Magic Quadrant for Managed Network Services

14 October 2024 - ID G00805580 - 66 min read

By: Ted Corbett, Nauman Raja, Jon Dressel, Lisa Pierce, Karen Brown, Danellie Young

Initiatives:I&O Operations Management

Enterprises use MNS to balance expense optimization with network and security service operations quality. I&O leaders seek AI/machine learning-enabled providers to achieve shorter cycle times and higher quality services via automation. This research will help navigate the competitive MNS market.

This Magic Quadrant is related to other research:

View All Magic Quadrants and Critical Capabilities

Strategic Planning Assumptions

By 2027, 65% of new software-defined wide-area network (SD-WAN) purchases will be part of a single-vendor secure access service edge (SASE) offering, an increase from 20% in 2024.

By 2026, generative artificial intelligence (GenAI) technology will account for 20% of initial network configuration, which is an increase from near zero in 2023.

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 that deliver current and emerging requirements to end users.

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 (MNS for security) functions** include health, configuration and maintenance support for security technologies. Service delivery is for a single vendor 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); and (5) network firewalling, with or without intrusion prevention system/intrusion detection system (IPS/IDS). 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.

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.

- **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.
- **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.

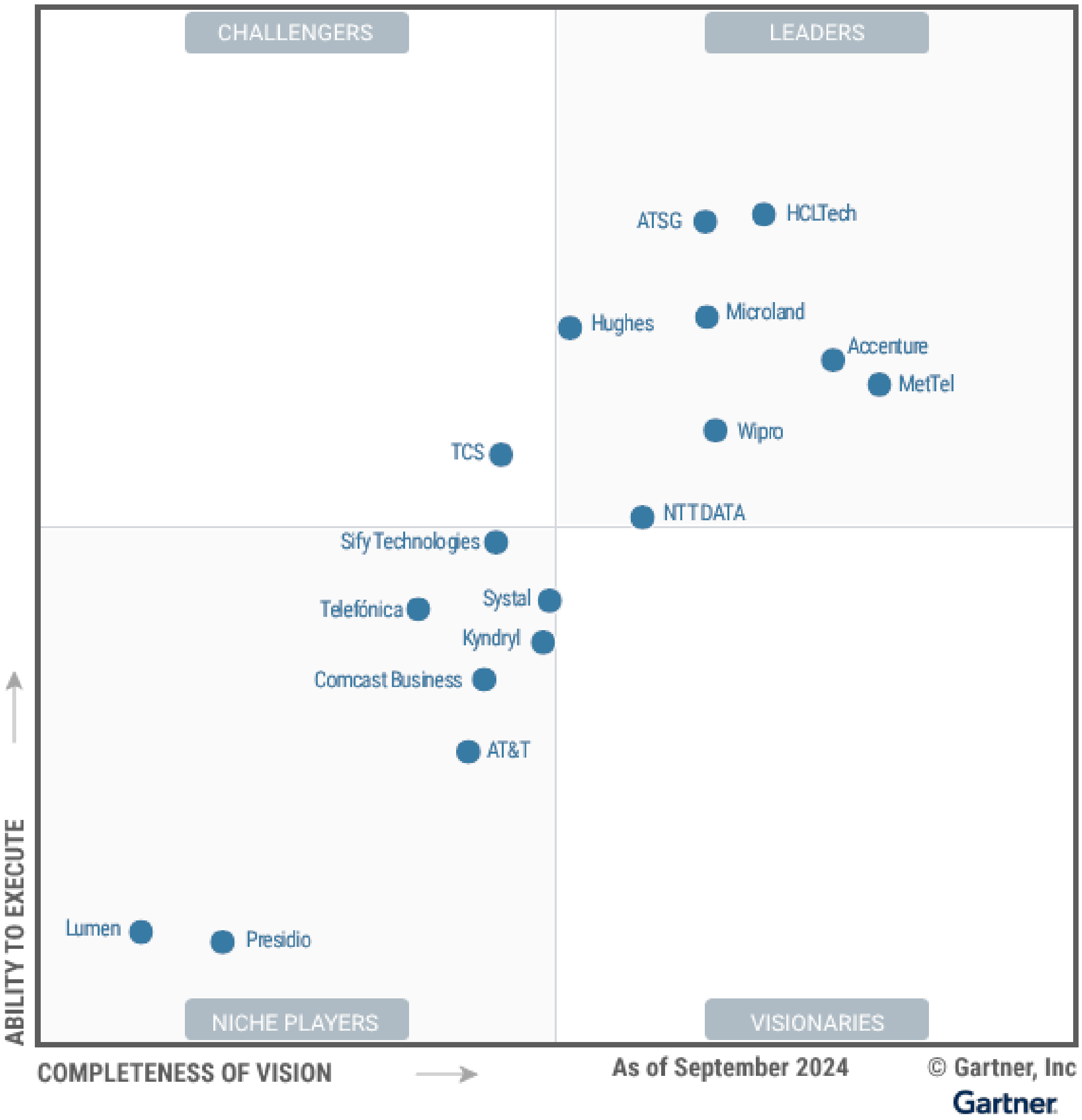
Note: The MNS market does not include any network or security products, software, maintenance, network services, or cloud-based services or products. These elements are covered by other Gartner research.

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.
- 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 resale or as OEM sale offers.

Magic Quadrant

Figure 1: Magic Quadrant for Managed Network Services



Vendor Strengths and Cautions

Accenture

Accenture is a Leader in this Magic Quadrant. Its products are broadly focused on providing substantial transformations of customers' IT operations across LAN, WAN and security. Its operations are geographically diversified, and its customers tend to be multinational organizations. It plans to continue to invest in its tools and its API integration strategy, which is focused on simplifying heterogeneous architectures. It will continue expanding its strategic partners in its solution enablement activities and joint go-to-market initiatives across all regions.

Strengths

- **Solution orientation:** Accenture's MNS offering enables customers to establish and strengthen alignment across LAN, WAN and security.
- **Extensible:** Accenture's MNS offerings extend options for private Long Term Evolution (LTE) and 5G network-enabled mobility use cases.
- **Security differentiation:** Accenture's Secure Programmable Network offering expedites the deployment of multiple MNS services by providing automation within the vendor's Cloud Network Operator (CNO) platform.

Cautions

- **Integration gap:** Accenture currently does not perform case management in IT service management (ITSM) systems, so it does not integrate with customer ITSM.
- **Scope:** Accenture has demonstrated diminished interest in narrow-scope MNS opportunities, such as single offer category opportunities with relatively narrow impact to achieving enterprise objectives.
- **Security portfolio:** Accenture's NAC offering is less mature and behind some others in this research.

ATSG

ATSG is a Leader in this Magic Quadrant. ATSG owns the former MNS pure-play vendor Optanix. Its MNS offering delivers standardized, scalable and automated MNS for LAN, WAN and security. Its operations are geographically diversified, and its customers tend to be midsize to large enterprises located primarily in the U.S. and Europe. ATSG is increasing its investments in automation and predictive analytics, while extending its focus on private 5G market use cases.

Strengths

- **Integrations:** ATSG continues to expand its wholly owned service delivery platform (SDP) capabilities with integrations to third-party AI platforms.

- **End-user experience:** ATSG's end-user experience monitoring for enterprise on-premises and cloud-based applications performance is in the top quartile, compared with others in this research.

- **Security roadmap:** With an emphasis on security orchestration, automation and response (SOAR), xSOAR and AI, ATSG has strong future plans for MNS security improvements.

Cautions

- **Platform:** The vendor offers a co-management option for enterprises that may create conflicts with its core MNS platform development priorities.

- **Security portfolio:** ATSG's threat detection and response capabilities are not as developed as the majority of its other service offerings.

- **Brand awareness:** Enterprise awareness of ATSG's brand is limited compared to other Leaders and has been further diminished by other similarly named entities.

AT&T

AT&T is a Niche Player in this Magic Quadrant. Its managed LAN, WAN and security services are available across all industry segments and verticals globally with its highest concentration of customers in the U.S. and Europe. Its MNS delivery operations are geographically diversified, and its customers tend to be enterprise customers of all sizes, across all geographies and all industry segments. The vendor continues to work on improving its impact on the MNS market amid its competing core asset leverage strategy.

