Breaking the Cycle: Eliminating Static Thresholds and Reducing False Positive Alerts

Using *nGenius* Analytics to Automate and Accelerate Network and Application Performance Problem Identification, Diagnosis, and Resolution

Many highly skilled IT staff are stuck in the never-ending and tedious cycle of manually setting and resetting thresholds, chasing down false positive alerts, and reacting to calls from end users notifying them of problems after they have reached the point of impacting the business. The sad truth is that these hours could be better employed working on projects that drive their company's business forward.

One of the fundamental problems to stopping this cycle is that network behavior is constantly changing. What is normal network activity on a Monday morning is not necessarily normal for a Thursday morning or a Sunday afternoon. And, what's normal on a weekly basis will inevitably change over time due to the addition of new users, applications, servers, etc. In other words, "normal" has many different meanings.

The variables involved in calculating "normal" network use are too vast to consider on an on-going basis when manually setting thresholds for performance management. Therefore, many network administrators set thresholds at a high water mark or eliminate alerting altogether in order to avoid the pitfalls associated with threshold alarms.

NetScout's *nGenius* Analytics' intelligent, automated anomaly detection and analysis can help break the cycle of setting and re-setting alarm thresholds. It analyzes traffic flows, learns behavior patterns and continuously updates usage models, automatically detects anomalies, and then automatically determines the root cause so that you can minimize disruptions, shorten downtime or even prevent it altogether.

The Challenge: Baselining Application Performance

Baselining is the process of measuring "normal" network and application behavior so that future anomalous behavior can be determined. But how do you account for all the variables that define normal behavior? Network traffic is continuously changing - from day to day, week to week, even season to season - making it tricky to establish what is anomalous and what is normal for any given day and time. For example, is the Tuesday morning spike due to the weekly payroll submission or a new virus running amok? Is Friday afternoon's blip due to a well-attended marketing webinar or is it the result of a regularly scheduled backup that should really be moved to non-peak hours?

The Downside of Static Thresholds

Because a single characteristic of "normal" network traffic can't be determined, thresholds alarms are often improperly or randomly set. For example, set thresholds too high and you may miss problems or see them too late. Set them too low and the volume of alerts can be overwhelming. Turn them off altogether and you're at risk of missing critical notifications that could avoid serious service degradations or outages. Many network administrators set thresholds at a high water mark and eliminate alerting altogether in order to avoid the pitfalls associated with threshold alarms. However, this can lead to incredible inefficiencies.

The High Watermark: Risking Business Employee Productivity

In a February 2006 survey conducted by industry analyst Dr. Jim Metzler of Ashton Metzler Associates in conjunction with NetScout Systems, 67% said their company sets thresholds at a high watermark (Figure 1). The trouble with this approach is that end users are the first to recognize that there is a problem almost half of the time (Figure 2). This means that by the time the alarm is triggered, business-critical processes have already been negatively impacted and the IT staff is forced to react with whatever method works fastest, rather than taking a measured, thoughtful approach.

> **"We utilize static alarms even though they are problematic. Because we don't want a lot of false positives we set the threshold high, unfortunately in a lot of cases, high is too high."**
>
> Director, Integrated Operations Center
> at a Fortune 500 property and casualty insurer

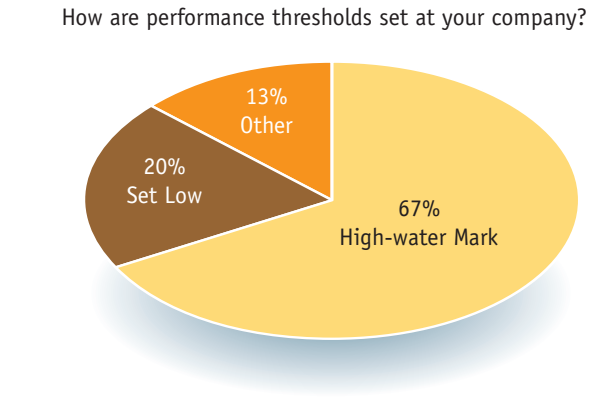

Figure 1. Two-thirds of all thresholds are set at high watermarks, limiting the number of alerts but also decreasing the chances of catching issues before they become service effecting.

