

Adjust Your Behavior: Network Management Incorporates Behavioral Analysis to Optimize Performance

The Bottom Line:	The dynamic interactions of end users and technology assets make understanding network behavior critical. Behavior-enhanced management and monitoring and NBA provide needed visibility that can help network managers restore some predictability to network and application performance in the Anywhere Enterprise.
Key Concepts:	Behavior analysis, NBA, network performance, virtualization, service orchestration
Who Should Read:	Network and security operations manager, VP of IT

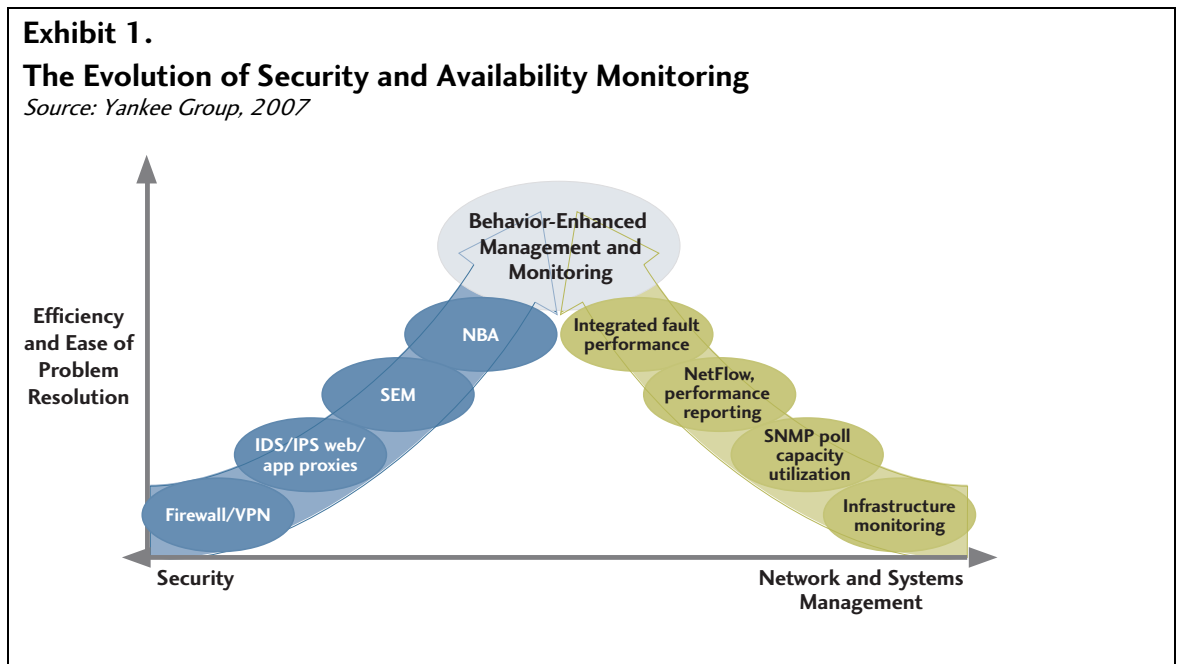
Practice Leader: Zeus Kerravala, Enterprise Research Senior Vice President, zkerravala@yankeegroup.com, 617-880-0235


Executive Summary

The rise of service-oriented architectures, rapid adoption of infrastructure virtualization, and the increasingly distributed and mobile workforce have made optimizing network performance a priority. Network and systems management tools generate tremendous amounts of data, but an Anywhere Enterprise• needs more to transform that data into actionable intelligence. The dynamic interactions of end users and technology assets make understanding network behavior critical. Network behavior analysis (NBA) vendors have extended the context of their solutions beyond network security to deliver visibility into performance and the end-user experience. This behavior-enhanced management and monitoring will be a network management requirement for an Anywhere Enterprise because it enables network managers to optimize their network for how users actually use it.

Exhibit 1.
The Evolution of Security and Availability Monitoring

Source: Yankee Group, 2007





Because user and technology interactions can be so dynamic and unpredictable, management systems must be able to learn, and adapt to the constant change. Behavior analysis tools model user interactions and understand the historical and real-time behavior of users, IT assets and applications. IT managers can then optimize the network and restore predictability to application performance.

In this Yankee Group Report, we discuss the evolution of behavior-enhanced management and monitoring and how enterprise network managers have already discovered the value of behavioral analysis for network optimization (see Exhibit 1). We also analyze the new competitive dynamic among NBA vendors and network performance management vendors, compare their relative strengths and weaknesses, and assess the future of the market segment. The competition is a good thing for enterprise network managers. They now have some advanced capabilities for managing technological change and understanding the impact to users, IT systems and the enterprise.

