HyperFRAME RESEARCH

FICHE DE RECHERCHE

Cisco AgenticOps

Repenser la résilience mondiale grâce à la mise en réseau autonome et à l'intelligence interdomaine

MARS 2026

Auteur :
Ron Westefall
Vice-président et chef de pratique pour l'infrastructure et le réseau

Synopsis

Les opérations de réseau organisationnel (NetOps) évoluent : elles passent de la simple gestion des appareils à la supervision d'un réseau de capacités distribuées optimisées par l'IA. Les cadres opérationnels existants ne suffisent plus, car ils ont été conçus pour des environnements statiques et une croissance linéaire. Aujourd'hui, la complexité des opérations NetOps est exponentielle. Les opérations couvrent désormais des millions d'entités infonuagiques éphémères et des milliards d'appareils de périphérie OT/IT qui génèrent des volumes de données de télémétrie dépassant les capacités cognitives humaines. Une salle de crise remplie d'ingénieurs qui analysent manuellement les journaux est trop lente pour diagnostiquer et corriger les problèmes ou empêcher l'arrêt du service. Une logique à la vitesse des machines est maintenant nécessaire pour assurer la stabilité du réseau, le routage du trafic et l'atténuation des menaces. Pour réussir cette transition, les organisations doivent passer d'une supervision passive à un système capable de comprendre le contexte et de s'autocorriger avant même qu'une intervention humaine soit possible. Ce système, c'est AgenticOps de Cisco.

AgenticOps de Cisco est un cadre permettant de gérer et de mettre à l'échelle des ensembles d'agents d'IA autonomes présentant différents niveaux d'autonomie au sein d'une entreprise. Il fournit la rigueur opérationnelle nécessaire au déploiement, à la gestion, à la supervision et à la gouvernance des agents d'IA autonomes dans les environnements informatiques. Le cadre permet aux agents d'observer l'infrastructure, d'analyser les problèmes et de prendre des mesures correctives avec une intervention humaine minimale. AgenticOps se concentre sur l'ensemble du cycle de vie d'un agent, en fournissant une infrastructure qui assure la fiabilité, la sécurité et la responsabilisation. Il offre également des mécanismes de gouvernance, de transparence et des contrôles qui permettent une supervision opérationnelle du niveau d'autonomie des agents et de leur exécution.

AgenticOps de Cisco représente la prochaine évolution des opérations informatiques (AIOps). Il combine des actions autonomes conçues selon une approche axée d'abord sur les agents, avec des mécanismes de supervision, pour créer une expérience unifiée où humains et agents collaborent de façon concertée. AgenticOps va bien au-delà de l'AIOps à plusieurs égards importants :

- L'AIOps applique l'intelligence artificielle générative et l'apprentissage automatique pour détecter les anomalies et mettre en corrélation les événements connexes. Les opérateurs humains doivent ensuite interpréter les recommandations, rédiger des scripts d'automatisation et approuver ou appliquer manuellement les correctifs.
- AgenticOps va plus loin, en permettant aux entreprises de déployer en toute sécurité et fiabilité des agents d'intelligence artificielle qui peuvent résoudre les problèmes de manière indépendante et effectuer, à la vitesse des machines, des tâches complexes comportant plusieurs étapes sur différentes plateformes logicielles et matérielles. AgenticOps apporte l'autonomie dans les opérations informatiques, renforçant la capacité et les compétences humaines. Il 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 s'éloigner d'un monde de tableaux de bord sans fin et de routage manuel des billets d'incident. Avec AgenticOps, les agents analysent et évaluent en permanence toutes les dépendances avant même qu'un ingénieur ne reçoive une notification concernant un goulot d'étranglement sur le réseau et n'identifie le problème. Des appareils locaux au nuage, les agents détectent et appliquent instantanément les correctifs. AgenticOps élimine les cloisonnements entre les différents domaines opérationnels, ce qui permet d'optimiser l'expérience globale liée aux services.

Un cadre AgenticOps doit s'ancrer dans la réalité des flux de travail existants de l'organisation; les opérations autonomes ne sont pas et ne devraient pas être instantanées. Les agents intégrés au cadre proposent des plans de correction précis qui sont soumis à l'approbation des intervenants humains et présentés dans une interface pour créer une expérience multijoueur unifiée. Cela permet aux équipes d'instaurer la confiance dans le système et de déléguer l'autorité de façon graduelle. Ainsi, le cycle de vie des TI passe d'un modèle exigeant des interventions manuelles constantes à un modèle fondé sur une supervision automatisée à haut niveau de confiance.

