Magic Quadrant for Managed Network Services

13 April 2026 - ID G00823802 - 43 min read

By: Karen Brown, Jon Dressel

Initiatives: Technologies and Markets

Managed network services (MNS) providers are racing to upgrade their service delivery platforms with AI to improve performance and gain a competitive edge, but not all have done so consistently. Heads of I&O should evaluate the following MNS vendors for their LAN, WAN and security management needs.

This Magic Quadrant is related to other research:

View All Magic Quadrants and Critical Capabilities

Strategic Planning Assumptions

- By 2030, at least five leading MNS providers will be offering fully autonomous, closed-loop network service assurance capabilities by leveraging AI and automation advancements.
- By 2030, AI agents will be the most common approach for executing network runtime activities, up from minimal adoption in late 2025.
- By 2030, 20% of organizations will shift from MNS to do-it-yourself (DIY) after adopting agentic NetOps, resulting in lower costs by at least 20%.

Market Definition/Description

The managed network services (MNS) market focuses on externally provided network operations center (NOC) functionality, as well as relevant network and security life cycle services.

Gartner defines the MNS market as globally capable providers of remote service management functions for the network and security operations of enterprise networks, including:

- Managed LAN services (MNS for LAN) must include the management of enterprise LAN customer premises equipment (CPE), such as campus switches and wireless access points. It provides single point of contact (SPOC) ownership for the life cycle management of these devices. These services may include the management of customer Internet of Things/Industrial IoT (IoT/IIoT) infrastructure and endpoints. These services may include managed operations services for other elements, such on-premises servers, storage, gateways and controllers.
- Managed WAN services (MNS for WAN) must include the management of site edge ingress and egress CPE and any WAN connections and service operations management. These services provide life cycle management for site edge CPE, such as routers, firewalls and software-defined WAN (SD-WAN), with or without security co-residency on site edge CPE. The services must include a SPOC, ownership for the life cycle management of these devices for site edge CPE and transport services connecting client sites to any destination. This includes hybrid cloud or other non-client-owned locations. These services may also include the operations management of enterprise customer IoT/IIoT infrastructure and endpoint management.
- Managed security services (MNS for security) supports branch offices, remote workers and on-premises general internet security, private application access and cloud service security functions for consumption use cases. Services include health, configuration and maintenance support for security technologies. Service delivery is for a single provider to enterprise clients of multiple vendors of converged network and security function life cycle management operations. These include the support of: (1) SD-WAN-embedded security functions; (2) secure web gateways (SWGs); (3) cloud access security brokers (CASBs); (4) network access control (NAC); (5) network firewalling, with or without intrusion prevention system/intrusion detection system (IPS/IDS); and (6) universal/ero-touch network access (UZTNA/ZTNA) architectures.

Mandatory Features

The mandatory features for this market include:

- **Service delivery platform (SDP):** This area is specific to the application tool infrastructure and the integration of the MNS provider's SDP. An MNS provider's SDP involves the integrated application architecture and the enabling technologies designed to support the standardized, high-quality and scalable delivery of managed network services to enterprise customers. The single MNS SDP supporting LAN and WAN may be separate from, but will be integrated with, a security-specific MNS SDP. The SDP includes an end-user portal from which all provided MNS interactions and reporting are provided and maintained with near-real-time accuracy of data presented.
- **Service management:** MNS management refers to the entirety of life cycle activities — supported by tool-based workflows, automation and customer support mechanisms that are performed by MNS providers. MNS providers deliver these services with internal employee resources for all enterprise customers and industry segments. These provider activities include reporting on end-user customer SLA performance of the MNS provider.
- **Operations automation:** This includes the automation of tasks and activities related to the SDP, service management functions and customer experience (CX) management to achieve consistent MNS service delivery quality.

Common Features

The common features for this market include:

- Support for customer endpoints beyond network and security that may include physical/virtual servers, storage, power, environmental systems, physical security, operational technology (OT) and IIOT.
- Formal continual service improvement programs for MNS customers.
- End-user portal XLA reporting on the performance of the end-user technologies portfolio included in the scope of the MNS agreement.
- Networking and security architecture design services.
- Certifications, such as ITIL v3/v4, relevant OEM vendor and system and organization controls (SOC) 2 certifications.
- Network and security product(s) resale or as OEM sale offers.

Magic Quadrant

Figure 1: Magic Quadrant for Managed Network Services

Gartner

Vendor Strengths and Cautions

Accenture

Accenture is a Leader in this Magic Quadrant. Accenture markets its LAN, WAN and security offerings as a vehicle for customers to transform their IT operations, create a digital core, enable cloud scalability and embed AI into operations. Accenture customers are concentrated in the Americas and Europe, with a smaller customer base in Asia/Pacific. It markets to all verticals, focusing on very large enterprise customers. Accenture plans to:

- Evolve LAN services from AI to agentic AI models to become predictive and autonomous.
- Further invest in secure access service edge (SASE) and secure WAN capabilities, including zero-trust and next-generation firewalls (NGFW) for advanced threat protection and postquantum cryptography (PQC) protection.

Strengths

- **Operations automation:** Accenture has automated much of its managed services delivery processes, supporting faster provisioning and incident resolution.
- **Innovation:** Accenture's agentic AI implementation plans for its managed services delivery platform are more ambitious than most providers in this research, including context-aware change decisions and some incident remediation tasks. This can potentially speed change management and incident resolution.
- **Zero-trust network access (ZTNA) offering:** Compared to others in this research, Accenture's ZTNA offering is more full-featured, supporting service-level agreement, edge and operational technology (OT) deployments. This can allow customers to more easily deploy ZTNA across IT and OT environments.

