

Market Trend: Agentic AI for CSP Autonomous Network Operations

23 July 2025 - ID G00832895 - 16 min read

By: Peter Liu, Will Rice, Pulkit Pandey, Kameron Chao

Initiatives: [Create Tech Solutions for the Communications Industry](#); [Artificial Intelligence Leadership](#); [Technology Market Essentials](#)

CSPs are exploring agentic AI for autonomous networks and operations, opening up new opportunities for technology vendors. Vendors can use this research to capitalize on emerging demands for autonomous AI agents, multiagent orchestration and trust frameworks, helping CSPs achieve their autonomous network ambitions.

Overview

Market Opportunities and Challenges

- **Specialized AI agents:** CSPs increasingly seek autonomous network management solutions, driving growth of AI agents. Vendors differentiate themselves by offering specialized agents like those for anomaly detection with advanced reasoning and real-time data access, enabling autonomous monitoring, proactive responses and automated tasks.
- **Multiagent coordination:** As CSPs expand AI agent deployments, coordinating multiple agents becomes critical. While emerging coordination protocols are being developed to enable decision making across distributed agents, true multi-agent orchestration remains largely theoretical, creating opportunities for vendors.
- **Agentic AI governance and security frameworks:** Agentic AI introduces governance challenges as agents operate autonomously without inherent security awareness and inherit system privileges. This drives demand for comprehensive guardrail frameworks encompassing policy enforcement, access control, and compliance auditing. Vendors must develop integrated governance solutions that establish robust guardrails and systematic oversight for autonomous agent operations.

Strategic Planning Assumptions

- By 2028, 65% of Tier-1 CSPs will have implemented AI agents aiming for autonomous network operations, compared to less than 5% in 2025.
- By 2028, 33% of enterprise software applications will include agentic AI, up from less than 1% in 2024.
- By 2028, over 40% of agentic AI projects will be canceled due to escalating costs, unclear business value or inadequate risk controls.

Introduction

AI agent definition: AI agents are autonomous or semiautonomous software entities that use AI techniques to perceive, make decisions, take actions and achieve goals in their digital or physical environments.

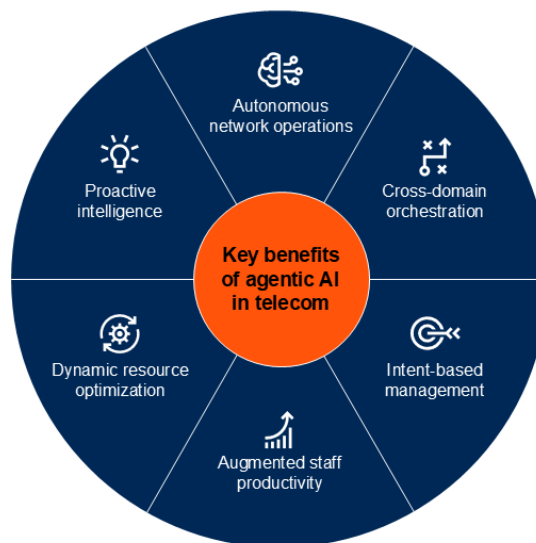
Agentic AI definition: Agentic AI is an approach to building AI solutions that are based on the use of one or multiple software entities that classify completely or at least partially as an AI agent (as defined by Gartner), possibly combined with other non-AI elements.

CSPs are navigating unprecedented complexity driven by 5G, edge computing, network slicing and the explosion of connected devices. Global telecommunications networks support billions of daily connections, creating massive data flows that make current human-centered and reactive operations inadequate.

To address these challenges, CSPs are exploring the potential of agentic AI — autonomous software entities that can perceive, reason, learn, decide and act independently. Unlike traditional AI and automation that execute predefined instruction sets, agentic AI can proactively monitor networks, identify anomalies, diagnose root causes and implement corrective actions with minimal human intervention (see Figure 1). This evolution represents a fundamental shift in network management and creates significant opportunities for technology vendors.

Figure 1: Agentic AI Enhancements to Autonomous Network Operations

Agentic AI Enhancements to Autonomous Network Operations



Source: Gartner
832895

Gartner

However, the market faces a critical challenge: significant “agent washing,” where vendors rebrand existing products — such as AI assistants, RPA tools and chatbots — without substantial agentic capabilities.

