Managed Network Services: The TCO Payoff

White Paper Sponsored by Time Warner Cable Business Class

Executive Summary

Three out of four midsize businesses describe themselves as network dependent. Cloud computing and mobility are important drivers of network-centric business models. Although many business benefits are derived from this new approach, its openness and always-on capabilities create management and technical challenges. Complex security policies are needed to control the exchange of information among users, devices and applications, including time of day and location. Quality and performance requirements are also increased. Network reliability becomes critical because a network outage will shut down the business.

Managed network services allow businesses to outsource the day-to-day operation of network links and equipment and ensure network security. The service provider can deliver comprehensive, high-quality service because it has a large, experienced staff that specializes in router and security technology. Managed networks are bigger and more robust than in-house networks, leading to greater reliability and resiliency with industry-average service-level agreements promising 99.95 percent availability. Service provider managed networks are monitored 24 hours per day, yielding the benefit of continuous review and fast response to network events.

ACG Research conducted two use cases to show how businesses are using managed network services to support their network-centric business strategies while minimizing management costs and freeing up internal staff for more strategic work. Each case study describes the role of the network in the business, identifies the benefits of the managed network and compares the total cost of ownership (TCO) of the managed network service to an internally staffed alternative. The first case study is a managed WAN service used by an automobile dealership with 400 employees and 5 sites, and the second is a managed Internet and security service used by a single site healthcare clinic with 27 employees.

In each case the managed network service solution provides better coverage, with broader and deeper access to technical expertise, at a much lower cost than augmented internal IT staffs can achieve.

KEY FINDINGS

Managed network services provide an all-in-one, easy solution for setting up, monitoring and operating network data, Internet and security services.

Use cases of managed network services compared to internally staffed network services found:

- 79% lower TCO for a managed WAN service deployed at a midsize multilocation automobile dealership.
- 84% lower TCO for a managed Internet and security service deployed at a single healthcare clinic.

Moving to a Network-Centric Business Model

As a result of increased user network dependency, barriers of time and distance are being eliminated while customers, partners and suppliers are brought together into a broad business ecosystem that accelerates business processes and innovation. Cloud computing and mobility are two important drivers of network-centric business models. Cloud computing involves moving applications from desktops and company data centers to service providers' networked data centers (the cloud)[1]. Mobility includes the use of business mobile devices, bring your own device, and guest access to the business network.

Although it offers many benefits, moving to a network-centric business model presents new management and technical challenges[2]. Bringing everyone together in a broad business ecosystem increases security challenges because the boundaries between private networks and the Internet are blurred. Bandwidth requirements are increased, as are varying quality and performance requirements. Video conferencing, streaming video, and e-learning are significant sources of increased bandwidth.

IT management priorities must also change as this network-centric approach is adopted. Previously, LAN management was the top priority because 80 percent of the traffic was on the LAN. Under this new approach 80 percent of the traffic is on the WAN, so awareness and control of the WAN must be the top management priority. The payoff is reduced operational uncertainty and risk by providing a more responsive and flexible IT infrastructure.

Managing the Network for the Network-Dependent Business

Managing the network to meet steadily increasing business requirements, ensuring the network's reliability and security and meeting continuous cost reduction objectives are challenging. Making WAN management a top priority involves adding more networking staff with broader and deeper networking skills. Management activities include:

- Ensuring network security. Cyber attacks are increasingly aimed at small and midsize businesses. Symantec, a global leader in security, reported in its latest annual security report that 31 percent of targeted attacks were aimed at businesses with fewer than 250 employees.
- Sustaining network reliability. The industry average reliability target is 99.95 percent availability, which is equivalent to 4 hours and 23 minutes of downtime per year[3]. Achieving this availability level requires not only continuous network monitoring, but also the 24-hour availability of a fault resolution team.
- Maintaining business continuity. Business continuity requires development of a network plan to identify risks and establish network recovery plans in the event of an unplanned service interruption. Disaster recovery facilities, staffing and training are essential to ensure a rapid response when an event occurs.

[1] Software as a Service and Infrastructure as a Service are elements of the cloud concept.

[2] See "Planning for the New Network: Ten Trends Rewriting the Rules for Midsized Business," Time Warner Cable Business Class.

[3] See http://www.acgresearch.net/UserFiles/File/Cisco%20Documents/Business%20Case%20for%20iWAN%20TCO_ACG.pdf for a discussion of business WAN reliability requirements.

