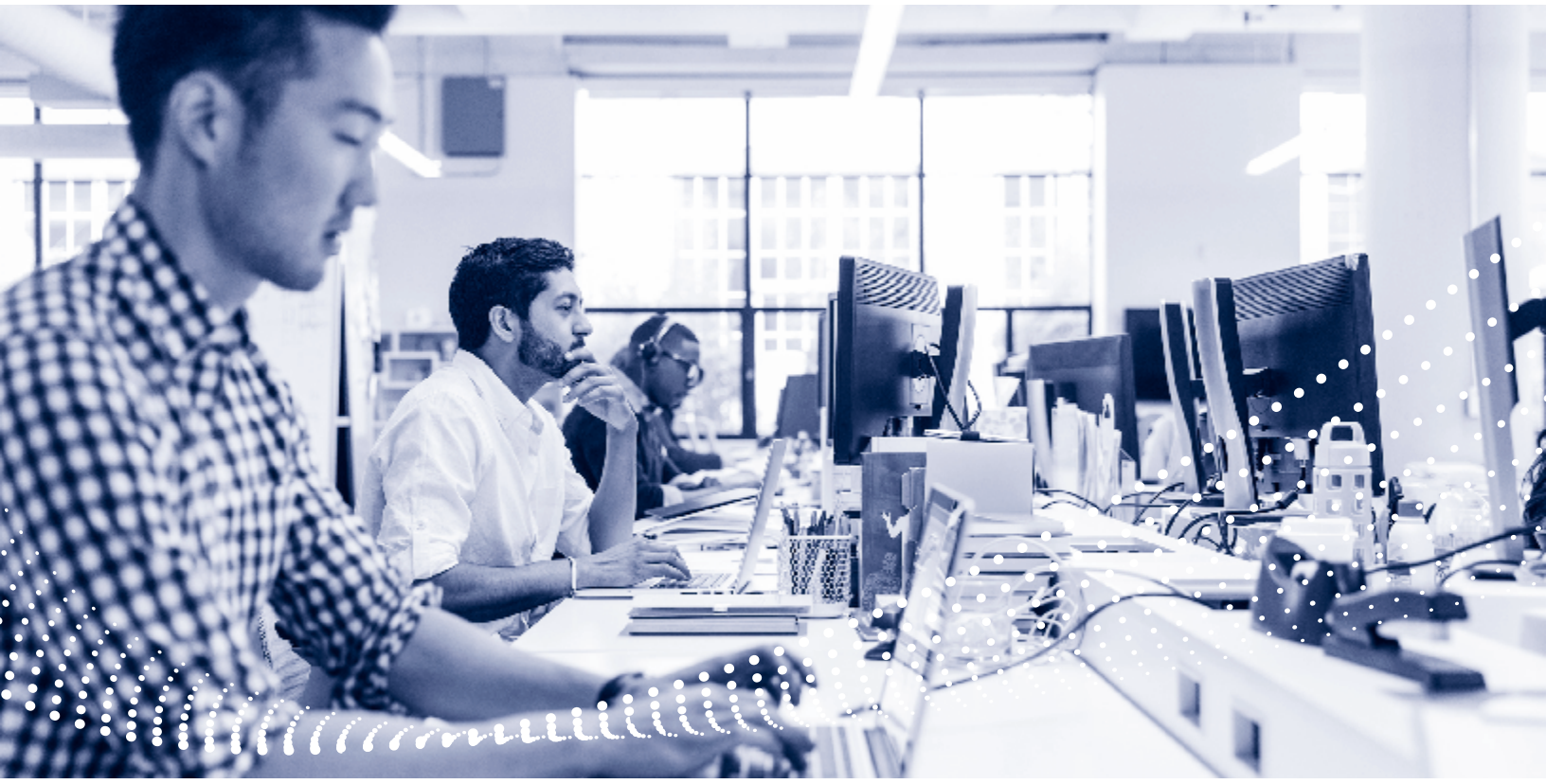
TechTarget | Custom Media
White Paper

HUGHES®
An EchoStar Company

DECISION TIME: CHOOSING THE RIGHT MANAGED NETWORK SERVICE PROVIDER



INTRODUCTION

Networks are the nervous system of digital business. But as data relentlessly proliferates, networks are becoming a highly complex web of telecom, Wi-Fi, SD-WAN and more, stretching the expertise of IT leaders to build and run them. Many are facing a crossroads: continue down the daunting path of managing their own networks or seek out a trusted managed network service provider (MNSP).