Cautions

- **Service SLAs:** Accenture's SLAs for LAN, WAN and security are not differentiated by service type, omit specific performance KPIs (including site availability) and provide lower service credits for violations compared to others in this research. Minimal SLA credits tend to result in substandard service reliability.
- **Customer experience:** Accenture's customer portal offers limited user application usage and experience visibility, which can present an incomplete picture of applications performance.

- **Security roadmap:** Accenture's planned investments for managed security services rely primarily on security vendors with few feature additions planned.

AT&T

AT&T is a Niche Player in this Magic Quadrant. Its market focus is to deliver outcome-based managed LAN, WAN and security tailored to specific enterprise customer segments. It has a high customer concentration in the Americas, with a smaller customer base in Europe and Asia/Pacific. AT&T focuses on manufacturing and transportation, retail and financial verticals. AT&T plans to:

- Expand automated incident triage, patch management and maintenance across its MNS products to reduce errors and speed incident resolutions.
- Add agentic AI-based predictive security capabilities, via security partner LevelBlue, to analyze traffic patterns and stop threats before they surface.

Strengths

- **First contact resolution (FCR):** AT&T's percentage of total incidents resolved through first contact has improved in the past year and is now among the highest in this research. This indicates it is more efficient in responding to customers' service issues.
- **Customer experience:** AT&T's customer portal has been upgraded in the past year, with added network visibility, security and analytics views. This supports improved customer experience.
- **Vertical strategy:** Compared to other providers in this research, AT&T's vertical market strategy is more sophisticated, with plans to further tailor managed services for specific verticals including healthcare in the next year.

Cautions

- **Operations automation:** This provider's operations automation lags other providers in this research, which may negatively impact service delivery.
- **Geographic expansion strategy:** AT&T's plan to strengthen its services to expand global MNS market share is weak compared to others in this research, lacking specific regional focus. This may not result in improved services outside the United States.

- **Security:** AT&T's security management, now supported through its LevelBlue joint venture partnership, has improved, but still lags others in this research. It notably offers comparatively limited security SLAs.

Comcast Business

Comcast Business is a Challenger in this Magic Quadrant. Comcast markets its managed LAN, WAN and security services as a composable stack to meet customers' current and future networking needs. Its customer base is primarily in the Americas, with a smaller base in Europe and Asia/Pacific. Its vertical focus includes retail, financial services, hospitality, food and beverage, manufacturing and public sector customers. Comcast plans to:

- Improve LAN switch/access point (AP) provisioning with automated test and turn-up, add standardized templates and improve configuration governance and autoreconsolidation.
- Expand firewall postquantum cryptography features to protect customers from future attacks on network security encryption.

Strengths

- **Customer experience:** Comcast Business offers excellent customer experience support, including comprehensive customer applications experience reporting and a full-featured customer portal.
- **Pricing:** Comcast Business' pricing for managed LAN, WAN and security devices is among the lowest compared to providers in this research.
- **Security data reporting:** The vendor has implemented good security data integrity management processes, which offer customers assurance of accurate security policy and configurations support.

Cautions

- **SLAs:** Comcast Business' MNS for LAN, WAN and security SLAs are substandard, relying heavily on weaker service-level objective targets for metrics including monitoring availability and offering weak service credits for SLA violations. Weak SLA credits tend to result in substandard service reliability.
- **Security roadmap:** This provider's plans to improve threat detection and SD-WAN security are not as comprehensive compared to other providers in this research, making it unlikely customers will see significant service improvement.

- **Geographic strategy:** Comcast Business' customer base is predominantly located in the Americas, and its strategy to improve MNS market share in other regions is weak compared to others in this research. This likely will not result in improved service availability in regions outside the Americas.

DXC Technology

DXC Technology is a Niche Player in this Magic Quadrant. Its managed LAN, WAN and security services focus on providing customers with consulting, network modernization and intelligent operations. Its customer base is distributed across the Americas, Europe and Asia/Pacific. Customer verticals include banking and finance, retail and automotive/manufacturing. DXC plans to:

- Unify wired and wireless networks management, offering seamless control of LAN, SD-LAN and wireless domains.
- Expand its unified network operations center/security operations center (NOC/SOC) locations to improve situational awareness and incident response through integrated dashboards, joint triage and shared governance.

Strengths

- **LAN management:** This provider has made significant improvements in its managed LAN services during the past year and has plans for significant upgrades, all of which likely will improve service delivery.
- **Threat detection upgrades:** DXC has recently upgraded its threat detection and response offerings to improve security protections for enterprise customers.
- **Customer portal roadmap:** DXC plans to add personalization capabilities and predictive analytics to its customer portal, which likely will improve usability.

Cautions

- **Portal update intervals:** DXC's end-user portal data update intervals are significantly slower than other providers in this research. This provides customers with a less than real-time view of their network and security environments.
- **WAN management:** This provider's WAN management capabilities lag others in this research, and it has made relatively modest investments that will likely not improve service delivery.

- **Vertical strategy roadmap:** DXC's vertical strategy roadmap lacks clear targets, making it unlikely it will improve its ability to sell into specific vertical segments.

HCL Technologies

HCL Technologies (d/b/a HCLTech) is a Leader in this Magic Quadrant. Its portfolio of managed LAN, WAN and security services are positioned as secure and AI-ready, enabling customers to transform their IT operations at scale. HCLTech's customer base is concentrated in the Americas and Europe, with a smaller customer base in Asia/Pacific. It markets services to a broad range of enterprise customer verticals. HCLTech plans to:

- Invest in AI- and automation-driven LAN operations, SD-branch products and cloud-managed LAN, and develop verticalized campus and private 5G offerings.
- Expand Cyber Assist, a persona-based cybersecurity delivery platform that uses AI agents to enhance service delivery.

