

November 2009

Network Behavior Analysis: Protecting by Predicting and Preventing

In Aberdeen's benchmark report on [*Leveraging Logs, Information and Events: Three Use Cases for What to Do with All That Data*](#) (March 2009), the companies achieving top results in maintaining secure, compliant and cost-effective IT infrastructure are increasingly using **Network Behavior Analysis** (NBA) in combination with traditional signature-based approaches to anti-virus, anti-malware, intrusion detection and prevention, and network event management. NBA technologies monitor network traffic for unknown or unusual deviations from normal patterns that might indicate zero-day exploits and malware for which signatures have not yet been developed. Solution providers that incorporate NBA most effectively will enable their customers to improve protection by *predicting* and *preventing* emerging threats before they cause harm, rather than by merely *explaining* events that have already ensued.

Business Context: Looking Out in Both Directions

In Roman mythology, the god *Janus* – from whose name we derive the month of January – is said to have been able to see both the past and the future, and was therefore depicted with two heads facing in opposite directions. Aberdeen's benchmark report on [*Leveraging Logs, Information and Events*](#) (March 2009) noted that top-performing enterprises are also looking out in multiple directions with respect to their IT infrastructure:

- In the present, to enhance security;
- In the past, to carry out forensic investigations and to demonstrate regulatory compliance; and
- Towards the future, to improve the efficiency and cost-effectiveness of their ongoing operations.

By going beyond merely reacting, responding and reporting on the security and compliance incidents that have already happened, Best-in-Class companies are successfully leveraging security-related logs, information and events to derive more value from the complex IT environments and services that are the foundations for running and growing their businesses.

One of the enabling technologies strongly correlated with the companies achieving top performance is *Network Behavior Analysis* (NBA). Current use of NBA is 2-times more prevalent among the top performers than among lagging performers, and based on planned deployments in the next 12 months the near-term growth opportunity appears to be very strong. Current evaluations also indicate a high level of interest in NBA (Figure 1).

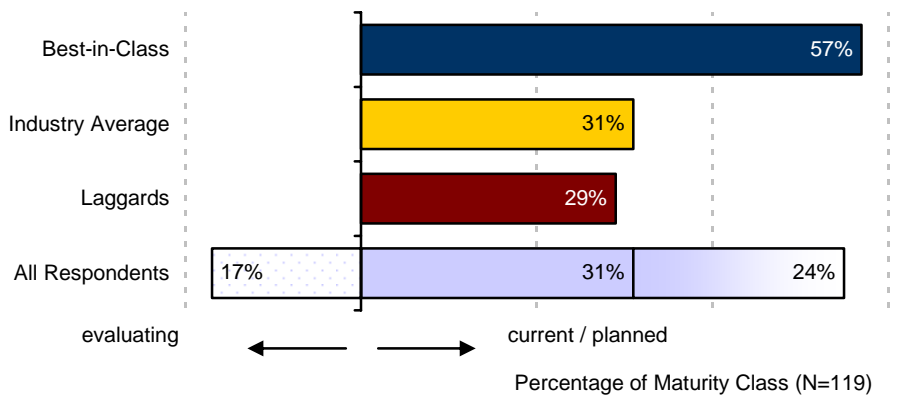
Research Brief

Aberdeen's Research Briefs provide an exploration of one or more specific findings from a primary research study, including key performance indicators, Best-in-Class insight, and vendor insight.

Definition

Network Behavior Analysis (NBA) technologies monitor network traffic for unknown or unusual deviations from normal patterns that might indicate the presence of a threat. Commonly used in combination with traditional signature-based approaches to anti-virus, anti-malware, intrusion detection and prevention, and network event management, NBA is especially well-suited for identifying new zero-day exploits and malware for which signatures have not yet been developed.