Strengths

- **SD-WAN:** AT&T supports leading SD-WAN vendors within its MNS for WAN services.

- **Customer ITSM integration:** AT&T's MNS platform is integrated with a large number of end-user customers for case management exchange.

- **Enhanced security:** AT&T has demonstrated improvement in the areas of threat correlation and community collaboration, and introduced a no-code custom app builder within its open extended detection and response (XDR) platform USM Anywhere.

Cautions

- **Operations and support:** Some clients report that AT&T subcontracts the delivery of services contracted to other third-party MNS providers. Clients should confirm who is supporting and delivering the managed network services.
- **Customer experience:** AT&T's MNS portal capabilities lag behind most others in this research.
- **Security maturation:** Reporting and SLAs on data integrity and availability within AT&T's managed security services are underdeveloped.

Comcast Business

Comcast Business is a Niche Player in this Magic Quadrant. This year, the vendor rebranded the Masergy assets it acquired three years ago to Comcast Business. Its managed LAN, WAN and security services focus on retail storefront-type WAN topologies. Its operations are focused primarily in the U.S., with a smaller number of international customer sites. Its customers tend to be enterprises across most industry segments and verticals. The vendor plans continued managed firewall enhancements in the near term.

Strengths

- **Change management:** Compared with other vendors in this research, Comcast Business delivers top-quartile cycle time performance for completing simple and complex move, add, change or delete (MACD) service requests.
- **Pricing:** Comcast Business's MNS pricing is within the top quartile of attractiveness, when compared with others in this research.
- **Security capabilities improvement:** The vendor offers several options for applications and vendor integrations for its NAC solution.

Cautions

- **Automation:** Comcast Business's incident automation performance lags most others in this research.
- **SLA:** Comcast Business's SLA metrics for MNS are incomplete, compared with most others in this research.
- **Security roadmap:** Comcast does not plan to add security capabilities to its SD-WAN during the next 12 to 18 months.

HCLTech

HCLTech is a Leader in this Magic Quadrant. Its SDP is focused on consistent data quality, process efficiency and automation. Its operations are focused in the Americas and Europe, and its clients tend to be enterprises across most industry verticals. It plans to invest in GenAI integrations with SD-WAN to deliver complete automation for life cycle operations. It is building a vendor-focused GenAI large language model (LLM) as part of its SDP.

Strengths

- **MNS:** Customers report that HCLTech's overall MNS capabilities are high-performing, compared with others in this research.
- **LAN:** The vendor has completed its planned microsegmentation support as a part of its focus on OT security use cases.
- **MNS for security:** HCLTech demonstrates strong key capabilities for MNS for security, including performance optimization, resilience and redundancy.

Cautions

- **SD-WAN/SASE:** HCLTech's progress on achieving a multivendor unified policy model lags behind some leaders in this research.
- **Pricing:** HCLTech's MNS pricing is higher than some leaders in this research.
- **SWG strategy:** HCLTech's vision for enhancing secure web gateway (SWG) is minimal compared with competitors.

Hughes

Hughes (also known as Hughes Network Systems) is a Leader in this Magic Quadrant. Its HughesON for MNS is focused on large retail and related verticals. Its operations delivery locations cover global regions including the Americas, Europe and Asia/Pacific (APAC), and its clients tend to be large enterprises, commonly with more than 150 sites. It is planning to expand self-installation capabilities for LAN and WAN devices within its SDP to reduce complexity and improve cycle time.

Strengths

- **API:** Hughes has added API integrations that incorporate business application visibility and alert fidelity to its customers' help desk operations.

- **Incident cycle time:** Hughes deploys an active power distribution unit (PDU) that enables reduction of specific incident-detection cycle times to one minute.

- **Security integration:** Hughes' managed NAC can integrate with an extensive number of vendors and applications.

Cautions

- **SD-WAN:** Hughes' portfolio of market-leading SD-WAN OEMs is smaller than most other vendors in this research.

- **Case management integrations:** Most customers are not two-way integrated for case management from their internal ITSM tool with Hughes' SDP.

- **Security OS:** Hughes lacks a programmatic approach for security OS management and maintenance.

Kyndryl

Kyndryl is a Niche Player in this Magic Quadrant. Its MNS offers for LAN and WAN are broadly focused on large enterprises that require transformation of their IT operations. Its operations are geographically diversified, and its customers tend to be large enterprises across the Americas, Europe and APAC. Kyndryl's focus on improving capabilities during the past 12 months has improved its overall MNS performance and strengthened its MNS brand awareness.

Strengths

- **LAN:** Kyndryl's MNS for LAN endpoint coverage is more extensive than most others in this research.

- **Portal:** Kyndryl's improved end-user portal provides customers with a uniform experience and ease of navigation.

- **Security portfolio:** Kyndryl is focused on improving capabilities for responding to new regulations and audits, while preparing customers for the next generation of threats.

Cautions

- **Support and operations:** Some clients report that Kyndryl often subcontracts the delivery of managed network services contracted to other third-party MNS providers. Clients should confirm who is supporting and delivering the managed services.

- **Pricing:** Kyndryl's firewall pricing is among the highest of the vendors evaluated in this research.

- **SD-WAN security:** Kyndryl MNS offer for SD-WAN security is less complete than most others in this research.

Lumen

Lumen is a Niche Player in this Magic Quadrant. Its MNS for LAN, WAN and security is focused on providing network product and services support across enterprise network estates. This complements the vendor's primary focus on its network services business. Its operations are focused in Europe and the Americas, and its clients tend to be traditional MNS buyers that also purchase network services from Lumen. Its MNS focus includes retail, manufacturing, financial services, healthcare and the public sector segments.

Strengths

- **Committed investments:** Lumen's MNS investments remain its focus, including services packaging, automation and customer experience (CX).

- **SD-WAN:** In the past year, Lumen added hosted gateway support for Versa and Fortinet.

- **Digital transformation:** Digital purchasing and provisioning is a plus for many down-market customers, and the integration of Rapid Threat Defense differentiates Lumen from some of its competitors.

Cautions

- **MNS pricing:** Lumen's MNS pricing is higher than most other vendors evaluated in this research.

- **Market understanding:** Lumen lacks market-focused execution of its MNS platform capabilities by offering fragmented levels of support options across its MNS offers.

- **Lack of NAC:** Lumen does not provide NAC, focusing instead on zero-trust network access (ZTNA), which may not be suitable for all use cases.

MetTel

MetTel is a Leader in this Magic Quadrant. Its range of MNS for LAN, WAN and security is applicable to all enterprises, using the same service management platform for managed LAN and WAN, with integrations for security. Its operations are mainly focused in the U.S., and its customers tend to be large enterprises and government entities located primarily in the U.S. and Europe. The vendor has expanded MNS delivery partnerships across federal and commercial market vendors, adding customers in an additional 35 countries during the past year.

Strengths

- **Customer-centric SASE/SSE:** MetTel provides a strong approach to rightsizing appropriate SSE or SASE implementations.
- **Improved cycle time:** MetTel added an automated PDU that reduces incident detection cycle time for LAN and WAN endpoints.
- **Managed POTS transformation:** MetTel has a large-scale digital transformation solution for managing and automating analog infrastructure life cycle extensibility.

Cautions

- **Pricing:** MetTel's MNS pricing is higher than most other vendors evaluated in this research.
- **Business application mapping:** MetTel's portal visibility scope does not include application-to-infrastructure service mapping.
- **SD-WAN security operations:** MetTel's secure SD-WAN OEM vendors' support options lag behind some others in this research.

Microland

Microland is a Leader in this Magic Quadrant. Its MNS for LAN, WAN and security provide automation-enabled service delivery capabilities. It includes service mapping analytics, visibility and user experience (UX) for multiple endpoint types. Its customers tend to be midsize to large enterprises across all verticals and regions. During the next 12 months, Microland plans to increase focus on its AI-enabled service capabilities with unified and adaptive security models for SD-WAN and SASE.

Strengths

- **Manufacturing:** Microland is a leading performer in this research for factory MNS, including IT/OT/IIoT integration, microsegmentation and policy-based segmentation.