Table of Contents

I. Introduction	3
II. Enterprise Challenges: Unpredictable Behavior	4
Increasing Network Complexity Demands More from Network Performance Management.....	4
III. Behavior-Enhanced Management and Monitoring Provides Critical Visibility.....	5
The Evolution of Behavior-Enhanced Management and Monitoring.....	5
Intensifying Competition in the Network Performance Management Market	6
What's Next in the Market?	8
IV. Conclusions and Recommendations.....	9
Recommendations for Enterprises	10
Recommendations for Vendors.....	10
V. Further Reading.....	11

I. Introduction

Today's distributed, mobile workforce has an insatiable appetite for connectivity to applications, content and communications services from anywhere via any device. Enterprises are aggressively consolidating data center and branch office infrastructure, applications are much more network-centric, and users are more mobile and using more devices to access the network and applications. Network and security operations managers are under pressure to optimize the performance and security of the enterprise network for the new, dynamic interactions of users.

Existing network management tools that focus on infrastructure lack the needed visibility into end-user behavior to optimize performance. The dynamic behavior of end users, the distributed nature of applications and the virtualization of infrastructure make it nearly impossible today to infer the end-user experience from monitoring infrastructure. IT needs to have visibility into user-to-user and user-to-technology interactions to optimize the end-user experience—end-user experience and behavior have become the critical metrics, more so than infrastructure availability.

II. Enterprise Challenges: Unpredictable Behavior

In many organizations the network is not optimized for how users interact with each other and the infrastructure. This results in performance degradation, lower user productivity, unacceptable security risks and longer troubleshooting times. The root cause is a lack of visibility into user activity and interactions with hosts systems, applications and services.

Increasing Network Complexity Demands More from Network Performance Management

Optimizing the IT infrastructure and the network requires visibility into the current and historical user behavior as well as applications and infrastructure configurations. But just as importantly, it requires *anticipating* the impact of new applications and how they'll affect the infrastructure and service levels. Current network management tools deliver key functionality for managing network infrastructure and reporting on performance. However, the dynamic nature of today's enterprise networks demands greater visibility into behavior so administrators can optimize the network for the way the business actually works. Without this visibility, administrators face the following challenges:

- **Poor view of end-user experience:** Infrastructure monitoring is good for checking the availability of infrastructure, but availability tells IT little, if anything, about the actual end user experience. At best, existing tools provide a snapshot in time of performance and user experience. It's not continuous—a necessity in today's rapidly evolving network.
- **Difficulty in managing the impact of change:** The applications, services and underlying IT infrastructure are not static. Change is a constant as users demand new capabilities and the business tries to make users more productive. Without detailed visibility into typical behavior and changes in behavior, performance issues are hard to pinpoint and technology investments are often made in the wrong areas. In addition, IT can't measure the effectiveness of the investments with any real metrics.
- **Longer troubleshooting times:** Mean time to repair (MTTR) is a key metric by which IT departments measure themselves. It also correlates directly with business impact. When support staff have poor visibility into changes in behavior that impact performance, troubleshooting takes longer and the performance issue has more business impact.
- **Increased risk of security events:** Security operations and network operations are often not in synch. Security is not just about protecting against data theft or loss, it also has a direct impact on performance and availability. Changes in behavior can signal performance problems or a security event. It's critical that security operations and network operations work together to mitigate both performance issues and security events.

Today, many network managers are increasing their visibility into the entire enterprise network through the use of behavior-enhanced management and monitoring solutions. Behavior-enhanced management and monitoring is the convergence of network behavior analysis (NBA) systems and network management, particularly performance management. NBA solutions began as security solutions, but network managers have discovered these solutions deliver value beyond security. They provide detailed and continuous network visibility that enhances existing network management tools and helps administrators optimize their network for actual end-user behavior.

III. Behavior-Enhanced Management and Monitoring Provides Critical Visibility

Behavior-enhanced management and monitoring has become a valuable solution to help network administrators bring predictability to a very unpredictable and ever-changing enterprise network.