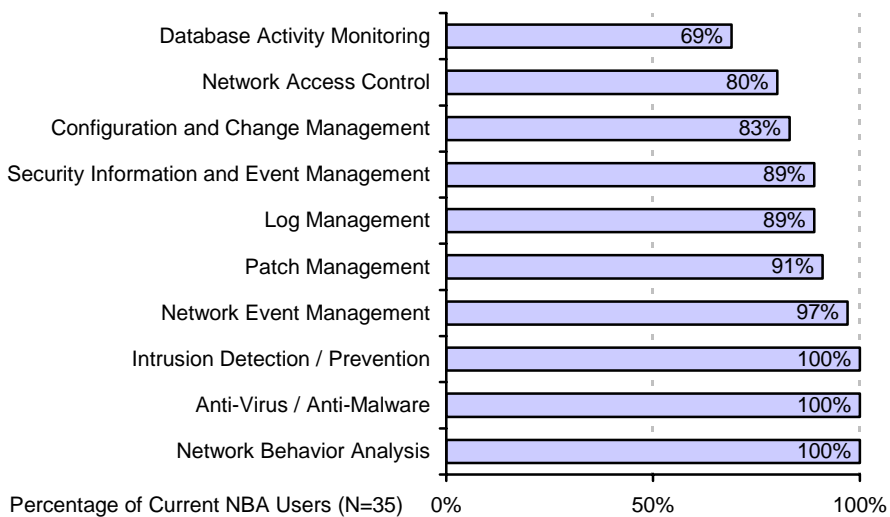
Figure 1: Current Use of NBA, by Maturity Class



Source: Aberdeen Group, October 2009

Aberdeen's research findings confirm that NBA is commonly used in combination with anti-virus, anti-malware, intrusion detection and prevention, network event management, other network security technologies (Figure 2). Integration and correlation of NBA data are essential to realizing additional value, rather than simply increasing the complexity of analysis. This Research Brief examines 35 current users of NBA in comparison to 84 non-users of NBA to see what other insights can be gained from the [Leveraging Logs, Information and Events](#) study.

Figure 2: NBA is Used with Other Network Security Technologies



Source: Aberdeen Group, October 2009

Determining the Best-in-Class

To distinguish Best-in-Class (top 20%) companies from Industry Average (middle 50%) and Laggard (bottom 30%) organizations in leveraging security-related logs, information and events, Aberdeen used the year-over-year changes in the following performance criteria:

- √ Number of actual security-related incidents
- √ Number of non-compliance incidents (e.g., audit deficiencies)
- √ Total management costs

The first two criteria were selected as measures of an organization's performance in improving security and compliance, while the third was selected as an indicator of operational improvement. In this way, both effectiveness and efficiency were included in the determination of maturity classes for this study.

Companies with top performance based on these criteria earned "Best-in-Class" status. For full details, see the [Leveraging Logs, Information and Events](#) benchmark report.

Network Behavior Analysis Users Earn Better Results

Like most topics in IT security, a collection of "verbs" such as those listed in Table I can be used to describe the process of leveraging security-related

logs, information and events in a **lifecycle** model, i.e., from the initial discovery of data sources to the eventual deletion of collected data. Most important are the verbs that describe **taking action**, such as *alert*, *report*, *prioritize* and *remediate*.

"Network behavior analysis is less valuable by itself than it is in context with other network security information and events. There's a lot of data, and without correlation and analysis it's just too much for mere mortals to make sense of."