- Improving economic efficiency. With scarce budgets and resources, IT staffs of all sizes are being asked to do more with less. This comes at a time when user demands are increasing.
- Delivering zero-touch service. Best practices require extensive automation of network service add/move/change processes. Unified provisioning and use of web portals for order entry are required to meet the industry baselines.

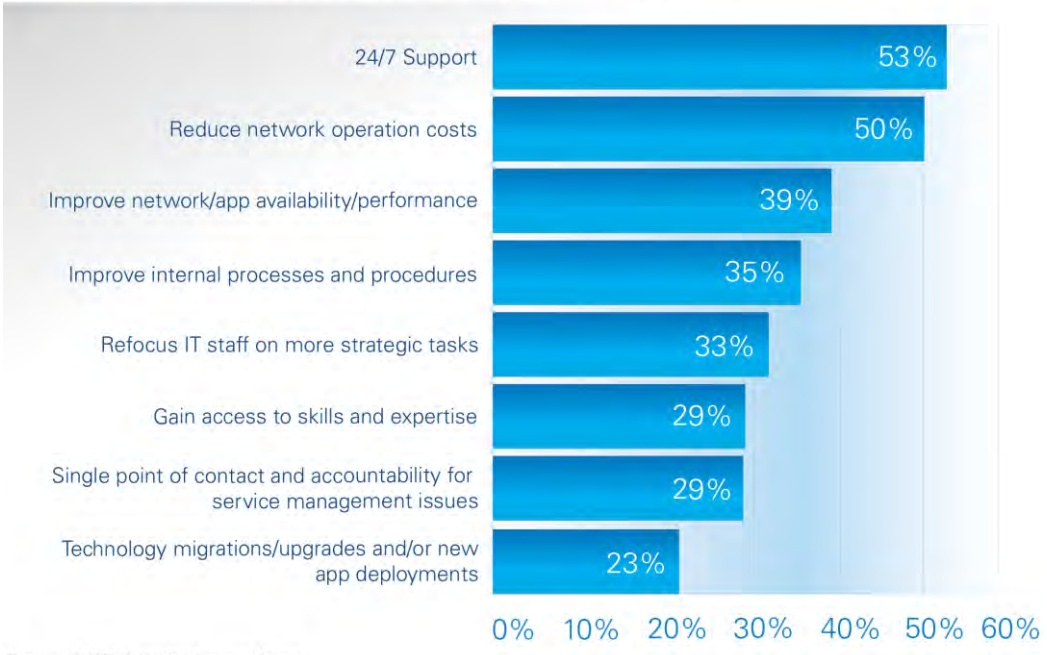
Internally delivered network management services must be staffed to ensure around-the-clock service delivery and coverage. Staff must have multiple technology certifications for networking equipment, including routers, Ethernet switches, firewalls, intrusion detection systems, content filtering, VPN devices, Wi-Fi, mobile devices and server, desktop and mobile operating systems. Each staff member requires continuous technical training to maintain skills in this rapidly changing field.

In more general terms, businesses are challenged by a lack of human and capital resources. IT and network engineering departments are considered to be cost centers and must, therefore, prove their value. They are being asked to:

- Simplify their end-to-end communications solutions through a "one-stop" shop
- Reduce communications hardware and software capital expense (CapEx)
- Offload network support requirements from limited internal IT staff

Managed network services provide an all-in-one, easy solution for setting up, monitoring and operating network data and security services. Figure 1 shows the top reasons why businesses choose managed network services.

Figure 1- Top Reasons for Choosing a Managed Network Service



Source: IDC U.S. WAN Manager Survey
NOTES: n=588 Base: Respondents who currently use managed network services or plan to do so within the next 12 months. Multiple responses allowed. Values represent the percentage of respondents ranking each factor #1, #2, or #3.

Providing 24/7 network support and reducing network operations costs stand out as the most frequently cited reasons for choosing managed network services. Providing 24/7 network support is a

serious financial and operational burden for a small or midsize business. Improving network and applications availability and performance as well as internal processes and procedures are the next most frequently cited reasons. These reasons are correlated in that better processes and procedures should yield improved availability and performance. Small and medium businesses lack the scale and scope to implement the necessary processes and procedures internally. Similarly, refocusing IT staff on more strategic tasks is an important reason for choosing managed network services. Though vital to business success, managing network services is typically not the top priority for most IT staffs.

