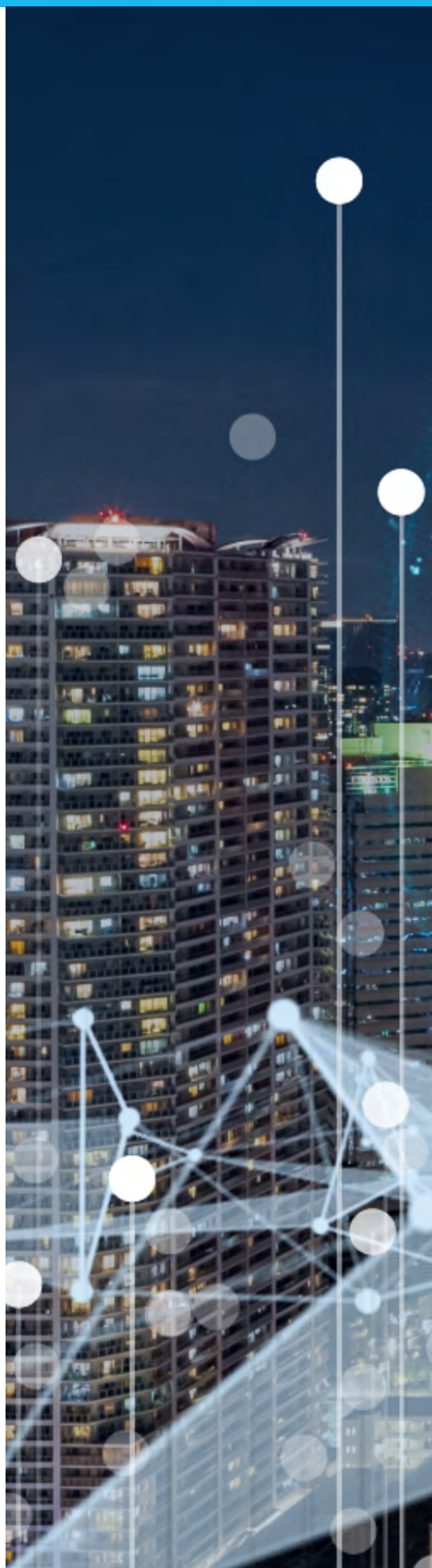
FROST & SULLIVAN

Adaptive Network Solutions

Enable Organizational Progress with Flexible Networks

FROST & SULLIVAN VBOOK

CONTENTS



Introduction: Network Modernization Creates New Paths For Progress

Connecting an organization's sprawling ecosystem of distributed users, applications, and data is a complex task. Enterprises and public organizations need a dynamic network—a network that is more reliable, secure, flexible, scalable, and intelligent than in the past. The evolved intelligent network allows organizations to virtually implement network services and manage network infrastructure using various advanced technologies, cloud-based applications, and platforms while minimizing the high maintenance costs, lack of scalability, and inconsistent performance of legacy networks. The result is operational efficiencies, improved customer experiences, and secure data management.

- **Deeply connected enterprise.** Organizations are conducting essential business far from corporate headquarters, requiring them to connect branch offices, edge locations, remote worker homes, field workers, partners, and customers seamlessly and securely.
- **Superior customer experiences at scale.** To succeed in today's fast-paced, dynamic, and demanding economy, organizations are evolving traditional business methods with new digital models that deliver expected customer experiences efficiently and securely. Businesses in every industry are now software companies, engaging with customers, partners, and employees via automated, self-service portals and collecting and utilizing this data to further improve experiences and operations.
- **Networked data fluidity.** Data and AI-enabled enterprises are increasingly collecting, storing, protecting, processing, and analyzing exponentially growing volumes of data at the edge, in the cloud, and on-premises.
- **Network mastery.** Modern networks are dynamic and complex. Investing in expert network teams with deep partner ecosystems and global experience to manage advanced technologies in an ever-changing environment can yield short- and long-term value.