~ IT Manager,
mid-size high tech firm

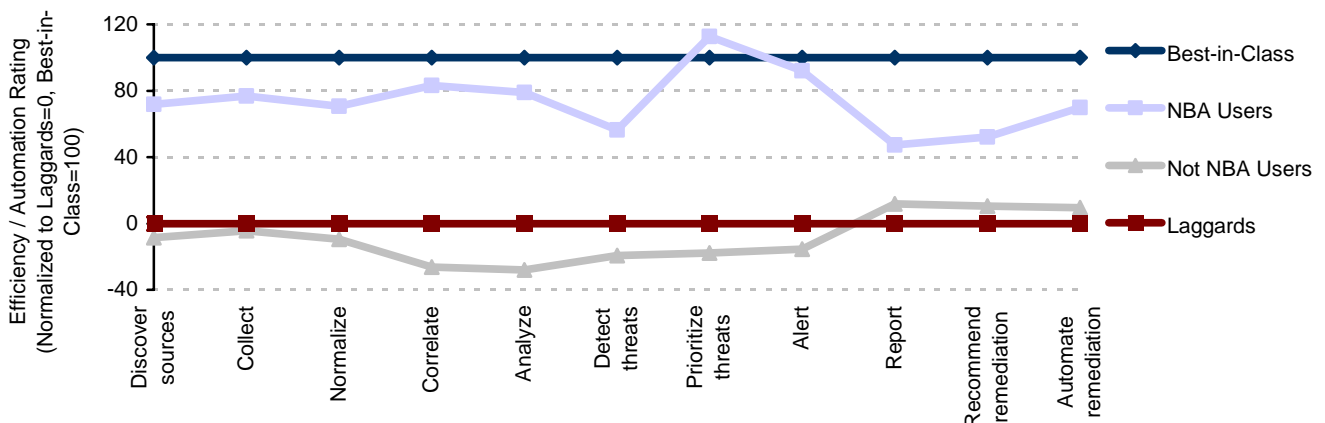
Table 1: The "Verbs" of Managing Logs, Information and Events

Generate Data	Manage Data	Interpret Data	Take Action
Discover sources Collect	Store Secure Retain Index Search Delete	Normalize Aggregate Correlate Analyze Detect incidents and threats Prioritize incidents and threats	Alert Report Generate information required for remediation Prioritize remediation Automate remediation

Source: Aberdeen Group, March 2009

In Figure 3, the current level of efficiency for elements of the security log / information / event lifecycle are summarized for 35 NBA users and 84 non-NBA users, in comparison to the leading and lagging performers in the study. The findings are normalized on a scale of 0 (Laggards) to 100 (Best-in-Class) to simplify the comparison: current users of NBA correlate strongly with Best-in-Class results, and non-users of NBA correlate strongly with Laggard results. NBA users in the study were particularly strong at *correlation* and *analysis*, and on average performed even higher than the Best-in-Class at *prioritizing incidents and threats*. *Reporting* and *recommending specific actions for remediation* are two explicit opportunities NBA users have for improvement.

Figure 3: Current Use of NBA Correlates Strongly with Best-in-Class Efficiencies



Source: Aberdeen Group, October 2009

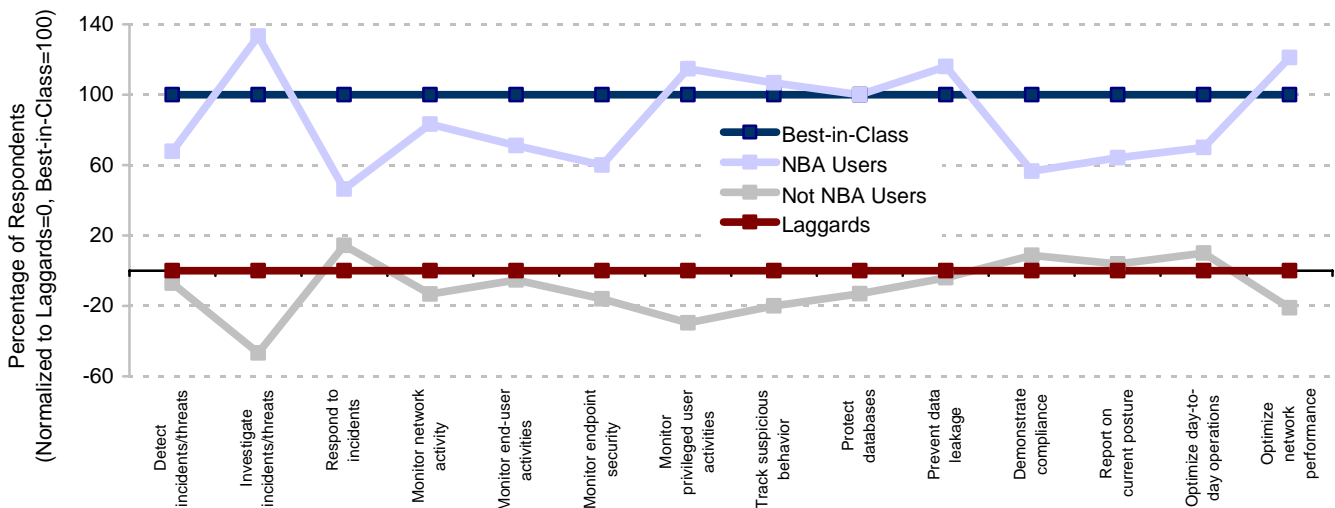
A general pattern seen across the arc of Aberdeen's IT Security research is that Best-in-Class organizations invest first to ensure that their IT infrastructure is **secure**, then to demonstrate and sustain **compliance**, and then to **optimize operations** to improve efficiencies and reduce overall cost (Table 2). In a presentation similar to that of Figure 3, current NBA users are shown in Figure 4 to be much more likely to *investigate security incidents and threats* (proactive) than to merely *respond* (reactive); they are proactively *monitoring privileged users* and *tracking suspicious behavior*; they are proactively *protecting databases* and *preventing data leaks*. Once again, NBA users in the study are generally found to correlate strongly with Best-in-Class performance, while non-NBA users correlate strongly with Laggards.