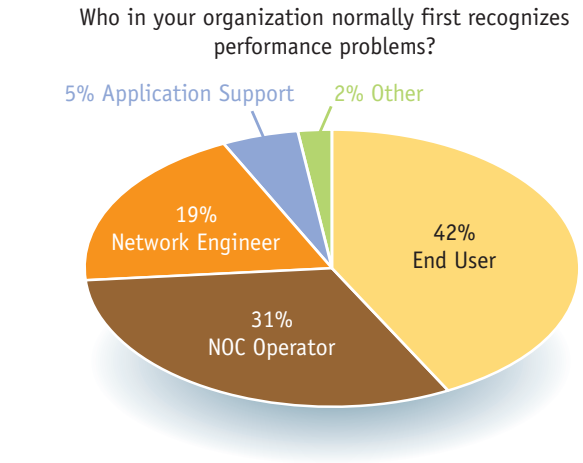

Figure 2. Nearly half the time, end users are first to recognize that there is a problem. When this happens, it's already too late and business has been negatively impacted.

Spinning Your Wheels Part 1: False Positive Alerts

Twenty percent of network managers said they set static thresholds low so they can catch problems before they impact the business (Figure 1). While a proactive approach is an admirable sentiment, the drawback is that the staff ends up spending unnecessary time fruitlessly chasing down false positive alarms or low-priority issues. That is, even though a threshold was exceeded, there was no real problem, just a change in what is "normal" for today.

A further potential danger of low thresholds is the "cry wolf" syndrome where, after chasing so many erroneous alerts, staff begins to doubt the validity of any alert they receive and ignores early warnings of real problems until they become service effecting.

Spinning Your Wheels Part 2: Redundant Alarms

Further, it is important to intelligently filter the number and type of alarms for a problem that occurs intermittently or that affects multiple segments and/or virtual circuits. This will save hours avoiding the need to set dozens of alarms on all the PVCs or VLANs in a segment, as well as hours spent triaging the hundreds of virtual circuits on a WAN trunk experiencing the same bandwidth constraint.

Side Effect of Tedium: Staff Productivity and Job Satisfaction

Staff productivity is also often a concern of management. Setting and resetting thresholds, spinning useless cycles on troubleshooting non-existent problems day in and day out can lead to burn out and job dissatisfaction. Whenever possibly, it's important to relieve highly trained IT staff of such tedious tasks and allow them to focus their skills on higher value, more strategic activities, such as capacity planning, improving business services, special projects, etc.

According to Jean-Pierre Garbani of Forrester Research, "As hardware and software technologies progress, the cost of operation especially the amount of human resources stranded in menial operational tasks becomes a glaring issue. Using IT personnel for more rewarding and strategic tasks requires that the more tactical ones be automated as much as possible."

The Ashton Metzler survey results are representative of the problem. More than half (56%) of the respondents had three or more people responsible for triaging alarms (Figure 3). Sixty-one percent (61%) of the organizations polled spent between one and three hours triaging alarms daily, while another 23% spent more than half of each day (Figure 4).

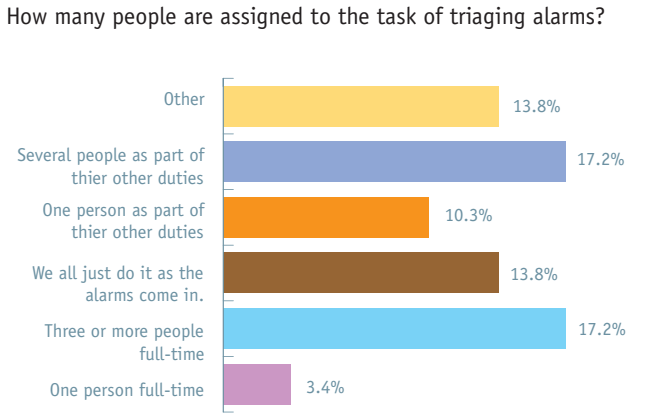

Figure 3. Often multiple network engineers are tasked with triaging alarms as part of their regular duties.

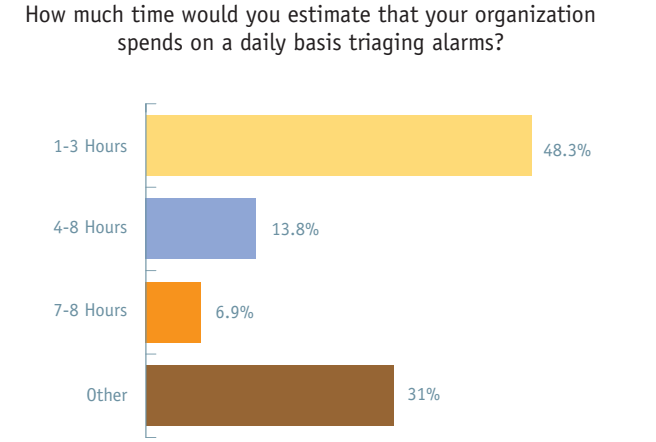

Figure 4. Network staff in large organizations spend several hours each day triaging alarms.