Distributed Users Require Access To Critical Business Applications

Today's businesses run around the clock, which means your employees, partners, and customers must have access to critical systems whenever they need them, wherever they are. Distributed users access business networks and applications from various locations, including public transit and coffee shops, as well as devices such as smartphones, laptops, and tablets. This new business environment creates stress on the network in several ways:

- The network must be scalable to handle large numbers of users and data traffic without performance degradation.
- It must be high-performance to handle high bandwidth business applications, such as video streaming and collaboration tools. The network must integrate security to protect data and applications from breach, loss, or unauthorized use. As network infrastructures evolve, the convergence of network and security becomes indispensable.

Organizations globally cited factors critical in their organization's network strategy for the next two years:[1]

- **51%** Convergence of network and security
- **48%** Network control and programmability
- **50%** More network functions will move to the cloud
- **47%** Flexible bandwidth
- **48%** Private 5G woven in the enterprise network
- **46%** Convergence of LAN and WAN

An intelligent network fabric is flexible enough to meet the dynamic needs of a distributed business environment, ensuring users and machines always have access to the applications they require.

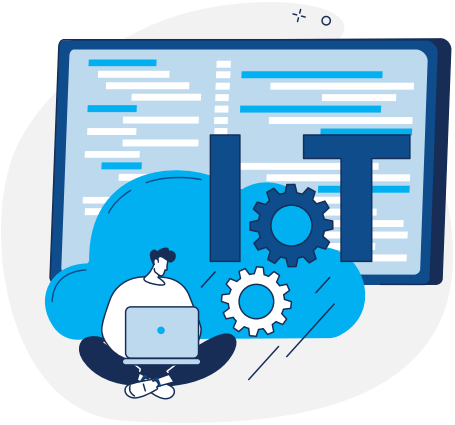
The Right NSP Can Accommodate Organizations' Dynamic Needs With Flexible Network Choices

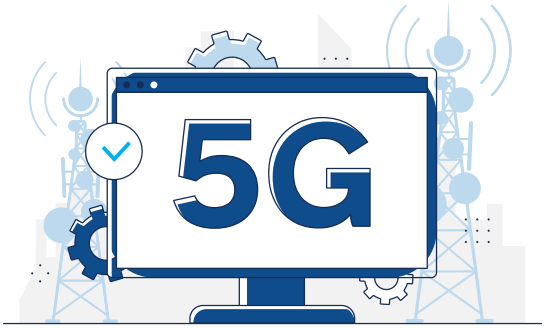
The most sophisticated network service providers (NSPs) offer a range of flexible network choices designed to support increasingly distributed business operations. Scalable and adaptable network solutions include the following:

- Organizations require **multiple connectivity choices** to run their network. Depending on business type, location, traffic volume, application needs, and even available network technologies, an organization will deploy a range of wireless and wireline services for primary and backup connectivity. 5G provides enormous capabilities, including secure and expansive coverage, connectivity range, capacity, and reliability.
- **Software-defined wide area network (SD-WAN)** solutions enable businesses to use multiple connectivity choices, automatically switching to the best available connectivity option. In the Frost & Sullivan 2024 Global Network and Wireless survey, 45% of network decision-makers cited SD-WAN as a critical technology for achieving their digitalization goals.
- Organizations invest in **hybrid and multi-cloud services** for their distributed IT infrastructure. A cloud connection service enables enterprises to seamlessly integrate their on-premises network with a cloud service provider. In the survey, 48% of respondents said they use hybrid cloud/multi-cloud services.

- To minimize the complexity of implementing and managing different network technologies, **network as a service (NaaS)** provides businesses the choice to buy network services on a subscription-based model. NaaS may include network access, cloud services, security, and virtual network services.
- **Private wireless networks (PWN)** are a response to increasing demand for flexibility and network security threats. Organizations with industrial sites, extensive facilities, or campuses prioritize PWN to benefit from higher reliability, efficiency, coverage, control, and security of their networks. In addition, it supports IoT platforms, enabling organizations to adapt and scale their network capabilities with evolving digital transformation needs.
- **Neutral host networks (NHN)** are gaining traction, allowing an organization's PWN (in a facility/building/hotel) to connect with multiple carriers through the multi-operator core network (MOCN) standard to extend indoor coverage. The NHN model is critical in replacing the traditional and expensive distributed antenna system (DAS) model used for indoor coverage. NHN incorporating PWN layers represents a significant path to modernization for brownfield or older network infrastructures.
- **Fixed wireless access (FWA)** addresses connectivity needs for organizations seeking flexible and scalable connectivity solutions or in areas with limited fiber optic infrastructure. FWA is quick to install, scalable, and cost-effective, making it best for temporary setups or remote locations. Wi-Fi brings similar cost-effectiveness, flexibility, and scalability of wireless connectivity but within the organization's premises, enabling employees to work seamlessly from anywhere within the workplace. In the 2024 Frost & Sullivan Global Network & Wireless survey, 63% of organizations cited engaging with a third-party provider for managed Wi-Fi solutions.