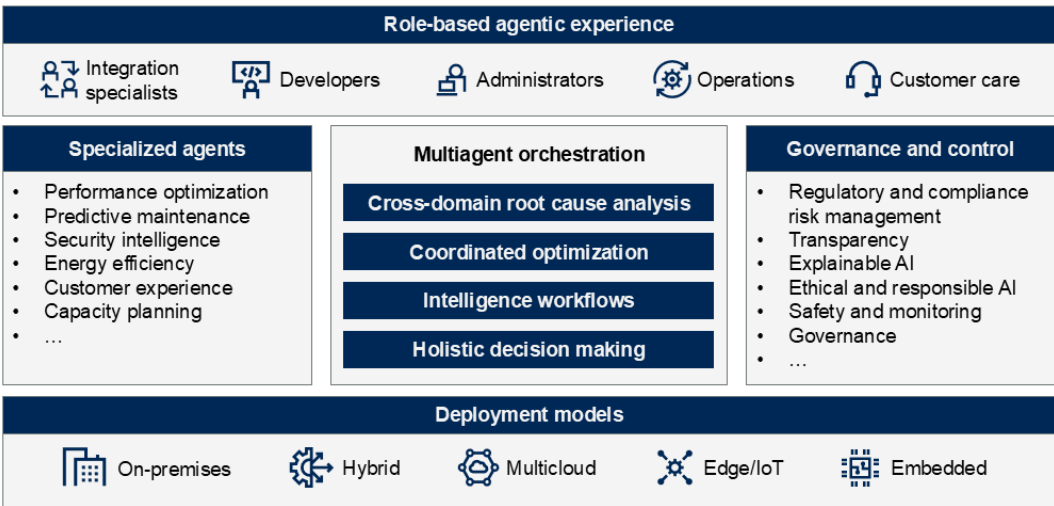
Market Reality Check: *While hundreds of vendors claim agentic AI capabilities, genuine autonomous intelligence that operates independently in mission-critical network environments remains limited. Most current implementations function as enhanced automation tools rather than truly autonomous systems, creating a fragmented landscape that is challenging for CSPs to navigate.*

This research explores three market opportunities within a proposed agentic AI framework that enable vendors to help CSPs achieve autonomous network operations (see Figure 2):

- 1. **Specialized AI agents** — Domain-specific autonomous entities that perform targeted network functions
- 2. **Multiagent collaboration** — Coordination features that enable specialized agents to work together across network domains
- 3. **Agentic AI security and governance** — Comprehensive systems ensuring transparent, responsible AI operation with proper access management

Figure 2: Agentic AI System Architecture

Agentic AI System Architecture



Source: Gartner
832895

Vendors can bridge the “reality gap” by offering specialized AI agents, multiagent coordination tools and AI trust, risk and security management (TRiSM) frameworks. By providing transparent and responsible AI solutions, and guiding CSPs through phased implementations, vendors can enable the safe and scalable deployment of autonomous network operations.