As with any technology decision, the first step is to take stock of existing capabilities. Although many organizations employ some skilled networking professionals, the growth of networks and the incorporation of multiple cloud-based services are likely to exacerbate an already significant IT skills shortage.

Faced with this conundrum, IT leaders will confront two inconvenient facts: First, skilled network professionals—especially cybersecurity experts—are rare, command high salaries and often prove difficult to retain; and second, building and running a multilayered corporate network is a basic requirement for digital business and might not by itself yield a significant competitive advantage.

These two realities lead to an alternative worth considering: Working with an MNSP that provides the latest high-bandwidth network technologies as well as the expert staff to manage and maintain them. This choice provides an organization with the networks required by digital business while freeing up in-house staff to focus on strategic business initiatives.

What to expect—and demand—from an MNSP

Connectivity. The first and most basic thing to expect from an MNSP is connectivity, although in today's multilayered networks, that's not as simple as it sounds. Network links must provide high bandwidth reliably and economically across a variety of circuits, including cable, fiber, gigabit Ethernet, satellite and fixed wireless. Each of these different links must be installed, tested, managed and maintained by skilled professionals. Further, the MNSP should provide a single, highly responsive point of contact for customer care, including a call center for employees to contact when issues arise.

Helpdesk Support. An MNSP should provide a single, highly responsive point of contact for customer care, including a call center for employees to contact when issues arise. The helpdesk should be able to triage a broad range of solutions, including software-defined networking (SDN), Wi-Fi, voice over IP (VoIP) and digital media.

Cybersecurity. Given the variety, frequency and sophistication of cyberthreats, protecting a network from cyber attack and ensuring regulatory compliance requires an arsenal that includes both technology and human expertise. Cybersecurity technology should provide real-time alerts that can be acted on right away—but not so many of them that cybersecurity staff ignores them due to information overload. Because threats are constantly changing, cybersecurity staff must be in a continual state of learning. It's pointless to defend against yesterday's threats while exposing an organization to new and innovative attacks.

Because attacks are so widespread and varied, it is necessary to implement principles of zero-trust—to treat even veteran employees and longstanding customers as if they have been compromised. Zero-trust implementations require expertise and discipline all their own, including micro-segmentation of data networks, multifactor authentication and highly granular policy-based access.

In addition, the cybersecurity technology deployed by an MNSP should focus on the most costly and widespread threats, such as ransomware, which often enters an organization due to employee carelessness. Regular and thorough backups are critical to thwart ransomware actors, and secure network connections to backup operations must be provided.

AIOps for cost-effective availability and transparency. High availability is important to many businesses, but the measures needed to assure availability, including failover, can be costly. As a result, many businesses can't afford the amount of uptime they truly need. To increase network reliability while keeping costs under control, artificial intelligence operations (AIOps) leverages AI and machine learning algorithms to ingest reams of data, including data from IoT sensors. Self-healing capabilities enable the network itself to respond to outages and re-route traffic automatically. Such a system should be highly transparent to network administrators, with dashboards that provide visualization of operations. With these tools, managers are able to intelligently evaluate tendencies in network performance, anticipate disruptions and take action to prevent downtime.

Application performance. Network traffic connects employees and customers with a variety of applications. Although each application has its own performance requirements, the network must perform equally well for all of them. And because bandwidth needs will tend to increase as organizations grow and applications process more data, network topology must be constructed with the future need for larger pipes in mind.

To mitigate the business impact of internet congestion, which may fluctuate throughout the day and over time, an MNSP should be familiar with all application types and their throughput needs. These include:

- Transactional applications. Low latency and high volume are required. Credit card transactions must be carried out according to the PCI data security standard.
- Streaming content. Audio and especially HD video require high-bandwidth connections. For high-quality VoIP experiences, network connections must be able to compensate for congestion, latency and lost packets.
- Large file downloads. Training videos, new software releases, medical images, CAD files and legal documents all require high bandwidth.
- Guest Wi-Fi. Customers expect high-bandwidth connectivity, whether in office buildings, hotels, shopping malls, hospitals or educational institutions.

To increase network reliability while keeping costs under control, artificial intelligence operations (AIOps) leverages AI and machine learning algorithms to ingest reams of data, including data from IoT sensors.

