



## Network Security Forensics: How the nGenius Solution Enables Rapid Investigation and Repair of Security Violations

### Challenges of Existing Security Tools

Network perimeter defenses such as firewalls, network intrusion detection systems (NIDS), intrusion prevention systems (IPS) and anomaly behavior systems are critical first measures of defense, but have limitations that prevent complete protection of today's complex and dynamic network environments. You need the extra level of information and protection that advanced network performance management tools with 24x7 packet capture and long-term storage provide to enable quick forensics analysis and remediation of potential security issues.

IDS/IPS systems are only as good as the content that is delivered to them. Signatures occasionally produce false negatives (i.e., miss an event) and often generate false positives. In a time of crisis, not having the ability to review packet data to validate a triggered signature or determine why it is not firing can prolong an outage, extending the window of vulnerability and potentially increasing damage.

Augmenting an IDS/IPS with a system that has full packet capture/replay capabilities will allow security operations to keep an IPS device optimized and have a deep forensic data source in times when basic IDS event data isn't enough, such as attacks that originate from:

- Rogue wireless devices
- Trojans or worms introduced via laptops, personal email services or flash-based storage devices (e.g., USB drives)
- Zero-day attacks for which signatures have not been implemented
- Unauthorized remote control "zombie", denial of service (DoS) attacks, or peer-to-peer software

### nGenius Solution Supplements Your Existing Security

Performance management products are not designed to be a first defense security solution. However, they can be effective in alerting you to an abnormal situation as it arises, or in researching suspicious traffic patterns or packets, so you can analyze them and stop an attack in its tracks. The nGenius Performance Management Solution can provide early warning of security-related performance problems; historical and real-time data to isolate the root cause; and packet capture and decode capabilities to prevent further damage.



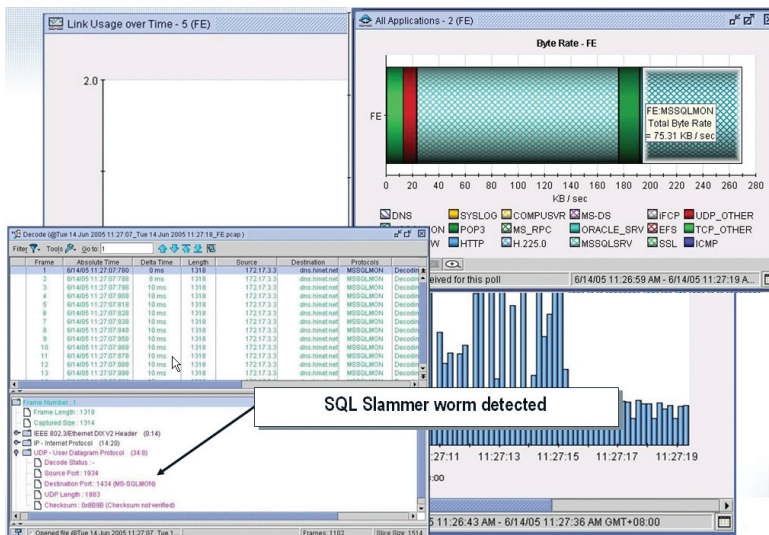
The nGenius Solution – nGenius K2, nGenius Performance Manager and nGenius InfiniStream – can supplement your existing security solutions, bridging your network and security operations teams and making them more effective by:

- Detecting significant changes in network and application behavior, providing early warning of changes in traffic patterns that may indicate security breaches or other performance issues.
- Diagnosing root cause, enabling speedy restoration of the network to normal operations and reducing mean time to repair (MTTR).
- Tracking all applications, conversations and hosts, not just the "Top N" applications or those that exceed a certain threshold of activity to catch low-level intrusions.
- Quickly identifying source and destination IP addresses in order to contain an attack before it propagates throughout the enterprise.
- Accelerating assessment and remediation of security issues, given our top-down viewpoint, configurable packet decode filtering and on-demand reporting capabilities.
- Recording and archiving continuous packet capture trace files, including full packet header and payload details on a 24x7 basis, enabling long-term recall for post-event forensics analysis and reconstruction.