Diagnosing Root Cause

Finally, assuming staff are sent only valid, actionable alarms, there's still the problem of where do you start. With most products, alerts generally lack context, meaning that there's no easy way to know if the problem on a particular link is due to a poorly performing application, the addition of a new applications, a sudden flood of users - the list is nearly endless. Without seeing the problem in the context of the entire application fabric infrastructure - the network, servers, application flows, etc - there's no easy way to figure out the root cause. Network staff must often resort to a hit-or-miss approach to troubleshooting. Putting the problem in context from the start can help you pinpoint the source faster, shortening mean time to repair.

"Based on our experience with the product, I'm positioning *nGenius* Analytics to help us meet organizational goals to be more proactive in optimizing the network and cutting resolution times. Its dynamic alerts could eliminate unnecessary time spent configuring alarm systems, triaging alarms and hunting for evidence of a suspected problem. We'd like to quickly escalate events to the proper network personnel before a situation becomes critical."

Senior Network Engineer, Transportation Company

nGenius Analytics: Automated Detection and Diagnosis

nGenius Analytics provides IT staff with an early warning system to automatically detect and diagnose anomalous usage and error conditions throughout the application fabric infrastructure. This leads to

- Fewer, more meaningful alerts
- Faster problem resolution
- Higher IT staff productivity

Once installed, *nGenius* Analytics immediately starts learning the usage patterns of all monitored interfaces and applications, and then continually updates the models as usage characteristics change over time. Using innovative and advanced statistical methods, it analyzes traffic flows across physical and virtual interfaces and QoS classes, comparing current activities to historical models and automatically alerting NOC staff to atypical behavior through the event dashboard and/or by sending the alert to an integrated Enterprise Management Systems (EMS) such as HP OpenView or IBM Tivoli NetView.

Once *nGenius* Analytics detects a utilization anomaly, it correlates the anomaly to the offending traffic and application(s). By analyzing packet-level details for traffic type (multicast, broadcast or unicast) as well as application details (SAP, Citrix, HTTP, etc.), it can precisely pinpoint the root cause of the increase in traffic volume, guiding and speeding the troubleshooting process.