Strengths

- **Service management functions:** HCLTech's continual service management improvement plan is disciplined and comprehensive, resulting in potential benefits to enterprise customers.
- **LAN:** HCLTech has made significant AI and automation upgrades to its managed LAN offerings, and it plans to make further AI and automation upgrades going forward. This will likely translate to improved performance and response for enterprise customers.
- **SD-WAN, cloud access security broker (CASB) management:** HCLTech's secure SD-WAN and CASB management processes are more comprehensive than most other providers in this research.

Cautions

- **FCR:** HCLTech's total FCR rate trails other providers in this research. This may lead to less efficient incident response, which could negatively impact customers.
- **Customer portal:** This provider's customer portal requires users to toggle between multiple management dashboards, resulting in a poor user experience.
- **Network access control (NAC) vendor support:** HCLTech supports a limited list of NAC vendor integrations, which may present implementation challenges for enterprise customers with diverse network environments.

Hughes Network Systems

Hughes Network Systems is a Leader in this Magic Quadrant. It positions Hughes Managed Services as an end-to-end, multitransport, secure hybrid enterprise service platform. Hughes' customers are concentrated in the Americas and Asia/Pacific, with a smaller number of customers in Europe. Its vertical focus includes retail, financial, government, aeronautical, oil and gas, transportation and defense, with plans to add manufacturing, logistics and prison operator customers. Hughes plans to:

- Develop a managed detection and response (MDR) platform enhanced with agentic AI and GenAI assistant to enhance threat analysis, decision making and remediation.
- Add NIST-approved PQC readiness to its secure web gateway (SWG).

Strengths

- **Pricing:** Hughes' pricing for managed LAN, WAN and security is lower than most other providers in this research.
- **WAN roadmap:** This provider's managed WAN service upgrade plans are more ambitious compared to many others in this research, including added AI network visibility and predictive usage features. This likely will improve flexibility for enterprise customers with WAN modernization needs.
- **Security integration:** Hughes' list of integrated NAC vendors and applications is expansive, offering greater deployment flexibility for enterprise customers.

Cautions

- **SD-WAN:** Hughes' portfolio of supported SD-WAN OEM vendors is smaller than most other vendors in this research. This offers customers fewer options to align service with their existing infrastructure investments and network modernization plans.
- **Digital experience:** Hughes' approach to end-user experience monitoring is limited and does not yet include digital experience monitoring tools within its managed services portfolio. This can impair customers' ability to consistently measure and validate applications' performance to meet their business needs.
- **Threat detection:** Hughes' improvements to threat detection lag others in this research.

Kyndryl

Kyndryl is a Niche Player in this Magic Quadrant. It markets its Kyndryl Bridge portfolio as a platform for secure, resilient, agile MNS solutions to help enterprises accelerate digital modernization. Kyndryl's largest customer base is in Asia/Pacific, but it also has a significant base in the Americas and Europe. Target verticals include financial services, industrial, retail, energy and healthcare, and it will widen its strategy to include government customers. Kyndryl plans to:

- Introduce AI agent workflows to accelerate response to LAN issues and create a path toward predictive and autonomous operations.
- Enhance OT and industrial-edge security, including a framework for OT security.

Strengths

- **Digital experience:** Kyndryl offers extensive end-user experience monitoring capabilities and a good lineup of digital experience monitoring (DEM) tools. This gives customers better ability to track end-user services performance compared to others in this research.
- **Customer portal:** Kyndryl's customer portal continues to improve, offering better navigation, user customization features and data update frequency than most providers in this research.
- **Security roadmap:** This provider's security upgrade plans include added microsegmentation and AI and automation upgrades. This will likely deliver noticeable security service improvements.

Cautions

- **WAN upgrades:** This provider's investments in WAN services lag others in this research, and its roadmap for future upgrades is comparatively lacking. These upgrades are likely to result in only minor WAN service improvements in the near future.
- **Data accuracy:** Kyndryl's process to ensure customer inventory data accuracy is poor, with only quarterly validation checks. This will not align well for customers with dynamic environments or ongoing service modernization projects.
- **SD-WAN security:** Kyndryl's managed SD-WAN security offering is more limited than others in this research. Its planned upgrades for SD-WAN security functions also are weak. This will likely result in only minor service improvements.

Lumen

Lumen is a Niche Player in this Magic Quadrant. Its MNS for LAN, WAN and security services are marketed as a platform for on-demand, network, cloud and edge capabilities integrated with managed operations and security. Its customers are concentrated in the Americas, with a smaller customer base in Europe and Asia/Pacific. Key vertical targets include financial services, healthcare, manufacturing and public sector. Lumen plans to:

- Deploy LAN AIOps to support predictive analytics, automated incident triage and zero-touch provisioning.
- Expand its AI-enabled Lumen Defender threat defense platform to all MNS offerings globally.

Strengths

- **Digital experience:** Lumen's end-user experience monitoring is more sophisticated than most providers in this research. This supports better ability for enterprises to track network and applications performance.
- **SD-WAN roadmap:** Lumen's managed SD-WAN product roadmap is strong, with plans to add Palo Alto Prisma as a vendor option and centralized orchestration for configuration changes, among other items. These upgrades are likely to offer enterprise customers improved vendor choice and service management.
- **NAC:** Lumen has added NAC to its security management portfolio, improving its ability to serve a wider range of customers.

