CONNECT | MANAGE | PROTECT

WHITE PAPER:

How Managed Services Help Achieve Synergy in Network Metrics

Managed Network Services can provide organizations the tools to balance security, reliability and cost

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com

MngdNetworkSerWP041020

SageNet
CONNECT | MANAGE | PROTECT

EXECUTIVE SUMMARY

Network connectivity is arguably the most critical component of today's IT infrastructure. Users need secure access to applications, data and other resources that may reside in remote data centers and the public cloud. Network downtime, performance problems and other issues have a direct, negative impact on productivity and customer service. A security breach could be devastating.

As the network has become increasingly important, it has also become more complex. IT teams typically lack visibility and control across the entire environment, from the data center to the cloud to the edge. Monitoring and management tools are often fragmented, and require human intervention for day-to-day administration. Security tools generate an overabundance of alerts, making it difficult to sort through the "noise" and respond to the most urgent threats.

At the same time, budgets are limited, and the network must contend for resources with other business requirements. So how does an organization achieve the right balance of reliability, security and costs? This whitepaper discusses the competing priorities faced when designing, implementing and maintaining the enterprise network. It also explains how managed network services can help improve network availability and security while controlling costs and freeing IT teams to focus on strategic initiatives.

AVAILABILITY

Network downtime is expensive. Gartner estimates that every minute of network downtime costs $5,600, on average. These costs include lost revenue, lost productivity, recovery costs and intangibles, calculated as follows:

- Lost revenue includes the amount of revenue generated per hour multiplied by the percentage of revenue that's dependent on network connectivity.
- Lost productivity is calculated as the average hourly salary of employees multiplied by the percentage of productivity that's dependent on network connectivity times the number of employees. Network dependence will vary from employee to employee, so multiple calculations will likely be required.
- Recovery costs include the salaries of IT staff and outsourced providers tasked with fixing the issue, replacement equipment, and lost data, if any.
- Intangibles include customer churn, damage to the business' reputation and brand, etc.

Calculating the cost of network downtime can help organizations determine the risk to their business and how much availability is required.

Network uptime is expressed as a percent of a year — 99.5 percent uptime means that the network is available 363.175 days per year. The flip side is that the network is unavailable 1.825 days or 43.8 hours per year or 3.6 hours per month — a costly proposition. Improving availability to 99.9 percent would reduce downtime to just 8.76 hours per year or 43.8 minutes per month.

Network issues aren't limited to downtime — performance problems can also have a serious impact on operations. A recent study found that network brownouts and other performance issues cost $600,000 on average. More than 80 percent of survey respondents said that brownouts were causing serious damage and frustrating employees.

In fact, the damages and losses from brownouts trailed only network outages and data breaches among the most concerning IT issues, according to survey respondents. Because organizations are relying more and more upon network connectivity to access their applications, data and cloud resources, the cost of brownouts is only expected to increase.

Network Vulnerability Assessments

A network vulnerability assessment can help organizations identify unreliable or inadequate equipment, and systems that are unsupported or nearing end of life. This enables organizations to prioritize investments in areas that present the greatest risk to the business.

SECURITY

Cybercrime has become big business, with the cost in the U.S. alone exceeding $139 billion. The headlines continue to be filled with news of massive security breaches, with organizations in a wide range of industry sectors falling victim.

According to data from KnowBe4, 95 percent of IT leaders are somewhat to very concerned about data breaches. They are also worried about credential compromise (93 percent), phishing attacks (91 percent) and ransomware (89 percent).

They have cause for concern. A recent PricewaterhouseCoopers survey found that less than half of organizations believe they are adequately prepared for a cyberattack. Approximately two-thirds admit that they don't have adequate safeguards in place, and about the same number say they don't regularly review their current security practices or assess their risk exposure.

It's not from a lack of security spending. According to a study by Varonis, cybersecurity budgets increased 141 percent between 2010 and 2018, and Gartner expects spending on information security products and services to reach $170.4 billion by 2022. Top areas of investment are security services, infrastructure protection and network security equipment.

However, KnowBe4 found 59 percent of respondents lack executive support for key security initiatives. The Varonis study found that 60 percent of executives believe their existing security solutions provide adequate protection, but just 29 percent of IT professionals agree.

Security is Becoming a Business Priority

In a recent Harvey Nash / KPMG survey, 56 percent of business leaders said "improving cybersecurity" is a key business issue that the board of directors wants IT to address. That's up from 49 percent the preceding year.

COST

Research firm Gartner publishes a quarterly forecast of worldwide spending on IT products and services. The most recent report shows a nominal 1.1 percent increase in IT spending over the prior year. Spending on core IT infrastructure is expected to decrease 2.8 percent as organizations shift more of their budgets to the cloud.

