HyperFRAME RESEARCH

STUDIENÜBERSICHT

# Cisco AgenticOps:

## Ein neues Maß an globaler Widerstandsfähigkeit durch autonome Netzwerke und domänenübergreifende Intelligence

MÄRZ 2026

Autor:
**Ron Westefall**
VP and Practice Leader for
Infrastructure and Networking

# Zusammenfassung


Der Netzwerkbetrieb (NetOps) in Unternehmen entwickelt sich vom reinen Gerätemanagement zur Überwachung eines komplexen Netzes aus verteilten, KI-basierten Funktionen. Die bisherigen Frameworks für den Betrieb können damit nicht mehr Schritt halten, da sie auf statische Umgebungen und lineares Wachstum ausgelegt sind. Die NetOps-Komplexität nimmt heute exponentiell zu. Betriebsabläufe umfassen inzwischen Millionen von kurzlebigen Cloud-Einheiten und Milliarden von OT-/IT-Edge-Geräten, die ein Volumen an Telemetriedaten generieren, das die menschliche Vorstellungskraft übersteigt. Ein Team von technischen Fachkräften, das sich manuell um die Protokolle kümmert, ist zu langsam, um Probleme zeitnah zu beheben oder einen Serviceausfall zu verhindern. Nur Systeme mit der entsprechenden Logik sind noch in der Lage, die Netzwerkstabilität, das Traffic-Routing und die Bedrohungsabwehr zu verwalten. Um diesen Wandel zu bewältigen, müssen Unternehmen vom passiven Monitoring auf ein System umstellen, das auf den erforderlichen Kontext zugreifen und sich selbst korrigieren kann, bevor menschliches Eingreifen überhaupt möglich ist. Ein solches System stellt Cisco mit AgenticOps zur Verfügung.

Cisco AgenticOps ist ein Framework für das Management und die Skalierung von Flotten autonomer KI-Agents in Unternehmen mit einem unterschiedlichen Maß an Autonomie. Die Lösung ermöglicht die Bereitstellung, Verwaltung, Überwachung und Steuerung autonomer KI-Agents in IT-Umgebungen. Unter Verwendung des Frameworks können Agents die Infrastruktur beobachten, Probleme analysieren und Korrekturmaßnahmen mit minimalem menschlichem Eingreifen einleiten. AgenticOps deckt den gesamten Lebenszyklus von Agents ab und stellt eine Infrastruktur bereit, die Zuverlässigkeit, Sicherheit und Nachvollziehbarkeit gewährleistet. Darüber hinaus sind Kontrollmechanismen, Transparenz und Steuerung gegeben, um eine betriebliche Überwachung der Autonomie und Ausführung der Agents zu ermöglichen.

Cisco AgenticOps ist die Zukunft des IT-Betriebs (AIOps). Agent-orientierte, speziell entwickelte autonome Aktionen werden in Kombination mit der Überwachung zu einer einheitlichen Erfahrung für mehrere User und Agents kombiniert. AgenticOps geht in verschiedener Hinsicht über AIOps hinaus:

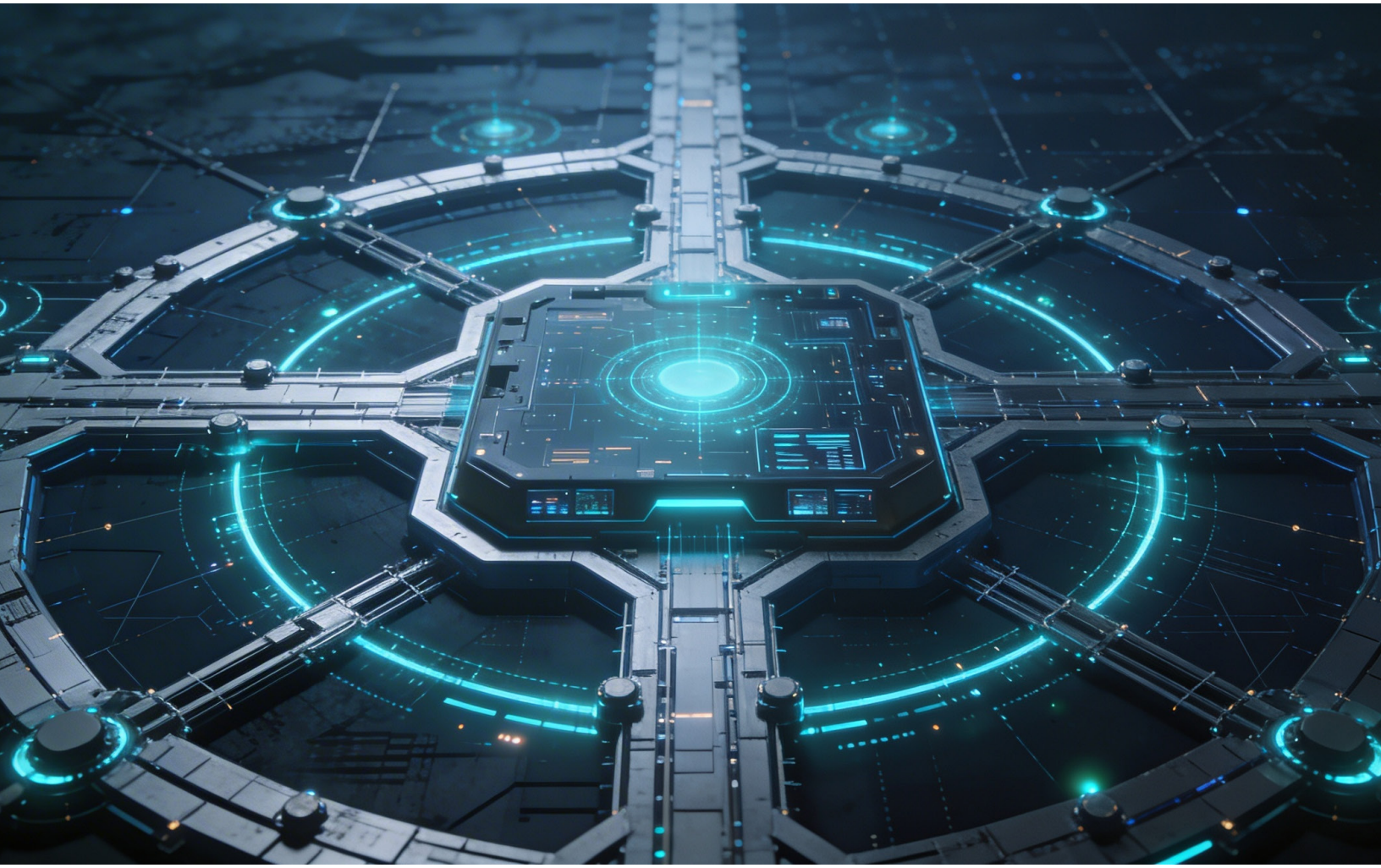
- Bei AIOps werden generative KI und Machine Learning eingesetzt, um Anomalien zu erkennen und die zugehörigen Ereignisse zu korrelieren. Die Interpretation der Empfehlungen, das Schreiben von Automatisierungsskripten und die Genehmigung oder Ausführung der Korrekturmaßnahmen müssen dabei jedoch weiterhin von den MitarbeiterInnen übernommen werden.
- AgenticOps dagegen ermöglicht es Unternehmen, auf sichere und zuverlässige Weise KI-Agents bereitzustellen, die Probleme selbstständig lösen und komplexe, mehrstufige Aufgaben über verschiedene Software- und Hardwareplattformen hinweg in Maschinengeschwindigkeit erledigen können. AgenticOps bringt Autonomie in den IT-Betrieb und erweitert die menschliche Kapazität und Kompetenz. So wandelt sich das Netzwerk von einem reaktiven zu einem proaktiven, sich selbst optimierenden System, in dem Argumentation, Simulation und Ausführung einen geschlossenen Kreislauf bilden.