Cautions

- **MNS pricing:** Lumen's MNS pricing for managed LAN, WAN and security continue to be higher than most other vendors evaluated in this research.
- **FCR:** Lumen has among the lowest FCR and zero-touch FCR rates among providers in this research. This indicates less efficient incident and service issue response, which can negatively impact customers.
- **Security roadmap:** Lumen's plans to upgrade ZTNA, firewall and SWG functions are limited and will likely not result in significant service improvement.

MetTel

MetTel is a Visionary in this Magic Quadrant. It positions its MNS services as a single source for customized LAN, WAN and security using a wide range of technologies. Its customer base is largest in the Americas, with a smaller base in Europe and Asia/Pacific. MetTel markets primarily to customers in the government, healthcare, financial, retail and industrial verticals. It plans to:

- Expand private 5G deployments, including the launch of its new, single-SIM, managed MetTel Mobile Core that supplies edge computing and roaming on public wireless networks.
- Automate integrations with additional access providers and connect MetTel's backbone to the Starlink network, followed by the Amazon Leo network.

Strengths

- **Monthly recurring charge terms:** MetTel does not add extra monthly charges for moves, adds, changes and drops (MACD), unlike most other providers in this research. This provides enterprise customers with better service cost predictability.
- **Service descriptions:** This provider's customer-facing service descriptions used in presales are better than most providers in this research, providing prospective customers with a good balance of technical detail and business value messaging.
- **Secure SD-WAN, SWG roadmap:** MetTel's upgrade plans for secure SD-WAN are robust, including unified microsegmentation from WAN to LAN to Wi-Fi. Its SWG roadmap is similarly strong, including data loss prevention (DLP) protection and domain name system (DNS)-layer security with AI phishing detection and domain reputation scoring to block threats.

Cautions

- **Operations automation:** MetTel's efforts to automate MNS processes lag other providers in this research. This may result in less efficient service delivery.
- **Pricing:** MetTel's pricing for managed LAN and SD-WAN is higher than most other vendors evaluated in this research.
- **SD-WAN security vendor options:** MetTel's secure SD-WAN OEM vendors' support options are more limited than most other providers in this research. This offers customers fewer options to align security services with their existing infrastructure investments and network modernization plans.

Microland

Microland is a Leader in this Magic Quadrant. It positions its intelligeni platform for MNS LAN, WAN and security offerings as AI-first and platform-driven, delivering measurable, transformative outcomes for customers. Microland's customer base is primarily in the Americas and Europe, with a smaller base in Asia/Pacific. Target industries include the healthcare, retail, manufacturing and government verticals, which will expand to include aerospace/defense. It plans to:

- Expand intelligeni anomaly detection to learn user/device behavior and flag deviations that could indicate a security threat or Internet of Things (IoT) device malfunction.
- Upgrade extended detection and response (XDR) to include a natively integrated detection and threat-hunting platform.

Strengths

- **Customer experience:** Microland's intelligeni MNS customer portal is above average compared to others in this research, offering good navigation, user customization options and visibility into network and security environments.
- **LAN, WAN roadmaps:** Microland's upgrade plans for managed LAN and WAN are more ambitious than most providers in this research, and they will likely translate to service improvements for enterprise customers.
- **ZTNA:** Microland's managed ZTNA offering is more full-featured compared to many others in this research, including microsegmentation and DLP capabilities and integration with a broad set of SASE vendors.

Cautions

- **Monthly recurring charge terms:** Microland's monthly charge terms limit "person-hours" for MACD more than other providers in this research, and it does not make exceptions for MACD via automation. This could lead to additional charges for MACD even if the task is automated.
- **Vertical strategy:** Microland's vertical strategy does not target financial services customers. Its services may not be well-aligned for these customers.
- **Secure SD-WAN roadmap:** Microland's plans to upgrade security for SD-WAN are weak compared to many others in this research.

NTT DATA

NTT DATA is a Leader in this Magic Quadrant. Its MNS services are positioned as AI-centric and future-ready, providing a secure digital foundation to support business outcomes. NTT DATA's largest customer base is in Asia/Pacific, followed by the Americas and Europe. Its vertical strategy is evolving from a broad industry focus to specifically target healthcare, financial services, manufacturing, retail and the public sector. NTT DATA plans to:

- Enhance SD-WAN monitoring with agentic AI orchestration integrated with vendor-native tooling.
- Use agentic AI to improve security incident triage, root cause analysis and response across distributed environments.

Strengths

- **FCR:** NTT DATA's rate of total FCR and zero-touch FCR are higher than most other competitors in this research. This indicates it offers good response levels for service issues.
- **Pricing:** This provider's average pricing for managed LAN, WAN and security is lower than most other providers in this research.
- **Security monitoring availability:** NTT DATA's reporting of security monitoring availability is more sophisticated than many others in this research, offering end-to-end availability rather than simpler device uptime. This supports a better view of WAN, LAN and security monitoring performance.

Cautions

- **CASB, threat detection upgrades:** This provider's recent upgrades to its MNS CASB and threat detection offerings are minor compared to other providers in this research and will likely not deliver significant service improvements.
- **Customer experience roadmap:** NTT DATA's customer portal navigation and ease of use is weaker compared to other providers in this research, and its planned portal upgrades are not likely to improve the experience.
- **NAC integration:** NTT DATA has minimal NAC application integrations, which may limit customers' device access control options.