90% of IoT decision-makers utilize SD-WAN to manage and orchestrate the flow of data traffic between on-premises data centers, edge, and cloud via a private wireless network.[2]





54% of network decision-makers cite private 5G and fixed wireless as the most crucial transport technology in their organization's strategy for the next two years.

Enterprises benefit when network services are flexible, offering dynamic bandwidth allocation to support changing needs. NSPs can remove the burden of complexity by providing a comprehensive and flexible suite of services.

The most appealing NaaS attribute to organizations:[3]

39%	37%	34%	34%
Online ordering, including signature and acceptance of a contract	Ability to add and manage multi-cloud interoperability	API monetization with network APIs	Overall observability

Self-Service Portals Deliver Even More With Streamlined Automation

To an organization, the primary interface to their dynamic, intelligent network is via a self-service portal. A streamlined self-service portal provides visibility into network operations and tools to automate tasks. These tools include usage analytics and alerts, resource scaling (up or down), automatic ticketing and troubleshooting, policy implementation, and integration of portals across different products and services.

This requires a distributed modern network that allows organizations to monitor, control, and manage their networks in real time. While organizations can manage their network independently, they can also partner with NSPs that have the right tools to maintain operational agility. Network management is particularly critical as organizations operate in hybrid work environments with fluctuating data traffic loads and an increasingly complex mix of cloud and on-premises resources.

Self-service portal features are critical for organizations to manage their network services:[4]

25%	Collaboration capabilities, e.g., web chat, text, click to call
24%	Ease of integration, e.g., APIs to ITSM, analytics tool
23%	On-demand capabilities, e.g., instantly increase or decrease bandwidth
20%	Usage analytics, reporting, and alerts

A self-service portal empowers organizations to track, monitor, and manage their networks with greater control. NSP can help organizations by building an intuitive, feature-rich portal that simplifies network management, automates routine tasks, optimizes performance, and streamlines troubleshooting. This improves network efficiency, reduces manual efforts, and ensures a seamless, proactive network management experience for organizations.

AI Workloads Require A Robust, Intelligent Network

As artificial intelligence (AI) takes root across all industries and business processes, networks play a critical role in securing and realizing the full benefit of real-time data. AI workloads process escalating volumes of data collected from multiple sources, often in near-real time. For instance, a logistics firm uses an AI-driven platform to analyze various parameters, including historical delivery data, real-time traffic data, and climate conditions on different available routes, to recommend the most efficient routes that reduce fuel costs, minimize delivery times, and improve operational efficiency. AI-driven solutions streamline various distributed processes while increasing operational efficiency and service quality.

To ensure their AI workloads perform as needed, organizations require a network that can handle real-time capacity and is designed for flexibility. Characteristics of an intelligent network include:

- Advanced network infrastructure (including high-capacity fiber and network equipment) that supports large volumes of data and real-time applications
- Scalability and flexibility to address current and future network demand
- Network automation and orchestration that support networked data fluidity and deliver optimized resources and increased operational efficiency
- Security incorporated by design principles (prioritizes security from the very beginning)
- Interoperability and standardization support through API integration and collaboration

AI is transforming business operations faster than any technology in history. However, unless organizations have the right network foundation, they cannot optimize their use of AI workloads.