Im täglichen Betrieb bedeutet dies, dass Sie sich von unzähligen Dashboards und manuellem Ticket-Routing verabschieden können. Mit AgenticOps können Agents kontinuierlich Abhängigkeiten erfassen und bewerten, bevor eine technische Fachkraft eine Benachrichtigung über einen Netzwerkengpass erhält, um das Problem zu identifizieren. Die Agents erkennen und beben Probleme sofort – von den lokalen Geräten bis in die Cloud. AgenticOps beseitigt Silos über verschiedene betriebliche Domänen hinweg und optimiert die Serviceerfahrung insgesamt.

Besonders wichtig ist, dass das AgenticOps-Framework fest in der bestehenden Workflow-Realität des Unternehmens verankert wird. Autonome Abläufe sind nicht unmittelbar und sollten es auch nicht sein. Die Agents stellen innerhalb des Frameworks spezifische Konzepte für Korrekturmaßnahmen bereit, die von den MitarbeiterInnen genehmigt werden können, sodass ein einheitliches Erlebnis für alle Beteiligten entsteht. Auf diese Weise können Teams Vertrauen in das System fassen und Zuständigkeiten schrittweise delegieren, wodurch der IT- Lebenszyklus ohne ständige manuelle Eingriffe auskommt und sich stattdessen zur automatisierten Überwachung mit hoher Vertrauenswürdigkeit wandelt.

In dieser Studienübersicht werden drei Kernpunkte vorgestellt:

1. Erstens: AgenticOps ist erforderlich, weil die Komplexität der modernen digitalen Infrastruktur einen kritischen Punkt erreicht hat, an dem eine autonome Ausführung in Maschinengeschwindigkeit unerlässlich ist, um die Lücke zwischen Echtzeittelemetrie und effektiven Korrekturmaßnahmen zu schließen.
2. Zweitens: Das AgenticOps-Framework von Cisco transformiert das Netzwerk zu einer autonomen Umgebung ohne Silos, in der Agents mit spezialisierten Funktionen für Fehlerbehebung, Optimierung und Validierung die domänenübergreifende Telemetrie sowie 40 Jahre Erfahrung nutzen, um gemeinsam mit den IT-Teams zu agieren.
3. Drittens: In der Studienübersicht wird untersucht, warum Cisco aufgrund seiner einzigartigen, umfassend integrierten und mehrschichtigen KI-Architektur, die optimierte Betriebsabläufe bietet und die Amortisierung durch eine vollständige domänenübergreifende Implementierung beschleunigt, der überlegene Anbieter von AgenticOps für NetOps ist. Abschließend erhalten Sie einen praxisorientierten Plan für die nächsten Schritte, der EntscheidungsträgerInnen dabei unterstützt, von der Strategie zur schrittweisen Umsetzung überzugehen.