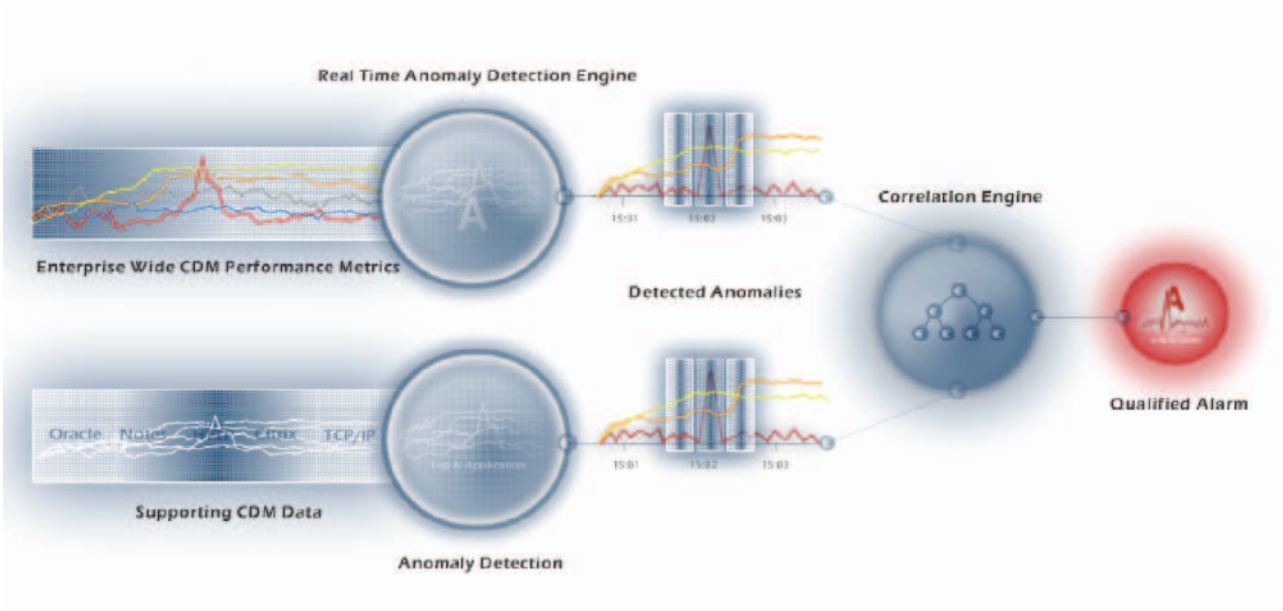

Figure 6. Two key components, the real-time anomaly detection engine and a correlation engine, combine their functionality within *nGenius* Analytics to automatically detect and identify anomalies prior to having a critical impact on IT infrastructure behavior.

Types of Anomalies Discovered

nGenius Analytics uses multiple analysis windows to detect common changes in network behavior. The most common and easily understood behavior is "the spike" - a sudden increase in traffic that is short lived. This could be from a burst of users as tickets to a hot concert go on sale in an e-commerce enterprise or an increase in an ERP application as annual enrollment for benefits commences. Dynamically watching for spikes with *nGenius* Analytics is essential, because all too often, as discussed, the spike may not reach the high water mark of a static threshold, yet still effect service.

Similar to the spike is "the shift" - a sudden increase in traffic that is sustained for a period of time. An increase in traffic volume to a data center might look like a shift or plateau following a consolidation of two or more data centers or the implementation of VoIP or some other business process that is newly networked.

One of the most difficult and elusive anomalies to manually identify is "the drift" - a slow but steady increase in overall traffic or for a particular application. Companies with increasing employee or customer use of the network may find this kind of evolution, but may only discover it when users start to experience congestion, degradations, and bottlenecks. For example, a financial company receives progressively larger files from its partners every day, consuming more and more bandwidth. By the time the problem is caught, it's a full outage.

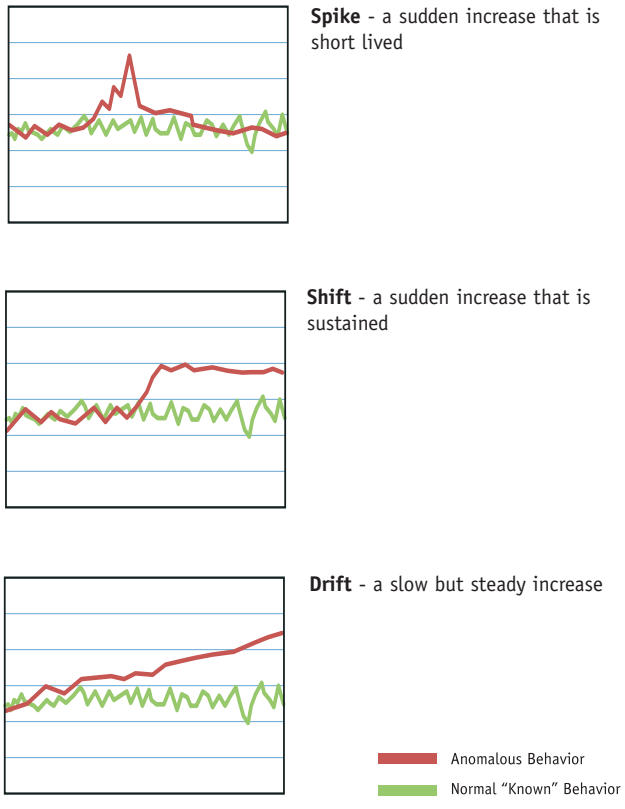

Figure 7. *nGenius* Analytics uses multiple analysis windows to detect common changes in network behavior - the spike, shift and drift.

nGenius Analytics combines the best of both baseline and time-over-threshold alarms by

- Utilizing Progressive Analytics (an award-winning patented algorithm that uses advanced modeling and analytics to establish statistically expected behavior values) to provide dynamic utilization alarming.
- Combining related alerts into a single event notification to reduce the clutter staff is forced to wade through.
- Providing automatic correlation to the offending application(s) to shorten mean time to repair as compared with manual diagnosis.
- Utilizing multiple analysis windows to identify short-lived problems and hard-to-catch, longer-term performance drifts.
- Providing increased visibility by monitoring all interfaces, including trunks, virtual interfaces and QoS levels.

Integration with Other nGenius Solutions

nGenius Analytics is fully integrated with NetScout's *nGenius* family, providing context to avoid the need to repeatedly recreate your research and analysis as you drill down into supplementary products for additional troubleshooting details. This condenses troubleshooting time and shortens MTTR.