However, a recent CompTIA study found that 36 percent of small to midsize businesses (SMBs) with up to 500 employees are dedicating most of their IT budgets to core infrastructure, including networking equipment. Researchers surmise that SMBs have held onto IT equipment past its useful lifecycle and are needing upgrades to meet basic business requirements.

These purchases are being made at the expense of investments in emerging technologies. More than half (53 percent) of SMBs say that emerging technologies could help them increase productivity, improve profitability and gain competitive advantages, and 39 percent said that tech spending should focus on productivity and the customer experience. Not surprisingly, 39 percent of SMBs say their annual IT spending is too low.

Organizations are also struggling with security investments. In a recent survey of North American organizations by KnowBe4, 75 percent of respondents said they do not have an adequate security budget. Another study found that 90 percent of organizations prioritize customer service, sales and other matters ahead of IT security when it comes to budget allocation. Hiring in-house security talent is an expensive proposition that's beyond the reach of many organizations.

THE ROLE OF MANAGED NETWORK SERVICES

Organizations struggling to balance competing network priorities can benefit from managed network services. Managed network service providers (MNSPs) specialize in the design, implementation and management of enterprise networks, either in partnership with the customer's IT team or as a fully outsourced solution.

Continuous monitoring and proactive management are key components of an MNSP's offerings. The MNSP will leverage state-of-the-art technologies and best-practices-driven methodologies to perform

preventive maintenance and respond quickly to performance problems before they result in business disruption. These services make costs more predictable, and give customers access to technologies they might not otherwise be able to afford. They also help improve productivity, reduce IT staff turnover and enable IT teams to shift their focus from maintenance tasks to strategic initiatives that drive the business forward.

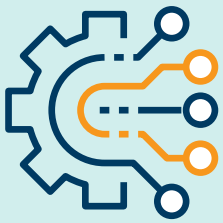
Managed network services also improve security across the entire network. A qualified provider will implement policy-driven tools that reduce the risk of network intrusions and malware. This not only protects applications and data but helps organizations comply with increasingly stringent compliance requirements such as HIPAA, PCI and NIST 800-53.

Best-of-breed managed services solutions feature an end-to-end approach that incorporates security and engineering, 24x7 coverage, a single point of contact, and problem ownership and resolution. The MNSP will offer flexible service level agreements with availability, mean-time-to-repair and other parameters customized to meet the customer's business objectives.

The MNSP can also provide expert consulting services to assist in the development of a cybersecurity strategy. A third-party provider offers an objective perspective that can bridge the differing viewpoints of executive, line-of-business and IT stakeholders. A qualified MNSP will also have the knowledge and experience to streamline deployments and upgrades, enabling customers to optimize infrastructure costs and see a faster time-to-value on their technology investments.

Managed Services Popular among SMBs

A recent CompTIA survey found that 53 percent of SMBs are currently utilizing a managed IT services provider. Another 34 percent have considered managed services although they are not currently working with a provider. Just 10 percent said they are not using managed services and have not considered it.



CONCLUSION

There's no question that a high-performing, highly secure network is essential to business operations. Network downtime and performance degradations can exact an enormous cost to organizations that rely upon connectivity. A security breach is a persistent threat. Yet organizations are struggling to allocate their limited IT budgets to meet business and compliance demands.

Managed network services can help organizations balance these competing priorities. By outsourcing to an MNSP, organizations gain a more predictable monthly expense with around-the-clock management and support for their critical network infrastructure. In-house IT staff can focus on strategic initiatives and business experiments while relying on the MNSP for network availability and security.

ABOUT SAGENET

SageNet is passionate about trusted connections. The company believes that by creating, discovering and nurturing trusted connections with its customers, associates and community, SageNet enhances the world that connects us all.

As a leader in managed network and cybersecurity services, SageNet connects, manages and protects technologies and devices across the enterprise. SageNet's collaborative approach provides peace of mind and systems-confidence that empowers an organization to focus on its core mission.

The company offers world-class service and support via its three US-based 24/7 Network Operations Centers (NOCs) and Security Operations Centers (SOCs), geographically-diverse teleports, a central National Logistics Center, multiple data centers, and a nationwide field service organization.

With a three-decade track record in managed services, SageNet boasts a long-term customer base that includes the nation's largest retail, healthcare, financial, utilities and energy organizations. SageNet manages communications at more than 220,000 endpoints. Headquartered in Tulsa, SageNet has regional offices in Washington, D.C., Atlanta, Chicago and Philadelphia.