Sify Technologies

Sify Technologies is a Leader in this Magic Quadrant. Its MNS services are positioned as a platform for secure, scalable solutions to support digital transformation and business outcomes. Sify's customer base is primarily in Asia/Pacific, with a smaller base in the Americas and Europe. Target verticals include financial services and manufacturing. Sify plans to:

- Offer unified observability, AI-assisted analytics and closed-loop automation across LAN, WAN, cloud and security domains.
- Enhance WAN application-level visibility, path analytics and experience-level agreements (XLAs), enabling faster root-cause isolation and proactive performance optimization.

Strengths

- **WAN management investments:** This provider's recent upgrades to its managed WAN portfolio include additional visibility across hybrid network environments, automated provisioning and configuration, and agentic AI support for select network incidents. These improvements are likely to improve service delivery.
- **Incident classification:** Sify's incident classification is more structured and detailed than other providers in this research. This will tend to support accurately prioritized response to service issues.
- **Security roadmap:** Sify Technologies' plans to improve its managed security services are better than many providers in this research, including the addition of AI-driven analytics, unified policy management and adaptive ZTNA.

Cautions

- **Pricing:** Sify Technologies' pricing for managed LAN and managed OEM SD-WAN includes hardware, licensing and security fees, and is therefore higher than most other providers in this research.
- **FCR:** Sify's FCR and zero-touch FCR are among the lowest of all providers in this research. This may lead to less efficient incident response that can negatively impact customers.

- **NAC integrations:** Sify Technologies does not enable NAC integration with other security tools, including endpoint detection and response (EDR), web application firewall (WAF) and security information and event management (SIEM). This may present implementation and security consistency challenges for customers.

Systal Technology Solutions

Systal Technology Solutions is a Leader in this Magic Quadrant. Its MNS offerings focus on moving customers from complex, multivendor environments to standardized, simplified and automated operations. Its customer base is primarily in Europe, with a smaller base in the Americas and Asia/Pacific. Key vertical targets include manufacturing, utilities and financial services customers. Systal plans to:

- Extend LAN telemetry to capture more network device performance metrics to correlate with application telemetry.
- Use its Systal Secure AI Manager (SAM) analytics tool to further tune security incident detection rules, microsegmentation policies and incident response workflows.

Strengths

- **Operations automation:** Systal's automation of incident and alert management processes is above average compared to other providers in this research and can support more efficient and responsive service delivery.
- **Customer experience:** Systal's MNS customer portal offers excellent navigation and full-featured user customization, incident management, network visibility and analytics tools. Its customer experience roadmap also is strong, featuring added behavioral, security and compliance dashboard analytics.
- **Security roadmap:** This provider's managed security upgrade plans are better than most providers in this research, including further process automation and proactive threat hunting. These upgrades are likely to improve service quality.

Cautions

- **Security pricing:** Systal's pricing for managed security appliances is higher than most providers in this research.
- **SLAs:** Systal's standard SLAs for managed LAN, WAN and security include weak service credits for SLA violations. Weak service credits tend to result in substandard service reliability and delivery.

- **Geographic strategy:** Systal's customer base is primarily in Europe, and its geographic expansion roadmap focuses only on the United States. This will likely not result in improved service availability in other regions, including Asia/Pacific.

Tata Consultancy Services

Tata Consultancy Services (TCS) is a Leader in this Magic Quadrant. Its MNS offerings are positioned as platform-led and automation-first to align with enterprise needs. TCS's customer base is concentrated in the Americas and Europe, with a smaller base in APAC. Target verticals include manufacturing, retail, warehousing, healthcare, utilities and logistics. TCS plans to:

- Build new interfaces with LAN OEM orchestrators and network devices to speed incident resolutions and applications usage visibility.
- Launch Network Cerebrum, a centralized console to integrate and orchestrate multiple OEM security appliances.

Strengths

- **Pricing:** TCS's pricing for managed LAN, WAN and security is lower than most other providers in this research.
- **LAN, WAN roadmap:** TCS's upgrade plans for managed LAN and WAN are more comprehensive compared to others in this research and likely will offer customers more technology options and better service delivery.
- **Managed security:** This provider's managed security service availability, CASB support, ZTNA offering and NAC integration support are better than most providers in this research. It also has added threat detection and NAC capabilities in the past year that will likely improve security service delivery.

Cautions

- **Customer portal:** TCS's customer portal is fragmented, requiring users to toggle between network status, event management and change management console views. This impairs customers' ability to see and manage their MNS service.
- **SLAs:** TCS's managed LAN, WAN and security service credits for SLA violations are not publicly released. This lack of transparency makes it challenging for prospective customers to evaluate TCS's service-level commitments.

- **Geographic roadmap:** TCS's plans to grow its market share outside India does not target any specific region. This will likely not result in improved service availability outside of India.

Telefónica

Telefónica is a Niche Player in this Magic Quadrant. Its MNS services are positioned to assume, manage and secure enterprise networks, allowing customers to focus on their core business. Telefónica's customers are primarily in Europe, with a much smaller base in the Americas and Asia/Pacific. Key verticals include healthcare, industrial manufacturing, retail, logistics, utilities and financial services customers. Telefónica plans to:

- Integrate Telefónica AI bots with LAN vendor-native AI to speed incident resolution, enable predictive maintenance and improve customer experience.
- Embed Network Information and Security 2 (NIS2) and Digital Operational Resilience Act (DORA) compliance natively to strengthen WAN resilience, governance and incident management.

Strengths

- **Pricing:** Telefónica's pricing for managed LAN and WAN is lower than most other providers in this research.
- **SD-WAN:** This provider has significantly improved its SD-WAN vendor portfolio, which is now better than most other providers in this research. This offers customers greater choice to align with existing infrastructure investments and network modernization plans.
- **Incident classification:** Telefónica's incident classification for managed LAN, WAN and security is better structured and detailed than other providers in this research. This will tend to support accurately prioritized response to service issues.