Managed Network Services

Managed network services allow businesses to outsource the day-to-day operation of network links and equipment and ensure network security. The service provider can deliver comprehensive, high-quality service because it has an extensive, experienced staff that specializes in router and security technology. Service provider managed networks leverage large existing investments in infrastructure, process and people, which contributes to greater reliability and resiliency. These managed networks are monitored 24 hours per day, yielding the benefit of continuous review and fast response to network events. The service provider's network scale and scope allow it to offer this broad and deep service coverage at a very low cost as compared to an in-house solution.

Managed network services are offered for private networks and Internet access services. Likewise, managed WAN/Internet and LAN services are provided for both network types. The WAN/Internet service includes connection management, routing management and optional bandwidth management. Management of auto-failover to diverse paths is also offered. The LAN service includes management of the LAN router, DHCP server and DNS relay. Security service is especially important for Internet access services and includes management of the firewall and intrusion protection service.

Two use cases illustrate the benefits of managed network services.

Use Case: Automobile Dealership

The dealership has five high-volume locations spread across a major metro area with nearly 400 employees in sales, service and parts operations. It depends on reliable, secure and uninterrupted voice and Internet services for staff and customers at all its locations. Network uptime, scalability and cost (total cost of ownership or TCO) are the top network management issues.

The heavy and increasing dependence on the network requires strengthened networking expertise and coverage. The dealership requires proactive monitoring, reporting and alerting of network performance 24/7/365. Continuous access to broad and deep networking expertise is needed to quickly resolve network performance issues and outages. Costs must also be controlled by minimizing CapEx investments and operation expenses (OpEx).

TCO Comparison for Use Case 1: Managed WAN Service

The TCO to manage network services using internal IT staff is compared to the TCO of a managed network services solution. Coverage, technical certifications, training and equipment capabilities are assumed to be identical for the internal and managed services alternatives.

The dealership's WAN is a point-to-multipoint private network[4] that connects its headquarters to four other sales and service sites.

TCO for Internally Staffed Alternative

TCO includes nonrecurring and recurring costs.

The nonrecurring costs are:

- Hourly labor costs[5] for engineer, furnish, and install (EF&I)
- Cost of router and management software for each site

Recurring costs are:

- Hourly labor costs for operations, administration and maintenance (OA&M)
- Hourly labor costs to perform software upgrades and patches
- Training, including the labor costs for trainee attendance and course fees
- Vendor service contract fees: an annual fee for 24/7/4 hour response onsite vendor support services plus access to software upgrades and patches

TCO for the internally staffed alternative assumes that one senior and two junior networking technicians/engineers are employed full time. This is a minimum staffing requirement for 24/7/365 coverage. However, only the hours these staffers incur on the nonrecurring and recurring cost items listed are charged to this TCO analysis. Travel time charges—though they could be substantial—are not included in the analysis. Table 1 summarizes the nonrecurring costs for the internally staffed alternative.

Table 1 – Nonrecurring Costs for Internally Staffed Alternative: Use Case 1

Nonrecurring Expense Item	Amount	Expense Type
Planning & Procurement	$8,800	Labor
Router Setup	$1,200	Labor
EF&I Subtotal	$10,000	
Routers & Management Software	$6,514	CapEx for 5 sites
Total Nonrecurring Cost	$16,514	TCO

Total nonrecurring cost for the internally staffed alternative is $16,514. Planning and procurement cost is the largest element of nonrecurring cost. This reflects the two-week labor cost of a network engineer

[4] Service charges for the WAN itself are excluded from this TCO analysis.

[5] Industry average loaded hourly rates for senior and junior network technicians are used throughout this paper.

to plan and procure the routers and network management software. The next largest cost is the CapEx of the routers and network management software. Table 2 summarizes the recurring costs for the internally staffed alternative.

Table 2 – Recurring Costs for Internally Staffed Alternative: Use Case 1

Recurring Expense Item	Annual Recurring Cost	Expense Type
Routine Maintenance, Admin & Changes	$9,600	Labor
Clear Major Outage	$282	Labor
Clear Minor Outage	$96	Labor
OA&M Subtotal	$11,491	
Software Upgrades & Patches	$3,720	Labor
Training	$12,771	Labor & Training Fee
Vendor Service Contracts	$401	Service Fee
Total Recurring Cost	$28,383	OpEx

Total recurring cost for the internally staffed alternative is $28,383 per year. Training is the largest recurring cost item, which includes the labor costs for three internal staff members to attend three days of training classes each year and the training fee for each staff member. Routine maintenance, administration and changes are the second largest recurring cost category, calculated as the cost for a network technician to spend two hours per month per router on these activities.