The Evolution of Behavior-Enhanced Management and Monitoring

Many enterprises have already discovered that a tool they have been using to address security concerns such as credentialed user threats, malware and mis-configurations, is actually well-suited to address a broader set of network management challenges: network behavior analysis (NBA). NBA systems grew from the need to identify threats that passed through firewalls and other early security techniques, including IDS/IPS, security event management (SEM), and vulnerability management. The signature-based dependencies of these early systems limited them to watching for only known problems. Limited deployment options further complicated their use, given that each network segment had to be individually instrumented. NBA technology, although initially developed to address these security shortcomings, has matured to provide full visibility into user activity and dependencies between users, applications and IT systems. This information has proved valuable for network managers and set the stage for an emerging market for network management tools incorporating behavioral analysis capabilities.

In the November 2006 Yankee Group Report, [NBA Finds Its True Calling by Adding Intelligence to Management and Monitoring Tools](#), we map out the next stages in the market evolution of NBA. Vendors such as Lancope and Mazu Networks learned that their customers were using their NBA tools to not only detect anomalous activity, but also to better understand user and technology interactions. NBA solutions reference visibility built up over time to give network and security managers contextual knowledge they can leverage to prioritize network and security events. Managers can respond more quickly to the most business-critical events and optimize future network projects.

Benefits of Behavior-Enhanced Management and Monitoring

Incorporating behavioral analysis into existing network and systems management tools provides deeper context to performance events. Behavior-enhanced management and monitoring complements existing tools and delivers the following benefits:

- **An optimized end-user experience:** Visibility into actual end-user interactions with other users and IT systems lets IT staff know who is accessing what, when and how. The network administrator has visibility into interactions between users and systems and other users. Infrastructure monitoring reports on managed nodes, but behavioral analysis monitors node interactions. This provides much greater visibility into the user experience and effectiveness of performance optimization solutions.
- **The ability to manage and monitor meaningful change:** Enterprises can view typical network behavior and use real-time behavioral monitoring to be alerted quickly to changes. In contrast to event consoles such as a manager of managers (MoM) or a security information and event management (SIEM) system, which can generate superfluous events and noise, NBA enables administrators to better understand user behavior and the impact of new application and service deployments.
- **Faster problem resolution:** By being able to model behavior and know exactly what changed during a performance issue, administrators can get to the cause of an issue more quickly. This reduces the length of a performance issue and lessens the business impact. In addition, incidents are diagnosed in the context of behavior, which means administrators are prioritizing events that have the most business impact rather than responding to red lights on a screen.

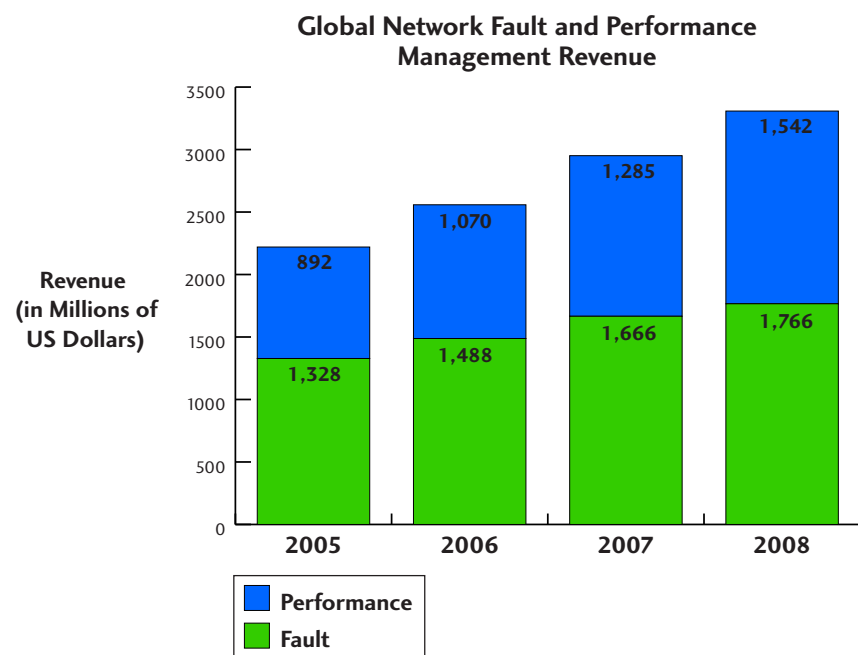
- **Effective management of infrastructure change:** Enterprises are aggressively pursuing data center consolidation projects and migrations, business continuity/disaster recovery (BC/DR) planning, convergence projects (e.g., voice over IP and data), and multitiered application deployments. NBA provides visibility into real-time and historical behavior to help administrators plan infrastructure changes and understand the impact to the infrastructure and user experience. They can make smarter technological and architectural decisions.
- **Balance between performance and security:** Performance and security are often in diametric opposition. Behavioral analysis incorporated within network monitoring and management gets security operations and network operations on the same page. As a result, they can leverage a common configuration management database (CMDB) and consistently implement best practices for support such as ITIL.