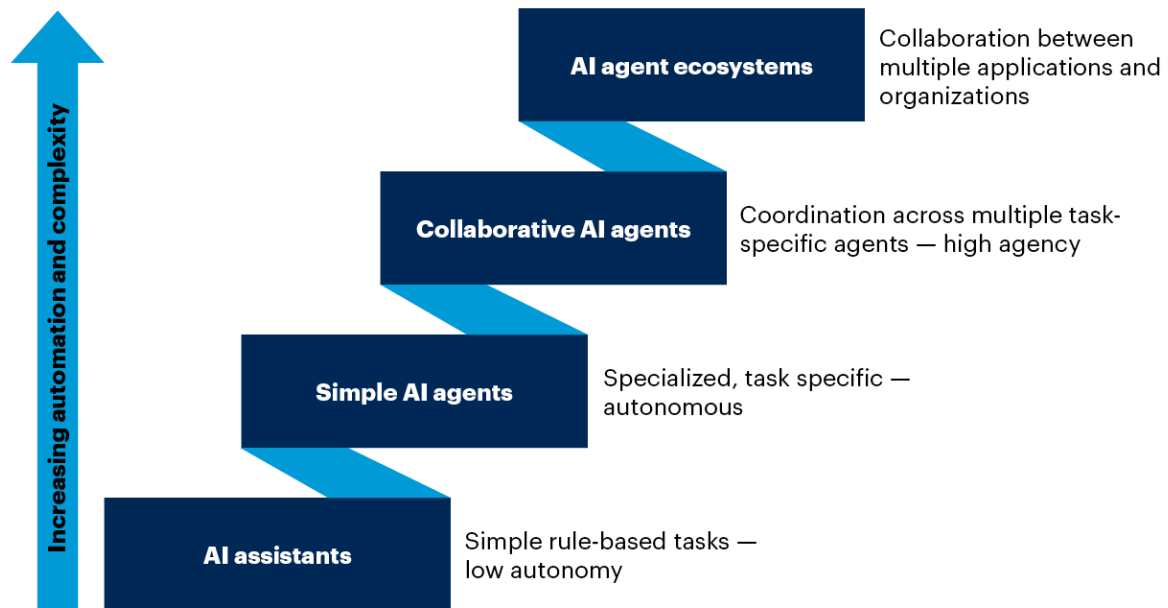
Market Trend

Gartner has identified agentic AI as a top technology trend for 2025, noting a 265% increase in venture capital investment from 2Q24 to 1Q25. The telecommunications industry is undergoing a shift toward agentic AI systems that can independently perceive, reason and act in the management of complex network operations. This trend marks a move from traditional rule-based automation to autonomous systems capable of achieving complex goals with minimal human oversight. This evolution reflects the industry's response to explosive data growth — where global networks generate over 3,800 terabytes of data per minute — and the complexity introduced by 5G, edge computing and network slicing convergence.

However, a significant gap exists between marketing claims and actual capabilities. Gartner reports that out of thousands of “agentic AI” vendors, only about 130 genuinely possess agentic capabilities, with many engaging in “agent washing” by rebranding existing automation tools. This creates confusion for CSPs assessing solutions and highlights the need for clear differentiation criteria (see Note 1).

Reaching true agentic AI is a phased journey, progressing through four key stages (see Figure 3). Most CSPs are currently in the early phases.

Figure 3: Evolution of Agentic AI

Evolution of Agentic AI

Source: Gartner
823982_C

Gartner

Despite significant industry hype around agentic AI, recent market developments reveal that most CSP implementations remain in early stages, with multiagent coordination primarily occurring through existing automation platforms that incorporate agent capabilities alongside traditional workflows. Nokia's new agentic AI capabilities across its autonomous networks portfolio and Ericsson's collaboration with Amazon Web Services (AWS) to drive autonomous networks using agentic AI represent some of the most concrete examples of telecom-specific implementations.^{1,2} In addition, NVIDIA's partnerships with SoftBank, Tech Mahindra, Amdocs, BubbleRAN and ServiceNow demonstrate how large telco models (LTMs) and AI agents are being custom-built for the telecom industry using NVIDIA NIM and NeMo microservices.³

The telecom market is showing a clear division in AI agent strategies: platform vendors partnering with telecom specialists to offer coordinated solutions, and established telecom vendors integrating AI agent capabilities for orchestration within their existing systems. For example, Blue Planet's Agentic AI Framework provides a purpose-built approach for telecom networks, enabling coordinated agent actions across diverse network infrastructures. ⁴ ServiceNow's AI agents in telecom provide CSPs with tailored automation and intelligence through coordinated multiagent systems. ⁵ Similarly, Fabrix.ai (formerly CloudFabrix) provides an agentic AI platform optimized for CSPs, focusing on multiagent orchestration to manage the complex AI agent life cycle for multivendor and multidomain agent discovery, composition and task execution. ⁶ Other strategic moves by major industry players signal the acceleration of this market, including:

- Deutsche Telekom and Google Cloud's partnership to develop the "RAN Guardian" agent using Gemini 2.0 that autonomously detects and resolves radio access network issues ⁷
- SoftBank's development of specialized LTMs trained on network data for autonomous reconfiguration ⁸
- Capgemini's "Dark NOC" solution leveraging agentic AI for autonomous network management with minimal human oversight ⁹

Implementation challenges persist, with vendors and CSPs needing clear guardrails for AI agents, including legal and ethical guidelines on autonomy, liability, security, explainability and data privacy. These considerations are critical for telecom networks where autonomous decisions can impact service availability.

A strategic warning accompanies this trend: Gartner projects that by 2027, over 40% of AI agent projects will be canceled due to escalating costs, unclear business value, or inadequate risk controls. This underscores the importance of selecting appropriate use cases where AI agents deliver measurable business value.