# Der strategische Imperativ: Warum ist AgenticOps unverzichtbar?

## AgenticOps: Herkömmliche AIOps-Lösungen sind nicht ausreichend

Herkömmliche AIOps-Lösungen haben eine Funktionsobergrenze. Zuerst wurde Machine Learning eingeführt, um Anomalien zu erkennen und Warnmeldungen zu generieren. Die nächste Generation von KI konnte das Problem auch erklären und Korrekturmaßnahmen empfehlen. Dann folgten AIOps-Plattformen, die Telemetrie erfassen, Ereignisse korrelieren und Warnmeldungen innerhalb einzelner funktionsbezogener Silos wie Netzwerk oder Sicherheit verbessern. AIOps trägt zwar zur Reduzierung des „Grundrauschens" bei, verändert aber nicht das Betriebsmodell. MitarbeiterInnen sind nach wie vor zentral für die Problembehebung, da sie die Lücken zwischen den isolierten Domänen und Einblicken manuell schließen müssen.

In einer modernen Infrastruktur entstehen Ausfälle und Leistungsverschlechterungen selten auf einer einzelnen Ebene. Sie sind vielmehr das Ergebnis komplexer Interaktionen zwischen Netzwerk, Cloud, Sicherheitsprotokollen und Anwendungs-Stacks. Da herkömmliche AIOps-Lösungen weiterhin größtenteils isoliert bleiben und nur der Beobachtung dienen, müssen Teams bei domänenübergreifenden Problemen Daten manuell korrelieren und in War Rooms zusammenarbeiten. AIOps erkennt Anomalien im System, überlässt die Interpretation aber den Usern. Diese Abhängigkeit von manueller Fehlerbehebung führt zu einer Überlastung durch zu viele Warnhinweise und einer Verlängerung der durchschnittlichen mittleren Reparaturzeit (MTTR).

Während AIOps nur auf strukturierte Daten und schwellenwertbasierte Warnmeldungen reagieren kann, beispielsweise in Form der Kennzeichnung einer Datenverkehrsspitze mit einer generischen Benachrichtigung zu einer hohen CPU-Auslastung, nutzt AgenticOps eine LLM-gestützte, mit Tools erweiterte Planung für die Navigation im gesamten Betriebs-Stack mit menschenähnlicher Argumentation. Statt einfach nur ein Technikerteam zu alarmieren, kann ein autonomer Agent die Ursache untersuchen, indem er Marketing-Workflow-Visualisierungen für aktive Umsätze abfragt, spezifische Runbooks zur Skalierung von Werbeaktionen aus internen Dokumentations-Repositorys abruft, die erforderlichen Skripte zur Skalierung von Ressourcen ausführt und schließlich die gesamte Lösung in einem Messaging-Kanal für das Team zusammenfasst. Durch diese Umstellung wandelt sich das System von einem passiven Beobachter historischer Muster zu einem aktiven Teilnehmer, der plattformübergreifende Recherchen durchführen und End-to-End-Aufgaben ausführen kann. Kurz gesagt: AIOps ist ein Modell, das nicht ausreichend skaliert werden kann, um die heutigen digitalen NetOps-Anforderungen zu erfüllen.

**AIOps vs. AgenticOps – die wichtigsten Unterschiede bei den betrieblichen Auswirkungen**

| NetOps-Aktivität | Herkömmliche AIOps | AgenticOps |
|---|---|---|
| **Monitoring und Beaufsichtigung** | TechnikerInnen überwachen Dashboards manuell und reagieren auf Warnmeldungen. | Agents überwachen das System kontinuierlich, während die MitarbeiterInnen die Aufsicht führen. |
| **Change Management** | Systemänderungen müssen manuell umgesetzt und überwacht werden. | Agents planen, simulieren und realisieren Änderungen unter Berücksichtigung sicherer Parameter autonom. |
| **Fehlerbehebung** | Die Untersuchung wird von Menschen durchgeführt: TechnikerInnen durchsuchen Protokolle nach der grundlegenden Ursache. | Die Diagnose erfolgt mit Agents: Sie ermitteln Probleme, wägen Lösungen ab und ergreifen mit oder ohne menschliche Validierung Maßnahmen. |

**Quelle: HyperFRAME Research**

AgenticOps verändert alles, indem es intelligente Maßnahmen priorisiert. Im Mittelpunkt steht das Konzept einer sich selbst korrigierenden Umgebung, die in der Praxis eingesetzt wird und mithilfe von KI-Agents Ausfälle vorhersagen und Korrekturmaßnahmen auslösen kann, bevor sich eine Leistungsverschlechterung oder andere Probleme auf das gesamte Netzwerk auswirken können. Durch die Umstellung vom passiven Monitoring auf die Ausführung in Maschinengeschwindigkeit können Unternehmen die Beseitigung von Infrastrukturschulden priorisieren. Gleichzeitig lassen sich die betrieblichen Ausfallzeiten reduzieren oder ganz ausräumen, die auftreten, wenn von MitarbeiterInnen geführte War Rooms mit der Geschwindigkeit der digitalen Störungen und Ausfälle nicht Schritt halten können.

Um ein Unternehmen auf AgenticOps vorzubereiten, sind folgende Schritte erforderlich:

1. Einrichtung eines Kontrollmechanismen-Frameworks, das klare Leitlinien für die Rechenschaftspflicht, Überprüfbarkeit und menschliche Überwachung der autonomen Agents definiert

2. Priorisierung einer modularen, datengesteuerten Architektur mithilfe eines schrittweisen Ansatzes, der eine hochwertige Daten-Fabric und eine Integration mit niedriger Latenz in die bestehenden Workflows und Systeme gewährleistet

3. Einführung eines End-to-End-Frameworks für AgenticOps, das domänenspezifische Intelligence mit einheitlicher, domänenübergreifender Telemetrie und menschlich überwachten Kontrollmechanismen kombiniert, um die Bereitschaft zu gewährleisten, den Fachkräftemangel zu beheben und die Einführung zu erleichtern