Network operations groups have already begun incorporating behavioral analysis so they can add behavioral context to their existing management systems. It will not replace existing management tools, but NBA tools can display network activity rolled back in time just before a performance event to accelerate root cause analysis and problem resolution. Network administrators still rely on existing network and systems management tools to isolate and apply fixes, but this capability ensures NBA's place in network operations and is sure to intensify competition with other network performance management tools.

Intensifying Competition in the Network Performance Management Market

The reasons for the entrance of NBA vendors into the network performance management market are twofold: 1) their customers are already using NBA for network performance and 2) the NBA solution vendors see it as an opportunity to expand their addressable market. Most NBA vendors are small, private companies but Yankee Group estimates the 2007 market for pure-play NBA tools at approximately \$125 million. The majority of that revenue come from behavioral IPS/IDS systems and growth in recent quarters has leveled off.

In contrast, the 2007 market for network performance management software is approximately \$1.3 billion, or 43% of the nearly \$3 billion market for network fault and performance management software (see Exhibit 2). This is an increase from 2005 when performance management constituted 40% of network fault and performance management. Yankee Group estimates that passive, agentless monitoring tools and probes that capture flow data to analyze performance comprise \$500 million of the \$1.3 billion performance management market. Leading vendors include NetQoS, NetScout, Network General, Fluke Networks (acquired Crannog and Visual Networks), Network Instruments and Network Physics. Many of these vendors are experiencing revenue growth between 10% and 20% per year, but some are experiencing more. NetQoS reports that 2006-2007 year-over-year revenue growth is on track to exceed 50%. The increasing reliance on distributed enterprise networks for the delivery of voice, video and increasingly diverse application traffic will drive demand for performance analysis and network optimization. This will maintain the market's attractiveness and entrance of new players.

Exhibit 2.**Performance Captures Increasing Share of Network Management Revenue***Source: Yankee Group, 2007*

In 2006 and 2007, NBA vendors began competing for the same IT dollars as network performance management solutions. NBA solutions and network performance management solutions both leverage flow data—particularly Cisco NetFlow data—as the basis of their performance analysis. But because of their different genealogies, they have different strengths and appeal to different buyers.

By virtue of their origins as security tools, NBA solutions have very in-depth analytical capabilities. Their early focus has been providing the most in-depth analytics to provide visibility into hard-to-detect attacks. Although some network management vendors have written algorithms, NBA vendors have years of experience with heuristics and interpreting behavior through the use of flow data. Network performance management solutions may not have the depth of experience in anomaly detection and security analytics but they offer more advanced reporting capabilities and present data usefully in a dashboard. Network performance management vendors also have more years of experience working with network operations groups and selling through the direct sales force and channels of network equipment vendors.

What's Next in the Market?

Merging of Network Performance Management and NBA

NBA and network performance solutions are complementary, albeit with some overlap in capabilities. The NBA vendors, particularly Lancope and Mazu Networks, have aggressive strategies for penetrating the enterprise market. Their task is to build out their reporting and dashboard capabilities while maintaining their sophistication of analysis. Both Lancope and Mazu support NetFlow and sFlow data and will add support for IPFIX. Mazu also has an API that makes its data exportable to third-party tools and customer portals. Within those IT management systems, operations can click on a link to view behavioral information related to that event. Lancope is developing a similar API and will offer similar capabilities.

Integration or partnerships between the pure-play NBA vendors and the network performance management tools such as Fluke Networks (acquired Crannog Software), NetQoS or NetScout is not going to happen. The last 18 months have established that Lancope and Mazu are targeting network operations managers in addition to security operations. Although more complementary, they view network performance management tools as eventual direct competitors. Their strategy is to build their reporting capabilities and integrate with event management systems. For the next 12 to 18 months, they'll still champion their behavioral analysis capabilities and will not aggressively pursue sales prospects whose primary need is performance reporting. But NBA and network performance management will merge and competition will intensify.