Specialized Agentic AI Transforms Network Operations

Telecom vendors must deliver measurable autonomous network intelligence capabilities as CSPs require solutions for increasingly complex network operations and operational efficiency demands.

CSPs face escalating network complexity, straining traditional automation solutions and creating a significant opportunity for AI-driven network operations. Leading telecommunications vendors are addressing this challenge by developing specialized agentic AI that enables autonomous network management, moving CSPs from reactive to proactive operations.

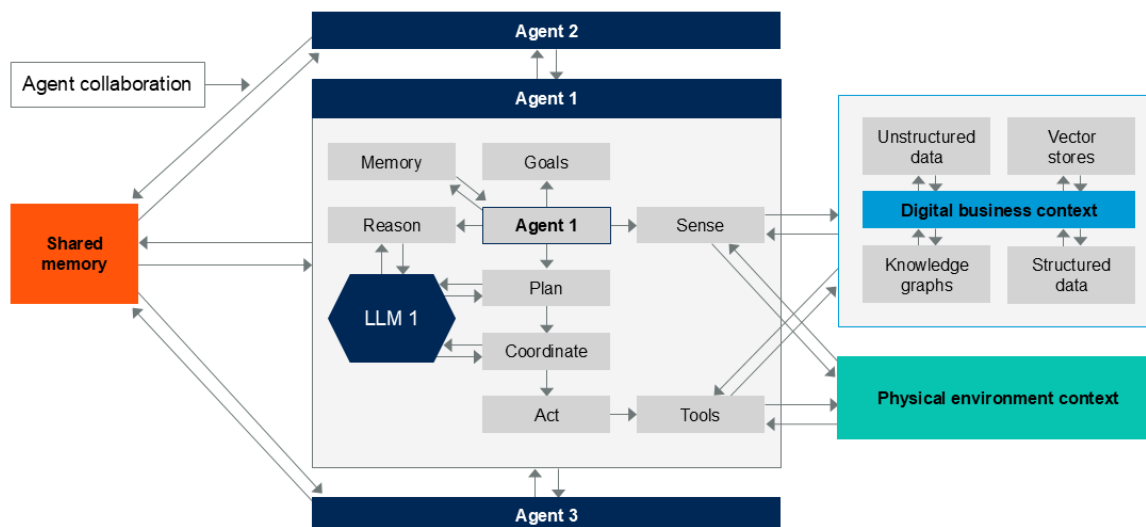
The market is evolving beyond conventional automation toward an ecosystem of specialized agentic AI (see Figure 4). These AI agents autonomously perform critical functions, including anomaly detection, root cause analysis, and corrective action implementation, leveraging technologies like LLMs and RAG to understand network conditions and execute tasks independently. This shift addresses CSPs' urgent need to reduce operational expenses and improve service quality.

To capitalize on this growth opportunity, vendors must prioritize verifiable autonomous intelligence. This includes demonstrating autonomous decision making, multimodal reasoning, and adaptive execution that learns and collaborates with other agents. Overcoming "agent washing" requires vendors to prove their agents' capabilities with measurable results.

Examples of leading vendor solutions include Nokia's AI-powered Threat Hunt Assistant, Tech Mahindra's Proactive Network Anomaly Resolution Hub and SoftBank's LTM-based reconfiguration engine.

Figure 4: Overview of the Agentic AI Agent System

Overview of the Agentic AI Agent System



Source: Gartner
832895

Gartner

The vendor market is evolving to offer a diverse ecosystem of specialized agentic AI, each focused on distinct network operations functions (see Note 2). Performance optimization agents provide autonomous parameter adjustment and traffic-aware optimization. Predictive maintenance agents deliver component health analysis and failure pattern recognition. Security intelligence agents enable real-time threat monitoring and autonomous threat neutralization.

As CSPs' ambitions to achieve L4 autonomous operations increase, vendors that provide complete, easily integrated solutions with demonstrable ROI and gradual adoption paths will capture premium market share. Success depends on moving beyond basic automation to deliver AI agents with clear explainability and measurable business outcomes. In addition, the following actions need to be addressed before the market can scale:

- Reengineer operational workflows to leverage AI agent capabilities while ensuring seamless integration with existing systems
- Provide clear visibility and explainability into agent reasoning and decision processes
- Demonstrate measurable ROI within months rather than years

- Enable gradual adoption paths with increasing levels of autonomy

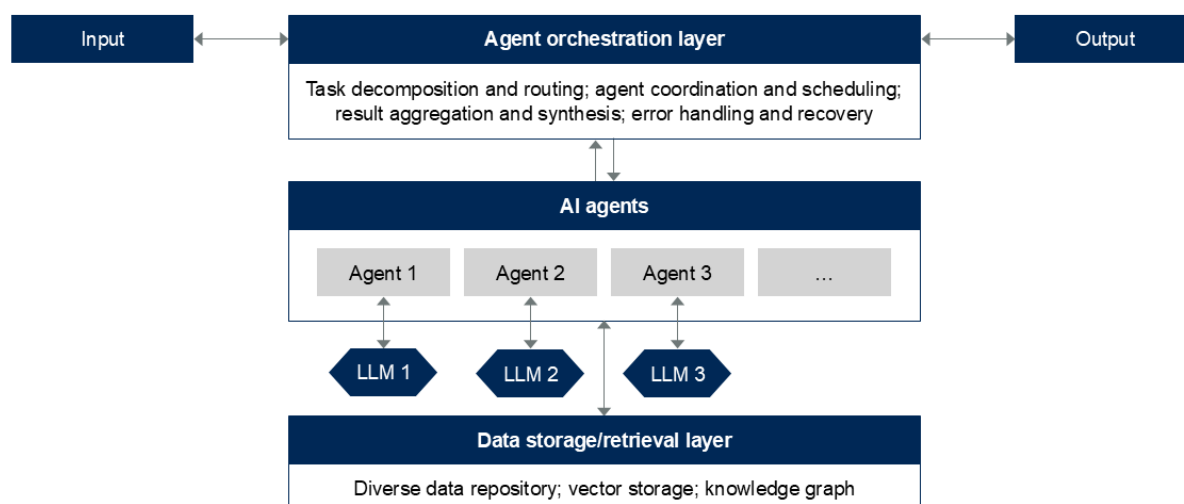
Multiagent Systems Enable Cross-Domain Orchestration

The true transformation occurs when multiple specialized agents collaborate within cohesive frameworks. Advanced AI agent coordination capabilities enable interagent communication, centralizing coordination across network operations, customer service and business processes.

As CSPs increasingly deploy specialized AI agents across their networks, a critical challenge emerges: how to coordinate these agents to ensure consistent, optimized performance across all domains. This challenge presents a significant opportunity for vendors to deliver multiagent platforms — systems that enable collaboration and coordinated action among autonomous agents, maximizing overall network effectiveness (see Figure 5).

Figure 5: Architecture Diagram for Multiagent Orchestration System

Architecture Diagram for Multiagent Orchestration System



Source: Gartner
832895

The market for multiagent orchestration is poised for rapid growth as CSPs recognize the limitations of siloed AI implementations. The value proposition of these multiagent systems extends beyond individual agent capabilities by enabling several of the factors that drive this demand:

- **Network complexity:** Requires coordinated decisions across domains (radio, transport, core)
- **Conflict prevention:** Prevents conflicting actions between independently operating agents
- **Cross-domain optimization:** Enables optimization opportunities that individual agents cannot achieve alone
- **Operational efficiency:** Drives gains through seamless agent collaboration
- **Cross-domain root cause analysis:** Identifies how issues in one domain impact other domains
- **Coordinated optimization:** Balances competing objectives (performance, energy efficiency, cost)
- **Intelligent workflow creation:** Dynamically assigns tasks to specialized agents
- **Holistic decision making:** Provides networkwide context rather than domain-specific views
- **System recoverability challenge:** Maintaining system recoverability is critical. With multiple agents performing different actions, rolling back to a known good state after a failure can be difficult or impossible

Leading vendors are developing multiagent orchestration platforms, each with a distinct approach:

- **Microsoft Copilot Studio (preview):** Enables multiagent coordination with data exchange, task collaboration and workload distribution within the Microsoft ecosystem
- **Google Agent Development Kit (ADK):** Offers workflow coordination capabilities for predictable pipelines or LLM-driven dynamic routing within Google's platform
- **AWS Bedrock:** Provides multiagent collaboration with supervisor mode and routing for optimized request handling within the AWS infrastructure

- **NVIDIA NIM and NeMo microservices:** Delivers a foundational layer for agent collaboration and knowledge sharing within NVIDIA's framework

Despite these advancements, significant challenges remain. Achieving true multiagent coordination is difficult. Maintaining system recoverability is critical, as rolling back to a working state after a failure can be complex with multiple agents involved. Most implementations are currently limited to single platforms, hindering the development of cross-platform, distributed agent systems.

The opportunity:

- **For CSPs:** Multiagent orchestration platforms enable truly autonomous networks that self-optimize across domains
- **For vendors:** These platforms create a strategic position as ecosystem enablers, fostering long-term relationships with CSPs and expanding revenue as more agents are integrated

To succeed, vendors must demonstrate seamless integration between agents from different sources and across diverse network domains. Developing standardized communication protocols, consistent decision-making frameworks and comprehensive orchestration capabilities will command premium pricing. The ultimate goal is to move beyond isolated automation and deliver coordinated intelligence that transforms network operations from reactive management to proactive optimization across all domains.

Agentic AI Governance and Guardian Systems

Agentic AI operates with probabilistic behavior, inherits user privileges, and accesses resources through APIs and UI scraping while lacking human motivation to follow logical security policies. This creates entirely new attack surfaces that existing security tools cannot effectively protect against.

CSPs recognize the immense potential of agentic AI to transform network operations. However, significant concerns around governance, security and operational oversight are hindering widespread adoption. Network operators are hesitant to relinquish control to autonomous systems without robust frameworks for monitoring, controlling and auditing agent behavior. This hesitation creates a substantial market opportunity for vendors offering comprehensive AI agent governance and guardian systems — platforms that extend beyond traditional security approaches to encompass security, operations and enterprise governance.

Gartner research (January 2025) confirms strong market interest, with 64% of organizations planning agentic AI initiatives within the next year. However, this rapid adoption also underscores the urgency for specialized governance solutions. AI agents introduce novel risks, including memory manipulation, prompt injection vulnerabilities and operational risks associated with autonomous decision making. Gartner predicts that over 50% of successful attacks against AI agents will exploit access control weaknesses, and operational failures will increasingly stem from inadequate governance frameworks.

This evolution creates multiple technology segment opportunities, including:

- **Proactive risk mitigation:** Real-time monitoring and intervention proactively prevent security breaches, operational failures and compliance violations stemming from AI agent actions, building trust and ensuring responsible AI deployment.
- **Enhanced system recoverability:** Enforcing operational boundaries and providing rollback capabilities mitigate risks associated with multiple agents executing potentially conflicting actions, ensuring system stability and rapid recovery from failures.
- **Improved auditability and compliance:** Comprehensive audit trails of agent behavior facilitate compliance with regulatory requirements and internal policies, demonstrating responsible AI governance.
- **Cross-domain coordination and optimization:** Monitoring agent interactions, preventing conflicts and aligning individual agent actions with overall network objectives enable coordinated optimization across network domains.
- **Scalable AI governance:** Guardian agent systems provide a scalable framework for governing a growing ecosystem of AI agents, enabling confident deployment of autonomous network operations without being overwhelmed by complexity.

The market opportunity extends beyond pure-play AI security vendors to established application security, identity management and infrastructure security providers who can adapt their platforms for agentic scenarios.

Key to success: Vendors who balance comprehensive oversight with operational efficiency will thrive. Demonstrating scalability across agents and domains, maintaining consistent oversight, and providing explainability are crucial for competitive differentiation and accelerated customer adoption.

Critical focus areas for vendors include integration with existing infrastructure, comprehensive audit solutions, advanced guardian systems combining security and operations, and multimodal governance for diverse data types.

Some CSPs and vendors are already implementing governance solutions:

- **Deutsche Telekom and Google Cloud:** These companies are partnering to implement guardian mechanisms that monitor RAN agents and ensure they operate within defined parameters
- **SoftBank:** Utilizing transparency layers within their LTM implementation to provide operators with clear visibility into AI reasoning processes
- **Nokia:** Incorporating comprehensive audit trails with natural language explanations of complex decisions into their autonomous networks portfolio

Acronym Key and Glossary Terms

dark network operations center (dark NOC)	An autonomous network operations center where AI agents handle routine monitoring, optimization and issue resolution with minimal human intervention
large telco model (LTM)	A specialized large language model trained specifically on telecommunications network data
retrieval-augmented generation (RAG)	An AI technique that enhances language models by retrieving relevant information from external knowledge sources

Evidence

- ¹ [Nokia Adds New Agentic-AI Capabilities Across its Autonomous Networks Portfolio #MWC25](#), Nokia.
- ² [Ericsson's Cognitive Network Solutions and AWS Collaborate to Propel Autonomous Networks With Agentic AI](#), Ericsson.
- ³ [Telecom Leaders Call Up Agentic AI to Improve Network Operations](#), NVIDIA.
- ⁴ [Blue Planet Agentic AI: Powering Your Autonomous Networking Journey](#), Blue Planet.
- ⁵ [Accelerating Telecom Transformation Through Agentic AI and Beyond](#), ServiceNow.
- ⁶ [Fabrix.ai's Enterprise-Grade Agentic AI Platform Generates Strong Interest at Cisco Live'25](#), Fabrix.ai.
- ⁷ [Deutsche Telekom and Google Cloud Partner on Agentic AI for Autonomous Networks](#), Deutsche Telekom.
- ⁸ [SoftBank Corp. Develops a Foundational Large Telecom Model \(LTM\)](#), SoftBank Corp.
- ⁹ [The Rise of the Dark NOC: A new era in Network Operations](#), Capgemini.

Note 1: AI Agent Characteristics, Descriptions and Examples

AI agents are characterized by specific capabilities that distinguish them from conventional automation systems, particularly relevant for telecom network operations (see Table 1).

Table 1: AI Agent Characteristics, Descriptions and Examples

(Enlarged table in Appendix)

Characteristic	Description	Telecom network application examples
Role generalization	Agents have functional behavior described in the context of a specific personality, role or persona, ranging from highly generalized to domain-specific	Network security agents with specialized threat detection personas vs. general network monitoring agents
Proactiveness	Advanced AI agents actively seek additional information from users or tools as required to meet their goal, rather than being only reactive to input	Proactively querying network databases and external threat intelligence when anomalies are detected
Planning	Agents can reason about how best to achieve goals within constraints, breaking problems into tasks and reassessing progress	Planning multistep network optimization workflows and adapting based on real-time performance metrics
Autonomy	Agents can take some or all actions required to achieve goals without human guidance (human review doesn't preclude autonomy)	Autonomous network configuration changes and traffic rerouting during peak usage periods
Goal seeking	Agents accept direction in the form of goals or desired outcomes rather than explicit instructions	Maintaining SLA targets while optimizing network resource utilization and energy consumption
Acting (sensing)	Agents use tools to retrieve information about their environment in a side-effect-free manner	Real-time monitoring of network telemetry across multivendor equipment and performance databases
Acting (effecting)	Agents use tools to take actions that have effects on their operating environment	Implementing configuration changes, traffic rerouting and resource allocation adjustments
Learning (behavioral memory)	Agents learn from past activities by recording actions with positive and negative outcomes	Learning from successful and failed network optimization strategies for future decision making
Memory (facts/context)	Agents retain short-term and long-term information that influences planning and action-taking behaviors	Maintaining historical network performance data and current task context for informed decisions

Source: Gartner (July 2025)

Note 2: Specialized AI Agents for Autonomous Network Operations

Table 2: Specialized AI Agents for Autonomous Network Operations

(Enlarged table in Appendix)

Specialized AI agents	AI agent capability	Technical implementation	Business impact
Network performance optimization agents	Real-time network optimization and traffic flow management	Multiagent systems that automatically adjust routing and bandwidth allocation based on performance	Handle peak traffic loads and optimize network efficiency without human intervention
Predictive maintenance agents	Autonomous fault prediction and prevention before service impact	LLM-based analysis of network telemetry with RAG-enhanced historical data	Reduce network downtime by predicting failures before they occur
Autonomous capacity planner	Predictive bandwidth requirements and automated resource provisioning	RAG-enabled agents assessing real-time network data and subscriber data to forecast and provision capacity detection	Optimize CAPEX investments through AI-powered prediction models
Self-healing network agent	Automated issue detection, diagnosis and resolution without human oversight	Continuous monitoring agents with autonomous remediation capabilities	Enable transition from Level 3 to Level 4 autonomous networks
Configuration automation agent	Dynamic policy enforcement and configuration management	LTM-trained on network-specific data for automated configuration changes	Reduce manual configuration errors and accelerate deployment cycles
Fault diagnostics agent	Root cause analysis and fault isolation across multiple network layers	AI agents that correlate alarm from diverse sources and generate automated resolution workflows	Improve forward-handling rates while reducing resolution time
Spectrum management agent	Autonomous spectrum allocation and interference mitigation	AI-driven spectrum analysis and dynamic allocation based on real-time usage patterns	Optimize spectrum utilization and minimize interference in wireless network
CAPEX = capital expenditure; LLM = large language model; LTM = large telco model; RAG = retrieval-augmented generation			

Source: Gartner (July 2025)

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

[Guide to Embedding Generative and Agentic AI Capabilities in Tech Product Offerings](#)

Emerging Patterns for Building LLM-Based AI Agents

Augment D&A Workflows With Agentic Analytics

Emerging Tech: Avoid Agentic AI Failure: Build Success Using Right Use Cases

Top Strategic Technology Trends for 2025: Agentic AI

© 2025 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

Table 1: AI Agent Characteristics, Descriptions and Examples

Characteristic	Description	Telecom network application examples
Role generalization	Agents have functional behavior described in the context of a specific personality, role or persona, ranging from highly generalized to domain-specific	Network security agents with specialized threat detection personas vs. general network monitoring agents
Proactiveness	Advanced AI agents actively seek additional information from users or tools as required to meet their goal, rather than being only reactive to input	Proactively querying network databases and external threat intelligence when anomalies are detected
Planning	Agents can reason about how best to achieve goals within constraints, breaking problems into tasks and reassessing progress	Planning multistep network optimization workflows and adapting based on real-time performance metrics
Autonomy	Agents can take some or all actions required to achieve goals without human guidance (human review doesn't preclude autonomy)	Autonomous network configuration changes and traffic rerouting during peak usage periods
Goal seeking	Agents accept direction in the form of goals or desired outcomes rather than explicit instructions	Maintaining SLA targets while optimizing network resource utilization and energy consumption
Acting (sensing)	Agents use tools to retrieve information about their environment in a side-effect-free manner	Real-time monitoring of network telemetry across multivendor equipment and performance databases
Acting (effecting)	Agents use tools to take actions that have effects on their operating environment	Implementing configuration changes, traffic rerouting and resource allocation adjustments
Learning (behavioral memory)	Agents learn from past activities by recording	Learning from successful and failed network

	actions with positive and negative outcomes	optimization strategies for future decision making
Memory (facts/context)	Agents retain short-term and long-term information that influences planning and action-taking behaviors	Maintaining historical network performance data and current task context for informed decisions

Source: Gartner (July 2025)

Table 2: Specialized AI Agents for Autonomous Network Operations

Specialized AI agents	AI agent capability	Technical implementation	Business impact
Network performance optimization agents	Real-time network optimization and traffic flow management	Multiagent systems that automatically adjust routing and bandwidth allocation based on performance	Handle peak traffic loads and optimize network efficiency without human intervention
Predictive maintenance agents	Autonomous fault prediction and prevention before service impact	LLM-based analysis of network telemetry with RAG-enhanced historical data	Reduce network downtime by predicting failures before they occur
Autonomous capacity planner	Predictive bandwidth requirements and automated resource provisioning	RAG-enabled agents assessing real-time network data and subscriber data to forecast and provision capacity detection	Optimize CAPEX investments through AI-powered prediction models
Self-healing network agent	Automated issue detection, diagnosis and resolution without human oversight	Continuous monitoring agents with autonomous remediation capabilities	Enable transition from Level 3 to Level 4 autonomous networks
Configuration automation agent	Dynamic policy enforcement and configuration management	LTMs trained on network-specific data for automated configuration changes	Reduce manual configuration errors and accelerate deployment cycles
Fault diagnostics agent	Root cause analysis and fault isolation across multiple network layers	AI agents that correlate alarm from diverse sources and generate automated resolution workflows	Improve forward-handling rates while reducing resolution time

Spectrum management agent	Autonomous spectrum allocation and interference mitigation	AI-driven spectrum analysis and dynamic allocation based on real-time usage patterns	Optimize spectrum utilization and minimize interference in wireless network
CAPEX = capital expenditure; LLM = large language model; LTM = large telco model; RAG = retrieval-augmented generation			

Source: Gartner (July 2025)