Ce dossier de recherche soulève trois points essentiels :

1. Tout d'abord, AgenticOps est nécessaire, car la complexité des infrastructures numériques modernes a atteint un point critique où une exécution autonome à la vitesse des machines est essentielle pour combler l'écart entre la télémétrie en temps réel et les mesures correctives efficaces.
2. Ensuite, le cadre AgenticOps de Cisco transforme le réseau en un environnement autonome et sans cloisonnement en déployant une main-d'œuvre agentique composée de capacités agentiques spécialisées axées sur le dépannage, l'optimisation et la validation. Ces agents utilisent la télémétrie interdomaine et 40 ans d'expertise codifiée pour agir en tant que partenaires de collaboration aux côtés des équipes informatiques.
3. Enfin, nous évaluons la raison pour laquelle Cisco est le fournisseur de choix d'AgenticOps destiné aux opérations NetOps, grâce à son architecture d'IA unique, profondément intégrée et multicouche. Celle-ci permet de simplifier les opérations et d'accélérer la concrétisation de la valeur grâce à une mise en œuvre complète dans tous les domaines. Nous concluons avec un plan d'action pratique sur les prochaines étapes afin d'aider les décideurs à transformer leur stratégie en une exécution progressive.

L'impératif stratégique : pourquoi AgenticOps est-il nécessaire?

AgenticOps : L'intelligence artificielle pour les opérations informatiques (AIOps) traditionnelle ne suffit pas

Les solutions AIOps traditionnelles ont des limites fonctionnelles. Tout d'abord, l'apprentissage automatique qui a permis de détecter les anomalies et de générer des alertes. Ensuite, l'IA générative est arrivée pour expliquer les problèmes et recommander des mesures correctives. Puis sont apparues les plateformes AIOps, conçues pour recueillir des données télémétriques, mettre des événements en corrélation et améliorer les alertes au sein de cloisons fonctionnelles individuelles comme la mise en réseau ou la sécurité. Bien que l'AIOps contribue à réduire le bruit, elle ne change pas le modèle opérationnel : les humains demeurent le moteur central de la résolution des problèmes, en comblant manuellement les écarts entre les domaines et les observations déconnectés.

Dans les infrastructures modernes, la réalité est que les pannes et la dégradation des performances proviennent rarement d'une seule couche. Elles résultent plutôt d'interactions complexes entre le réseau, le nuage, les protocoles de sécurité et les piles d'applications. Étant donné que les solutions AIOps traditionnelles demeurent largement cloisonnées et axées sur l'observation, les problèmes interdomaines obligent les équipes à effectuer manuellement des corrélations et à réunir des salles de crise. L'AIOps détecte les anomalies dans le système, mais laisse les humains s'en occuper. Cette dépendance à l'égard du dépannage dirigé par l'humain entraîne une fatigue liée aux alertes et prolonge le délai moyen de réparation (MTTR).

Par exemple, alors que l'AIOps se limite à réagir aux données structurées et aux alertes basées sur des seuils, comme le signalement d'une hausse du trafic au moyen d'une notification générique de processeur élevé, AgenticOps utilise une planification enrichie par des outils et propulsée par de grands modèles de langage (LLM) pour parcourir l'ensemble de la pile opérationnelle avec un raisonnement semblable à celui d'un humain. Au lieu d'alerter simplement un ingénieur, un agent autonome peut enquêter sur la cause première d'un problème en interrogeant les visualisations de flux de travail marketing pour vérifier les activités commerciales en cours, en récupérant des procédures d'exécution précises pour la mise à l'échelle promotionnelle à partir de référentiels de documentation internes, en exécutant les scripts nécessaires pour ajuster les ressources, et enfin en résumant l'ensemble de la résolution dans un canal de messagerie d'équipe. Ce changement fait passer le système d'un observateur passif des tendances historiques à un participant actif capable d'effectuer des recherches interplateformes et d'exécuter des tâches de bout en bout. En résumé, l'AIOps est un modèle qui ne peut pas évoluer pour répondre aux exigences actuelles des opérations NetOps numériques.