# Vom Tool zum Teammitglied – der Aufstieg der Cisco Agents

Bei AgenticOps nimmt KI die Form autonomer digitaler Teammitglieder an. Durch die Einbettung einer speziell entwickelten Logik auf CCIE-Niveau in die Plattform bietet Cisco stets verfügbare Funktionen, die über die grundlegende Automatisierung hinaus eine aktive Zusammenarbeit ermöglichen. Die Agent-Funktionen nutzen umfassende betriebliche Intelligence für proaktives Netzwerkmanagement und bieten flexible Autonomieebenen, die von manuell ausgelösten Untersuchungen bis hin zu kontinuierlichen, tiefgreifenden Bewertungen der Umgebung reichen. Damit wandelt sich KI zum Partner für die Zusammenarbeit, der das Netzwerk an der Seite der MitarbeiterInnen verwaltet. Es entsteht eine Partnerschaft zwischen Mensch und Agent, bei der KI und das Fachwissen der MitarbeiterInnen zusammengeführt werden, um das Netzwerk zu orchestrieren.

Cisco hat kürzlich die nächste Entwicklungsstufe seines AgenticOps-Frameworks vorgestellt, das vereinfachte Betriebsabläufe und KI-gesteuerte Lösungen priorisiert, um den Wandel zu einem autonomen Netzwerk ohne Silos voranzutreiben. Im Vordergrund dieser Weiterentwicklung steht die Einführung erweiterter Agent-Funktionen für Fehlerbehebung, Optimierung und Validierung, die den Betrieb von Netzwerkumgebungen mit minimalen manuellen Eingriffen ermöglichen sollen. Diese Agent-Funktionen sind neben erweiterten KI-Verbesserungen in häufig verwendete IT-Schnittstellen integriert, darunter Cisco AI Assistant, Agent-Workflows, die Cisco Cloud Control-Plattform, AI Canvas (demnächst verfügbar) sowie Drittanbieteranwendungen.

## Agent-Funktionen bei Cisco

| Agent-Funktion | Hauptaufgabenbereich | Wichtigste Funktionen | Erweiterte Tools |
|---|---|---|---|
| **Autonome Fehlerbehebung** | Zuständigkeit für Vorfälle (von der Erkennung bis zur Behebung) | Agents ermitteln anhand der Telemetrie die Ursache, validieren mehrere Hypothesen gleichzeitig und führen mit einer Genauigkeit auf CCIE-Niveau deterministische Korrekturmaßnahmen durch. | KI-Paketerfassung (Korrelation von mehreren Tausend Signalen in Echtzeit) |
| **Durchgängige Optimierung** | Kontinuierliche Verbesserung (Leistung und Effizienz) | Agents optimieren durchgehend die User Experience, indem sie auf der Grundlage von dynamischen Einblicken in die End-to-End-Netzwerkbedingungen autonome Maßnahmen zur Feinabstimmung auf der RF-, QoS-, Pfad- und Kontrollebene durchführen. | KI-Konfigurationsempfehlungen (proaktive Optimierung für bessere Planbarkeit) |
| **Vertrauenswürdige Validierung** | Sicherheit von Änderungen (von der Absicht bis zum Ergebnis) | Agents validieren Netzwerkänderungen unter Berücksichtigung der Risiken anhand von Live-Topologie, Konfiguration und Telemetrie und ermitteln auch die Auswirkungen und den Wirkungsradius. | Auswirkungsmodellierung (Wie setzen sich Änderungen im System fort?) |

**Quelle: HyperFRAME Research**

Der erste Faktor sind Agents für die autonome Fehlerbehebung, die in erster Linie für Vorfälle, von der Erkennung bis zur Behebung, zuständig sind. Diese Funktionen untersuchen, analysieren und lösen Probleme über mehrere Domänen hinweg, indem Telemetriedaten der Netzwerk-, Sicherheits- und Internetebene in Echtzeit korreliert werden. Sie verlassen sich nicht auf Annahmen, sondern analysieren Signale im großen Stil, um die Ursache zu ermitteln und Korrekturmaßnahmen zu empfehlen oder durchzuführen. Ergänzt werden diese Funktionen durch neue Tools wie die KI-Paketerfassung, mit der Agents Tausende von Signalen gleichzeitig verarbeiten und so in Minutenschnelle verlässliche Nachweise und Erklärungen liefern können.

Die für die kontinuierliche Optimierung zuständigen Agent-Funktionen unterstützen die Integrität des Netzwerks. Sie sind als digitale Betreiber auf die fortlaufende Verbesserung von Leistung und Effizienz ausgelegt. Diese Agent-Funktionen agieren proaktiv, indem sie Konfigurationsabweichungen erkennen und Verschlechterungen in Wireless-, Switching- und WAN-Umgebungen prognostizieren, bevor diese sich negativ auf die User auswirken. Die Agents warten nicht, bis ein Support-Ticket eingeht, sondern erkennen aufkommende Risikomuster und optimieren die Umgebung innerhalb definierter Leitlinien. Diese Funktionen werden unter anderem um KI-Konfigurationsempfehlungen erweitert, die proaktiv für eine planbare Netzwerkleistung sorgen.