- **Complete offers:** Nearly all Microland customers procure all three of the vendor's MNS offerings.

- **Firewall capabilities:** Microland added significant capabilities to its firewall offering, including AI, automated compliance and a reduction in provisioning time due to adopting a NetDevOps approach.

Cautions

- **Market awareness:** Microland's brand awareness for MNS is relatively low among global enterprise buyers.

- **Pricing:** Microland's MNS pricing overall is average, as compared with others in this research.

- **Security processes:** Microland's maintenance of the security OS processes are lacking discipline with change management.

NTT DATA

NTT DATA is a Leader in this Magic Quadrant. Its MNS for LAN, WAN and security is focused on enabling clients to transform their networks with software-defined capabilities. Its operations are geographically distributed, and its clients tend to be large enterprises across all verticals. It plans to continue investments in GenAI to enhance self-service reporting, analytics and operations capabilities, while expanding its API gateway support for more log and telemetry data sources.

Strengths

- **Pricing:** NTT DATA customers report high satisfaction with the vendor's pricing for MNS.

- **Upgraded SDP.** NTT DATA has delivered improved customer outcomes across cycle time performance and portal visibility during the past 12 to 18 months.

- **Security:** NTT DATA rapid detection, response and remediation via threat- and incident-specific playbooks.

Cautions

- **Responsiveness:** NTT DATA's incident response cycle time is longer than most others in this research.

- **Customized to standardized MNS migrations:** Enterprises that are aligning their services to NTT DATA's standardization of MNS delivery should govern closely to ensure that quality is maintained.

- **NAC integration:** NTT DATA has minimal application integrations available for NAC.

Presidio

Presidio is a Niche Player in this Magic Quadrant. Its globally available MNS for LAN, WAN and security is focused on fulfilling OEM product sourcing, design, implementation and MNS for its clients to meet buyers' network life cycle requirements. Its operations are geographically distributed, and its customers tend to be midsize enterprises spanning most industries, with the majority in the Americas and the rest in Europe and the APAC region. Presidio continues to develop its automation capabilities to improve customer experience across cycle time and service quality.

Strengths

- **Portal:** To deliver a unified experience, Presidio is improving its portal features, navigation and reporting for customers.

- **Life cycle provider:** Customers value Presidio for its ability to partner with them across their enterprise networking and security life cycles.

- **Security controls:** NAC and ZTNA operations for mixed environments are a key differentiator.

Cautions

- **Integrations:** Presidio's customer integrations to its ITSM platform for case management and configuration management database (CMDB) continue to lag behind other vendors evaluated in this research.

- **Pricing:** Presidio's MNS pricing is among the highest, compared with others in this research.

- **Security approach:** Presidio's overall security approach is less comprehensive in both vision and execution and, therefore, is lacking compared with competitors.

Sify Technologies

Sify Technologies is a Niche Player in this Magic Quadrant. Its MNS for LAN, WAN and security is focused on network service provider (NSP)-agnostic MNS. Its operations are focused primarily in the APAC region, where more than 90% of its customer sites are located. During the next 12 to 18 months, Sify plans to invest in expanding its presence in the banking, financial services and insurance (BFSI) and manufacturing sectors. Its incident classification data management discipline and accuracy investments have increased its overall service delivery quality year over year. It also plans to invest in multivendor SD-WAN orchestration capabilities.

Strengths

- **OEM expansion:** Sify Technologies is enabling unified management for Cisco SD-WAN and SD Access support capabilities.
- **Portal:** Sify Technologies is investing in a more integrated and navigable view of service status, performance reports and service request management.
- **Security offerings:** Sify Technologies provides consistent performance across security categories, with availability management and data integrity management specifically cited as better than most others in this research.

Cautions

- **Automation:** Sify Technologies' performance with first contact resolution (FCR)-automated incident resolution lags behind other vendors evaluated in this research.
- **Pricing:** Sify Technologies' market prices for MNS do not align with downward trends in the market, especially for firewall management.
- **NAC integrations:** Sify Technologies does not enable integrations of security tools into its NAC environment.

Systal

Systal is a Niche Player in this Magic Quadrant. Its MNS for LAN, WAN and security is focused on NSP-agnostic MNS buyers. Its operations are located primarily in Europe, and its customers tend to be large enterprises across a variety of verticals; most are MNS for LAN clients. During the next 12 to 18 months, Systal plans to increase its support for automated self-service and automated, simple standard change requests.

Strengths

- **Portal:** Systal's MNS end-user portal provides a simple ease of navigation experience for its customers.
- **Integrations:** The number of SDP integrations with customers' ITSM that Systal provides is among the highest of vendors evaluated in this research.
- **Security:** Systal's managed secure SD-WAN capabilities exceed most others in this research.

Cautions

- **Limited geographic focus:** Systal's customer base is primarily in Europe and most purchase MNS for LAN.
- **Automation:** Systal's zero-touch incident management network automation FCR performance lags compared to others evaluated in this research.
- **Availability management:** The vendor's availability management execution lags behind in its vision because it relies primarily on integration with ITSM reporting.

TCS

Tata Consultancy Services (TCS) is a Challenger in this Magic Quadrant. Its managed LAN and WAN services are focused on delivering MNS in close collaboration with regional and global network service providers (NSPs). Its operations are focused mostly in the Americas and Europe, with a smaller presence in APAC, and its customers tend to be midsize to large enterprises across most industry segments and verticals. The vendor's SDP transformation has improved automation and service delivery quality across MNS for LAN, WAN and security.

Strengths

- **Pricing:** TCS' pricing for enterprise buyers is lower than most providers in this research.
- **Predictive analytics:** TCS' MNS for LAN predictive analytics increases the vendor's proactive operations performance and capacity-tuning insights, resulting in higher preincident remediation.
- **SD-WAN security:** TCS provides strong SD-WAN security execution overall.

Cautions

- **SD-WAN:** TCS' capabilities across managed SD-WAN assurance-focused service elements lags some others in this research.

- **Incident classification:** TCS' "before" and "after" incident classification lacks granular specificity, which hinders continual service improvement automations.

- **MNS for security:** SD-WAN security execution progress in MNS for security is lagging behind many others in this research.

Telefónica

Telefónica is a Niche Player in this Magic Quadrant. Its range of MNS for LAN and WAN is focused on partnering with NSPs with its MNS offerings. Its operations are globally diversified, and its clients tend to be small- to midsize businesses and large-enterprise customers seeking combined network transport and MNS. Investments in improving its enterprise end-user experience focus have strengthened the vendor's service delivery platform during the past 12 months, yielding positive service quality and assurance capability improvements.

Strengths

- **Pricing:** Telefónica customers' satisfaction with pricing ranks among the highest of the vendors evaluated in this research.

- **Service mapping:** Telefónica provides an integrated network and security portal experience that includes application service mapping to infrastructure elements.

- **SD-WAN security:** Telefónica's SD-WAN embedded security includes SD-WAN segmentation over a single overlay.

Cautions

- **Automation:** Telefónica's incident resolution performance is lower than most others in this research.

- **SD-WAN support:** Telefónica's quantity of leading OEM support for SD-WAN is lagging most other vendors in this research.

- **Security operations:** Security OS management and maintenance lacks comprehensiveness, because it focuses primarily on server patching.

Wipro

Wipro is a Leader in this Magic Quadrant. Its MNS for LAN, WAN and security focuses on service delivery, automation and customer satisfaction. Its operations are geographically diversified, and its clients tend to be large global enterprises. Wipro plans to invest in carrier-neutral SD-WAN solutions to help customers source connectivity options and enhance their multicloud network integration performance.

Strengths

- **Continual service improvement:** Wipro engages directly with customers through a customer collaboration portal to increase the speed of capability delivery.
- **Incident response:** Wipro's FCR performance ranks favorably among other Leaders in this research.
- **NAC:** Wipro offers a complete NAC offering with advanced integration capabilities.

Cautions

- **Automation progress:** Wipro's year-over-year automation performance improvements continue to lag behind the other Leaders in this research.
- **Onboarding:** Wipro customer reports of slow onboarding cycle times after contract execution persist. This can challenge commitments to business stakeholders.
- **Firewall security:** Wipro's added firewall capabilities are minimal and focused on services, rather than firewall capabilities.