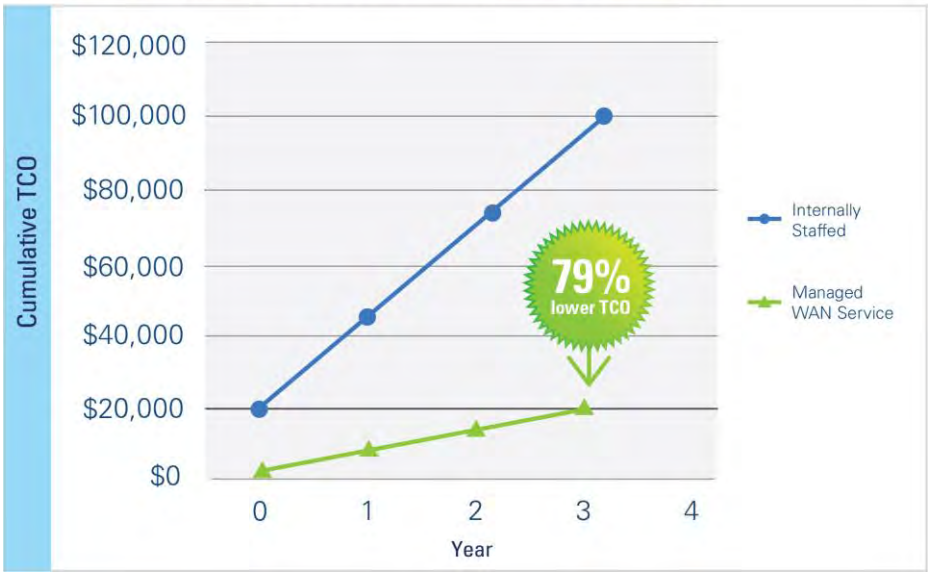
TCO for Managed WAN Service

The dealership uses an Ethernet point-to-multipoint private networking service. Managed WAN service pricing for an Ethernet network is based upon the following factors:

- Number and bandwidth of each site. A fixed nonrecurring charge of an integrated service router and its installation is assessed for each site. A per-site monthly recurring service charge is also assessed; it depends on the bandwidth. In this use case the lowest bandwidth tier (up to 35 Mbps) is used for the four sales/service locations, and the next tier (35 Mbps to 100 Mbps) is used for the hub site.
- Service features. Basic and optional service features are offered (see the previous section). The price of the basic managed WAN service is used in this use case.
- Contract length. Contract lengths are one through five years. A three-year contract is used for this use case. TCO also is computed for three years.

Managed WAN service nonrecurring and recurring charges for the dealership are calculated using industry average prices and each of the factors above. The dealership's nonrecurring cost is $1,125; its annual recurring cost is $6,696. Figure 2 compares the total cumulative TCO of the alternatives for three years.

Figure 2 – Cumulative TCO for WAN Management: Use Case 1



TCO for the managed network service alternative is 79 percent less than the internally staffed alternative for three years. Under a managed network services contract the dealership has no capital expense, and its internal staff is freed up to work on other business-building initiatives. Furthermore, the service provider has much greater technical breadth and depth to manage the dealership's network. The service provider is able to deliver these services much more cost effectively because it can leverage its staff across hundreds of networks and thousands of routers.

Use Case 2: Healthcare Clinic

This healthcare clinic has 27 employees working at a single site. Its operation is, nonetheless, vitally dependent on highly reliable, high-performance, and secure Internet services with adequate bandwidth to support critical applications. The clinic exchanges large medical diagnostics files (for example, CT, MRI and radiology), patient records and scheduling information with other clinics and hospitals. It participates in multiple managed-care provider networks to file and process health insurance claims. Also, its staff engages in distance learning, video conferencing and online education programs to develop and maintain skills.

The network usage by the clinic must conform to Health Insurance Portability and Accountability Act (HIPAA) requirements to maintain the security and privacy of individually identifiable health information. A managed security service provides the rigorous levels of security and privacy HIPAA requires.

TCO Comparison[6] for Managed Internet and Security Service

A comparison is made between the TCO to manage Internet router and security services using internal IT staff versus the TCO of a managed network services solution. Coverage, technical certifications, training and equipment capabilities are assumed to be identical for the internal and managed services alternatives.

[6] The service charge for the Internet access service itself is excluded from the TCO comparison.

Table 3 shows the nonrecurring costs, and Table 4 shows the recurring costs of providing Internet router and security services using internal staff.