Die nächste Komponente sind Agent-Funktionen für die vertrauenswürdige Validierung. Sie sollen Netzwerkänderungen sicherer und besser planbar machen. Diese Funktionen modellieren vorab die potenziellen Auswirkungen und den Wirkungsradius einer Änderung und decken so verborgene Abhängigkeiten und nachgelagerte Risiken auf. Sobald eine Änderung implementiert wurde, überprüfen die Agents automatisch das Ergebnis und lernen daraus, um zukünftige Maßnahmen zu verbessern. Diese Funktionen analysieren, wie sich Änderungen im System verbreiten, und stellen so sicher, dass jede Aktualisierung das Netzwerk näher an seinen vorgesehenen Zustand bringt – ohne unbeabsichtigte Folgen.

Die Agent-Funktionen von Cisco sind auf Flexibilität ausgelegt und arbeiten je nach dem erforderlichen Grad an Autonomie in verschiedenen Modi:

1. On-Demand-Funktionen werden von MitarbeiterInnen ausgelöst und sind für konkrete Ziele wie die Behebung eines bestimmten Client-Problems vorgesehen.
2. Umgebungs-Agents sind stets verfügbar und verfolgen fortlaufende Ziele wie die Wi-Fi-Optimierung oder die Korrektur von Richtlinienabweichungen.
3. Der Modus für tiefgreifende Analysen wird für langfristige, komplexe Ziele wie umgebungsweite Validierungen oder umfangreiche Planungen eingesetzt.

Es ist zu erwarten, dass im Laufe der Zeit jede Agent-Funktion im Cisco Ecosystem alle drei Modi abdecken kann, sodass ein umfassendes, anpassungsfähiges Supportsystem für IT-Teams entsteht.

# Von der Telemetrie zur Vertrauenswürdigkeit – die grundlegende Architektur von Cisco AgenticOps

Das Agent-Framework von Cisco basiert auf vier strategischen Architektursäulen, beginnend mit der Grundlage der domänenübergreifenden Telemetrie. Die Agent-Technologie von Cisco beruht auf einem der branchenweit umfangreichsten Telemetriesysteme, das Campus-, Zweigstellen-, WAN- und Rechenzentrumsumgebungen sowie Sicherheitsebenen und Anwendungspfade abdeckt. Dieser umfassende End-to-End-Beobachtungspunkt ermöglicht es den Agents, im gesamten System Analysen durchzuführen und Maßnahmen einzuleiten, um sicherzustellen, dass die Einblicke auf dem gesamten Netzwerk statt auf isolierten Datenpunkten basieren.

Bei der zweiten Säule stehen Ensemblemodelle und das spezielle Know-how von Cisco im Mittelpunkt, sodass aus allgemeiner KI spezielle betriebliche Intelligence wird. Durch die Kombination von Frontier- und Grundlage-Modellen mit speziell entwickelten Modellen wie dem Deep Network Model stützt Cisco seine Agent-Funktionen auf CCIE-Wissen (Cisco Certified Internetwork Expert) und von Menschen kuratierte Runbooks. Diese Bandbreite an Modellen wird eingesetzt, damit das System immer das passende Tool für die jeweilige Aufgabe auswählen kann – je nachdem, ob die Situation schnelle Reaktionen, präzise Fehlerbehebung oder die Lösung komplexer Architekturherausforderungen erfordert.

Damit diese Aktionen sicher ausgeführt werden, umfasst die dritte Säule integrierte Tools, Leitlinien und Vertrauenswürdigkeit. Die Agent-Funktionen von Cisco arbeiten nicht blind. Sie nutzen MCP und APIs, um Daten zu erfassen, und agieren innerhalb klarer Leitlinien und vom Kunden definierter Genehmigungsmodelle. Um Transparenz zu gewährleisten, wird jede Maßnahme von einer klaren Argumentation, Nachweisen und einem vollständigen Prüfpfad begleitet. Cisco behandelt Vertrauenswürdigkeit als grundlegende Systemeigenschaft statt nur als Merkmal. Die IT-Teams behalten immer die Kontrolle über die automatisierte Ausführung.

Abgerundet wird die Architektur zudem durch multimodale Interaktion, da IT-Teams Flexibilität bei der Nutzung von KI benötigen. Statt eine einzige Schnittstelle zu erzwingen, stellt Cisco seine Agent-Funktionen über verschiedene Berührungspunkte zur Verfügung, darunter die vorhandenen GA-Dashboards und der AI Assistant sowie neue Plattformen wie AI Canvas, Messaging-Systeme und Tools von Drittanbietern wie ServiceNow. Durch die Integration mit ereignisgesteuerten Warnmeldungen und Schnittstellen von Drittanbietern passt sich das System an die etablierten Workflows moderner IT-Abteilungen an, sodass die Teams überall dort unterstützt werden, wo sie am produktivsten sind.

## Das Cisco AgenticOps-Framework für NetOps: die vier strategische Säulen

| Säule | Kernziel | Wichtigste Funktionen | Bedeutung |
|---|---|---|---|
| **Domänenübergreifende Telemetrie** | Sichtbarkeit und Kontext | Umfasst Campus-, Zweigstellen-, WAN-, Rechenzentrums-, Sicherheits- und Anwendungspfade. | Beseitigt Silos, indem es Agents eine Argumentation unter Berücksichtigung des gesamten Systems ermöglicht. |
| **Ensemblemodelle und Fachwissen** | Betriebliche Intelligence | Kombiniert Grenzmodelle mit einem speziell entwickelten Deep Network Model und CCIE-Wissen. | Ermöglicht den Wechsel von allgemeiner KI zu einer speziellen Fehlerbehebungslogik auf Expertenniveau. |
| **Tools, Leitlinien und Vertrauenswürdigkeit** | Sichere Ausführung | Nutzt MCP/APIs innerhalb expliziter Leitlinien und liefert Argumente und Prüfpfade. | Stellt sicher, dass KI nicht „blind“ agiert und MitarbeiterInnen die Kontrolle behalten. |
| **Multimodale Interaktion** | Workflow-Integration | Der Zugriff ist über Dashboards, AI Assistants, AI Canvas und Messaging möglich. | Passt sich an die Arbeitsweise von IT-Teams an, statt eine einzige Schnittstelle zu erzwingen. |