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

- Accenture
- Telefónica

Dropped

The following vendors did not meet the first contact resolution performance Inclusion Criteria for this research:

- BT
- Orange Business

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 basis for customer locations globally.
- 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.
- Operate a multitenant SDP for MNS customers using primarily internal employees. Provide services for customers' existing LAN, and WAN and security environments (for example, "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 measurement details are required to demonstrate compliance for inclusion in this research.
- Confirm service management processes and tools for MNS (specifically for MNS for LAN, WAN and security only) achieve a minimum average of 20% first-contact resolution for all incidents via automation (with zero manual touch). Proof of specific percentage attainment and all underlying method details are required to demonstrate compliance for inclusion in this research.

- Currently offer at least four of the following five 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)

- 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 (for example, quantities of devices) is required to be included in this research (under active MNS contracts). Evidence provided shall include customer locations for MNS for each of LAN, WAN and security on a global basis in at least three of the following regions: North America, Europe, APAC, Middle East/Africa and Latin/South America.

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

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

Source: Gartner (October 2024)

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

↓	↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	High
Vertical/Industry Strategy	High
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2024)

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 no obvious gaps in their portfolios.

Challengers

A vendor in the Challengers quadrant demonstrates sustained execution in the marketplace and will have clear and long-term viability in the market. However, it may not have a complete and competitive MNS offering set. In addition, Challengers may not have the ability to shape and transform the market with differentiating functionality or to serve a broad, global customer base.

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 demonstrates a near-complete product offering. However, it may not be able to control development or provide differentiating functionality due to other core focus areas the provider deems more critical. Niche Players also may lack strong go-to-market capabilities that would enhance their reach or service capabilities in their MNS offerings.

Context

Over the course of this research, several key observations emerged from providers' responses, Gartner analysis and MNS customers' feedback. Organizations should consider these carefully during their network and security operations sourcing strategy formulation and MNS provider selection.

MNS providers are either traditional network service providers, systems integrators (SIs) or pure-play MNS providers. MNS offers should all be available without the requirement of enterprises to buy any other products or services from the MNS provider. This includes related hardware/software or any network transport services. In fact, all providers in this research reported that no other products or services beyond MNS offers are required to be purchased by customers.

However, Gartner does not commonly observe this transport-provider agnosticism from NSPs competing in the MNS market. Our research reveals that NSPs rarely demonstrate interest in enterprise MNS opportunities that do not include buying network transport services from them. We continue to recommend that buyers seek flexibility with their contracting practices, allowing buyers to negotiate more effectively amid continued downward price pressure trends for traditional network services.

The prevalence of enterprise requirements for hybrid and multicloud support, combined with SD-WAN (usually with at least two diverse NSP WAN connections) continue to inflate enterprise demands for carrier-agnostic support from MNS providers, whether the MNS provider is an NSP or not. Enterprises report that long-term contracts with network service providers, inclusive of their on-net access, where available, reduce their flexibility to select the optimal price and performance of local access network access facilities.

Similarly, enterprises should be alert to any of the SI or pure-play MNS providers that demonstrate their preference for a single dominant carrier, either in their partnerships or in negotiations. This behavior is fundamentally no different and diminishes any noncarrier's claim of agnosticism to network services providers.

We are also observing some NSPs seeking direct GTM partnerships with SIs this past year. We believe this will be difficult for enterprise buyers to consider the veracity of any network transport agnosticism from these partnerships. At the same time, this type of partnership also creates strain on the SI-type MNS provider for the opposite reason — the veracity of any agnosticism toward network services providers becomes questionable.

In the context of MNS operations scope, changing transport types and providers is relatively simple as compared to changing between MNS providers, while at the same time, changing network OEMs is also easier than changing out MNS providers. These two points make it clear that agnostic MNS providers are preferred by enterprise buyers.

For many years, AI and ML have often been conflated by the vendor market; it's been dominantly ML with little to no AI until very recent years. The AI dimension is showing evidence of reaching the scale and complexity of MNS providers. The initial AI use cases are appearing in production or planned this coming year for most providers in this research.

The AI impact to overall MNS provider performance is becoming prevalent across many providers in this research. The most impactful evolution of AI for MNS providers is the application of AI to achieve high-performance, zero-human-touch incident resolution.

The MNS market's progress on the development of a complete, cross-technology stack, incident management process using AI and LLMs (and not people) is underway in the MNS market, but the full impact is yet to be experienced. We expect the efficacy of the models built today will be very attractive to enterprises as performance, reliability and quality will substantially increase, while MNS operations cycle times will decrease, along with enterprise costs for MNS. The advent of these capabilities will be in high demand for enterprises due to the enterprise cost of incident disruptions to business continuity that are lessened with currently unreachable incident resolution cycle time and quality performance.

These AI models are currently being trained and moving increasingly toward unsupervised capabilities at scale. The most mature MNS providers today are closest to achieving these outcomes, since their maturity with current ML dominant automations enable them to leverage the fidelity of their historic incident and data management discipline more rapidly than others. Their operations demonstrate discipline in process elements such as incident classification accuracy (automation), zero-touch incident automation, and highest-data quality management for effective incident management. In turn, the AI models for different vendor/type incidents can be built and deployed more rapidly by the most mature MNS providers.

Current MNS operators are increasingly employing AI chatbots, ChatGPT and natural language processing (NLP) technologies. The primary use cases in place today are mostly related to MNS end-user interactions. NLP provides faster and simpler access to provider documentation across a range of customer interests, including:

- Service requests
- Incident inquiry status and reports
- Root cause analysis reporting
- Transcriptions of major incident management calls

AI capabilities are extending to GenAI-based network assessments poised to accelerate cycle time for third-party network assessments while reducing or potentially removing enterprise assessment costs. Initially used in MNS presales, these assessments are rapidly conducted at a very low cost to the provider — and likely no cost to enterprises, when the provider is not the incumbent. Thus, potentially higher-performing alternate MNS providers will have much improved data from which to make high-quality, accurate offers — data that, without being the incumbent, typically requires enterprise direct expense for a typical network assessment provider. These assessments will be of value to enterprises regardless of whether they change providers. At the least, the assessments will confirm how the current operations provider is performing from an agnostic source. At the same time, a GenAI assessment from an MNS provider, as compared to enterprise internal operations (DIY) or custom IT outsourcing provider operations, is increasingly likely to have a higher impact for enterprises navigating the overall market shifts.

These market shifts for enterprises may ease the rising complexity of IT operations by increased adoption of end-to-end accountable provider choices that enterprises have for standardized, composable, automated and orchestrated MNS. These shifts are recognized by enterprises seeking to optimize their costs, increase flexibility and improve performance of their operations within the overall managed IT services industry.

This year's research revealed that nearly all of the MNS vendors have added MNS support for private 5G deployments, primarily partnering with the 5G OEMs; yet, these OEMs are also providing managed private 5G solutions. MNS vendors are directly contracting with enterprises for private 5G (P5G) deployments and management with their own MNS for P5G and some with their own 5G core. Managed public wireless services (e.g., 5G, LTE, 4G, Citizens Broadband Radio Service, satellite) are also employed as the second circuit for enterprise sites with SD-WAN.

Beyond a single mobility carrier mobile service, multicarrier (eSIM) access optimization has proven effective at achieving higher reliability and coverage performance for enterprises than any single mobile carrier. A multicarrier (or hybrid) approach is increasingly used by MNS providers and mobile virtual network operators: the MNS customer sites are provisioned to use whichever mobility carrier has the best reception for each site, then changed as needed in response to an outage incident.

We are seeing some providers limiting their interest in small and midsize enterprise customers by maintaining the account relationship, but with the service delivery subcontracted to others. Many of these subcontractors do not offer complete MNS; buyers should be cautious.

A few MNS providers choose to offer tiered services, each with different service levels, quality and cost to enterprises. For example, bronze, silver, gold packaging. This research recognizes the highest tier of these service offers, only. We have observed the outcomes from the lower tiers in the market for enterprises, and recommend enterprises focus their consideration at the recognized highest tier of service from any MNS provider that offers lower quality packages.