Table 2: Patterns of Maturity: Secure, Compliant, and Well-Managed (in that order)

2. Compliant	1. Secure	3. Well-Managed
<ul style="list-style-type: none"> ▪ Demonstrate regulatory compliance ▪ Report on current posture for management ▪ Report on current posture to business owners ▪ Report against an initial baseline and against targeted goals 	<ul style="list-style-type: none"> ▪ Detect security incidents / threats ▪ Investigate security incidents ▪ Respond to security incidents ▪ Monitor network activity ▪ Monitor end-user activities ▪ Monitor endpoint-related security ▪ Monitor privileged user activities ▪ Track suspicious behavior ▪ Protect databases ▪ Prevent data leakage 	<ul style="list-style-type: none"> ▪ Reduce total cost of security ▪ Reduce total cost of compliance ▪ Reduce total cost of management ▪ Implement industry standards and best practices (e.g., COBIT, ISO) ▪ Optimize day-to-day operations ▪ Optimize network performance ▪ Increase visibility / correlate with additional data sources
Sustain Compliance <i>after the fact</i>	Enhance Security ← t = 0 →	Optimize Operations <i>proactive / predictive</i>

Source: Aberdeen Group, October 2009

Figure 4: For What Purposes Does Your Organization Use Security Logs, Information and Events?



Source: Aberdeen Group, October 2009

Quantifying the Advantages of Top Performance

The findings thus far about current users of Network Behavior Analysis technologies are interesting, but the real question is: are they impactful? A high-level analysis of the research findings summarized in Table 3 will help to sketch the business impact of top performance at leveraging security-related logs, information and events.

Table 3: Average Number of Incidents Experienced in the Last 12 Months, by Maturity Class

Type of Incident	Best-in-Class (top 20%)	Industry Average (middle 50%)	Laggards (bottom 30%)	Performance Gap (Best - Worst)
Malware infections	4	25	44	40
Data loss / exposure	1	3	8	7
Audit deficiencies	1	3	11	10

Source: Aberdeen Group, October 2009

Malware Infections – In the [Leveraging Logs, Information and Events](#) study, Aberdeen asked about the average time to respond to and remediate a valid network security alert. The average time for current NBA users was 3.5 hours, as compared to 5.9 hours for non-NBA users. The business impact of an extra 2.4 hours per alert is a calculation unique to each organization. As a back-of-the-envelope example, however, note that with respect to the average number of malware infections in the last 12 months, the difference between the Best-in-Class (4) and Laggards (44) is 40, which translates to roughly 100 total hours per year. At a fully-loaded cost of US\$125,000 per year, this translates to about US\$7,000 per person involved with remediation – which in no way fully captures the total economic impact in terms of business disruption, opportunity cost, data loss or exposure, and so on.