Table 3 – Nonrecurring Costs for Internally Staffed Internet and Security Services: Use Case 2

Nonrecurring Expense ItemAmount	Amount	Expense Type
Planning & Procurement	$3,960	Labor
VPN Setup	$80	Labor
Router Setup	$240	Labor
Security Appliance Setup	$160	Labor
EF&I Subtotal	$4,440	
Security Software	$150	CapEx
Routers & Network Management Software	$1,244	CapEx
Total Nonrecurring Cost	$5,834	TCO

Table 4 – Recurring Costs for Internally Staffed Internet and Security Services: Use Case 2

Recurring Expense Item	Annual Recurring Cost	Expense Type
Routine Maintenance, Admin & Changes	$4,000	Labor
Clear Major Outage	$282	Labor
Clear Minor Outage	$96	Labor
Security Monitoring	$913	Labor
OA&M Subtotal	$5,291	OpEx
Software Upgrades & Patches	$3,600	Labor
Training	$8,754	Labor & Training Fee
Vendor Service Contracts	$134	Service Fee
Total Recurring Cost	$17,779	OpEx

Total nonrecurring cost is $5,834. Planning and procurement make up most of the cost, consisting of 36 hours of the services of a senior network technician to plan and procure an integrated services router and the security software.

Total recurring cost is $17,779 per year, with training expense as the largest portion. Two networking technicians must receive three days of training per year to ensure 24/7/365 coverage and comply with

strict HIPAA mandates. OA&M expense is the second largest recurring cost, consisting of four hours per month of services of a senior network technician.

TCO for Managed Internet and Security Service

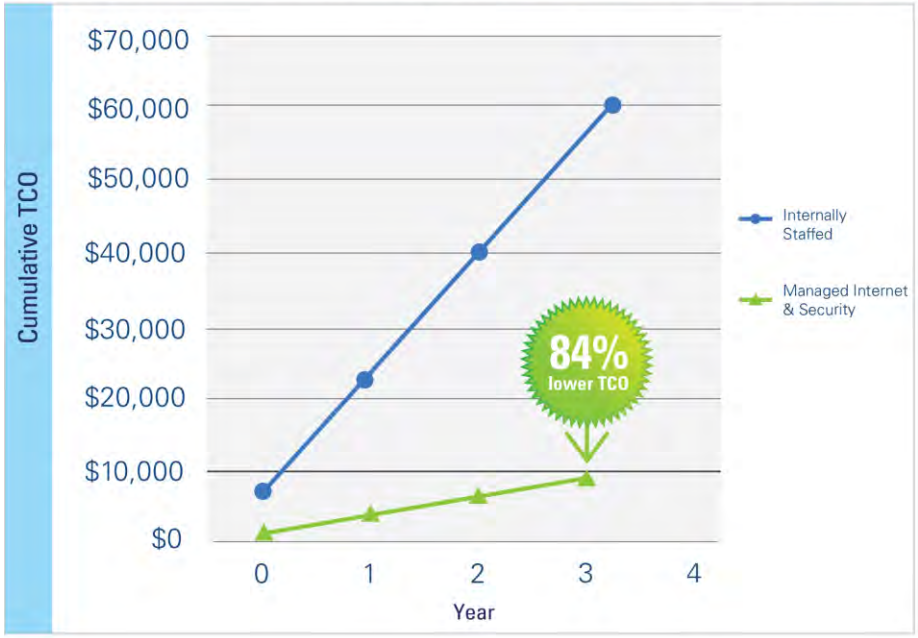
The recurring price for managed Internet service is structured much like managed WAN service. In this case the clinic has only one site, with the Internet service bandwidth falling into the lowest tier (less than 35 Mbps). The basic feature package and three-year contract are used to compute the price of the managed Internet service.

The recurring price for managed security service is for a single Internet interface and is the same regardless of the data rate (bandwidth). The price drops modestly with increasing contract length (three years in the use case).

The security service is hosted on the integrated service router used to provide managed Internet service; thus, no additional nonrecurring charge is applied for managed security service.

Industry average pricing is used to calculate the cost of managed Internet and security service. It has a nonrecurring cost of $225 and annual recurring cost of $2,988[7]. Figure 3 compares the cumulative TCO of the alternatives.

Figure 3 – Cumulative TCO for Managed Internet & Security Service: Case Study 2



TCO for the managed Internet and security service alternative is 84 percent less than the internally staffed alternative for three years. The service provider is able to spread the costs of a employing a technical staff with broad and deep expertise over thousands of integrated services routers and hundreds of networks to achieve a very low operating cost point. In contrast, even the three days of technical training provided to two internal networking technicians makes the internally staffed

[7] The recurring charge is based on use of an integrated service router with 35 Mbps throughput capacity.

alternative too costly for this business. The service provider is also able to cost effectively deploy sophisticated management infrastructure that is beyond the reach of the clinic.