Many providers in this year's research are extending their MNS for LAN more actively for Cisco Application Centric Infrastructure (ACI) in data centers and, notably, are developing and pursuing software-defined LAN (OEM solutions) deals. This is in response to the increasing demand for enterprisewide ZTNA and SASE initiatives, with the key LAN evolution being microsegmentation within MNS for LAN offers. We are mostly seeing Cisco's Software Defined Access and Aruba EdgeConnect SD-Branch supported within MNS agreements. While we are seeing a relatively low number of customers implementing these approaches, interest continues to grow as security threats continuously expand, especially to achieve control of east-west LAN movements in highly critical environments (both IT and OT). Implementing OEM vendor microsegmentation is getting less difficult as providers build their experience.

The growing SASE market amid transformation objectives for enterprises contributes to buyers' increased tendency to combine both MNS and the rapidly evolving MNS for security offer component of MNS. For example, SSE/SASE-focused managed SASE (MSASE) enterprise migrations, in conjunction with MNS for security core functions from the same MNS provider, are expanding. A growing number of providers in this research report that the majority of their MNS customers purchase MNS for LAN, WAN and security from them. Today's buyers are less likely to contract with different MNS providers for LAN, WAN and security, opting to replace governance complexity and silos with a single MNS provider (see How Should I Choose a Managed SASE Provider? for more information).

MNS pricing trends continue downward for on-premises wireless LAN controllers and increasingly for firewalls of all configurations (e.g., with SD-WAN, Gen5 or stand-alone). The historical pricing norms for these elements are now observed at average selling prices of less than 25% of the average selling price (from MNS providers) less than two years ago in competitive bids.

We are seeing a continued year-over-year downward market price trend in the adjacent network services market. At the same time, these network services are, from a practical perspective, far more readily changeable to competitor offers than MNS, as buyers seek to maintain price alignment to the sliding network services market prices. We continue to observe enterprises reducing the number of service vendors they contract with, seeking standardization, less overhead from governance and accountability, and achievement of improved overall service experience. Meanwhile, network and security estate complexities continue to increase.

Gartner commonly sees buyer interest in MNS from every industry category, across public and private organizations globally. Meanwhile, many buyers believe they incur higher costs when managing their network operations internally versus taking an MNS approach. There is truth to this, primarily due to low execution cost impacting norms regarding process, tools and people for most DIY network operators. Such norms result in higher costs to enterprises with DIY approaches versus enterprises that use MNS. Enterprises are more informed by increasing their focus on total costs; incorporating the cost of quality, versus only operating budgets in isolation. In this manner, enterprises make more informed, data-driven decisions and have more accurate business cases in support of their IT operations management selection.

The primary challenge and underperformance of cost management is due to too many people resources, which drives up operations life cycle costs and is the most difficult to later optimize. Most life cycle costs are operating expenditures (opex), primarily labor. The amount of highly skilled labor required to plan, design, build and operate DIY network operations centers (NOCs) and security operations centers (SOCs) internally is considerable. Hence, we do observe some enterprises reducing costs with MNS options, but these also tend to incur higher life cycle costs in the current DIY operations from which they seek to move. Enterprises at the highest end of maturity for DIY performance (e.g., top-performing cycle time, service quality and cost optimization KPIs), estimated to be fewer than 10% of all enterprises, are successful at performing at or better performance and cost than some Leaders in this research.

MNS is core to all network as a service (NaaS) offers, and is “as a service” already, like all network services. For “all opex” offers for networking solutions, the networking hardware and software are rented (that is, provided as an operational lease) and no end-user ownership is contemplated for the included network elements.

Most vendors and providers have characterized NaaS solutions as something new. Naturally, an opex-only payment model of network hardware/software/network services is decades-old and remains a common procurement option. The primary longer-term opportunity for enterprise buyers will happen if dominant OEM control over hardware and software license policies and costs are upended by competitive price/value offers that do not (also) benefit from this model (e.g., end of sale, end of life to force cyclical refresh cycle spending from buyers). For NaaS offers constrained to dominant OEM hardware and software business models, the likelihood for enterprise life cycle savings will remain scarce.

The market overall has numerous offer types, yet the NaaS market remains emergent. Vendor marketing and offer activity continued to significantly increase in 2024. In the MNS context, NaaS offers are always opex-only, with no notion of buyer ownership. Other elements (hardware and software) delivered as opex are simply the consumption pattern choices of buyers, which may or may not be combined with MNS offers. Notably, some providers offering NaaS seek to charge on a sliding usage scale. For example, pricing elements may be the amount of bandwidth consumed on a port, the number of ports, or number of users at a site. We observe enterprises clearly expecting to pay lower costs based on their usage, yet evidence that this is the case is uncommon.

WAN transport services have always been opex. This is because circuits are leased from carriers — except for enterprises that have obtained their own fiber infrastructure (for example, dark fiber, owned or leased) to operate and support their business models (DIY or managed services).

Ownership and operations of private fiber networks in this context are most common among energy producers and their distribution networks worldwide, as well as cities, counties and states globally. Notably, the energy industry sector specifically is predominantly DIY for its OT due to the critical nature of these networks and minimal third-party managed services expertise.

A clear gap in buyer trust exists with a managed service provider's ability to manage field area networks (FANs) with the specialized expertise required amid certifications, cycle time, service quality and cost optimization demands. Similarly, enterprise manufacturers commonly exclude their engineering (e.g., plants and supply/distribution) from enterprise-IT-led MNS procurements, strongly preferring DIY operations.

By contrast, MNS providers more commonly support state and local government initiatives that own and operate their own fiber infrastructure (for example, public Wi-Fi, broadband, smart cities, and universities). These same enterprise entities, meanwhile, are separately eschewing managed networks services for their public utility FANs.

Many providers consider the requirement for buyer transparency to be limited to performance KPIs and metrics in support of SLAs and service-level objectives (SLOs). These measurements are necessary, but insufficient, for MNS buyers.

MNS is not at the maturity stage of commodity services, such as a water or electrical utility. Insight and improved SLA/KPI metrics reporting transparency into underlying provider capabilities are required for informed selection and governance. For example, buyers should require service quality reporting on behaviors controllable by MNS providers — those directly related to their activity cycle time for incident resolution and service request performance.

As a best practice, buyers should ensure their provider governance framework includes MNS provider KPI metrics and reporting related to their workflows and automation methods for improving service quality and decreasing activity cycle time.

Stark differences exist among MNS providers when broken down into the contextual elements that define activities included in the service, versus those that are either optionally charged or not available. For example:

- Few providers charge separately for single point of contact for transport troubleshooting, whereas most include this in the device monthly recurring charges (MRCs).
- Some include a quantity of simple changes in the device's MRCs; others don't include any changes, while yet others include unlimited simple changes.

This lack of provider specificity (service inclusions and exclusions) within underlying elements of MNS proposals can have a costly effect on financial governance of agreements and cost predictability. A lack of visibility into the components and the activity details of offers commonly results in unexpected higher costs to buyers of these services.

Gartner observes that service request management, especially the costs for infrastructure changes that result from inadequately defined services definitions and formal agreements, is the highest unexpected cost category experienced by enterprises. We have seen increases to MNS fees by as much as 30% on an annualized basis (see Tool: RFP for Managed Network Services).

As enterprises continue to expand requirements, multicloud and hybrid networks are becoming common. Enterprises continue shifting applications to the cloud, embracing the internet as transport, network and security in support of users/endpoints anywhere, and applications residing anywhere. Increasingly, MNS providers are providing support for cloud resident microservices and ephemeral workloads as part of agreements.

Compared with on-premises workloads (for example, private data center or hosted), visibility into cloud resources and the networks connecting them remains comparatively limited, yet this is changing. This year, a growing number of MNS providers offer service visibility, contextualization and service mapping across the entire estate, including public cloud visibility, and enhance this with business impact reporting. Others are on the path to achieving improved end-to-end capabilities via digital experience monitoring (end user to application experience) and application performance monitoring (APM) via MNS extensions to their owned platform. This is being done with both enterprise-owned APM and APM that is operated and delivered as an extension of the MNS agreement. These agreement extensions commonly include integrations with vendors such as AppDynamics, New Relic or Dynatrace, whether provider-owned and delivered or enterprise-owned and operated.