**Quelle: HyperFRAME Research**

# Der Cisco Vorteil: Sicherheit für die Zukunft autonomer Netzwerke durch AgenticOps

Das AgenticOps-Framework von Cisco zeichnet sich dadurch aus, dass seine Intelligence auf unterschiedliche Kundenanforderungen zugeschnitten ist. Dazu zählt Folgendes:

1. **Deep Network Model:** Ein speziell entwickeltes großes Sprachmodell (LLM), das mit dem geistigen Eigentum von Cisco aus mehr als vier Jahrzehnten trainiert wurde, um die zugrunde liegende Logik des Netzwerkbetriebs zu interpretieren und Echtzeiteinblicke durch die direkte Integration mit Live-Telemetrie zu liefern.
2. **Domänenübergreifende Einblicke:** Einheitliche Transparenz für alle Cisco Workloads aus den Bereichen Netzwerk, Sicherheit und Zusammenarbeit.
3. **Datengrundlage:** Ein riesiger Data Lake, der durch die Nutzung von Splunk (Sicherheit und Protokollierung), ThousandEyes (Internet- und SaaS-Transparenz) und Meraki (Cloud-Netzwerke) unterstützt wird.
4. **Intelligence durch verbundene Agents:** Die Integration und Koordination von Technologien für Netzwerk, Sicherheit und Zusammenarbeit über alle Plattformen und Lösungen von Cisco hinweg ermöglicht es Agents und Tools, nahtlos Informationen auszutauschen und in Echtzeit zusammenzuarbeiten.

Das Cisco Deep Network Model stattet Agents mit umfassender betrieblicher Intelligence aus. Während Mitbewerber oft innerhalb von Silos aus Wireless-Diagnosen oder Rechenzentrumsautomatisierung agieren, stützen sich die Agent-Funktionen von Cisco auf einen riesigen Data Lake, der durch die Nutzung von Splunk, ThousandEyes und Meraki Funktionen unterstützt wird. Auf diese Weise kann das AgenticOps-Framework über die einfache Mustererkennung hinausgehen und mithilfe von Logik auf CCIE-Niveau komplexe, autonome Aktionen ausführen, die sich über den gesamten Unternehmens-Stack hinweg erstrecken – von den Geräten der User bis zur Cloud-Anwendung. Zusätzlich optimiert wird das Modell durch über 3.000 Denkpfade, bei denen es sich um von Fachkräften abgeleitete logische Pfade handelt, die sicherstellen, dass die KI die Schritte einer professionellen menschlichen Diagnose nachahmt, statt sich auf statistische Annahmen zu verlassen.

Die Splunk Plattform als Data Moat ist ein Differenzierungsmerkmal des Cisco AgenticOps-Frameworks gegenüber den Angeboten von HPE Juniper und Arista. Die Agents von Cisco agieren mit domänenübergreifenden Kontextinformationen, die den gesamten Paketlebenszyklus abdecken. Cisco kombiniert Echtzeittelemetrie aus Meraki, ThousandEyes und der umfassenden Sicherheits- und Protokolldaten-Fabric von Splunk zur einheitlichen Umgebung von AI Canvas. Diese bietet Agents die Transparenz, die sie benötigen, um die User Experience vom Wi-Fi zu Hause über das öffentliche Internet bis zum Cloud-nativen Anwendungs-Back-End zu verfolgen.

Dank dieser Telemetrie kann Cisco nicht nur eine isolierte Diagnose für einzelne Domänen durchführen, wie bei Mitbewerbern üblich. In einer von Cisco unterstützten Umgebung kann ein autonomer Agent einen Einbruch der Anwendungsleistung mit einem bestimmten Sicherheitsupdate oder einem regionalen ISP-Ausfall in Verbindung bringen und so die Ursache aufdecken, die für Anbieter, die sich strikt auf das interne Netzwerk konzentrieren, verborgen bliebe. Diese umfassende Datengrundlage stellt sicher, dass ein Cisco Agent die geschäftlichen Auswirkungen genau kennt, wenn er Aktionen wie das Umleiten von Datenverkehr oder das Anpassen von Sicherheitsrichtlinien durchführt. So entsteht ein Maß an betrieblicher Full-Stack Intelligence, das für Arista und HPE Juniper unerreichbar ist.

Hinzu kommt bei Cisco domänenübergreifende Intelligence durch verbundene Agents, bei der Agents über Tools für Netzwerk, Sicherheit und Zusammenarbeit wie Webex hinweg zusammenarbeiten und Probleme ohne manuelle Übergaben beheben können. Mitbewerber wie HPE Juniper oder Arista, die sich auf ein enger umgrenztes Portfolio konzentrieren, können mit dieser Integration nicht Schritt halten. Diese horizontale Integration stellt sicher, dass Leistungsprobleme über verschiedene Abteilungen und Technologie-Stacks hinweg entschärft werden, bevor es zu Störungen bei den End Usern kommt. So kann beispielsweise ein Netzwerk-Agent, der eine Latenz erkannt hat, automatisch mit einem Webex Agent zusammenarbeiten, um die Anrufqualität zu verbessern, oder die Isolierung eines kompromittierten Geräts durch einen Sicherheits-Agent auslösen – und das alles ohne manuelle Eingriffe oder Übergaben zwischen IT-Silos.