AIOps et AgenticOps : principales différences en matière d'incidence opérationnelle

Activité NetOps	AIOps traditionnelle	AgenticOps
Surveillance et supervision	Les spécialistes en ingénierie surveillent manuellement les tableaux de bord et répondent aux alertes.	Les agents surveillent constamment le système; les humains passent à un rôle de supervision.
Gestion du changement	Les changements de système nécessitent une exécution manuelle et une surveillance humaine constante.	Les agents planifient, simulent et exécutent les changements de manière autonome dans des paramètres sécurisés.
Dépannage	Enquête dirigée par des humains où les ingénieurs fouillent dans les journaux pour trouver la cause première.	Diagnostic dirigé par des agents où les agents déterminent les problèmes, réfléchissent à des solutions et prennent des mesures avec ou sans validation humaine.

Source : HyperFRAME Research

AgenticOps établit une distinction claire en accordant la priorité aux actions intelligentes. Il ancre le concept d'un environnement d'auto-réparation dans l'exécution concrète, en utilisant l'intelligence artificielle agentique pour prédire les défaillances et déclencher des mesures correctives avant qu'une dégradation des performances, ou pire, ne puisse se propager dans le réseau. En passant d'une supervision passive à une exécution à la vitesse des machines, les organisations peuvent donner la priorité à la réduction de la dette d'infrastructure tout en diminuant et en éliminant les temps d'arrêt opérationnels qui surviennent lorsque les salles de crise dirigées par des humains ne parviennent tout simplement pas à suivre le rythme des perturbations et des défaillances numériques.

Pour être prêtes à adopter AgenticOps à l'échelle de l'entreprise, les organisations doivent d'abord :

1. Établir un cadre de gouvernance qui définit clairement les responsabilités, la traçabilité des audits et des garde-fous humains dans la boucle pour les agents autonomes.

2. Donner la priorité à une architecture modulaire et axée sur les données, en utilisant une approche d'exploration, de parcours et d'exécution, qui garantit une structure de données de haute qualité et une intégration à faible latence dans les flux de travail et les systèmes existants.

3. Adopter un cadre AgenticOps de bout en bout qui combine des renseignements propres à un domaine avec une télémétrie interdomaine unifiée et une gouvernance humaine dans la boucle pour assurer la préparation, gérer les pénuries de compétences et faciliter l'adoption.

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

AgenticOps fait évoluer l'intelligence artificielle en une main-d'œuvre sophistiquée de pairs numériques autonomes. En intégrant une logique de niveau CCIE conçue sur mesure dans la plateforme, Cisco offre des capacités disponibles en tout temps qui vont au-delà de l'automatisation de base pour s'étendre à la collaboration active. Ses capacités agentiques tirent parti d'une intelligence opérationnelle approfondie pour gérer le réseau de manière proactive, offrant des niveaux d'autonomie flexibles qui vont des enquêtes déclenchées par l'humain aux évaluations environnementales continues et approfondies. Ce changement marque une transition transformatrice vers l'IA en tant que partenaire collaboratif qui gère le réseau aux côtés des opérateurs humains, formant ainsi un partenariat agentique, où l'IA et l'expertise humaine se combinent pour orchestrer le réseau.

Cisco a récemment dévoilé la prochaine évolution de son cadre AgenticOps, qui privilégie les opérations simplifiées et les solutions optimisées par l'IA pour favoriser la transition vers un réseau autonome et sans cloisonnement. Au cœur de cette évolution se trouve l'introduction de capacités agentiques élargies en matière de dépannage, d'optimisation et de validation, conçues pour exploiter les environnements réseau avec un minimum d'intervention manuelle. Ces capacités agentiques, ainsi que les améliorations apportées à l'intelligence artificielle, sont intégrées dans les interfaces informatiques couramment utilisées, notamment AI Assistant de Cisco, les flux de travail agentiques, la plateforme Cisco Cloud Control, AI Canvas (à venir), ainsi que des applications tierces.

La main-d'œuvre agentique de Cisco : les capacités agentiques

Capacité agentique	Mandat principal	Fonctionnalité clé	Outils avancés
Dépannage autonome	Propriété de l'incident (de la détection à la résolution)	Appliquer le raisonnement de la télémétrie à la cause première, en validant plusieurs hypothèses simultanément et en exécutant des corrections déterministes avec une précision de niveau CCIE.	AI Packet Capture – Saisie de paquets par l'intelligence artificielle (corrélation de milliers de signaux en temps réel).
Optimisation continue	Amélioration continue (rendement et efficacité)	Maintient en permanence l'expérience de l'utilisateur en ajustant de manière autonome la RF, la QoS, le chemin et les plans de commande avec une compréhension en temps réel des conditions du réseau de bout en bout.	Recommandations de configuration de l'IA (ajustement proactif visant à assurer la prévisibilité).
Validation fiable	Sécurité du changement (de l'intention au résultat)	Les évaluations agentiques tenant compte des risques valident les modifications réseau en fonction de la topologie en temps réel, de la configuration et de la télémétrie, notamment en identifiant l'incidence potentielle et le rayon d'impact.	Modélisation de l'incidence (raisonnement sur la façon dont les changements se propagent dans le système)