LAN technology support from MNS providers includes all common LAN components — access points, switching and wireless LAN controllers (WLCs). These are the minimum typical scope elements for the MNS for LAN market. Beyond these core components, almost any LAN-connected IP device can be monitored and maintained by most MNS providers. Cloud-managed networks (for example, cloud-based WLCs) are not typically managed by the MNS provider.

A set of managed IoT endpoints have long been supported within MNS offers, and this trend is expanding significantly in the form of increased sensor and surveillance applications across most industry segments. The expansion of the product market for these endpoints has increased choice and flexibility, and allowed for more managed service entrants, as well as incumbent growth. These endpoints include OT, SCADA and IoT networks across energy, utilities, smart city, building automation and IIoT for manufacturing plants and warehouses. Notably, enterprises within these industry segments seeking MNS will find fewer MNS provider options for standardized, automated and scalable endpoint services than the broader cross-industry segment MNS for LAN offerings.

WAN site edge technology support from MNS providers includes the common network edge CPE, including routers, WAN optimization and and the leading vendor OEM variants of SD-WAN, as well as security functions, and firewalls. Support for leading network product OEMs is near-universal in capability, because nearly all MNS providers in this research support the five performing OEMs for SD-WAN, and their security platforms.

When assessing MNS providers, infrastructure and operations (I&O) leaders responsible for network and security operations should leverage these recommendations:

- Choose DIY for operations when your network is fundamentally critical to the performance and differentiation of your business/industry. MNS providers commonly seek to differentiate within industry verticals. However, be careful to protect your intellectual property (IP) to sustain differentiation in your business. If you seek direct alignment to your model and market differentiation, you would best be served by a customized offer in which MNS can still be delivered as a component element within a broader-scope enterprise estate. Examples include energy and utility OT networks and manufacturing OT environments. It is common to see MNS providers managing the IT “side” of these types of enterprises, then the OT side is managed internally.
- Ensure that all stakeholder requirements are met by engaging a cross-functional team, including business leaders, when negotiating MNS agreements to effectively reduce cycle time, improve service quality and optimize operations expenses.
- Know your own capabilities and total costs first — don’t presume that MNS will deliver better quality or be more cost-effective than DIY.

- Prioritize the reduction of higher-impact MNS operation expenses by expanding beyond technology-focused provider selection criteria to include current automation performance for incident and service request management, and user experience monitoring and reporting.

- Improve MNS performance by adding service operations metrics to network-technology-centric SLAs. Consider full network outsourcing instead of MNS for complex, custom or otherwise unique service management support. These special requirements do not scale well for MNS providers, and enterprise costs are typically much higher than standardized MNS.

- Be advised that when custom managed service providers build capabilities that become unique or highly differentiating for them, they will find creative methods to leverage these newfound capabilities with other clients within the bounds of legal and ethical behaviors. In some cases, this reuse can end up in a worst-case scenario, in which you paid for the unique capabilities and unwittingly end up enabling a competitor. Protect your IP at all times, regardless of the operations model you choose.

- When required to maintain internal IP and capabilities, continue to source your own NOC/SOC management tools and operate DIY (that is, tools beyond owned ITSM and APM tools compatible with MNS offers). Procure staff augmentation models required for volume spikes or to free resources for project work, instead of using MNS. Enterprises with mission-critical industry infrastructure components (such as in manufacturing, energy and healthcare) more commonly choose DIY approaches for their most sensitive requirements, as overall vendor trust is less common.

- Avoid requiring MNS providers to use any of your tools to actively monitor and manage your network estate, which increases risks and costs for buyers.
    - The exceptions to this are certain API integrations to ITSM or APM tools. Increasingly, MNS for security is included with integrations of other enterprise tools. For example, other enterprise integrations may be to the SIEM and SOAR platforms used by MNS providers for enterprise MNS delivery — these integrations can also include other enterprise data, enterprise network taps and others.
    - If you require external providers to use your enterprise tools, employ a staff augmentation or a custom NOC outsourcing services acquisition model. Requiring MNS providers to use enterprise-operated tools often results in diminished value and scalability of the provider's platform automation, as well as decreased service delivery quality and cost optimization.
    - If enterprises want all/most of their own NOC/SOC tooling platform to be used, MNS offers are not suited for these requirements. A custom managed service, typically with labor rate/full-time equivalent-driven fee, is often more appropriate. At the same time we have been seeing an increase of enterprise proposals presented as managed services, yet many of these are simply staff augmentation and nothing like a managed service.

- Inform stakeholder leadership about the implications of a first-time MNS decision by reinforcing that once a decision is made, a future reversal back to DIY is significantly more difficult, risky, time-consuming and costly. Over time, key NOC/SOC processes, tools and skilled resources will diminish or disappear from your enterprise, and you will need to reinvest and start over if reversing the initial decision to move to DIY.

- Beware of sourcing highly custom-managed IT services, commonly referred to as outsourcing, by exerting diligent planning. Ensure that standard offers like MNS or DIY alternatives are not better than custom offers at cycle time reduction (automation), service delivery quality and cost optimization. The more any enterprise IT, network and security operations are customized, the more likely enterprises are to experience drawbacks. These include lower cycle time performance, service delivery quality deficiencies and higher costs than alternative approaches, such as DIY, MNS or a replacement custom IT outsourcing agreement. On a related note, very large enterprises with highly customized IT outsourcing agreements that have been in place for many years will find it considerably more difficult to change course and move to any other model. They may need to undergo yearslong transformation programs to complete the migration, along with exposing themselves to the commensurate execution risks to the enterprise.
- Confirm your process, NOC tooling and people skills maturity level by leveraging Gartner's IT Score assessment results to inform your preparation for an MNS decision (see IT Score for Infrastructure and Operations).

Market Overview

All providers in the Magic Quadrant and Critical Capabilities for MNS globally support multiple LAN, WAN edge and security function vendors, servers, virtual machines, and microservices operations assurance and protection, whether focused on domain integration or work unit.

MNS are remotely delivered services from the provider's NOC/SOC, with a separate disaster failover hot site as a minimum. The NOC personnel are commonly deployed at the physical NOC/SOC location and/or deployed regionally.

The providers in this market are traditional network service providers, SIs or pure-play MNS providers. The MNS market does not include network services (e.g., WAN transport services), or network/security products.

Three mission-critical capabilities are highly interdependent in the MNS market:

- **Service delivery quality:** Process efficiencies, data accuracy and integrated service management across the MNS solution.

- **Network automation:** High-performing FCR for automated incident resolution, leveraging AI/ML with automation orchestrations to deliver high-functioning troubleshooting automations.
- **Customer experience:** Near-real-time, configurable, automated updates and easily navigable portals that display key metrics performances for all services.

The MNS market is a volume operations business model, not a complex operations model that is prone to the challenges of managing high customization. Volume-based models focus on optimizing products and services in a relatively mature market (for example, LAN, WAN and security environments). Volume models deliver standardized services, undergirded by repeatable processes and tightly integrated tools with high degrees of automation, to achieve high-scale efficiencies, resulting in higher delivery quality and optimized costs. Provider differentiation comes in the form of consistently higher-performing cycle time metrics, improved service quality, and cost-effectiveness. This Magic Quadrant is focused on the volume operations MNS provider business model, not custom-managed NOC offers (see How to Choose the Correct Network Operations Model for Your Enterprise).

The MNS volume delivery model has been in place for many years. It has evolved from a complex operations delivery model, which is similar to today's customized IT outsourcing agreement delivery models. Network and security technologies continue to evolve, and the software to manage these networks has improved substantially during the past 10 years.

However, some MNS providers are also IT outsourcers that operate both models and straddle the two markets. Specifically, MNS is highly standardized and scalable, whereas common IT outsourcing agreements are substantially customized for a specific enterprise. The customized models commonly have lower standardization for scale efficiencies, less predictable costs and more prevalence for labor-driven pricing models.