Cisco priorisiert die Sicherheit und Vertrauenswürdigkeit von KI durch zuverlässige Erklärbarkeit und integrierte Schutzmaßnahmen. Um dies zu gewährleisten, liefert das System für jede Agent-Aktion eine transparente Argumentation. Das ermöglicht Folgendes:

- **Eindämmung von KI-Halluzinationen:** Zu jeder autonomen Aktion gibt es einen Argumentationspfad, aus dem die spezifischen Daten und die Logik hinter einer Schlussfolgerung hervorgehen.
- **Rollback-Automatisierung:** Diese schützt das Netzwerk vor unbeabsichtigten Auswirkungen. Das Framework umfasst automatische Rollback-Mechanismen, die Konfigurationen sofort zurücksetzen, wenn die KI-initiierte Änderung zu Leistungsverschlechterungen führt. So wird auch bei automatisierten Optimierungen eine hohe Verfügbarkeit gewährleistet.

Cisco ist daher als Anbieter einzigartig dafür aufgestellt, die Lücke zwischen Netzwerk-, Sicherheits- und Anwendungsplattformen zu schließen.

## Vergleich zwischen Cisco und Mitbewerberlösungen

| Funktion | Cisco AgenticOps | HPE Juniper/Arista |
|---|---|---|
| **Intelligence-Engine** | **Deep Network Model:** Trainiert mit geistigem Eigentum von Cisco aus mehr als 40 Jahren und CCIE-Logik | Allgemeine Modelle oder isolierte AIOps-Musterabstimmung |
| **Datenumfang** | **Domänenübergreifend:** Vereint Netzwerke, Sicherheit und Zusammenarbeit (Webex) | Schwerpunkt auf internen Netzwerken oder Wireless-Silos |
| **Datengrundlage** | **Splunk + Meraki + ThousandEyes:** Ein enormer „Data Moat“, der sich über eigene und fremde Netzwerke erstreckt | Beschränkt auf proprietäre Telemetrie oder bestimmte Cloud Tools |
| **Agent-übergreifende Synchronisierung** | **Horizontale Integration:** Agents in einer Domäne können Agents in anderen Domänen signalisieren, dass sie Probleme ohne manuelle Übergaben beheben sollen | Vertikale Silos; manuelle Übergaben zwischen verschiedenen IT-Abteilungen erforderlich |

**Quelle: HyperFRAME Research**

# Der Vorteil des Cisco Portfolios: Vorreiter für autonome Unternehmen durch AgenticOps

Wir sind davon überzeugt, dass der Hauptvorteil von Cisco in dem transformativen AgenticOps-Framework liegt, durch das sich das Netzwerkmanagement von manuellen Aufgaben zu einem automatisierten, einheitlichen digitalen System wandelt. Diese Entwicklung wird von einem spezialisierten Team aus KI-Agent-Funktionen für Fehlerbehebung, Optimierung und Validierung vorangetrieben, die als digitale CCIEs alles von der Fehlerbehebung bei Vorfällen bis hin zur Sicherheit von Änderungen managen. Die End-to-End-Architektur stützt sich auf die vier wichtigsten Säulen von Cisco für AgenticOps:

1. Umfassende, domänenübergreifende Telemetrie
2. Ein Ensemble aus Modellen, an denen Fachkräfte mitgewirkt haben
3. Strikte Vertrauensleitlinien
4. Flexible multimodale Schnittstellen wie Cisco AI Assistant und AI Canvas

Unserer Meinung nach ist Cisco der zuverlässige Partner, den Unternehmen für eine erfolgreiche AgenticOps-Implementierungsstrategie benötigen. Das Cisco Deep Network Model, das eine genaue Diagnose ermöglicht, wird mit der riesigen Daten-Fabric von Splunk kombiniert, die auf Telemetrie von Cisco Meraki und ThousandEyes beruht. So entsteht ein zentraler Netzwerküberblick, den nur wenige Mitbewerber ansatzweise bieten können. Die Agent-Funktionen von Cisco sind äußerst vielseitig und können im On-Demand-, Umgebungs- oder tiefgreifenden Modus eingesetzt werden, um den individuellen Betriebsanforderungen und Autonomiestufen des Unternehmens gerecht zu werden.

Da 68 % der Unternehmen planen, ihre Basismodelle jedes Jahr zu ersetzen[1], bietet Cisco AgenticOps einen entscheidenden Vorteil gegenüber Mitbewerbern, da es den nahtlosen Wechsel zwischen KI-Engines ermöglicht, ohne die zentrale Geschäftslogik zu beeinträchtigen oder die technischen Schulden zu erhöhen. Darüber hinaus geht Cisco AgenticOps direkt auf die Bedenken hinsichtlich Halluzinationen und Sicherheit ein, die 90 % der UmfrageteilnehmerInnen äußern[1]: Es werden nachvollziehbare, über Agents aufrufbare APIs und Sicherheitsleitlinien bereitgestellt, damit die autonomen Aktionen kontrolliert und zuverlässig bleiben.

Zusammenfassend empfehlen wir Unternehmen, einen schrittweisen Weg zum autonomen Netzwerkbetrieb einzuschlagen. Wir gehen davon aus, dass AgenticOps von den meisten Unternehmen nach und nach eingeführt wird: beginnend mit Agent-gestützten Diagnosefunktionen und von MitarbeiterInnen genehmigten Korrekturmaßnahmen über die Ausführung im geschlossenen Kreislauf für nachvollziehbare, risikoarme Aktionen mit klaren Rollback-Pfaden bis hin zu autonomeren, durch Agents verwalteten Abläufen, wenn das Vertrauen in das System zunimmt. Mit der Zeit wird AgenticOps für Kontrollmechanismen, Überprüfbarkeit und die Eindämmung von Angriffen ebenso wichtig werden wie die KI selbst.