Cautions

- **FCR:** Telefónica's FCR and zero-touch FCR have improved recently, but they are still among the lowest of all providers in this research. This may lead to less efficient incident response that can negatively impact customers.

- **Security SLAs:** Telefónica's managed security SLAs include weaker service-level objectives that do not include guarantees for monitoring availability or service credits for SLA violations. Overall, this does not give customers service guarantees for service reliability and delivery.
- **Security roadmap:** This provider's plans for improving SD-WAN security, firewall and threat detection functions is weak compared to others in this research. The planned upgrades are likely to result in only minor managed security support improvements for these functions.

Wipro

Wipro is a Visionary in this Magic Quadrant. Wipro markets its MNS services as AI-based, supporting enterprises' cloud, security and digital transformation goals. Its global customer base is distributed across Asia/Pacific, the Americas and Europe. Key verticals include financial services, healthcare, retail, manufacturing and energy. Wipro plans to:

- Implement its unified LAN, WAN and security service delivery architecture for its MNS customers.
- Embed WAN GenAI features, including automated assessments, policy generation, drift detection, ticket summarization and guide change management.

Strengths

- **Portal update frequency:** Data update frequency on Wipro's MNS customer portal is far better than most providers in this research. This ensures that customers have an accurate, current view of their network and security services.
- **WAN roadmap:** Wipro's planned managed WAN service upgrades include added automation, additional SASE integration and improved incident remediation. These upgrades are likely to improve customer underlay and overlay options and improve service delivery.
- **Secure SD-WAN:** Wipro has added multiple managed SD-WAN capabilities including zero-trust principles and SASE integration, end-to-end life cycle management and additional automation and vendor integrations. This will likely improve security protection and service delivery.

Cautions

- **Pricing:** Wipro's pricing for managed LAN and managed OEM SD-WAN is higher than most other providers in this research.

- **SLAs:** Wipro's SLAs for managed LAN, WAN and security lack defined service credits for SLA violations. This makes it challenging for prospective customers to evaluate Wipro's service level commitments.
- **Customer portal:** Wipro's customer portal is difficult to navigate, requiring users to click through multiple console views to see network and security status, change management, incidents and analytics. This makes it difficult for customers to see and manage their MNS service.

XTIUM

XTIUM, formerly ATSG, is a Leader in this Magic Quadrant. Its XTIUM MNS offerings focus on simplifying complex MNS for LAN, WAN and security, linking operational performance to business outcomes. XTIUM's customer base is mostly in the Americas and Europe, with a smaller customer base in Asia/Pacific. It focuses on large, multinational customers in the retail, healthcare, financial services, manufacturing and tech sectors. XTIUM plans to:

- Enhance WAN AI-powered predictive path selection capabilities and incorporate business context and application criticality.
- Integrate with security orchestration and automation response (SOAR) platforms, including Cortex XSOAR and Fortinet FortiSOAR, and expand its XDR capabilities.

Strengths

- **Operations automation:** XTIUM's managed services delivery platform is highly automated, and it has one of the highest rates of zero-touch first contact automation seen in this research. This supports more efficient managed service delivery to enterprise customers.
- **LAN management:** This provider has made significant investments in LAN service delivery in the past year and has a strong roadmap for upgrades in the next year, including expanded AI integration and ZTNA capabilities expansion. This makes it more likely customers will see meaningful LAN service improvement.
- **Security management:** XTIUM's security data integrity and service availability management is stronger than most providers in this research. This indicates strong service delivery capabilities.

Cautions

- **Customer-facing service descriptions:** This provider's customer facing service descriptions are overly lengthy and don't present a clear picture of business outcome benefits. This potentially is a turn-off for prospective customers.
- **SLAs:** Xtium's SLAs are not differentiated across LAN, WAN and security segments and offer weak service credits for SLA violations. This may lead to uneven service performance.
- **WAN roadmap:** Xtium's plans for managed WAN upgrades focus entirely on security, with no improvements to core network visibility or management.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- DXC: DXC has gained market visibility and met the inclusion criteria.

Dropped

- Presidio: Presidio did not meet inclusion criteria.

Inclusion and Exclusion Criteria

For inclusion in this Magic Quadrant, vendors must have generally available services that support all the following capabilities:

Service capabilities

- Provide MNS to enterprises for networking products and related network services on a 24/7/365 basis for customer locations globally from an internally operated and maintained SDP.
- Offer a fixed monthly subscription fee for each device managed for enterprise customers for MNS for LAN, WAN and security offers.

- Provide MNS for network operations life cycle management of networking hardware/software in support of both LAN and WAN technologies, as defined by the MNS market definition.
- Internally operate a multitenant SDP for MNS customers using primarily internal employees. Provide services for customers' existing LAN, WAN and security environments (e.g., "greenfield"/"brownfield" environments and managed takeover), in addition to transformed LAN, WAN and security customer environments, or otherwise adopting updated network and security networking technologies.
- Confirm service management processes and tools for MNS achieve a minimum average of 80% FCR for all incidents, whether manual or automated. Proof of specific percentage attainment and all underlying method details are required to be demonstrated and provided to verify compliance for inclusion in this research. FCR is defined as all incidents resolved at the first contact of the MNS operations. The contact may be either human or nonhuman via incident automation resolution for the total FCR percentage. FCR percentages do not include any incidents resolved after first contact of any type, manual or automated.
- Confirm service management processes and tools for MNS (specifically for MNS for LAN, WAN and security only) achieve a minimum average of 25% first contact resolution for all incidents via automation only (with zero manual touch). This percentage does not include any first contact incident resolution that is touched by a human. Proof of specific percentage attainment and all underlying method details are required to be demonstrated and provided to verify compliance for inclusion in this research.
- Offer at least five of the following six categories of security products for MNS for security services, including:
  - SD-WAN (with or without embedded security functions)
  - Secure web gateway
  - Cloud access security broker
  - Network access control
  - Network firewalling (with or without IDS/IPS)
  - ZTNA

- Provide evidence of current and planned security incident automation methods, tools and performance KPIs that are tracked and reported, applicable specifically to MNS for security.