In cases where the provider's operations delivery uses both models to serve customers, provider performance is often broadly impaired. Shared provider operations resources with high variabilities in standardization, automation and performance quality standards commonly demonstrate diminished value at a higher cost to buyers. This happens for both types of managed services in the market when providers share common resources across these two disparate delivery models, since the provider's offerings, investments and focus collide.

The current network and security trends enabling the expansion of MNS provider support are:

- Increased AI capabilities incorporated into user experience, documentation and service queries.
- Fixed wireless access with multicarrier eSIM capability could become strong alternatives to fixed cable broadband access.
- New LEO satellite services are moving toward mainstream adoption, specifically those operating at nonlegacy altitude orbits.
- 5G private mobile network (PMN) and Wi-Fi 6 continue to gain traction. Many providers in this research support both of these technologies. Additionally, increased IoT and IIoT support is becoming more widespread among most MNS providers in this research.
- Microsegmentation implementation and operations support is growing within the MNS providers' capabilities to implement and operate (via MNS). Implementations of this model are increasing in critical data infrastructures such as manufacturing, healthcare and utilities to restrict current exposures to east-west LAN traffic. (See 2024 Strategic Roadmap for SASE Convergence for more information.)
- Customer experience monitoring tools and approaches are expanding. There is a shift from the current datasets from tools' analytics capabilities toward analyzing data and providing insights, leading to plans to achieve proactive monitoring across all user application sessions for anomaly detection. The goal is for MNS providers to capture live and real-time experience data, learn what's normal (with higher frequency and fidelity than typically seen historically) and proactively avoid degradation or loss of service.
- The majority of providers continue to improve the breadth and depth of their security offerings while having enhanced alignment between MNS LAN/WAN and security. AI and ML continue to drive improvements across the breadth of MNS offers.

The components of service delivery quality include:

- **Service delivery process frameworks.** An example is adapting the ITIL framework to the provider's service delivery model. MNS providers must display a high degree of process discipline. This discipline must be embedded in their MNS offers (for example, standardized service offers). Quality is best achieved via repeatable, standardized automated processes. A high degree of custom nonstandardized processes reduces quality and increases costs to buyers.

- **Service delivery platforms (SDPs).** These comprise the multitenant hardware, software, applications, security and scalability components of the provider's infrastructure for delivering MNS. The platform's core purpose is to deliver service management and service assurance capabilities to support the provider's offers.

- **API capabilities and integrations.** These are most commonly the provider's own ITSM tools and customer-owned ITSM tools (for example, ServiceNow or BMC Helix ITSM [formerly Remedy]) and/or customer-owned APM tools (such as AppDynamics, Dynatrace and New Relic). However, some MNS providers are increasing their inclusion of APM, which is a positive development, though these offer features are typically feature-limited compared to leading commercial off-the-shelf (COTS) APM tools that an end customer may use.

- **Endpoint and link monitoring via SNMP.** Most MNS providers also ingest flow data (for example, IP Flow Information Export [IPFIX]) as part of their service, which improves visibility and context of application-impacting events. Packet data capture is not a capability included in offerings currently in this market. We are observing the emergence of improved cycle time for the initial steps of incident handling. The common cycle time metric is 15 minutes to detect, classify, declare and assign an incident (assignment to a human, first contact or acted upon [zero human touch]) via automation. A few MNS providers offer selective sub-five-minute cycle times on a limited set of endpoint types today. We expect this trend to accelerate and expand over time to one-minute cycle time performance or less.

- **Enterprise end-user experience monitoring and performance anomaly detection.** As user applications shifted from mostly internally hosted applications to cloud service providers, many enterprises recognized the need for better end-to-end visibility. Amid a changed working environment, this requirement has become more commonplace.
    - Some providers offer end-user experience monitoring (or digital experience monitoring [DEM]), whether the actual experience of end users (for example, PC agents) is via synthetic measurements or a combination of actual and synthetic measurements. These approaches give enterprises greater visibility into the user experience by displaying the types of applications being used and geographic location variabilities. These capabilities also improve providers' abilities to detect anomalies and take proactive measures to avoid incidents.
    - Meanwhile, some providers in this market are delivering on end-user experience and service mapping, and toward proactive anomaly detection. Realistically, this is one of the very few proactive categories today. The intent and outcome of effective anomaly detection is to achieve sufficient behavioral baselining of user-to-application norms with data analytics insights, via higher granularity/frequency data collection source methods and automation. Then, when typically nonservice or minimally impactful anomalies are identified, these can be proactively remediated as practical before detrimental end-user experience is perceived.
- **Service request management.** High volume and short cycle time service request management requirements (for example, complex changes, with over two hours to execute the change) are often subject to additional change fees or delivered as separate statements of work to accommodate projects. All MNS providers commonly offer a fixed number of simple changes included in the fixed price per device/per month. When the fixed volume number exceeds monthly limits, per-change fees may apply.

- **Onboarding.** Fees for onboarding are commonly quoted separately and are one-time and fixed. Onboarding typically runs eight to 12 weeks. However, depending on the level of complexity, it could be as short as four to six weeks or as long as several months. Enterprises seeking transformational networking initiatives in parallel with choosing an MNS provider should select the MNS provider first and have it stabilize the current estate of the enterprise network before participating in the transformation. Furthermore, MNS buyers should not choose network product OEM technology amid a transformation and then seek out an MNS provider. Choose the MNS provider before — or, better, in conjunction with — any new network products to confirm support. This will minimize mistakes that are likely to cause procurement redo and dissatisfaction, and incur other unexpected costs.

- **Security for MNS.** Cybersecurity continues to grow in criticality. The market for MNS and the management of SASE architectures are converging. For example, for many years a common model for IT, MNS and security has been leveraged for on-premises firewalls and related edge and site security endpoints. The NOC primarily monitors assurance (OS and down) and the SOC manages the security functions. Both NOC and SOC continue to grow in enterprise mission criticality, with a trend toward combining NOC/SOC, and potentially conflating network and security staff skills and expertise. The markets for both MNS and security are converging to a SASE/SSE model. Today, MNS providers commonly manage enterprise on-premises firewalls (legacy through current generations), delivering firewall as a service, ZTNA and deployment. This on-premises security services delivery model is following security perimeter posture shifts and preference for more consolidation of security functions to fewer suppliers. Cloud-based security consumption patterns are common strategies for buyers. Achieving and maintaining a ZTNA is becoming the core security objective for all enterprises. This trend favors providers that offer higher-performing MNS and adjacent-market managed security services (MSS) along with migration and transformation employing professional services, as the professional services criticality has substantially increased for MNS providers. Enterprise buyers increasingly expect these capabilities, as network/IT operations combine with provider MSASE offers (see Where Do I Start With SASE Evaluations: SD-WAN, SSE, Single-Vendor SASE, or Managed SASE?).

- **Security, audit and data protection compliance certifications.** Example certifications for enterprise buyers range across different industries and geographies. The standards that tend to drive the contents of newer privacy legislation, both globally and for states in the U.S., include:
  - The U.S. Health Insurance Portability and Accountability Act (HIPAA)
  - Privacy Shield
  - Service Organization Controls (SOC) 1
  - Statement on Standards for Attestation Engagements (SSAE) 18 Type 2
  - International Organization for Standardization (ISO) 27001 and 9001
  - The EU's General Data Protection Regulation (GDPR)
  - The California Consumer Privacy Act
- **Expansion of SDP support beyond primarily network-centric devices.** This includes device support for voice/video infrastructure, such as on-premises unified communications, unified communications and collaboration, session border controllers, compute (virtual or physical in nature), on-premises storage, and security devices at the host level. Additional endpoint support from MNS providers continues to expand. Most MNS providers also support physical servers, storage, virtual machines, microservices, IoT, video, physical access control and environment sensors.

For MNS, automation is the key to delivering superior cycle time performance, predictable service quality and pricing at scale.

The key underlying components include tools that must be multitenant and commonly comprise AI for IT operations, observability, IT operations management, ITSM, network performance monitoring and diagnostics, and network automation tool capabilities covered by Gartner research. While these underlying components are key, MNS for security incorporates more and different tools, and commonly offers additional integrations with other systems. MNS for security providers commonly employ the same ITSM tool, share network taps for telemetry ingestion, and leverage network source of truth from the MNS for LAN and WAN operations.