Your MNSP Checklist

Organizations and their network requirements can vary widely. Here's what you need to keep in mind when evaluating an MNSP:

Breadth of capabilities. Since your organization will grow and its needs are likely to change over time, you should evaluate MNSPs with a broad range of capabilities, some of which you might not need right away. Here are some of the most important:

- Managed SD-WAN. The needs of high-bandwidth applications are driving SD-WAN deployments, often replacing legacy MPLS connections. Market-leading SD-WAN solutions vary widely in features and functionality. MNSPs should provide extensive expertise in understanding which solutions fit which circumstances. A broad SD-WAN solutions portfolio is essential for optimal performance.
- Secure Access Service Edge (SASE). A zero-trust blueprint for cloud-based cybersecurity developed by Gartner, SASE is being embraced by many vendors and enterprises. Organizations should become familiar with SASE and look for products and providers that implement SASE principles.
- Business solutions and office connectivity. Employees and guests expect to seamlessly communicate over VoIP and Wi-Fi. Digital media such as network-connected signage and menu boards keep them informed with the latest news and updates. Analytics applications help optimize business performance. Training applications provide live, two-way communications between managers and employees, reducing excessive travel. By caching content locally, network traffic is kept to a minimum.

Site-specific customer service levels. Throughout an organization, remote locations may vary widely in their service requirements based on business performance. Some locations produce such a high volume of business that real-time proactive monitoring premium services are required. While other locations with substantially lower business volumes may require more cost-effective alternatives, MNSPs should provide a full portfolio of service options provisioned in alignment with the business needs of the remote location.

Responsiveness. The ability of an MNSP to fulfill a site-specific service-level agreement (SLA) is critical to the continuity of business operations and customer interaction. Ultimately, networks consist of physical devices and connections. Although network bottlenecks and outages can be viewed remotely from a dashboard, many repairs can only be performed by field technicians. Not all outages are of the same urgency, however. Next-day response is acceptable in some cases; same-day response is needed for others; four-hour response is needed for emergencies. A well-staffed call center and help desk are essential to provide outstanding customer care by evaluating the urgency of reported problems and dispatching field technicians when required.

Geographic coverage. An MNSP's network coverage should match your needs. Sometimes local- or metropolitan-area networks are sufficient. However, financial services, healthcare or retail networks are more likely to demand regional or national coverage. For organizations that operate internationally, only a provider capable of providing and maintaining links within and between countries and continents will suffice.

Physical coverage is another area in which the demands of growth should be kept in mind. Although its operations might be regional today, a successful company might soon find itself crossing into new regions and expanding nationally and internationally. A provider that has global capabilities can support a company's rapid growth.

Cybersecurity. Although AI, ML and automation are important defensive weapons, at some point, skilled and knowledgeable humans must study alerts and make decisions. Because of the scarcity of cybersecurity experts, an established MNSP is more likely than most commercial organizations to have experts on staff at the highest skill levels. Likewise, an MNSP should run a security operations center (SOC) with a full array of best-of-breed cybersecurity technologies, including SIEM, MDR, EDR, antivirus, antimalware and sandboxing.

Because of its ubiquity, ransomware must be defended against. A corporate network, managed by an MNSP, should include links to backup facilities, including air-gapped storage, so that an organization can recover its data with minimal disruption, rather than pay the demands of ransomware actors.

Size and scale of operations. Although a local MNSP might meet the needs of a small organization, the size of a large MNSP confers many benefits for organizations of all kinds.

For example, a large MNSP offers economies of scale, including the ability to obtain network services at volume discounts, passing the savings on to customers, whether large or small. In addition, a large MNSP is more likely to receive priority service from telecommunications carriers.

Conclusion: Making the right MNSP decision

Although many organizations try to build and manage their own networks, few have the expertise to build, secure and maintain their networks at a high level, while achieving a differentiated business advantage to justify the expense. For many organizations, an MNSP is the best choice. For over 50 years, Hughes Network Systems has provided a broad range of capabilities supported by deep expertise. With global coverage, highly skilled cybersecurity specialists, AIOps technology and vertical industry expertise, Hughes Network Systems has on numerous occasions been formally recognized by trusted industry analysts as a market leader. Hughes has been cited for its proven capability to simplify technology and help organizations achieve a competitive business advantage.

For more information on choosing a MNSP, please refer to **Business.Hughes.com**

This content was commissioned by Hughes and produced by TechTarget Inc.