- Correlating anomalous events discovered by your enterprise security product with actual, observed network traffic behavior.

### nGenius K2 Detects Small but Significant Changes

nGenius K2 helps identify changes in network behavior due to security breaches within minutes after the break in occurs, helping to contain and limit damage. nGenius K2, NetScout's early warning system, looks for abnormalities and patterns that could indicate a zero-day virus, zombie bots sending spam from compromised desktops, or denial of service attacks. Because K2's Advanced Analytics engine recognizes small but significant changes in network behavior, it provides another layer of security; it can help network and security teams detect these types of threats before the environment is significantly impacted.



Rapidly discover the applications associated with the surges in link utilization with easy, intuitive drill downs to all applications. A list of All Applications shows substantial use of MSSQLMON, which is rarely used. Identify the source of the worm by accessing the packet trace file for decode analysis. In this case, the packet-level decode shows that a SQL Slammer worm is the source of abnormal performance.

#### Reducing False Positives

The security group at a US Federal agency, in conjunction with the network engineering group, is finding the nGenius Solution helpful for discovering and isolating potential network threats. For instance, when there is a potential false positive alarm from the IDS system, the security team requests help from the network team to troubleshoot the problem. Utilizing top-down application and conversation-level views, followed by deep packet inspection with packet capture and sophisticated decoding, the groups work together to isolate the actual traffic type and/or the affected hosts. Then they can determine the source IP addresses and if the traffic is “good” or “bad.”

Then, the instant an attack or break-in is suspected, nGenius InfiniStream provides all the evidence from the break in. It acts like a video surveillance camera on the network, passively collecting packet-level data until it is needed for reviewing the scene of the crime. This packet data contains the “who”, “what” and “where” of the security breach and enables retrospective analysis and playback – displaying all traffic associated with the break-in, and gathering all information required to restore the network to a secure state. nGenius InfiniStream also acts as an audit trail which can archive all evidence for future prosecution.

Using the analogy of a jewelry store... would you rather know that someone entered the store at 10pm, that the alarm sounded and they left three minutes later with the “goods” (a typical IDS) or would the police rather get video tape of the suspects showing exactly which pieces of jewelry they took, a photo of their license plate and an indication of which direction the car was headed when they left the store (the nGenius Solution)?

### Insightful Forensic Analysis Facilitates Remediation Efforts

Despite best efforts, networks occasionally still come under attack. In these situations, the nGenius Performance Management Solution delivers insightful forensic analysis, which network operators and security administrators can jointly use to pinpoint root cause, identify affected hosts and perform detailed attack analyses – in real time or historically. The analysis of flow details facilitates easy detection and understanding of attacks in order to better assess the impact and assist remediation of security events.

nGenius InfiniStream is a high-capacity, highly available appliance that combines monitoring and continuous packet capture for high-performance recording and infrastructure monitoring. The InfiniStream creates a detailed and easy-to-digest trail of information about network activities – down to the actual packet trace file with full header and payload details – that can be summarized through real-time application-level views and shared using

ad hoc and scheduled reports. Armed with this critical information, network and security professionals can quickly trace the source of attacks, significantly reducing mean time to repair. By using nGenius InfiniStreams to record packet details on key network segments on a 24x7 basis, organizations can simplify problem identification and quickly resolve network security issues due to:

- Surges in traffic due to viruses, worm, Trojans or other malware running on the network
- Denial of service (DoS) and other network-layer attacks
- Application-layer intrusions and attacks, both from within and outside the network
- Attacks from new applications like VoIP, instant messaging, and peer-to-peer
- Malware introduced through non-standard devices, such as rogue wireless devices, printers, and IP phones

The nGenius Solutions' expert data mining helps you quickly pinpoint the cause of a security incident and the conditions that led up to it. Through graphical trace analysis, you can effortlessly comb through massive amounts of data to zero in on the exact traffic spike – down to the sub-second. Flexible filtering allows you to refine the data set and look at the exact time, user or application associated with the network disturbance. To extend the analysis, you can view the packet decode or export it to your favorite trace expert tool.