From *nGenius* Analytics, network staff can easily drill down to *nGenius* Performance Manager for one-minute historical granularity on all applications, utilization, and conversation details of network activity.

If the problem is particularly troublesome and requires packet-level analysis of post-event incidents, for example, when trying to determine whether a financial transaction completed, or whether a retail transaction was completed in the inventory database, network staff can further drill down into *nGenius* Flow Recorder or *nGenius* Application Fabric Monitor for packet trace details.

Integration with Third-Party EMS

In addition, *nGenius* Analytics can forward its highly-qualified alarms to third-party enterprise management systems (EMS) such as HP OpenView and IBM Tivoli NetView for a consolidated, enterprise-wide view of network events. Alarm messages are embedded with plain-text descriptions and URLs that launch context-sensitive graphs into *nGenius* Analytics or *nGenius* Performance Manager for easy drill downs into additional details.

"*nGenius* Analytics epitomizes a product supporting the evolutionary progression of IT tools, encompassing increasing automated intelligence for networked applications monitoring and management. The advanced analytics in this NetScout product reduces the time to identify, diagnose, and properly repair networked application performance issues. This enables more efficient IT operations by reducing MTTR and freeing IT to perform strategic activities rather than firefighting, thus providing better support for corporate business services and enhanced capacity to develop new services for additional revenue streams"

Jeffrey Nudler, Senior Analyst, Enterprise Management Associates

Case Studies

Healthcare

A West Coast-based healthcare organization utilizing *nGenius* Analytics discovered an anomaly in their network which turned out to be the widespread download of virus protection updates during prime business hours. While the activity did not create an end-user affecting problem at that moment, the IT organization recognized the potential and used the incident to develop new internal update processes and procedures.

Transportation

A North American railroad leader tested *nGenius* Analytics on their core WAN circuits. Taking advantage of the product's unique capabilities, the company configured *nGenius* Analytics to monitor and detect performance issues on both physical and virtual network interfaces as well as for QoS classes carrying key business services. Using this capability, the company was able to prioritize the servicing of alarms in their top "Business Critical" QoS class for VoIP and mainframe applications running rail business services, over their secondary QoS classes for less critical traffic such as email and desktop management updates.

According to the senior network engineer, "Through *nGenius* Analytics, I've been alerted to weird activity that I probably wouldn't have known about before, such as updates during business hours. Having a tool that reports on anomalies, especially at the application layer is definitely a plus for our Network Optimization Team."

Financial Services

A leading payment processing company is interested in *nGenius* Analytics because they had previously had some problems that were very difficult to track down. They wanted to model their network over different volume periods and use that information to identify when things changed.

One recent problem they experienced, if caught sooner, would have prevented a more significant and costly problem. Service stations FTP a settlement file to the company every day. Over a period of time, this file was getting increasingly larger and consuming more bandwidth. By the time they caught the problem, it had manifested itself into a full outage. They realized that had they been using *nGenius* Analytics they would have been able to catch this "drift" problem by looking at link utilization on various size analysis windows and increased the network bandwidth in time to avoid a more serious problem.

Summary

NetScout's *nGenius* Analytics addresses IT infrastructure performance issues by automating anomaly detection and diagnosis, shortening mean time to repair, and enabling IT to better focus on improving corporate business productivity and profitability.

Lower MTTR. By automating the identification and diagnosis of network anomalies, *nGenius* Analytics significantly cuts troubleshooting time. Using Analytics' contextual drill down to *nGenius* Performance Manager, IT staff can unearth source addresses - who are the users, where are they located. Further drill down to *nGenius* Application Flow Monitor leads to packet-level analysis for packet trace details, such as ports, source and destination IP address identification.

Reduce TCO. One vendor, one solution. NetScout provides a comprehensive set of integrated solutions - *nGenius* Performance Manager, *nGenius* Analytics, *nGenius* Probes, and *nGenius* Application Fabric Monitor - that help IT maximize bandwidth consumption, understand and predict usage patterns, and more effectively troubleshoot issues to ensure maximum accessibility, performance and quality of network services.

nGenius Analytics also provides measurable productivity savings - enabling highly skilled IT staff to break the endless cycle of repeatedly setting and resetting thresholds, numbly chasing down false alerts, triaging the same problem affecting multiple virtual circuits and segments due to multiple alarms, and impetuously reacting to critical business-effecting issues. *nGenius* Analytics allows you to do it once with one alarm displaying all the affected segments.