Source : HyperFRAME Research

Le premier élément de cette main-d'œuvre agentique est le dépannage autonome, dont le mandat principal est de prendre en charge les incidents, de leur détection jusqu'à leur résolution. Ces capacités analysent les problèmes, effectuent un raisonnement et les résolvent à travers différents domaines en corrélant en temps réel les données télémétriques provenant des couches réseau, de sécurité et Internet. Plutôt que de s'appuyer sur des hypothèses, elles analysent les signaux à grande échelle pour déterminer les causes premières et recommander ou mettre en œuvre des mesures correctives. Cette capacité est renforcée par de nouveaux outils, comme AI Packet Capture, qui permettent à l'agent de traiter simultanément des milliers de signaux afin de fournir des preuves et des explications convaincantes en quelques minutes.

Les capacités agentiques d'optimisation continue et les opérateurs numériques axés sur l'amélioration continue du rendement et de l'efficacité soutiennent la santé du réseau. Ces capacités agentiques adoptent une approche proactive en détectant les dérives de configuration et en prédisant la dégradation dans les environnements sans fil, de commutation et WAN avant que les utilisateurs ne soient touchés. Au lieu d'attendre la création d'un dossier d'assistance, elles identifient les modèles de risque émergents et adaptent l'environnement dans le cadre de garde-fous définis. Ces capacités font l'objet de compétences élargies, notamment des recommandations de configuration par l'intelligence artificielle, conçues pour assurer de façon proactive des performances réseau prévisibles.

Les prochains acteurs de cette main-d'œuvre agentique sont les capacités agentiques de validation de confiance, qui sont chargées de rendre les modifications du réseau plus sécuritaires et plus prévisibles. Ces capacités modélisent l'incidence potentielle et le rayon d'impact d'un changement avant qu'il ne se produise, ce qui révèle les dépendances cachées et les risques en aval. Une fois qu'un changement est mis en œuvre, les agents vérifient automatiquement le résultat et tirent des enseignements des résultats obtenus afin d'améliorer les actions futures. En analysant la façon dont les changements se propagent dans le système, ces capacités veillent à ce que chaque mise à jour rapproche le réseau de l'état souhaité, sans conséquences imprévues.

Les capacités agentiques de Cisco sont conçues pour être flexibles et fonctionnent selon différents modes selon le niveau d'autonomie requis :

1. Les capacités à la demande sont déclenchées par les humains et axées sur des objectifs précis, comme la résolution d'un problème particulier touchant un client.
2. Les capacités agentiques ambiantes sont toujours actives et poursuivent des objectifs continus, comme l'optimisation du Wi-Fi ou la correction des dérives de politiques.
3. Le mode de raisonnement approfondi gère des objectifs complexes de longue durée, comme les validations à l'échelle de l'environnement ou la planification à grande échelle.

Avec le temps, il est prévu que chaque capacité agentique de l'écosystème Cisco couvre les trois modes, offrant ainsi un système de soutien complet et adaptatif aux équipes informatiques.

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

Le cadre agentique de Cisco repose sur quatre piliers architecturaux stratégiques, à commencer par une base de télémétrie interdomaines. Nous constatons que la technologie agentique de Cisco utilise l'un des ensembles de données télémétriques les plus vastes du secteur, couvrant les environnements de campus, de succursales, de réseau étendu (WAN) et de centres de données, ainsi que les couches de sécurité et les chemins d'application. Ce point d'observation complet et de bout en bout permet aux agents de raisonner et d'exécuter des actions dans l'ensemble du système, garantissant ainsi que les informations s'appuient sur l'ensemble de la portée du réseau plutôt que sur des points de données isolés.

Le deuxième pilier porte sur les modèles d'ensemble et l'expertise codifiée de Cisco, qui transforment l'intelligence artificielle générale en renseignements opérationnels spécialisés. En combinant des modèles de pointe et des modèles fondamentaux avec des modèles conçus sur mesure comme le Deep Network Model, Cisco intègre ses capacités agentiques aux trousses de connaissances Cisco Certified Internetwork Expert (CCIE) et aux guides d'exécution élaborés par des experts humains. Nous considérons que cette série de modèles permet au système de choisir l'outil le plus approprié pour chaque tâche, que la situation nécessite une intervention rapide, un dépannage granulaire ou la résolution de défis architecturaux complexes.