nGenius InfiniStream's extensive data mining capabilities enable users to quickly derive actionable information from captured traffic using:

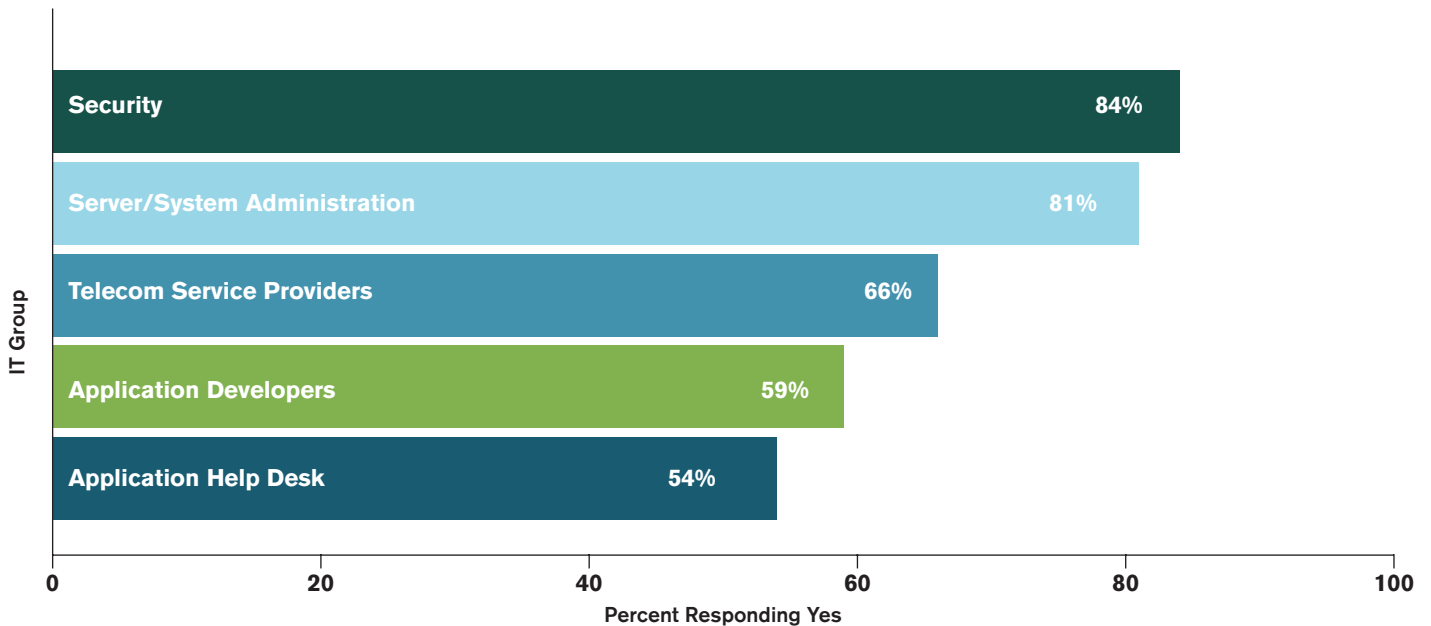
- Expert Views with drill-downs to graphically analyze captured packets to zero in on the exact time, user or application associated with the network disturbance.
- Pre- or post-capture filters to create custom rules to identify the precise combination of addresses, ports, applications and patterns for security-related events that you want to identify.

- Detailed packet decode functionality to perform in-depth analysis and playback of selected packets.

**Furthering Collaboration between NetOps and Security**

Many NetScout customers use the nGenius Solution to assist other internal stakeholders on an ongoing basis by providing them with tailored reports on application usage and bandwidth consumption, helping to validate architectural, device and application performance. Network operation teams receive requests for reports from Internet operations, application, security, and desktop support teams, all of whom have become accustomed to having a view of what is happening on the network and how their specific applications are behaving. The network operations and security teams often have the closest working relationships. In a recent survey, 84% of NetScout users said they collaborate closely with their security group (Figure 1).