The network performance management vendors still have a solidly competitive position. Although they do not offer the in-depth anomaly detection and security analytics of Lancope or Mazu, firms such as NetScout have had some analytics and behavior analysis algorithms available for some time. NetQoS will likely offer some algorithms for more detailed analysis in the near future as well. However, its focus will remain on performance analysis and management. The opportunity for network performance managers is following the lead of network equipment vendors, particularly supporting vendors in the application networking market. Application networking includes data center and WAN optimization solutions such as those offered by Cisco, F5, Riverbed, Citrix Systems and several others.

The WAN Optimization Opportunity

There's a tremendous opportunity for a NetFlow-based performance management tool that can accelerate the adoption of WAN optimization and application acceleration solutions offered by Riverbed, Cisco and many others. It is a challenge, regardless of WAN optimization solution, to get an accurate end-to-end picture of WAN performance and the efficacy of the WAN optimization solution. Because of the very nature of many WAN optimization techniques, they can "trick" existing network management tools. A report may show excellent performance, but it's only seeing the traffic from the server to the WAN optimization appliance in the data center—not what's traversing the WAN. This is just an example of the many idiosyncrasies of WAN optimization and application acceleration that network performance management vendors can help the equipment vendors solve.

The market for WAN optimization is also at a critical inflection point. Riverbed has done remarkably well as an overlay to the existing network infrastructure solving immediate performance problems. Enterprises will require more integrated solutions rather than continue building an overlay infrastructure. The trouble with an overlay infrastructure is optimizing and tuning it for variable application traffic. Plus, network operations often rely on multiple management tools—each network appliance can have its own tool—to continuously tune the optimization and acceleration features. Regardless of solution vendor, network managers will need common management with more accurate visibility into the overall effectiveness of the solution. If a network performance management vendor can help the WAN optimization vendors instrument their solutions accurately, it will be a unique competitive advantage that the competition will not easily replicate. On July 24, 2007, NetQoS and Cisco announced the results of a joint-development effort that does just that. The result is more accurate performance management and monitoring of Cisco WAAS implementations. Enterprise demand for all WAN optimization solutions is very strong and that will feed demand for more accurate performance monitoring.

IV. Conclusions and Recommendations

In the next few years, the rapid adoption of virtualization, web services, unified communications and mobile applications will make it impossible for IT departments to infer application and service performance from infrastructure monitoring. And they will no longer be able to limit how users interact with technology to maintain service levels. They'll need to better understand end-user behavior and user-technology interactions. Transactions are more predictable and easier to manage, interactions are dynamic and unpredictable. But interactions are also what provide value in the Anywhere Enterprise.

Network and security administrators have already discovered the value that behavioral analysis has beyond security threat detection. Behavioral analysis provides visibility into all the network activity to optimize the end-user experience, understand and monitor for meaningful change, troubleshoot performance issues faster, and deliver value to both network and security operations. Enterprises are experiencing the benefits today but complexity is not going away and behavioral context will become even more critical in the future.

Enterprises have more choices for incorporating behavioral analysis into existing management tools. The right choice depends on whether the buyer is more concerned with security or performance needs. They can leverage APIs that integrate NBA with their event management tools, or they'll soon be able to use new capabilities within network performance management tools. The bottom line is that behavior-enhanced management and monitoring provides needed visibility that can help network managers restore some predictability to network and application performance.

Recommendations for Enterprises

- **Place a premium on integration of behavioral analysis with existing management tools.** NBA solutions can extend the value of existing management tools and provide visibility into actual user and application behavior. Focus your evaluation on the depth of analytics and the ability to translate that into actionable intelligence.
- **Buy NBA tools that satisfy security and network operations demands.** While NBA has its roots as a security tool, network operations can benefit greatly. Network operations should consult with security operations so that both support organizations leverage a common investment and can correlate events that impact both.
- **Ask your network performance management vendor to incorporate NBA capabilities and vice versa.** If you have an infrastructure for collecting NetFlow and sFlow data, ask about extending their behavioral capabilities. If you have NetFlow collection for behavioral analysis, ask about plans for performance management and reporting. You may not be using all the capabilities of your NetFlow infrastructure.