Pour garantir que ces actions sont exécutées en toute sécurité, le troisième pilier intègre des outils, des garde-fous et la confiance dès la conception. Les capacités agentiques de Cisco n'agissent pas à l'aveugle : elles utilisent MCP et des API pour recueillir des données tout en fonctionnant dans des gardes-fous explicites et selon des modèles d'approbation définis par les clients. Pour maintenir la transparence, chaque action s'accompagne d'un raisonnement clair, de preuves et d'une piste d'audit complète. Pour Cisco, la confiance est considérée comme une propriété fondamentale du système plutôt que comme une simple fonctionnalité, ce qui permet aux équipes informatiques de garder le contrôle sur l'exécution automatisée.

Enfin, l'architecture est complétée par une interaction multimodale, reconnaissant que les équipes informatiques ont besoin de flexibilité dans la manière dont elles interagissent avec l'IA. Plutôt que d'imposer une interface unique, Cisco met ses capacités agentiques à disposition à travers différents points de contact, y compris les tableaux de bord GA existants et AI Assistant, ainsi que des plateformes émergentes comme AI Canvas, les systèmes de messagerie et des outils tiers comme ServiceNow. En s'intégrant aux alertes pilotées par les événements et aux interfaces tierces, le système s'adapte aux flux de travail établis des organisations de TI modernes, en rejoignant les équipes là où elles sont les plus productives.

Cadre agentique de Cisco pour les opérations réseau (NetOps) : les quatre piliers stratégiques

Pilier	Objectif principal	Principales capacités	Importance
Télémétrie interdomaine	Visibilité et contexte	Couvre les environnements de campus, de succursales, de réseau étendu (WAN), de centre de données, ainsi que la sécurité et les chemins d'applications.	Élimine les cloisons en permettant aux agents d'analyser l'ensemble du système.
Modèles d'ensemble et expertise	Intelligence opérationnelle	Combine des modèles de pointe avec un Deep Network Model et des trousses de connaissances CCIE conçus sur mesure.	Va au-delà de l'IA générale grâce à une logique de dépannage spécialisée de niveau expert.
Outils, garde-fous et confiance	Exécution sécuritaire	Utilise les MCP et les API dans le cadre de garde-fous explicites; fournit des pistes de raisonnement et d'audit.	Veille à ce que l'IA n'agisse pas « aveuglément » et garde les opérateurs humains aux commandes.
Interaction multimodale	Intégration des flux de travail	Accessible via les tableaux de bord, les assistants IA, AI Canvas et la messagerie.	S'adapte au fonctionnement des équipes informatiques plutôt que d'imposer une interface unique.

Source : HyperFRAME Research

Cisco Edge : sécuriser l'avenir des réseaux autonomes grâce à AgenticOps

Le cadre AgenticOps de Cisco se distingue par sa capacité à adapter son intelligence pour répondre aux besoins particuliers des clients, notamment en ce qui concerne les points suivants :

1. **Deep Network model :** un grand modèle de langage (LLM) conçu spécialement et entraîné sur plus de quatre décennies de propriété intellectuelle de Cisco. Il interprète la logique sous-jacente des opérations réseau et fournit des informations en temps réel grâce à son intégration directe avec la télémétrie en direct.
2. **Portée interdomaine :** une visibilité unifiée couvrant toutes les charges de travail Cisco liées aux réseaux, à la sécurité et à la collaboration.
3. **Substrat de données :** un vaste lac de données reposant sur l'exploitation des capacités de Splunk (sécurité et journaux), de ThousandEyes (visibilité sur Internet et les logiciels-services) et de Meraki (réseaux infonuagiques).
4. **Intelligence agentique connectée :** l'intégration et la coordination des technologies réseau, de sécurité et de collaboration au sein des plateformes et solutions Cisco permettent aux agents et aux outils de partager de l'information de façon transparente et de collaborer en temps réel.