**Do you collaborate with other IT Groups?**



**Figure 1. 84% of NetScout users collaborate with their security team.**

## Bottom Line

The nGenius Solution saves organizations time and money by reducing the resources required to optimize security and network operations.

With the nGenius Solution, network and security staff have a single, common data source for essential network optimization and security data. It passively monitors all network traffic across all segments of all internal networks to deliver a true, real-time overview of what is happening inside the enterprise.

With contextual drill-downs from nGenius K2 to nGenius Performance Manager to

nGenius InfiniStream, administrators can quickly connect any individual network breach with the users or applications responsible for the anomaly.

Equipped with accurate data and clear reports, network and security staff can find out WHY network traffic patterns are abnormal, including which applications are at fault, which sources are generating the traffic and with whom they are trying to communicate. All of this information is especially critical in finding and containing infectious, malicious code to limit further damage.

### Case Study: Double Teaming on Security

Today's airlines depend heavily on their Websites to provide services to travel agents, partners and consumers. These web sites frequently handle millions of hits per day from customers checking flight schedules, making reservations and conducting advance check-in, accounting for millions in revenue a day. Web site downtime is very costly.

A US-based airline's network operations team works especially closely with the security team to prevent downtime of their web site. Like most organizations, the airline is concerned about security issues, including possible virus and other hacker attacks that could disrupt the network. Fortunately, security isn't a huge headache for this airline since they supplement their security tools by relying on the nGenius Solution to report attacks on the network. For example, users sometimes bring viruses in through a home device or a POP email account. Based on reports detailing recent virus outbreaks from their ISP and security vendor, the network team creates custom protocols and filters in nGenius Performance Manager using the popular ports that each virus uses. They then apply these filters to monitor their hosts and conversations. If anything uses these protocols, the nGenius System will proactively notify the network team and they in turn let the security group know what the offending virus is, who brought it in, how, and, if possible, block it from happening again.

Rapidly discover the applications associated with the surges in link utilization with easy, intuitive drill downs to all applications. A list of All Applications shows substantial use of MSSQLMON, which is rarely used. Identify the source of the worm by accessing the packet trace file for decode analysis. In this case, the packet-level decode shows that a SQL Slammer worm is the source of abnormal performance.



### About NetScout Systems

NetScout Systems provides advanced network and application service assurance solutions that deliver complete visibility into real-time, packet/flow-based operational intelligence. IT operators at the world's largest enterprises, government agencies, and service providers use the Sniffer and nGenius solutions to troubleshoot service degradations faster and more efficiently in order to reduce MTTR.

### Our world-renowned Sniffer and nGenius solutions include:

- Intelligent Data Sources for high capacity, deep-packet recording and monitoring
- Analysis Software for real-time and historical network and application performance management, troubleshooting, capacity planning, and reporting
- Advanced Intelligence for early detection and in-depth analysis of complex or specialized application services
- Comprehensive, global support, consulting and training services

### Corporate Headquarters

310 Littleton Road  
Westford, MA 01886-4105  
Phone: 978-614-4000  
Toll Free: 888-999-5946  
[www.netscout.com](http://www.netscout.com)

### European Headquarters

NetScout Systems (UK) Ltd.  
100 Pall Mall  
London SW1Y 5HP  
United Kingdom  
Phone: +44 (0)20 7321 5660

### Asia/Pacific Headquarters

Room 105, 17F/B, No. 167  
TunHwa N. Road  
Taipei, Taiwan  
Phone: +886 2 2717 1999  
[www.netscout.cn](http://www.netscout.cn)

©2008 NetScout Systems, Inc. All rights reserved. NetScout, the NetScout logo, Network General, the Network General logo, nGenius, Sniffer, InfiniStream, Business Container, Business Forensics, NetVigil and Quantiva are trademarks or registered trademarks of NetScout Systems, Inc. Other brands, product names and trademarks are property of their respective owners. NetScout reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.

TN0808\_15revA