Data Loss or Data Exposure Incidents – Aberdeen's research showed that the average number of data loss or data exposure incidents with known financial impact in the last 12 months was one for Best-in-Class organizations, and eight for Laggards. Based on an average financial impact of each data loss incident estimated at US\$640,000 (from *The 2009 Aberdeen Report*, May 2009), the relative advantage of top performance translates to seven incidents per year, times US\$640,000 per incident, or a whopping US\$4.5 million per year.

Audit Deficiencies – In terms of the average number of relevant audit deficiencies in the last 12 months, Aberdeen's research indicated one for the Best-in-Class and eleven for Laggards. If left unaddressed, these audit deficiencies could leave the companies exposed to malware infections or data loss or exposure incidents, which may eventually lead to the sort of calculations in the two previous examples. But investigating, addressing, and demonstrating successful remediation of these audit deficiencies also consumes valuable time and resources. Based on an average estimated US\$7,000 per incident for remediation (from [PCI DSS and Protecting](#)

Cardholder Data, June 2008), the relative advantage of achieving top performance translates to 10 incidents per year, times US\$7,000 per incident, or US\$70,000 per year.

Case in Point: Air Transportation Industry Credit Union

Founded by a small group of airline employees during the Great Depression, a leading federal credit union serving employees of the air transportation industry today has more than 200,000 members, manages assets of more than US\$5 billion, and offers account access through a network of more than 3,600 service centers and 28,000 ATM locations nationwide.

According to the company's Director of Network Infrastructure and Information Security, the company was looking to implement better "eyes in the network", to "see what was happening on the network and to respond quickly and decisively", something that their existing tools and processes did not allow them to do. In addition, the company was beginning to feel regulatory pressures to implement an intrusion detection system with more capabilities than the incumbent solution.

After reviewing and testing alternatives from several vendors – including Cisco, IBM ISS and SecureWorks – the company ultimately selected and deployed a solution from Global DataGuard (GDG). Technical capabilities were prominent among the selection criteria, in particular the built-in behavioral capabilities that were unique to the GDG solution. The decision was also influenced by non-technical capabilities, however, including "exceptional customer service, which is very important to me." Although the initial deployment was undertaken using internal resources, "I found it much more cost-efficient to outsource these tasks to GDG, who has the trained staff that can assist with the solution. The results of the rollout have exceeded our expectations, and I have been very happy with GDG's solution, service and support."

"Using only internal resources, the time commitment needed to support, monitor and respond to network traffic was overwhelming. We can now see what is happening on the network and respond quickly and decisively."

~ Director of Network Infrastructure and Information Security, Air Transportation Industry Credit Union

Solutions Landscape

An illustrative list of vendors offering solutions that incorporate Network Behavior Analysis is provided in Table 4.

Table 4: Solutions Landscape for Vendors Incorporating Network Behavior Analysis (illustrative)

Company	Solution(s)	Description
Global DataGuard www.globaldataguard.com	Enterprise UTM++ SRM Managed Security Services	Global DataGuard's Enterprise UTM++ solution consists of a family of appliances and add-on modules that provide real-time, actionable root-cause information and long-term context for network security threats. Patented behavioral analysis and correlation tools are part of an architectural approach that also integrates packet analysis, intrusion detection, intrusion prevention, vulnerability scanning, vendor alerts, correlation systems, asset database and dashboard. Alternatively, the Enterprise UTM++ solution is made available as an outsourced solution via Global DataGuard's Security Risk Management (SRM) Managed Security Services.

