue unifiée du réseau que peu de concurrents sont aujourd'hui en mesure d'égaliser. Les fonctionnalités agentiques de Cisco sont très polyvalentes et peuvent fonctionner en mode à la demande, ambiant ou à raisonnement approfondi pour répondre aux différents besoins opérationnels et aux niveaux d'autonomie de chaque entreprise.

Alors que 68 % des entreprises prévoient de remplacer leurs modèles de base chaque année¹, Cisco AgenticOps offre un avantage considérable sur ses concurrents en assurant une commutation fluide entre les moteurs d'IA, sans impact sur la logique métier sous-jacente ni accumulation de dette technique. En outre, Cisco AgenticOps répond directement aux préoccupations liées aux hallucinations de l'IA et à la sécurité exprimées par 90 % des personnes interrogées dans le cadre de notre enquête¹, grâce à des API traçables et exploitables par les agents, ainsi qu'à des garde-fous de sécurité qui assurent la gouvernance et la fiabilité des actions autonomes.

En résumé, nous recommandons aux entreprises d'adopter une approche progressive vers des opérations réseau autonomes. Nous prévoyons que la plupart des entreprises adopteront AgenticOps par étapes : d'abord avec des diagnostics assistés par des agents et des actions correctives validées par des humains, puis avec une exécution en boucle fermée pour des opérations bien maîtrisées et à faible risque avec des mécanismes de restauration clairement définis, avant d'évoluer vers des opérations plus autonomes à mesure que la confiance dans le système s'installe. À terme, la gouvernance, l'auditabilité et la maîtrise du périmètre d'impact constitueront des composantes aussi essentielles d'AgenticOps que l'IA elle-même.

1 (HyperFRAME Research Lens: 1Q 2026)

Recommandations pour évaluer et adopter les opérations agentiques

- **Favoriser une transformation stratégique grâce à AgenticOps :** les principaux décideurs, tels que les CTO, DSI, vice-présidents de l'infrastructure/des opérations, vice-présidents des opérations réseau (NetOps), vice-présidents des opérations de sécurité (SecOps), directeurs de la stratégie cloud/IT et architectes en chef doivent faire de l'évaluation du cadre AgenticOps de Cisco une priorité. Celui-ci transforme l'IA d'un simple outil de productivité en une main-d'œuvre agentique composée d'agents spécialisés capables d'assurer de manière autonome le dépannage, l'optimisation et la validation d'environnements complexes à grande échelle. En s'appuyant sur quarante années d'expertise réseau formalisée et sur une télémétrie unifiée couvrant les domaines NetOps, SecOps et cloud, ce cadre réduit significativement les risques opérationnels et accélère la résolution des problèmes, tout en maintenant une supervision humaine grâce à des garde-fous transparents fondés sur la confiance.
- **Mettre l'accent sur des opérations réseau autonomes de bout en bout :** les entreprises doivent envisager d'adopter le cadre Cisco AgenticOps, qui met à leur disposition une main-d'œuvre agentique complète capable d'assurer de manière autonome le dépannage, d'optimiser les performances de façon proactive et de valider les changements en tenant compte des risques dans les environnements réseau complexes, renforçant ainsi directement les capacités de leurs équipes. Fonctionnant selon divers modes d'exécution, allant de l'assistance à la demande à la planification fondée sur un raisonnement approfondi, ces agents exploitent la télémétrie en temps réel pour résoudre et prévenir les problèmes avant qu'ils n'affectent les utilisateurs.
- **Faire de l'adoption d'un cadre agentique fondé sur la confiance une priorité :** Cisco devrait être considéré comme un partenaire de confiance pour AgenticOps, car son cadre s'appuie sur quarante années d'expertise et sur une télémétrie multi-domaine pour garantir que les actions autonomes sont guidées par des informations opérationnelles spécialisées, supervisées et validées par des humains. Le cadre AgenticOps de Cisco favorise également la transparence et le contrôle grâce à des garde-fous clairement définis et à des interfaces multimodales. Ainsi, chaque action de l'agent est traçable et conforme aux workflows IT établis.





À PROPOS D'HYPERFRAME RESEARCH :

HyperFRAME Research fournit des analyses et des études approfondies sur l'ensemble de l'écosystème technologique mondial, des clouds publics hyperscale aux environnements mainframe, ainsi que toutes les infrastructures intermédiaires. Nous proposons des services de conseil stratégique, des rapports d'étude personnalisés, des consultations personnalisées, des événements numériques, mais aussi des programmes de planification de mise sur le marché, de test de la communication et de génération de leads.

Nos analystes spécialisés réalisent des évaluations rigoureuses, qualitatives et quantitatives, des solutions technologiques, des enjeux métiers, des dynamiques de marché et des attentes des utilisateurs finaux dans de nombreux secteurs d'activité. HyperFRAME Research travaille en étroite collaboration avec vos équipes responsables des relations avec les analystes, des produits et du marketing afin de développer et de valoriser votre expertise, tout en renforçant la visibilité et la reconnaissance de votre marque et de vos solutions. Grâce à des contenus conçus pour capter l'attention des lecteurs, des spectateurs et des auditeurs, nous veillons à ce que votre message trouve un écho sur l'ensemble de vos canaux de communication.

POUR CONTACTER HYPERFRAME RESEARCH :

Steven Dickens

PDG et analyste principal | HyperFRAME Research

Adresse e-mail :

steven.dickens@hyperframeresearch.com

Numéro de téléphone :

+1 845 505 1678

X : @StevenDickens3

LinkedIn : Steven Dickens

BlueSky : Steven Dickens

CONTRIBUTEURS

Ron Westewall

Vice-président et responsable de l'infrastructure et du réseau

DEMANDES

Contactez-nous si vous souhaitez discuter de ce rapport. HyperFRAME Research vous répondra rapidement.

CITATIONS

Ce document peut être cité par la presse et les analystes accrédités, mais doit être cité dans son contexte et afficher le nom de l'auteur, la fonction de l'auteur et « HyperFRAME Research ». Les personnes non accréditées doivent obtenir l'autorisation écrite d'HyperFRAME Research pour toute citation.

LICENCES

Ce document, y compris les supports qui l'accompagnent, est la propriété d'HyperFRAME Research. Cette publication ne peut être ni reproduite, ni distribuée, ni partagée sous quelque forme que ce soit sans l'autorisation écrite préalable d'HyperFRAME Research.

DÉCLARATIONS

HyperFRAME Research fournit des services de recherche, d'analyse et de conseil à de nombreuses entreprises du secteur des hautes technologies, y compris celles mentionnées dans ce document. Aucun collaborateur de notre cabinet n'occupe de poste dans une entreprise citée dans ce document.