Le Deep Network Model de Cisco permet aux agents d'exécuter des tâches grâce à une intelligence opérationnelle étendue. Alors que les solutions concurrentes fonctionnent souvent dans les cloisons axées sur le diagnostic des réseaux sans fil ou l'automatisation des centres de données, les capacités agentiques de Cisco s'appuient sur un vaste lac de données alimenté par l'exploitation des capacités de Splunk, de ThousandEyes et de Meraki. Cela permet au cadre AgenticOps de dépasser la simple reconnaissance de modèles et d'utiliser une logique de niveau CCIE pour exécuter des actions complexes et autonomes qui couvrent l'ensemble de la pile de l'entreprise, de l'appareil de l'utilisateur jusqu'à l'application infonuagique. Ce modèle est encore affiné grâce à plus de 3 000 pistes de raisonnement, qui sont des chemins logiques élaborés par des experts qui garantissent que l'intelligence artificielle reproduit les étapes de diagnostic d'experts professionnels plutôt que de s'appuyer sur de simples estimations statistiques.

Le bassin de données de la plateforme Splunk fait la distinction entre le cadre AgenticOps de Cisco et les offres de HPE Juniper et d'Arista. Les agents Cisco fonctionnent avec un contexte interdomaine qui couvre l'ensemble du cycle de vie des paquets. Cisco combine la télémétrie en temps réel de Meraki, ThousandEyes et la vaste structure de données de sécurité et de journaux de Splunk dans un AI Canvas unifié, offrant ainsi aux agents la visibilité nécessaire pour suivre l'expérience d'un utilisateur à partir d'une connexion Wi-Fi domestique, sur le réseau Internet public, jusqu'aux services dorsaux d'applications natives en nuage.

Cette télémétrie permet à Cisco d'aller au-delà des diagnostics cloisonnés et limités à un seul domaine qui caractérisent généralement les solutions concurrentes. Dans un environnement optimisé par Cisco, un agent autonome peut mettre en corrélation une baisse du rendement d'une application avec une mise à jour de sécurité précise ou une panne de fournisseur d'accès à Internet régional, ce qui lui permet de déterminer les causes premières qui resteraient invisibles pour des fournisseurs se concentrant uniquement sur le réseau interne. Ce substrat de données complet garantit que lorsqu'un agent Cisco intervient, par exemple en réacheminant le trafic ou en ajustant les politiques de sécurité, il le fait avec une compréhension globale de l'impact sur l'entreprise. Il offre ainsi un niveau d'intelligence opérationnelle complète de bout en bout qui demeure hors de portée pour Arista et HPE Juniper.

Enfin, Cisco mise sur une intelligence agentique connectée interdomaine qui permet aux agents de travailler ensemble à l'aide des outils de mise en réseau, de sécurité et de collaboration tels que Webex, pour résoudre les problèmes sans intervention manuelle. Il s'agit d'un niveau d'intégration que des concurrents comme HPE Juniper ou Arista, qui ont une portée plus étroite de la gamme, ne peuvent pas égaler. Cette intégration horizontale garantit que les problèmes de rendement sont atténués dans les différents services et les différentes piles technologiques avant toute perturbation de l'expérience des utilisateurs finaux. Par exemple, un agent de réseau qui détecte un problème de latence peut automatiquement se coordonner avec un agent Webex pour améliorer la qualité des appels ou déclencher l'intervention d'un agent de sécurité afin d'isoler un appareil compromis, le tout sans intervention manuelle ni transfert entre les silos informatiques.

Cisco accorde une importance primordiale à la sécurité de l'IA et à la confiance grâce à de solides mécanismes d'explicabilité et à des mesures de protection intégrées. Pour assurer la fiabilité, le système fournit un raisonnement transparent pour chaque action effectuée par un agent, ce qui permet notamment :

- **L'atténuation des hallucinations de l'IA :** chaque action autonome est accompagnée d'un chemin de raisonnement de la chaîne de pensée qui explique les données précises et la logique utilisées pour parvenir à une conclusion.
- **L'automatisation de la restauration :** un mécanisme qui protège le réseau contre les conséquences imprévues. Le cadre comprend des mécanismes de restauration automatique qui annulent immédiatement les configurations antérieures lorsqu'une modification initiée par l'IA entraîne une dégradation des performances, assurant ainsi une haute disponibilité même lors des optimisations automatisées.

Par conséquent, nous constatons que Cisco occupe une position concurrentielle unique en tant que seul prestataire capable de combler l'écart entre les plateformes de mise en réseau, de sécurité et d'applications.