Global organizations are prepared to integrate intelligent technologies into their business operations:[5]

Critical technologies for achieving digital transformation:

48% Generative AI (GenAI), natural language processing (NLP), large language models (LLMs)

44% Machine learning (ML)

46% AI in network operations (AIOps) will be critical to their network strategy in the next two years

32% ML/AI will drive the highest growth in their total network bandwidth in the next two years

AI At The Edge

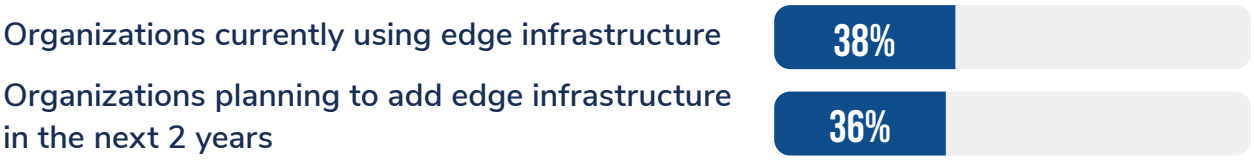
In the not-too-distant past, transactions performed at branch locations would be batched for transmission to headquarters perhaps once a day. In the modern landscape, such a practice translates into lost time, decreased efficiency, security issues, and potential revenue loss.

Edge computing processes data closer to the source, resulting in quicker response time and supporting low-latency use cases, particularly AI workloads requiring real-time processing. Edge applications are deployed to monitor, control, or automate specific business processes (e.g., smart cameras for surveillance, smart lighting, or smart thermostats to optimize energy consumption). They generate enormous volumes of data that need to be transferred to centralized systems for analysis to derive further control actions. Edge devices, applications, and data centers are components of edge infrastructure that businesses are already using or planning to implement in the next few years.

Edge devices integrated with AI algorithms enable real-time data processing at the source without reliance on centralized servers or cloud infrastructure. AI at the edge strengthens privacy and security by keeping sensitive data local, lowering the risk of data breaches. It also optimizes bandwidth usage by minimizing persistent communication with centralized servers, enabling efficient network utilization.

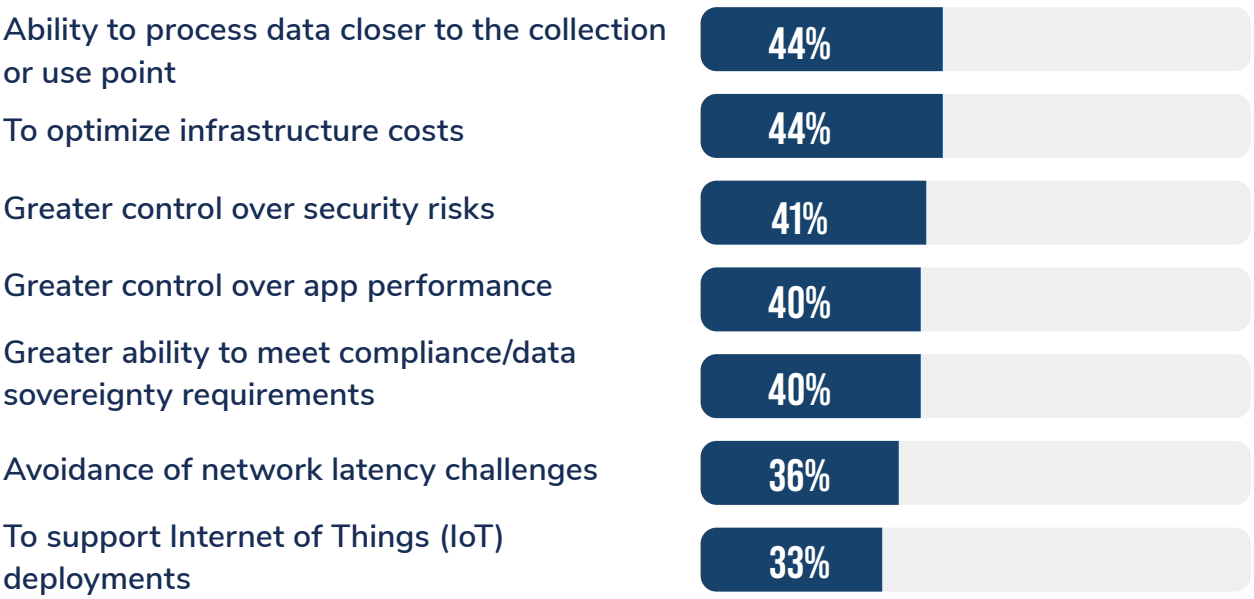
AI is transforming edge infrastructure, bringing intelligence and automation to the network's edge. AI algorithms optimize resource allocation, predict network demands, and enhance network security at the edge. This transformation enhances data management, improves user experiences, and empowers organizations with powerful insights, ultimately driving innovation and efficiency across business operations.