Core tools for MNS may be integrated and automated from COTS vendors, or may be original tool developments by MNS providers integrated with COTS components of the provider's SDP. The automations are, in part, configurable to varying degrees within the COTS tooling. More commonly, they are enhanced with overlay network automation orchestration platforms that are implemented to enable cross-functional (process) automations and orchestration of these automations. These overlay-type frameworks to the SDPs typically are forms of message bus/bot workflow frameworks for run book/playbook technologies that orchestrate multiple automations and the requisite workflow processing, and serve as an ephemeral data store.

We see a very large number of bots used for automation within the MNS provider's SDP. Simply, these bot automations are composable single-function scripts that are orchestrated together to support automation use cases. Bots are most commonly used to automate configuration and event management tasks, and for enhancing ML and, increasingly, AI capabilities. For example, many MNS providers use bots to automate repetitive tasks that a human would otherwise have to perform manually. More mature providers may have thousands of bots as part of their network automation codebase.

Service requests affecting change and configuration, event processing (primarily ML today) and incident management activities are the most common automations. Together, these three encompass the broadest automation impacts to quality and scale efficiencies, where both the provider and customers benefit. That is, providers improve their margins via automation, while customers enjoy higher-quality services, fewer errors and improved cost predictability. In this context, enterprise agreements with MNS providers increasingly contain terms that emphasize collaboration between a provider's continual service improvement activities and its enterprise customer IT operations teams — a best practice to mutually embrace with any provider.

MNS providers must maintain an accurate CMDB of the customer's production networking estate, and many provide two-way integrations to customer-owned ITSM tools. These two-way API integrations cover both the CMDB and case management, at a minimum (for example, for service requests and incident management). Regardless of whether enterprises choose to sync their ITSM tool with the provider's platform, the accuracy of this underlying data is a mission-critical requirement for providers and their customers. Accurate network-source-of-truth data (e.g., digital twins) is fundamental to maintaining quality and efficiency via automation within the provider's change and configuration management, incident management functions, and all reporting, which commonly are automated as part of MNS providers' SDP.

With a CMDB and change/configuration process discipline in place, automations are particularly efficient to the service assurance processes — event management and fault isolation (and recovery), as well as the initiation of incident declaration. These combine with ticket enrichment automations that inject metadata related to the initial incident classification, along with many other elements providers use to improve accuracy and drive more automation. Beyond these basic and required fundamental elements, the automations often attempt recovery from a fault before making a formal incident declaration. These attempts may include automated restarts of services or the device itself, as well as other action-oriented workarounds for restoration of service.

High-quality MNS customer experience is possible when supported by the appropriate SDP with high degrees of automation, service metrics detail, and near-real-time, flexible reporting. The key component from providers to support customer experience is an always-available customer portal. This category is not the specific end-user experience that is typically discussed. This category is directly related to MNS end users of the provider portal. These users are primarily operations-related, application and/or business unit stakeholders, and some are in procurement.

The following are considered the minimum capabilities for quality results and cost predictability in customer experience management:

- **A near-real-time updated customer portal.** This is required for most interactions with MNS providers. The portal should persistently update all service requests, incidents and performance statuses related to the entire scope of the MNS provider's responsibility. The portal should be easy to navigate (minimal click-through steps) and the end-user experience for accessing reporting should be configurable by end users.

- **Service-mapping capabilities from their MNS provider.** Service mapping is most commonly done in the ITSM tool component (for example, ServiceNow) of the provider's SDP, while others include service mapping within the MNS provider's platform.
  - Not all customers require a two-way integration with their internal ITSM tool and the provider's (for example, for CMDB and case management). However, this capability should be delivered in the MNS provider's SDP and be part of the provider's portal in support of customer experience.
  - Customers should expect visibility from MNS providers into enterprise applications, mapped to the correlated overlay and underlay of the enterprise networking estate (managed devices and connectivity). This contextualization between applications and their managed network elements provides valuable granular detail and insights, hence benefiting customers and easing consumption by non-IT business stakeholders — as well as optimizing providers' troubleshooting and automation efforts.
- **Anomaly detection.** The enterprise network infrastructure and application traffic patterns are constantly monitored, and the production behavior of users and their applications is baselined for documenting the known patterns and usage behaviors. From this continuously known baseline, anomalies can be identified proactively. This is different from threshold-crossing alerts on network traffic or capacity measurement statistics, which are basic and common. This anomaly capability is more granular and enables proactive measures from providers that can prevent incidents from occurring.
- **Business impact reporting.** This provides business-level context for customer stakeholder leadership. These capabilities can be configured to the individual enterprise's business-critical elements that are in scope for the MNS provider.

- **SLAs.** The nature of MNS means enterprise technology stack performance typically is not the responsibility of the MNS provider.
  - The performance of LAN or WAN CPE or the network transport is ultimately accountable to the product OEM and NSP. However, the key SLAs for MNS should focus on the activities of the MNS provider — those for which it is entirely accountable. These include their own service availability (for example, their SDP).
  - In addition to cycle time to complete all service activities, SLAs require added items, including speed of answer responsiveness, request and incident acknowledgment and assignment for resolution, FCR incident performance, automation metrics, and content reporting frequency and accuracy. These and others can be crafted as SLAs with penalties in most cases (see Tool: RFP Template for Managed Network Services).
- **SLOs.** Because MNS providers are managing infrastructure on an enterprise's behalf, tying SLA penalties to underlying technology failure is difficult. However, enterprise SLAs may be set as objectives for the MNS providers (absent the penalty portion, these are effectively SLOs). In this context, enterprises can use more common networking SLOs that are related to performance of the technology stack (CPE and transport). This is key, because enterprises must manage their own technology supply chain and, when using MNS, they typically do not have the visibility internally to do so. This visibility into the performance of these supply chain participants is a growing requirement and valuable in addressing any vendor deficiencies, because these issues can have a supporting fact base when MNS providers offer SLO reporting.

- **Co-management.** A broad swath of requirements and use cases for the MNS market are being developed.

  - Though still in its early stages and gaining moderate interest, several MNS providers are marketing these service extensions. In this context, co-management was appearing within application policy routing for SD-WAN. It has now expanded to other use cases, affecting change, configuration and very limited incident management. Hence, this is a potential growth market for about 50% to 60% of enterprises globally, including self-managed (DIY) networking teams, and potentially operating a licensed SDP from an MNS provider.

  - Among the usual challenges of governance in any co-management model, many other obstacles and valid concerns exist for both providers and enterprise customers. One of the largest is accountability and liability for errors made. Even if it seems apparent who is "at fault," it becomes less obvious the more co-management is embraced. Whether it's enterprise MNS buyers looking for lower pricing or a DIY enterprise licensing its (presumably) former MNS provider's service delivery platform, there is plenty of work ahead for providers and enterprises seeking to expand this model to its fullest. We are seeing this emerge already.

- **Commonly added adjacent services**. The MNS market's most common adjacency among enterprise buyers is with MSS and/or SASE solutions, including components within, such as firewalls. The second most common adjacency is a range of IoT and OT endpoints, usually as add-ons to MNS for LAN. The IoT endpoints include surveillance devices/video and sensors. Capabilities for any providers of MNS for security, MSS, managed SASE or other delivery models include the markets adjacent to MNS, professional services and system integration capabilities to assist enterprise buyers.

Evidence

Gartner analysts conducted over 2,500 client inquiries on the topics of networking, network operations and MNS for LAN and WAN between 1 August 2023 and 1 August 2024.

In 2024, 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. 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

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.

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 - 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

Critical Capabilities for Managed Network Services

Tool: RFP for Managed Network Services

Where Do I Start With SASE Evaluations: SD-WAN, SSE, Single-Vendor SASE, or Managed SASE?

Is SD-WAN Dead?

© 2024 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: Ability to Execute Evaluation Criteria

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

Source: Gartner (October 2024)

Table 2: Completeness of Vision Evaluation Criteria

↓	↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	High
Vertical/Industry Strategy	High
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2024)