Strategic Vendor Partner. In a time when physical links are growing to 10 Gigabit Ethernet and OC-48, the user community is expanding, and applications are becoming more complex and virtualized, you need a vendor focused on reducing costs, improving productivity, increasing network availability, and reducing overall MTTR. NetScout is an innovative and forward-looking vendor partner doing precisely that. In addition, we listen closely to our customers' requests and pay attention to changes happening in their environments and to the challenges those changes bring to managing performance.

Problem	*nGenius* Analytics Solution
Static Thresholds Setting static thresholds is like the Goldilocks of networking… set static thresholds too high and you don't see problems until it's too late. Set them too low and you're overwhelmed by false positives. What's needed is an automated system that gets them just right!	**Threshold-less Alarm Management** • Fully automates the baselining and thresholding processes, eliminating the need to manually set and reset static thresholds. • Self-learns your network's patterns of normal behavior and continuously updates the model • Increases alarm accuracy and reliability, reducing false positive alerts. • Reduces false positive alerts.
Too Many Alerts Relying on manually set static thresholds means the NOC can be forced to wade through hundreds, if not thousands, of alerts daily - most of them false positives.	**Intelligent Alerts** Our dynamic thresholding process alerts you to only those issues that need to be acted upon. • Automatically detects anomalies by comparing current network activities to continuously updated historical models. • Consolidates related alerts into a single intelligent alert. If 100 related DLCIs trip, you receive one intelligent alarm instead of 100 separate alarms! • Reduces false-positive alerts.
Missed Performance Issues Some problems can't be seen at all by static thresholds.	**Multiple Analysis Windows** • Monitors items that are otherwise too dynamic to monitor • Uses multiple analysis window sizes to detect different types of anomalies, including: - Sudden, short-term spikes - Sudden, sustained shifts - Long-term, prolonged drifts
Slow, Difficult Problem Diagnosis Typically most alerts lack the context needed for quick diagnosis of the underlying problem.	**Automated Diagnosis** *nGenius* Analytics speeds problem diagnosis and resolution, reducing MTTR. • Color-coded alerts instantly highlight which problems require immediate attention. • Problems are described in plain English. • One-click drill down to root cause analysis to guide and speed troubleshooting. • Early-warning indicators prevent impending failures.
Unproductive IT Staff Time The process of estimating baselines, setting and adjusting performance thresholds, and weeding through false trouble tickets is tedious, time consuming and unrewarding.	**Reduce IT Costs Dramatically** • Reallocate time saved on manual processes to more strategic work. • Speed problem diagnosis and resolution.

nGENIUS

The *nGenius* Performance Management System
The *nGenius* Solution addresses the complex requirements of network and application performance management in today's converged, virtualized environment and is comprised of:

- ***nGenius* Performance Manager:** Software that analyzes the information collected by *nGenius* Probes, Flow Collectors, Application Fabric Monitors, and other intelligent network devices and delivers integrated network and application monitoring, troubleshooting, capacity planning, and reporting in a single product.
- ***nGenius* Probes:** Dedicated hardware monitoring devices that passively identify, collect, and analyze application-level traffic data across the enterprise.
- ***nGenius* Flow Collectors:** Dedicated hardware devices that collect application conversation data via NetFlow records.
- ***nGenius* Application Fabric Monitors:** Appliances that combine *nGenius* Flow Recorder and *nGenius* Probe functionality for high performance, high reliability, high capacity recording and infrastructure monitoring.
- ***nGenius* Analytics:** Appliance-based software that delivers automated, proactive early detection and diagnosis of network and application performance anomalies.

NETSCOUT

Corporate Headquarters
NetScout Systems, Inc
310 Littleton Road
Westford, MA USA
Ph: 978.614.4000
Fax: 978.614.4004
www.netscout.com

European Headquarters
100 Pall Mall
London SW1Y 5HP
United Kingdom
SL1 4DX UK
Ph: +44 20 7321 5660
Fax: +44 20 7321 5663

Asia/Pacific Headquarters
Room 105, 17F/B, No. 167
Tun Hwa N. Road
Taipei, Taiwan
Ph: +886 2 2717 1999
Fax: +886 2 2547 7010

North American Offices
New York City, NY
Washington DC
Chicago, IL
San Jose, CA
Toronto, Ontario,
Montreal, Quebec

European Offices
Frankfurt, Germany
Paris, France
Oslo, Norway

Asian Offices
Beijing, China
Guangzhou, China
Hong Kong, China
Tokyo, Japan
Singapore
Pune, India