Considering the importance of edge infrastructure in enhancing operational efficiency, organizations are strategizing their network planning:[6]



Organizations cited top functions/purposes for deploying edge infrastructure over the next two years:[7]

Other key reasons for choosing an edge location were related to operational requirements:[8]



Use Case: Healthcare Industry Requires Intelligent Robust Network At the Core

Healthcare aspires to unlock digital acceleration in order to improve patient and clinician experiences. The available technological advancements that can transform healthcare ecosystems need a network designed to support specific use cases as they increasingly rely on intelligent devices, sensors, and connected equipment to deliver care.

Healthcare organizations use advanced technologies in their day-to-day pursuit to provide quick and effective services, including collecting and processing patient data, diagnosing and developing treatment plans, creating and maintaining electronic medical records (EMRs), performing telemedicine and remote patient monitoring, and exchanging healthcare information such as medical imaging and diagnostics. Technologies that make these daily functions efficient include:

IoT-enabled medical devices and sensors enable real-time monitoring and data collection of patients' vital signs, track medication usage, detect possible risks, improve patient safety, and ensure proactive care. IoT devices allow remote patient monitoring, helping healthcare providers monitor patients' health outside the hospital setting, thus reducing hospital stays and improving patient outcomes.

Connectivity, including wireline access, provides high-speed internet connecting numerous devices, instruments, and equipment, ensuring seamless data access and transfer across departments, medical devices, and systems. Wi-Fi and cellular networks, including 5G networks, provide campus-wide connectivity, enabling healthcare professionals to stay connected and access patient data via tablets to communicate efficiently within healthcare facilities. With improved security and low latency, PWN supports telemedicine, IoT integration, and advanced healthcare applications.

Healthcare organizations are adapting to evolving technologies as healthcare professionals and patients increasingly use newer connected medical devices and equipment. These connected/IoT devices and equipment are latency-sensitive and susceptible to security threats, mainly endpoint devices with geographically distributed sites. A robust, intelligent network at the core of the healthcare infrastructure ensures seamless and efficient operations.

Edge computing enables real-time processing and analysis of patient data at the network edge, reducing latency and response times. Additionally, data processing at the edge ensures data privacy (by keeping sensitive information localized) in compliance with data residency requirements.

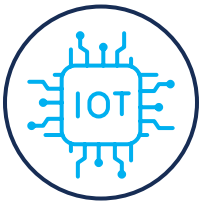
Data collected from IoT-enabled devices needs to be stored and accessed when needed. **Hybrid/multi-cloud solutions** enable quick access to advanced healthcare applications without the need for extensive on-site infrastructure. For instance, cloud-based electronic health record (EHR) systems enable fast, secure access to patient information across departments and locations.

AI algorithms process vast amounts of patient data, medical images, including scans and x-rays, and clinical studies to uncover various health patterns, predict diseases, and create personalized treatment procedures. Moreover, AI-powered virtual assistants and chatbots can improve patient engagement, offer individualized health advice, and manage administrative duties with greater efficiency and satisfaction.

To safeguard patient information, security solutions, including firewalls, encryption, application security, and access control mechanisms, must be incorporated into the network to prevent unauthorized access and potential data breaches. Patient data is sensitive and regulated by the Health Insurance Portability and Accountability Act (HIPAA). Network security is critical in protecting patient data from cyber threats, physical security, and insider threats.

In a healthcare setting, IoT-enabled medical devices are closely supported by edge computing and AI. However, security and cloud services complement the healthcare ecosystem.