Company	Solution(s)	Description
QI Labs www.qilabs.com	QRadar SIEM	QRadar SIEM is designed to centralize previously discrete network security management functions into a single, cohesive framework. Correlation of network behavior analytics with security event information provides enhanced security intelligence in a network context. QRadar's highly automated approach is designed to reduce the complexity of analysis and to provide organizations with a proactive threat monitoring capability that is network-, security-, application-, and identity-aware. Under OEM relationships, QRadar technology is also licensed to Enterasys and Juniper Networks.
Enterasys www.enterasys.com	Dragon Security Command Console	The Dragon Security Command Console (DSCC) integrates network activity data, security events, logs, vulnerability data, and external threat data into a centralized management dashboard. DSCC provides a baseline for normal network behavior by collecting, analyzing, and aggregating network flows (including JFlow, NetFlow, and sFlow), discerns network traffic patterns that deviate from this norm, and flags anomalous behavior for correlation and remediation.
Juniper Networks www.juniper.net	STRM Series	Juniper's Security Threat Response Manager (STRM) Series of appliances integrate log management, security information and event management, and network behavior analysis in a single console to improve IT efficiency and reduce the cost of managing security. Central management of network and security events, network and application flow data, vulnerability data, and identity information is designed to reduce false positives and detect threats that independent security solutions miss.
Arbor Networks www.arbornetworks.com	Peakflow X	Arbor's Peakflow X solution uses network behavior analysis technology to identify the normal behavior of network traffic and applications, and to generate alerts for abnormalities due to traffic and usage violations, malicious activities, configuration errors, and zero-day threats that can slip by existing anti-virus and intrusion detection systems.
Hewlett-Packard www.procurve.com	HP ProCurve Network Immunity Manager	HP ProCurve Network Immunity Manager is designed to detect and automatically respond to network threats, leveraging security and traffic-monitoring features such as sFlow and network behavior analysis to detect attacks, provide visibility into network threat activity, and help to increase network availability.
Lancope www.lancope.com	StealthWatch	Lancope's StealthWatch system leverages NetFlow, sFlow, and packet capture data to combine behavior-based anomaly detection with network performance monitoring to delivering unified visibility across both physical and virtual networks.

Source: Aberdeen Group, October 2009

Aberdeen's IT Security research consistently shows that most security and compliance initiatives continue to operate independently of one another, in "silos". Best-in-Class organizations, however, are clearly moving towards a more strategic, enterprise-wide approach to deploying and managing their IT security solutions, and to integrating them with other IT security management tasks. Such **convergence** can manifest itself in a number of ways, including:

- The consolidation, normalization and correlation of security and compliance information in the back-end
- The evolution from multiple, disparate management systems towards the ideal of a single, integrated management platform
- The consolidation of software installed and managed at the endpoints

The preponderance of tactical, project-oriented point solutions often has the effect of end-user organizations acting as their own systems integrators – or absorbing the operational inefficiencies of managing a hodge-podge of discrete systems. To address this issue, forward-looking solution providers are building out a “platform” or “ecosystem” approach, for example:

- Establishing a consistent *architecture* to facilitate integration and interoperability of multiple IT security technologies
- Centralizing the *collection, archival, normalization, correlation, analysis, monitoring, auditing, and reporting* on security and compliance-related data

This vision is consistent with the Best-in-Class view of security and compliance as a strategic, sustainable program, as opposed to a series of one-time events.

From a purely practical point of view, the leading factors driving organizations to invest in the “unified” approach versus the “independent” approach are **reducing cost** and **reducing complexity**, along with the obvious requirements for specific **functionality**. Table 5 shows the factors (listed in relative order of importance, from left to right and from top to bottom) that are currently driving the unified approach, as identified in Aberdeen's benchmark study in [Unified Threat Management](#) (September 2008).

"Regardless of which Network Behavior Analysis tool you use, one issue is finding staff that has experience in tuning, analyzing and interpreting the data. Even attempting to implement a free utility can be difficult unless your team is able to analyze the data. I think this is an important consideration for any size organization."

~ Network Security Manager,
government agency

Table 5: Factors Driving the "Unified" versus "Independent" Approach to Network Security

Reducing Cost	Reducing Complexity	Extending Functionality
<ul style="list-style-type: none"> ▪ Reduce the cost of managing multiple dedicated solutions ▪ Reduce the total cost of service and support contracts for dedicated solutions ▪ Reduce the total cost of licenses for dedicated solutions ▪ Reduce power consumption of multiple dedicated devices 	<ul style="list-style-type: none"> ▪ Reduce the number of service and support contracts for dedicated solutions ▪ Reduce the number of licenses for dedicated solutions ▪ Reduce the number of physical devices ▪ Preference for a single-vendor solution ▪ Lack of sufficient IT, Network, or Security staff for dedicated solutions ▪ Reduce physical space requirements for multiple dedicated devices 	<ul style="list-style-type: none"> ▪ Need for specific security functionality ▪ Flexibility for future expansion of security functionality ▪ Expansion or changes to network topology ▪ Upgrade / replacement for existing services