Analyse comparative : Cisco face à ses concurrents

Fonctionnalité	Cisco AgenticOps	HPE Juniper / Arista
Moteur intelligent	**Deep Network Model :** entraîné sur plus de 40 ans de propriété intellectuelle Cisco et de logique de niveau CCIE.	Modèles à usage général ou mise en correspondance de modèles AIOps cloisonnée.
Portée des données	**Interdomaine :** unifie la mise en réseau, la sécurité et la collaboration (Webex).	Principalement axé sur le réseau interne ou les silos sans fil.
Substrat de données	**Splunk + Meraki + ThousandEyes :** un vaste « bassin de données » couvrant les réseaux détenus et non détenus.	Limité à la télémétrie du matériel propriétaire ou à des outils infonuagiques spécifiques.
Synchronisation interagents	**Intégration horizontale :** les agents d'un domaine peuvent signaler aux agents des autres domaines de résoudre les problèmes sans transfert manuel entre les équipes.	Silos verticaux; nécessite des transferts manuels entre les différents services informatiques.

Source : HyperFRAME Research

Avantage du portefeuille de Cisco : ouvrir la voie à l'entreprise autonome grâce à AgenticOps

Nous pensons que le principal avantage de Cisco réside dans son cadre AgenticOps transformateur, qui fait évoluer la gestion du réseau d'un ensemble de tâches manuelles vers un système numérique unifié et automatisé. Cette évolution est dirigée par une équipe spécialisée dans les capacités agentiques d'IA dédiées au dépannage, à l'optimisation et à la validation, qui agissent comme des experts CCIE numériques pour tout gérer, de la résolution des incidents à la sécurisation des changements. L'architecture de bout en bout est soutenue par les quatre piliers clés de Cisco pour AgenticOps :

1. La télémétrie interdomaine étendue
2. Un ensemble de modèles éclairés par des experts
3. Des garde-fous stricts en matière de confiance
4. Des interfaces multimodales flexibles, comme AI Assistant de Cisco et AI Canvas.

À notre avis, Cisco se positionne solidement comme le partenaire de confiance dont les entreprises ont besoin pour mener à bien la mise en œuvre de leur stratégie AgenticOps. Cisco combine son Deep Network Model, qui assure l'exactitude des diagnostics, à la vaste structure de données de Splunk ainsi qu'à la télémétrie de Meraki et de ThousandEyes afin d'offrir une vue unifiée du réseau que peu de concurrents sont en mesure d'égaler. Les capacités agentiques de Cisco sont très polyvalentes et fonctionnent dans les modes « à la demande », « ambiant » ou de « réflexion approfondie », afin de répondre aux différents besoins opérationnels et aux divers niveaux d'autonomie de chaque organisation.

Alors que 68 % des entreprises prévoient de remplacer leurs modèles de base chaque année[1], Cisco AgenticOps offre un avantage considérable par rapport à la concurrence en permettant une commutation transparente des moteurs d'IA, sans affecter la logique opérationnelle essentielle ni accumuler de dette technique. De plus, AgenticOps de Cisco répond directement aux incertitudes et aux préoccupations de sécurité de 90 % des répondants à notre sondage[1], en fournissant des API traçables pouvant être appelées par les agents ainsi que des garde-fous de sécurité qui garantissent que les actions autonomes demeurent encadrées et fiables.

En résumé, nous recommandons aux organisations d'adopter un chemin différentiel vers l'autonomie des opérations de réseau. Nous prévoyons que la plupart des entreprises adopteront AgenticOps selon une approche en trois étapes (ramper, marcher, puis courir) en commençant par un diagnostic assisté par des agents et une correction approuvée par des humains, puis en évoluant vers une exécution en boucle fermée pour des actions bien comprises et à faible risque avec des mécanismes de restauration clairement définis, avant de passer à des opérations plus autonomes gérées par des agents autonomes à mesure que la confiance envers le système augmente. Au fil du temps, les contrôles de gouvernance, la traçabilité des audits et la limitation du rayon d'impact d'AgenticOps deviendront aussi importants que l'IA elle-même.