Business/Financial Performance

- Have at least 1,000 MNS for LAN customer sites, at least 1,000 MNS for WAN customer sites and at least 500 MNS for security customer sites (under active MNS contracts). Specific site-level customer data (e.g, quantities of devices) is required to be included in this research in at least three of the following regions: North America, Europe, APAC, Middle East/Africa and Latin/South America. Evidence provided must include customer location quantities for MNS for each of LAN, WAN and security on a global basis.
- For purposes of this research, “sites” that are subcontracted to Asia/Pacific party MNS providers are not counted toward satisfying the inclusion criteria above.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of their processes, systems, methods and procedures. These criteria enable MNS providers' performance to be competitive, efficient and effective, and to positively affect revenue, retention and reputation in Gartner's view of the market.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	High

Source: Gartner (April 2026)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to convincingly articulate logical statements. This includes current and future market direction, innovation, customer needs and competitive forces, and how well they map to Gartner's view of the market.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	High
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Low

Source: Gartner (April 2026)

Quadrant Descriptions

Leaders

A provider in the Leaders quadrant demonstrates the ability to fulfill a broad variety of customer requirements through the breadth of its MNS offerings. Leaders have the ability to shape the market and provide complete and differentiating services, as well as global service and support. Leaders maintain strong relationships with their channels and customers, and have limited obvious gaps in their portfolios.

Challengers

A vendor in the Challengers quadrant demonstrates sustained execution in the marketplace and will likely have clear and long-term viability in the market. However, Challengers are less likely to shape and transform the MNS market with differentiating functionality going forward.

Visionaries

A vendor in the Visionaries quadrant demonstrates the ability to add features to its MNS offerings to provide a unique and differentiated approach to the market. A Visionary will have innovated in one or more of the key areas of MNS (for example, service delivery quality, automation and customer experience). The ability to apply differentiating functionality across the MNS scope will affect its position.

Niche Players

A vendor in the Niche Players quadrant focuses on specific capabilities or concentrates its marketing on certain regions. It therefore may not provide broad functionality or wide geographic availability. Niche Players also may lack strong go-to-market capabilities that would enhance their reach or service capabilities in their MNS offerings.

Context

The MNS market is highly competitive. During the past 12 months, MNS providers seeking a competitive advantage have rapidly expanded their investments in automated processes and AI to improve network visibility and end-user experience. They also have applied AI and automation upgrades to speed incident detection and faster remediation of network outages or security breaches.

That said, offerings vary widely in service quality and the extent of support and monitoring. Providers that have implemented more process automation and AI into their service delivery platforms tend to have higher scores in key metrics, such as FCR and repair times, both of which are indicators of a better quality service provider.

This variability requires heads of I&O to choose their MNS partner carefully. To assist in that evaluation, this Magic Quadrant focuses on key features and support levels for MNS providers' managed LAN, WAN and security service delivery to global enterprise customers. This includes choice of vendor partners, quality of service-level agreements and improvements in service delivery and customer support.

Market Overview

Market Remains Highly Diverse and Growth-Oriented

The MNS market remains highly competitive and diverse, including:

- Pure-play MNS providers
- Network service providers

- System integrators
- Network equipment providers

It also is a growth market, particularly for managed SD-WAN and managed security services, and is projected to grow by 7.0% and 9.4% yearly through 2029 (see Market Opportunity Map: Enterprise Network Services, Worldwide).

However, service features and capabilities vary dramatically, including service response times, the ability to monitor and manage underlay circuits and equipment, and the extent of security services monitoring. Providers also vary in their MNS bundling strategies. Some require MNS customers to buy other products and services such as hardware, software or network circuits. All providers in this research do not require these additional bundled purchases.

Gartner also has observed an increasing trend among MNS providers to outsource some elements of their service delivery to third-party support or technology vendors. Coordination between two organizations for service delivery tends to result in slower response times, but much depends on how providers manage these relationships and the extent of the outsourced support.

If, for example, a provider tightly integrates an AI security vendor's authentication control technology into its service delivery platform, it may strengthen overall security access control functions with little resulting service delivery delay. In contrast, if a provider outsources a large portion of its network operations center support to a third party, it can lead to miscommunications and delays in incident response. For this reason, Gartner recommends that heads of I&O require prospective MNS providers to reveal the extent of third-party involvement in service delivery.

MNS Players' AI Use Deepens, Evolves Toward Agentic AI

During the past several years, MNS providers have been transitioning from manual to automated network processes to make their service delivery platforms more responsive and efficient. This has laid the necessary groundwork allowing them to move to AI for IT operations (AIOps), which relies heavily on automation. AIOps is now widely used among major MNS players to analyze network telemetry and events more quickly than humans, allowing them to provide customers with greater visibility into their networks. AI also supports faster detection and resolution of network outages and security issues.