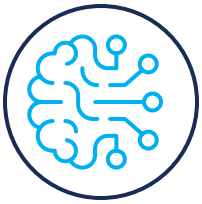
Healthcare organizations cited important technologies to achieve their digitalization goal:[9]



43%
IoT

43%
Network security

43%
Application security



42%
AI

40%
Hybrid cloud/multi-cloud strategy

37%
Edge computing

Healthcare organizations indicated factors critical for their network strategy in the next two years:[10]

42%
Flexible bandwidth

38%
Private 5G weaved in networks

35%
Artificial Intelligence in network operations (AIOps)

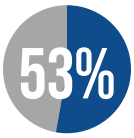
Use Case: 5G Transforms the Manufacturing Industry

Connectivity is crucial for next-generation factories, with 5G emerging as a game-changing and vital component for manufacturers transitioning to smart manufacturing and the future factory. Manufacturers can use 5G connectivity to leverage automation, AI/ML, AR/VR, and robotics technologies and improve production line interconnection and robots in smart factories. In addition, 5G-enabled autonomous robots support human safety by real-time video monitoring and rapid response to hazards. Robots can patrol facilities, detect risks, and perform risky tasks without human intervention. The low latency of 5G allows instant halting of operations when safety threats are identified, reducing workplace accidents and injuries. Manufacturing sites operating on legacy equipment with limited connectivity require retrofitting and integrating wireless protocols to bridge communication gaps compared to modern factories with built-in connectivity, incorporating advanced IIoT infrastructure for seamless integration.

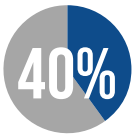
With its high reliability, security, low latency, and capacity to handle high data volumes, 5G benefits manufacturing by lowering energy costs, improving efficiency, and boosting productivity across the value chain. This high-speed environment enables greater flexibility for mass personalization and customization, accelerating the design-to-manufacturing process and enabling smart manufacturing.

Private 5G networks offer much promise to manufacturing organizations because they provide data security and sovereignty with 5G capabilities. Private 5G networks deliver the high performance required for data-dense environments and where processes are based on real-time responsiveness, such as connected factories and video analytics. Private 5G networks support the latency and bandwidth requirements for industrial applications at the edge. In the Frost & Sullivan Global Network & Wireless survey, 51% of manufacturing organizations stated private 5G as critical for their network strategy in the next two years.

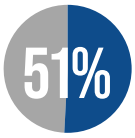
Manufacturing organizations currently using 5G as:[11]



As part of a hybrid network

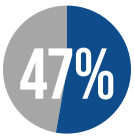


As part of the IoT strategy

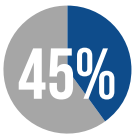


As a primary access

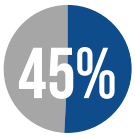
Drivers for considering 5G among manufacturing organizations:[12]



Deploy private network capabilities (extended coverage, range, security, capacity, and reliability) in a cost-effective manner



Support IoT strategy



Support cloud or edge computing capabilities

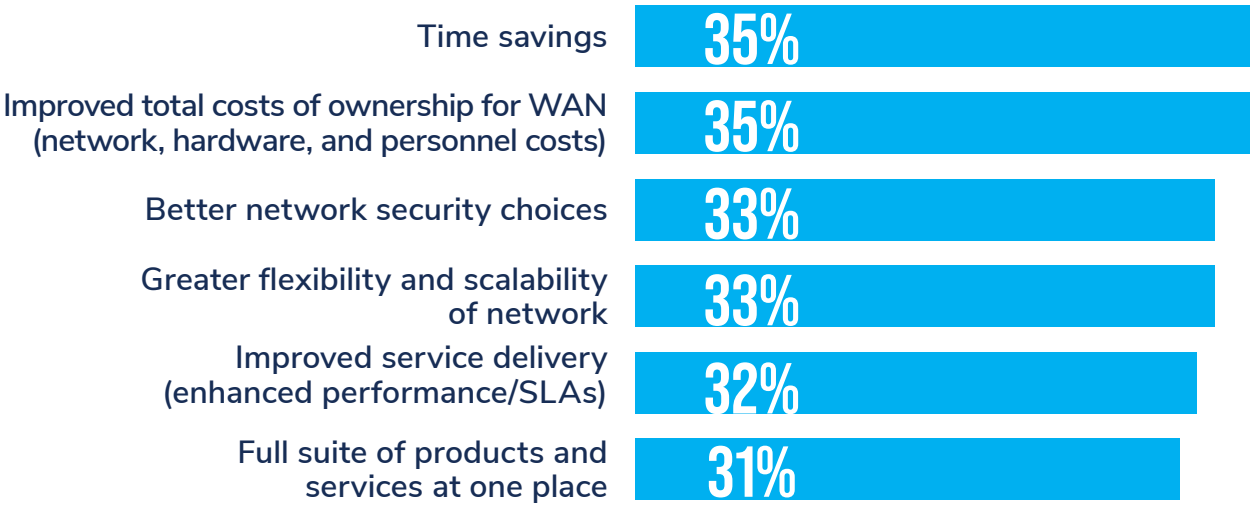
With the growing demand for edge services, organizations are considering strengthening their connectivity alternatives to accommodate upcoming high-bandwidth applications, and 5G delivers the flexibility and scalability required by future applications.