Recommendations for Vendors

- **Piggyback the NEMs.** If you help Cisco, Riverbed and others sell more gear, you'll be a member of the family. Application acceleration and WAN optimization is hugely important for enterprises and the network equipment vendors. Giving enterprises visibility into the efficacy of their WAN optimization and application acceleration tools benefits the enterprise and the equipment provider. NBA and network performance will be critical to the next stage of market growth.
- **NBA vendors need to be a product and a feature.** It's a delicate balancing act. NBA tools need to deliver value on their own in addition to being a component of an enterprise's overall network management framework. Invest in three crucial areas: in-depth flow analysis, integration with event management viewers, and standalone reporting and dashboard capabilities. Most are small, private firms so the firms that can most effectively balance these investment priorities will have staying power.
- **Network performance management vendors will need to get behavioral.** NBA is catching on and some emerging vendors such as eTelemetry and Xangati are positioning themselves to network operations. Market definitions are still nebulous, but NBA is a hot technology and important for optimizing the distributed network of the Anywhere Enterprise. Network performance management vendors have to build it in.

V. Further Reading

Yankee Group Link Research

[In the Anywhere Enterprise, IT Operations Prepares for User-Driven IT](#), Report, January 2007

[NBA Finds Its True Calling by Adding Intelligence to Management and Monitoring Tools](#), Report, November 2006

[Application Performance Management Market Offers Attractive Benefits to European Service Providers](#), Report, August 2006

Yankee Group

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

Corporate Headquarters

31 St. James Avenue
BOSTON, MASSACHUSETTS 02116-4114
617-956-5000 phone
617-956-5005 fax
info@yankeegroup.com

Europe

55 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
44-20-7307-1050 phone
44-20-7323-3747 fax
euroinfo@yankeegroup.com

Yankee Group | the global connectivity experts™

A global connectivity revolution is under way, transforming the way that businesses and consumers interact beyond anything we have experienced to date. The stakes are high, and there are new needs to be met while power shifts among traditional and new market entrants. Advice about technology change is everywhere—in the clamor of the media, the boardroom approaches of management consultants and the technology research community. Among these sources, Yankee Group stands out as the original and most respected source of deep insight and counsel for the builders, operators and users of connectivity solutions.

For 35 years, we have conducted primary research on the fundamental questions that chart the pace and nature of technology changes on networks, consumers and enterprises. Coupling professional expertise in communications development and deployment with hundreds of interviews and tens of thousands of data points each year, we provide qualitative and quantitative information to our clients in an insightful, timely, flexible and economic offering.

Yankee Group Link

As technology connects more people, places and things, players must confront challenging questions to benefit from the changes: which technologies, what economic models, which partners and what offerings? Yankee Group Link™ is the research membership uniquely positioned to bring you the focus, the depth, the history and the flexibility you need to answer these questions.

Yankee Group Link membership connects you to our qualitative analysis of the technologies, services and industries we assess in our research agenda charting global connectivity change. It also connects you to unique quantitative data from the dozens of annual surveys we conduct with thousands of enterprises and consumers, along with market adoption data, comprehensive forecasts and global regulatory dashboards.

Yankee Group Link Research

As a Link member, you have access to more than 500 research reports and notes that Yankee Group publishes each year. Link Research examines current business issues with a unique combination of knowledge and services. We explore topics in an easy-to-read, solutions-oriented format. With the combination of market-driven research and built-in direct access to Yankee Group analysts, you benefit from the interpretation and application of our research to your individual business requirements.

Yankee Group Link Interaction

Our analysts are at your further disposal with data, information or advice on a particular topic at the core of a Link membership. We encourage you to have direct interaction with analysts through ongoing conversations, conference calls and briefings.

Yankee Group Link Data

Yankee Group Link Data modules provide a comprehensive, quantitative perspective of global connectivity markets, technologies and the competitive landscape. Together with Link Research, data modules connect you to the information you need to make the most informed strategic and tactical business decisions.

Yankee Group Consulting

Who better than Yankee Group to help you define key global connectivity strategies, scope major technology initiatives and determine your organization's readiness to undertake them, differentiate yourself competitively or guide initiatives around connectivity change? Our analysts apply Yankee Group research, methodologies, critical thinking and survey results to your specific needs to produce expert, timely, custom results.

Yankee Group Live!

The global connectivity revolution won't wait. Join our live debates to discuss the impact ubiquitous connectivity will have on your future. Yankee Group's signature events—conferences, webinars and speaking engagements—offer our clients new insight, knowledge and expertise to better understand and overcome the obstacles to succeed in this connectivity revolution.

www.yankeegroup.com

The people of Yankee Group are the global connectivity experts™—the leading source of insight and counsel for builders, operators and users of connectivity solutions. For more than 35 years, Yankee Group has conducted primary research that charts the pace of technology change and its effect on networks, consumers and enterprises. Headquartered in Boston, Yankee Group has a global presence including operations in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific.