

Network Behavioral Analysis Optimizes the Enterprise Network for the Business

yankee
group

www.yankeegroup.com

by George Hamilton | January 2007

Executive Summary

Network and systems management tools collect a tremendous amount of data, but network and systems managers need more to transform that data into actionable intelligence. The mission-critical nature of the enterprise network, the rise of service-oriented architectures, the rapid adoption of infrastructure virtualization and the need to deliver applications to a distributed workforce make understanding network behavior critical. Therefore, network behavior analysis (NBA) vendors such as Mazu Networks have extended the context of their solutions beyond network security to deliver visibility into performance and user experience. This behavioral context enables enterprise managers to address network performance issues more quickly and optimize their networks.

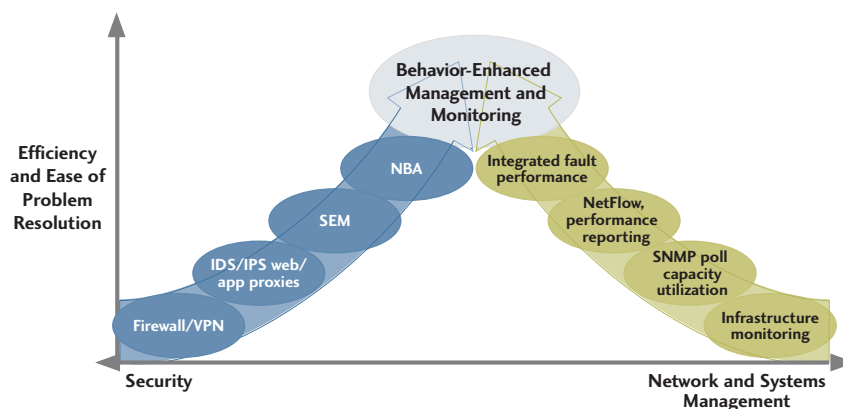
In this Yankee Group Report, we discuss the evolution of NBA tools and how enterprise network managers have already discovered the value of behavioral analysis (see Exhibit 1). Behavior-enhanced management and monitoring helps administrators optimize the end-user experience, manage the impact of change and deliver value to both security and IT operations.

Without the visibility that NBA tools provide, enterprises are flying blind—the network is running the business rather than the business running the network. Behavior-enhanced management and monitoring, powered by NBA, delivers that visibility and serves as a valuable tool for managing technological change and understanding the impact to users, IT systems and the enterprise.

Exhibit 1

The Evolution of Security and Availability Monitoring

Source: Yankee Group, 2007



This custom publication has been funded by Mazu Networks.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

This Yankee Group Consulting Report is published for the sole use of Yankee Group clients. It may not be duplicated, reproduced or transmitted in whole or in part without the express permission of Yankee Group, 31 St. James Avenue, Boston, MA 02116. For more information, contact Yankee Group: info@yankeegroup.com; Phone: 617-956-5005. All rights reserved. All opinions and estimates herein constitute our judgment as of this date and are subject to change without notice.

Table of Contents

I. Introduction	2
II. Enterprise Challenges: The Need for Continuous Network Visibility	2
Increasing Network Complexity Demands Global Visibility	2
III. Behavior-Enhanced Management and Monitoring Provides Critical Visibility	3
The Evolution of Behavior-Enhanced Management and Monitoring	3
Benefits of Behavior-Enhanced Management and Monitoring	4
Requirements for Behavior-Enhanced Management and Monitoring Solutions	4
IV. Vendor Profile: Mazu Networks	5
Customer Examples	6
V. Conclusions and Recommendations	7
Recommendations	7
A Look Ahead	7

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 infrastructures. 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 all enterprise users.

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

II. Enterprise Challenges: The Need for Continuous Network Visibility

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 host systems, applications and services. The network is running the business instead of the business running the network.

Increasing Network Complexity Demands Global Visibility

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 tracking the availability of infrastructure, but availability tells IT little, if anything, about the actual end-user experience. At best, the 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 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 businesses try 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 has poor visibility into the 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 with one another. Security is not just about protecting against data theft or loss, it also directly affects 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 with 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 that these solutions deliver value beyond security. They provide detailed and continuous network visibility that enhances existing network management tools and helps administrators optimize their networks 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 behavioral analysis.

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 restricted them to only watching for known problems. Limited deployment options further complicated their use, given that each network segment had to be instrumented individually. 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 proved valuable for network managers and set the stage for an emerging market for network management tools that incorporate 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 Mazu Networks learned that their customers were using their NBA tools not only to detect anomalous activity, but also to understand user and technology interactions. Their NBA solutions leverage visibility built up over time to optimize future network projects, add critical time-saving knowledge that network and security managers can use to prioritize network and security events, and respond more quickly to the most business-critical events.

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 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, as well as 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 the 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 an SEM system, which can generate superfluous events and noise, NBA enables administrators to understand user behavior and the impact of new application and service deployments better.
- **Faster problem resolution:** By being able to model behavior and know exactly what changed during a performance issue, administrators can more quickly get to the cause of an issue. 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 simply responding to red lights on a screen. Most importantly, behavior analysis is proactive—it can identify a change in behavior before that change can degrade performance and affect users.

- **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. As a result, 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.

Requirements for Behavior-Enhanced Management and Monitoring Solutions

When evaluating NBA solutions, network and security administrators should base their evaluations on the following requirements:

- **Global visibility of the network and network activity:** The NBA solution should have an integrated, holistic view of the users and the systems with which they're interacting. It should also provide visibility into where the users are and when they access systems. The NBA solution should provide visibility into the "who/what/where/when" of the network.
- **Automatic heuristics:** The NBA solution should feature automatic heuristics that monitor behavior for security and performance issues. An NBA solution should understand typical and historical behavior and apply heuristics to identify changes in behavior as well as possible performance and security issues.

- **Custom rule generation:** The NBA solution should have the ability to create custom rules such as application access and usage policies to monitor for policy violations, changes in normal activity and other special conditions.
- **Integration with existing networking and security products:** Integration with existing tools makes it easier for IT staff to operationalize the NBA tool. Specifically, network and security administrators should look for tools that allow their staff to invoke the NBA features within their existing management tools and avoid “swivel chair monitoring.”
- **Agentless architecture:** Most enterprises are hesitant to deploy and manage yet another agent or a collection of probes. The NBA solution should not require changes to the network architecture.

An NBA solution that incorporates these functional requirements increases the effectiveness of network and security operations. Operations managers can respond more quickly to the most important events and solve problems faster without taxing the skills of their staff. One NBA solution that incorporates these requirements and has demonstrated success with network as well as security operations is offered by Mazu Networks.

IV. Vendor Profile: Mazu Networks

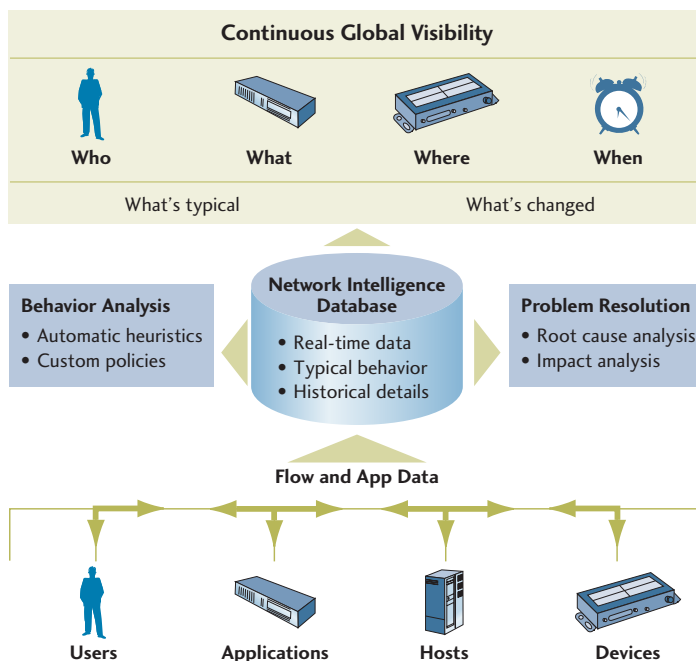
One best-of-breed NBA provider that is succeeding in integrating with network and systems management tools is Mazu Networks. Mazu integrates with many network and systems management products as well as vulnerability management tools, quickening incident response.

Mazu’s solution computes global behavior profiles of the running applications, the consumers of those applications, the profiles of their normal use patterns, and the interactions and dependencies between them (see Exhibit 2). This information is collected passively via a network appliance and is stored in Mazu’s Network Intelligence Database. The system then automatically calculates typical behavior, to which heuristics are constantly compared.

Network and systems administrators gain an enterprise-wide view of activities, usage and dependencies between users, devices, applications and IT systems. Mazu’s automatic behavior analysis continually monitors activity to determine if it is meaningfully different from typical behavior. Mazu provides two types of behavior analysis. First, Mazu delivers automated heuristics that can be run out-of-the-box. The automated heuristics are preconfigured, giving administrators the ability to start quickly and implement ongoing behavior analysis with minimal effort. Second, Mazu enables administrators to define and build custom policies to monitor specific conditions. In each case, the analysis leverages the global behavior profile that Mazu continuously updates.

Mazu’s solution is designed to make all incidents—whether security- or performance-related—more actionable. By pulling in Active Directory identity information, application names instead of port numbers and routing topology, Mazu can quickly show what is happening across the network. An API makes this data exportable to third-party tools and customer portals.

Exhibit 2
 Mazu Networks Solution
 Source: Mazu Networks and Yankee Group, 2007



The API, which enables network and systems management tools to pull contextual reports about network behavior directly into their products, is a unique strength. Network administrators can click on a link within an event in their network management console and view an embedded report, which gives them deep behavior-based context about the event. This provides real-time and historical user and behavior-specific information about that event.

Mazu has developed partnerships with more than 30 leading NSM vendors such as IBM Tivoli, Micromuse and HP OpenView. Enterprise customers can increase the value of their existing tools with Mazu's behavioral capabilities.

Mazu Networks cites four areas in which network operations groups can benefit from its products. These benefits include:

- Troubleshoot performance issues seven to 10 times faster.
- Detect behavior changes that affect performance before they disrupt users.
- Analyze WAN usage to improve availability and reduce cost.
- Optimize and accelerate infrastructure change.

Customer Examples

Troubleshoot Performance Issues Seven to 10 Times Faster

One of the world's leading universities was experiencing internet connectivity problems at one of its US-based locations every day around 9:30 a.m. The network team placed a sniffer on the link for several weeks, but the amount of traffic and packets sent prevented them from understanding what was happening on the network.

Mazu enabled the networking team to see that port 80 was the top service at the time of the surge and allowed the team to examine the packets. Through the visibility that Mazu provided, the team learned that the hosts were downloading updates directly from Symantec instead of from a local definition distribution service, due to a desktop mis-configuration. Mazu enabled the university to correct the mis-configuration and rectify its internet connectivity issues.

Detect Behavior Changes That Affect Performance Before They Disrupt Users

The world's leading provider of mail-stream solutions had a recurring application outage that was jeopardizing its relationship with one of its largest customers. Mazu identified a suspicious connection to the server and notified the company. Mazu informed the mail-stream provider that the connection had originated from the application development team.

After following up on the Mazu alert, the company found that a developer had made an unscheduled and unauthorized change, which caused the outage. Mazu enabled the team to quickly identify, isolate and remediate the problem. Additionally, Mazu provided the team members with the information they needed to give the customer with a full report of the incident. Mazu also provided a description of the implemented internal controls to ensure it would never happen again.

Today, the mail-stream solutions provider uses Mazu's behavior analysis to determine if its current network activity is meaningfully different from typical behavior. Mazu warns the company of a network issue, a security threat or an application problem—before its users do.

Analyze WAN Usage to Improve Availability and Reduce Cost

One of the largest US-based integrated oil and gas companies experienced intermittent connectivity failures to its oil rig's metering devices. With distributed mail servers in the field, all of the company's oil rigs report their metering via UDP. When the oil rigs began having problems with their metering updates, the company examined whether it had enough bandwidth to support the field's activity.

According to its reports, bandwidth consumption was not identified as an issue. However, Mazu showed the company that its distributed Microsoft Exchange environment was indeed consuming nearly all of the bandwidth at certain times during the day. Through Mazu's holistic view of the activities, usage and dependencies between users' applications and IT infrastructure, the company was able to identify and rectify its bandwidth consumption issues.

Optimize and Accelerate Infrastructure Change

When two leading providers of investment products and services merged, it presented a major challenge for the network and security teams from both organizations. The company decided it would retain the security team from one organization and the networking team from the other organization. As a result, each team inherited environments it did not understand. The merged organization used Mazu to migrate important applications from the legacy networks of both companies and to decommission redundant applications selectively.

V. Conclusions and Recommendations

Network, systems and security administrators have already discovered the value that behavioral analysis has beyond security threat detection. Behavioral analysis provides visibility into all 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 the complexity is not going away and behavioral context will become even more critical in the future.

Recommendations

- **Base NBA solution evaluation on the key requirements.** Key requirements include visibility of the network and network activity, automatic heuristics to identify changes in behavior and possible performance and security issues, custom rule generation to monitor special conditions, integration with existing networking and security products so IT staff can operationalize the NBA tool, an agentless architecture for deployment and management simplicity.

- **Place a premium on the 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. When evaluating solutions, don't get distracted by a litany of technical features. Focus on actionable intelligence and integration and reporting capabilities.
- **Both network and security operations should incorporate NBA.** Although NBA has its roots as a security tool, network operations can benefit greatly. Network operations should consult with security operations so both support organizations leverage a common investment.

A Look Ahead

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 understand end-user behavior and user-technology interactions better. Transactions are more predictable and easier to manage; interactions are dynamic and unpredictable. But interactions are also what provide value in the enterprise of today and the future.

The visibility that NBA tools provide means enterprises are no longer flying blind; the business can run the network, not the other way around. Behavior-enhanced management and monitoring, powered by NBA, delivers that visibility today so network and security operations can optimize their network for how it is used today and for how it will be used in the future.

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

Canada

260 Terence Matthews Crescent, Suite 200
Ottawa, ONTARIO K2M 2C7
CANADA
613-591-0087 phone
613-591-0035 fax
canadainfo@yankeegroup.com



Solution Centre Limited
Vickers House
Priestley Road
Basingstoke, RG24 9NP.
Tel: 01256 818600
Fax: 01256 819600
E-Mail: sales@solutioncentre.co.uk
www.solutioncentre.co.uk

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.

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.