Further, MNS providers are now deploying network AI assistants, an extension of AI technology that allows humans to interact with AI-powered network management systems via natural-language chat conversations. And in the past year, MNS providers have begun to adopt agentic AI, an evolutionary step from network AI assistants.

Unlike network AI assistants that provide support at the direction of human engineers, AI agents are goal-oriented, acting autonomously to complete network tasks with little or no human oversight. In the past year, MNS providers have started to deploy AI agents primarily to perform network configuration tasks or oversee dynamic path selection, switching traffic to an alternative connection if a primary connection falls below certain requirements for critical applications.

In time, we expect MNS providers will rely on AI agents to carry out a larger number of network tasks, leading to more automated networks. Still, this transition is in early stages. MNS providers' level of AI agent adoption varies widely from pilot phase to full implementation. Moreover, the service benefits for end enterprise users are mixed. While providers claim AI agents as part of a larger AIOps operating strategy have significantly improved on-time activation, incident detection and network outage repair times, there is little evidence of this in their SLAs. These SLAs have changed little in the past few years.

And while AI and agentic AI can help MNS providers improve their service delivery, the technology itself poses an existential threat to managed services. Networking and security vendors also are building AI and agentic AI capabilities into their products, giving them greater network traffic analysis and troubleshooting capabilities. This opens the door for end enterprise customers to self-manage and monitor their networks, thereby lessening the demand for MNS (see Why Agentic NetOps Will Move Enterprises Away From Managed Network Services).

Gartner has seen continued client interest in MNS services during the past year, particularly in the multicloud enterprise segment, where IT staff is limited and has a greater need for MNS support. There also is continued interest in co-managed services, where the enterprise retains certain management responsibilities, such as security policy control and network device configuration. Moreover, these customers now have access to expanding AI and agentic AI management capabilities built into network equipment vendors and SaaS providers' offerings to help them co-manage their networks alongside an MNS partner.

Security Drives MNS Service Growth

MNS providers' managed LAN and WAN services are relatively stable, with improvements mostly focused on AI monitoring and management features. In contrast, managed security services are rapidly expanding, with added SASE vendor options and protections such as threat hunting, XDR and cloud security.

MNS providers' managed security investment strategy focuses on expanding AI and now agentic AI integrations to improve traffic monitoring and security incident detection. Some MNS providers also are integrating NOC and SOC operations as the security and network interconnection deepens. For the end enterprise, this offers greater choice and depth of managed security products and potentially fewer successful cyberattacks that result in damaged operations and revenue loss.

A handful of forward-looking MNS providers also have added features such as PQC protection. This offers protection from the threat that hackers, armed with quantum computers, will break basic network encryption and steal sensitive user/customer identity information or intellectual property.

However, as with other managed services, providers are at varying stages of managed security service evolution. Capabilities vary, so Gartner recommends using competitive RFPs that require providers to spell out their managed security capabilities. Also, Gartner recommends that enterprises ask prospective managed security providers about their service roadmaps for AI and PQC security.

NaaS and Consumption-Based Pricing Offers Proliferate

During the past year, MNS providers have ramped up marketing for network-as-a-service (NaaS) options, often promoting them more heavily than traditional fixed-price service delivery options. Gartner defines NaaS as a standardized, highly automated delivery model that supports dynamic scaling of network resources and is primarily owned and operated by the provider. Pricing is either consumption-based or as a subscription based on usage metrics.

How providers define NaaS varies. Most providers in this research have launched a NaaS option, but they range from design, installation, leased hardware and monitoring service for a single fixed monthly price to packages that allow customers to add or drop services or adjust service levels via their customer portal.

While NaaS offerings are often marketed as a more convenient and economical option, heads of I&O should proceed with caution. Such offerings frequently lack billing transparency, include excessive equipment lease prices and limit customers' ability to reduce service levels. In addition, NaaS offerings that include consumption-based billing lack price predictability, making them unpopular with company chief financial officers.

Therefore, Gartner recommends that enterprises require MNS providers to provide NaaS service proposals with clear pricing of all service elements. This will allow heads of I&O to accurately calculate the long-term costs and compare that to standard service pricing models with purchased and installed equipment and monthly fees only for ongoing monitoring and maintenance support.

Evidence

Gartner analysts conducted over more than 1,100 client inquiries on the topics of managed network operations and MNS for LAN and WAN between 30 November 2024 and 30 November 2025.

In 2026, all providers included in this research responded to an extensive questionnaire regarding their current/future MNS offerings, and provided multiple offer, proposal, market penetration and services artifacts.

We reviewed all available vendor end-customer Peer Insights for quality purposes but not inclusion in this research. All providers in this research had the opportunity to encourage customer peer reviews. These end-customer insights (Peer Insights) can be found on the Gartner client portal by market name and provider name across numerous covered markets.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Document Revision History

Magic Quadrant for Managed Network Services - 14 October 2024

Magic Quadrant for Managed Network Services - 8 November 2023

Magic Quadrant for Managed Network Services - 3 October 2023

Magic Quadrant for Managed Network Services - 10 November 2021

Magic Quadrant for Managed Network Services - 9 November 2020

Recommended by the Authors

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

How Markets and Vendors Are Evaluated in Gartner Magic Quadrants

Tool: RFP for Managed Network Services

Why Agentic NetOps Will Move Enterprises Away From Managed Network Services

Market Trend: The $8 Billion Opportunity in WAN Networking

AI Will Transform Managed Network Services in the Next Three Years

Top Technology Trends in Enterprise Communication Services for 2026

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	High

Source: Gartner (April 2026)

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	High
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Low

Source: Gartner (April 2026)