Organizations Need To Engage With A Managed Service Partner To Optimize Network Value

Organizations are increasingly adopting advanced technologies as part of their digital transformation initiatives. Implementing and managing these technologies are complex tasks, requiring skilled IT and network staff who can continuously analyze and tweak existing infrastructure to achieve evolving business goals. Because hiring and training in-house staff to address complex multi-technology, multi-vendor environments is challenging, an increasing number of organizations are choosing to engage with third-party service providers to manage their digital infrastructure. Optimally, the organization's trusted network service provider has the skills and expertise to act as a managed service provider (MSP), with a portfolio of options to co-manage or fully manage the entire network infrastructure of the organization.

An MSP relies on a partner ecosystem of SDN vendors, cloud service providers, security services vendors, and appliance vendors to offer a wide choice of vendors (e.g., best-of-breed vendors or multi-vendor approaches) that accommodate specific business requirements. In addition, an MSP can offer AI/ML-based network automation, enhanced portal capabilities, and the ability to integrate GenAI capabilities at the network function level.

Organizations cited factors that influence engagement with a managed network service provider:



Organizations engage with third-party providers for managed network services:[13]

Increasing complexity and urgency are leading more enterprises to seek expert assistance regarding their network strategy from their MSP. Many organizations find that managed services deliver a shorter time-to-value than do-it-yourself options, making it a cost-effective investment.

Evolve Your Network

- With distributed business operations, the foundation of network infrastructure needs to be strong and flexible. Multiple connectivity choices, SDN, cloud services, and security services form the base of a robust network infrastructure supporting evolving business needs.
- Ensure the tools are in place to deliver a seamless experience between distributed locations. Integrating network automation tools and upgrading network infrastructure to accommodate high bandwidth demand from AI-enabled applications and solutions.
- Partner with an MSP that can address distributed businesses' network service needs, including a range of network services supported by advanced technologies such as AI/ML that simplify network operations while enhancing operational efficiency.

Endnotes

1 2024 Frost & Sullivan Global Network & Wireless Survey, conducted in Oct-Nov 2024. The web-based survey received responses from 1,285 network decision-makers, representing a range of industries, company sizes, and geographies.

2 2024 Frost & Sullivan Global IoT & MEC Survey

3 2024 Frost & Sullivan Global Network & Wireless Survey

4 2024 Frost & Sullivan Global Network & Wireless Survey

5 2024 Frost & Sullivan Global Network & Wireless Survey

6 2024 Frost & Sullivan Global Cloud Survey

7 2024 Frost & Sullivan Global Cloud Survey

8 2024 Frost & Sullivan Global Network & Wireless Survey

9 2024 Frost & Sullivan Global Network & Wireless Survey

10 2024 Frost & Sullivan Global Network & Wireless Survey

11 2024 Frost & Sullivan Global Network & Wireless Survey

12 2024 Frost & Sullivan Global Network & Wireless Survey

13 2024 Frost & Sullivan Global Network & Wireless Survey

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. ➜

FROST & SULLIVAN