Source: Aberdeen Group, September 2008

One final consideration: although solutions in this area are commonly offered as network appliances, managed security services options are steadily becoming more widely available. Aberdeen's research in [Selecting and Consuming Managed Security Services](#) (January 2008) found the leading drivers of current investments in managed security services to be:

- Improve security: 55% of all respondents
- Reduce the cost of ongoing management: 33%
- Reduce the cost of acquisition and deployment: 30%
- Gain access to security expertise that is not available in house: 30%

Summary and Recommendations

Network Behavior Analysis (NBA) is a powerful enabling technology that can help close the gaps in traditional signature-based network security and foster proactive management of an organization's security and compliance initiatives. Aberdeen's research shows that integration of NBA data with other security-related log, information and event data helps companies to look forward (proactive remediation and prevention) as opposed to only looking backwards (forensics, incident investigation, and post-incident response). Sooner or later, you have to look forward to move ahead.

The overall industry trend is towards a more holistic and integrated approach, for example one in which a traditional perimeter firewall system is combined with intrusion detection and prevention capabilities, which is combined with network access control for keeping unclean or unauthorized systems off the network in the first place. In this scenario NBA is highly complementary to the other solutions, helping to alert the organization when something goes undetected by the other lines of defense. On their own, none of these technologies could be relied upon to keep a network secure, but in combination they are likely to be much more effective.

The key to realizing the benefits of this approach lies in how effectively the technologies are **integrated** and able to share, correlate, and analyze information. NBA can significantly enhance the value of the data generated by the other security systems and applications, by analyzing and correlating large amounts of otherwise independent information and discrete events. Advanced approaches to behavioral analysis can include not only pattern-matching, but also continuous tracking of resources, thresholds, policies and protocols, as well as regression and statistical analysis on historical data to predict what will happen next so it can be prevented. This brings up the critical importance of the consoles and dashboards of NBA-enabled solutions, and the vital ongoing role of **human** intelligence to research, customize and tune the analysis to be more sensitive to events affecting specific systems, based on their knowledge of the network.

Solution providers that incorporate NBA most effectively will enable their customers to improve protection by predicting and preventing emerging threats before they cause harm, rather than by merely explaining events that

"NDA has real promise if it is part of an integrated approach with existing firewalls, intrusion prevention, and network access control. As a network engineer, the idea of adding yet another separate system to my network to learn and manage is far less appealing than sticking with the same vendor and getting some kind of centralized threat management."

~ Network Engineer,
food services company

have already ensued. Buyers interested in Network Behavior Analysis should engage with the solution providers for detailed discussions about their respective approaches to integration and interoperability of multiple IT security technologies, and to understand how effectively they can extract meaning from the normalization, correlation, analysis, monitoring, auditing, and reporting of disparate security- and compliance-related data.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
<u>Leveraging Logs, Information and Events: Three Use Cases for What to Do with All That Data</u> ; March 2009	<u>WatchGuard Acquires Borderware: Aiming at the Middle</u> ; August 2009
<u>IT GRC: Managing Risk, Improving Visibility, and Reducing Operating Costs</u> ; May 2009	<u>LogLogic Rolls Forward with the Acquisition of Exaprotect</u> ; May 2009
<u>The 2009 Aberdeen Report</u> ; May 2009	<u>NitroSecurity Expands SIEM Integration</u> ; March 2009
<u>Unified Threat Management - What's In, What's Next, and Why</u> ; September 2008	<u>Deploying IT Security: Keeping the Threats and Headaches Outside</u> ; March 2009
<u>Vulnerability Management: Assess, Prioritize, Remediate, Repeat</u> ; July 2008	<u>PCI DSS and Protecting Cardholder Data</u> ; June 2008
<u>The 2009 Aberdeen Report</u> ; May 2009	<u>Best Practices in Choosing and Consuming Managed Security Services</u> ; January 2008
Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)	

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. (071309b)