1 (HyperFRAME Research Lens: 1. Quartal 2026)

# Empfehlungen für den Übergang zu AgenticOps und die Evaluierung der Lösung

- **Fördern Sie die strategische Transformation mit AgenticOps:** Wichtige EntscheidungsträgerInnen wie CTO, CIO, VP of Infrastructure/Operations, VP of Network Operations (NetOps), VP of Security Operations (SecOps), Director of Cloud/IT Strategy und Chief Architect sollten die Evaluierung des AgenticOps-Frameworks von Cisco priorisieren, da es KI von einem grundlegenden Produktivitätstool zu einem Team aus spezialisierten Agents transformiert, das die Fehlerbehebung, Optimierung und Validierung in komplexen Umgebungen im großen Stil autonom durchführen kann. Auf der Grundlage von spezialisiertem Netzwerk-Know-how aus 40 Jahren und einheitlicher Telemetrie über NetOps-, SecOps- und Cloud-Domänen hinweg reduziert das Framework betriebliche Risiken erheblich und beschleunigt die Problembehebung, während gleichzeitig die menschliche Kontrolle durch transparente, vertrauensbasierte Leitlinien gewährleistet bleibt.
- **Achten Sie auf umfassende autonome NetOps:** Unternehmen sollten die Einführung des Cisco AgenticOps-Frameworks erwägen, da es ein umfassendes Team aus Agents bietet, die Fehler autonom beheben, die Leistung proaktiv optimieren und Änderungen in komplexen Netzwerkumgebungen risikobewusst validieren können, was unmittelbare Vorteile bringt. In den verschiedenen Ausführungsmodi, von der On-Demand-Unterstützung bis hin zur tiefgreifenden Planung, nutzen die Agents Echtzeittelemetrie, um Vorfälle zu beheben und Probleme zu verhindern, bevor sie sich auf die User auswirken.
- **Priorisieren Sie die Einführung eines vertrauensorientierten Agent-Frameworks:** Cisco kann als vertrauenswürdiger AgenticOps-Berater betrachtet werden, da das Framework auf 40 Jahren Erfahrung und domänenübergreifender Telemetrie basiert. So ist sichergestellt, dass hinter den autonomen Aktionen spezialisierte, von Menschen kuratierte betriebliche Intelligence steht. Das Cisco AgenticOps-Framework priorisiert zudem Transparenz und Kontrolle durch klare Leitlinien und multimodale Schnittstellen. So ist sichergestellt, dass die Aktionen der Agents nachvollziehbar und an den bestehenden IT-Workflows ausgerichtet bleiben.

## INFORMATIONEN ZU HYPERFRAME RESEARCH:

HyperFRAME Research bietet umfassende Studien und Einblicke zur globalen Technologielandschaft – von Hyperscale-Public-Clouds bis zum Mainframe und alles dazwischen. Unser Angebot umfasst strategische Beratungsservices, individuelle Studien, maßgeschneiderte Beratung, digitale Events, Markteinführungsplanung, Nachrichtentests und Programme zur Lead-Generierung.

Unsere BranchenanalystInnen sind auf die strikte qualitative und quantitative Bewertung von Technologielösungen, geschäftlichen Herausforderungen, Marktkräften und End-User-Anforderungen in verschiedenen Branchen spezialisiert. HyperFRAME Research arbeitet eng mit Ihren Analyse-, Produkt- und Marketingteams zusammen, um Ihre innovativen Lösungsansätze auszubauen und zu stärken. So positionieren Sie Ihr Fachwissen so, dass Sie die Marken- und Produkterkennung verbessern. Durch Inhalte, die LeserInnen, BeobachterInnen und ZuhörerInnen gleichermaßen ansprechen, stellen wir sicher, dass Sie über alle Kanäle hinweg wahrgenommen werden.

## KONTAKT ZU HYPERFRAME RESEARCH:

**Steven Dickens**
CEO & Principal Analyst | HyperFRAME Research

**E-Mail-Adresse:**

steven.dickens@hyperframeresearch.com

**Telefonnummer:**

+1 845 505 1678

**X: @StevenDickens3**

**LinkedIn: Steven Dickens**

**BlueSky: Steven Dickens**

## MITWIRKENDE

**Ron Westefall**
VP and Practice Leader for
Infrastructure and Networking

## ANFRAGEN

Kontaktieren Sie uns, wenn Sie über diesen Bericht sprechen möchten. HyperFRAME Research antwortet Ihnen umgehend.

## ZITATE

Die Angaben in diesem Dokument können von der akkreditierten Presse und AnalystInnen zitiert werden, müssen jedoch im Kontext mit dem Namen des Autors, dem Titel des Autors und „HyperFRAME Research“ genannt werden. Nicht-Pressemitglieder und Nicht-Analysten müssen für Zitate die vorherige schriftliche Genehmigung von HyperFRAME Research einholen.

## LIZENZIERUNG



## OFFENLEGUNGEN

HyperFRAME Research leistet Forschung, Analyse und Beratung für viele High-Tech-Unternehmen, u. a. für die in diesem Dokument erwähnten Unternehmen. Keine MitarbeiterInnen halten Aktienbestände bei den in diesem Dokument genannten Unternehmen.


HyperFRAME
RESEARCH