1 (Cadre d'analyse HyperFRAME Research : 1er trimestre 2026)

Recommandations pour la transition vers AgenticOps et son évaluation

- **Faire progresser la transformation stratégique avec AgenticOps :** les principaux décideurs, comme les directeurs techniques, les directeurs informatiques, les vice-présidents de l'infrastructure et des opérations, les vice-présidents des opérations réseau (NetOps), les vice-présidents des opérations de sécurité (SecOps), les directeurs de la stratégie infonuagique et informatique ainsi que les architectes en chef doivent accorder la priorité à l'évaluation du cadre AgenticOps de Cisco, puisqu'il transforme l'IA d'un simple outil de productivité en une main-d'œuvre agentique composée d'agents spécialisés capables de dépanner, d'optimiser et de valider de manière autonome des environnements complexes à grande échelle. En s'appuyant sur 40 ans d'expertise réseau codifiée et d'une télémétrie unifiée dans les domaines NetOps, SecOps et infonuagique, ce cadre réduit considérablement les risques opérationnels et accélère le délai de résolution, tout en maintenant une supervision humaine grâce à des garde-fous transparents fondés sur la confiance.
- **Mettre l'accent sur des opérations réseau autonomes complètes :** les entreprises doivent envisager d'adopter le cadre Cisco AgenticOps, car il offre une main-d'œuvre agentique complète qui peut gérer de manière autonome la résolution de problèmes, optimiser le rendement de façon proactive et valider les changements en tenant compte des risques dans des environnements réseau complexes, ce qui renforce directement les capacités de leurs équipes. En travaillant selon différents modes d'exécution, allant de l'assistance à la demande à la planification par raisonnement approfondi, les agents utilisent la télémétrie en temps réel pour résoudre les incidents et prévenir les problèmes avant qu'ils n'aient une incidence sur les utilisateurs.
- **Donner la priorité à l'adoption d'un cadre agentique axé sur la confiance :** Cisco doit être considéré comme le conseiller de confiance pour les agents AgenticOps, car son cadre s'appuie sur quarante années d'expertise et sur une télémétrie interdomaine, garantissant que les actions autonomes sont guidées par une intelligence opérationnelle spécialisée et élaborée par des experts humains. Le cadre AgenticOps de Cisco accorde également la priorité à la transparence et au contrôle en utilisant des garde-fous clairs et des interfaces multimodales, garantissant ainsi que les actions de chaque agent sont vérifiables et alignées sur les flux de travail informatiques établis.

À PROPOS DE HYPERFRAME RESEARCH :

HyperFRAME Research fournit des recherches et des observations approfondies dans l'ensemble du paysage technologique mondial, couvrant tout, du nuage public hyperévolutif à l'ordinateur central, en passant par tout ce qui se trouve entre les deux. Nous proposons des services de conseil stratégiques, des rapports de recherche personnalisés, des missions de conseil sur mesure, des événements numériques, la planification du marché, des tests de messages, et des programmes de génération de pistes de vente.

Nos analystes du secteur se spécialisent dans les évaluations qualitatives et quantitatives rigoureuses des solutions technologiques, des défis commerciaux, des forces du marché et des demandes des utilisateurs finaux dans les différents secteurs d'activité. HyperFRAME Research collabore étroitement avec vos équipes de relations avec les analystes, des produits et de marketing pour créer et développer votre leadership éclairé, en positionnant votre expertise pour améliorer la reconnaissance de la marque et des produits. Grâce à un contenu qui mobilise les lecteurs, les spectateurs et les auditeurs, nous veillons à ce que votre voix trouve un écho dans l'ensemble des canaux.

COMMUNIQUER AVEC HYPERFRAME RESEARCH :

Steven Dickens
PDG et analyste principal | HyperFRAME Research

Adresse courriel :

steven.dickens@hyperframeresearch.com

Numéro de téléphone :

+1 845 505 1678

X : @StevenDickens3

LinkedIn : Steven Dickens

BlueSky : Steven Dickens

CONTRIBUTEURS

Ron Westefall
Vice-président et chef de pratique pour l'infrastructure et le réseau

DEMANDES DE RENSEIGNEMENTS

Communiquez avec nous si vous souhaitez discuter de ce rapport. HyperFRAME Research répondra rapidement aux demandes de renseignements.

CITATIONS

Des extraits de ce document peuvent être cités par des analystes et des représentants accrédités de la presse, à condition qu'ils soient cités en contexte et que le nom de l'auteur, le titre de l'auteur et « HyperFRAME Research » soient indiqués. Les personnes qui ne sont ni des analystes ni des représentants accrédités de la presse doivent avoir obtenu de HyperFRAME Research une autorisation écrite avant de citer des extraits du présent document.

LICENCE

DIVULGATIONS

HyperFRAME Research fournit des recherches, des analyses, des conseils et des services de consultation à de nombreuses entreprises de haute technologie, y compris celles mentionnées dans ce document. Aucun salarié de l'entreprise ne détient des positions en titres de participation dans les entreprises citées dans ce document.


HyperFRAME
RESEARCH