What to Look for in a Managed Network Services Provider

Ensuring network security, sustaining network reliability and improving economic efficiency are the primary objectives of a strong managed network service. The capabilities of a service provider need to meet the following objectives:

- End-to-end management. This requires both physical and logical control of CPE, network facilities and network software.
- Reliability. While tightly linked to end-to-end management, reliability also requires redundant and diverse network equipment, network facilities, network operations center and field service staff.
- Security. This also is linked to end-to-end management. Broad and deep technical expertise must be maintained in-house.
- Customization/consulting. A large, diverse and experienced consulting organization is required in addition to the operations staff.
- Dedicated support. This is needed to deliver end-to-end management, reliability, and security, especially during network outages.
- Best-of-breed technology. In a rapidly changing industry, product life cycles are three years or less.

Using this list of capabilities, Table 5 compares the strengths and weaknesses of managed network services providers.

Table 5 – Strengths and Weaknesses of Managed Network Services Providers

Decision Criteria/Provider	Carrier	Equipment Vendor	IT Integrator or VAR	Cloud Provider
End-to-End Management	Strong	Weak	Average	Weak
Reliable	Strong	Weak	Average	Weak
Secure	Strong	Weak	Average	Average
Customize/Consulting	Average	Average	Strong	Weak
Dedicated Support	Strong	Average	Average	Average
Best-of-Breed Technology	Strong	Strong	Strong	Average

Strong Average Weak

The ability to deliver highly reliable and secure network services requires an end-to-end management capability. Carriers are unique in that they can provide their own networking infrastructure and a large 24/7/365 local field service capability. Also, they maintain their own network operations centers that are staffed by a large pool of expert engineers and technicians. Equipment vendors offer technology depth but lack their own network facilities and large local support staffs. IT integrators and value-added

resellers offer extensive customization and consulting capabilities and have access to many vendors' solutions to offer best-of-breed technology. However, they lack networks and network operations centers comparable to those of the carriers. Cloud providers are also poorly positioned to offer end-to-end management services. They lack a local presence, field service capabilities and their own network facilities.

Meeting the Network Challenge

Networks are increasingly critical to business success. Network dependence, however, also brings new management and technical challenges. Security requirements, device diversity, remote workers and the use of cloud services are all increasing. Traffic patterns are changing and performance, reliability and business continuity requirements have become much more stringent. Network management must be given a higher priority to meet these new requirements. Small and midsize businesses are challenged by a lack of human and capital resources.

A use case of an automobile dealership with 5 sites and about 400 employees found that a managed WAN service had 79 percent lower TCO than an internally staffed alternative. A use case of a single-site healthcare clinic with 27 employees found that a managed Internet and security service had 84 percent lower TCO than an internally staffed alternative.

In addition to operational and capital savings, managed networks also provide service coverage, technical depth and access to expert levels of skill and experience beyond the reach of most businesses. Additional benefits include 24/7 support, improved network reliability and performance and the opportunity to refocus internal IT resources.

In summary, managed network services provide an all-in-one, easy solution for setting up, monitoring and operating network data and security services while delivering the TCO payoff that businesses seek.

About ACG Research

ACG Research is an analyst/consulting firm that focuses in three areas: quantitative market sizing, business case analysis and service creation in the networking and telecom industry. Quantitative market sizing includes market share and forecast reports as well as custom cuts of data. Business case analysis focuses on TCO/ROI models that map features or services for economic benefit. Service creation workshops focus on the refinement or creation of new services. Our SMEs also deliver speeches, whitepapers, videos, custom research and market impacts for all areas of the networking/telecom business. ACG is a boutique firm focused on the Why before the What. For more information, visit www.acgresearch.net.

About Time Warner Cable Business Services

Time Warner Cable Business Services, a division of Time Warner Cable, offers a full complement of business communications tools to small, medium and enterprise-sized companies under its Time Warner Cable Business Class brand. Its Internet, voice, television, network and cloud services are enhanced by award-winning customer service and local support teams. Through its NaviSite subsidiary, Time Warner Cable Business Services also offers scalable managed services, including application services, enterprise hosting, and managed cloud services primarily in the U.S. and U.K. Time Warner Cable Business Services, founded in 1998, serves approximately 625,000 business customers throughout Time Warner Cable's service areas. For more information, visit http://business.twc.com.