



Improving Service Delivery Performance  
*Using Predictive Intelligence to Prevent Network Meltdowns*

# Improving Service Delivery Performance

## *Using Predictive Intelligence to Prevent Network Meltdowns*

### Executive Summary

Today's modern IP network is fraught with increasing complexities. In some ways, virtualization in the data world is creating a new and special set of network challenges, and yet, on a basic business level the challenges remain essentially the same: organizations rely on today's modern IP network to not only support, but drive the business to meet its goals. Unfortunately, service-delivery slowdowns and outages are still all too common and frequently have a monumental impact on the ability of an organization to meet its goals.

In order to ensure that the business is operating at peak efficiency, IT professionals have turned to high-level service dashboards, key performance indicators (KPIs) and advanced analytical capabilities to preemptively recognize changes in service-delivery behavior. By recognizing these changes early, IT professionals are frequently able to prevent business-impacting problems before end users are affected and maximize service delivery performance and availability.

### Three Approaches to Problem Solving

There are three fundamental approaches to identifying, solving and avoiding service delivery issues: responsive, preemptive and preventative. An organization that uses all three approaches to managing service delivery is one that optimizes service delivery performance and availability. Understanding when, where and how to apply them is the key.

#### **Responsive Problem Resolution**

In many IT organizations, end user complaints to the help desk are still the most common means of discovering service delivery issues. The most common reason the help desk receives so many complaints is that traditional, threshold-based monitoring tools have not been optimized to detect the more subtle issues. Thresholds are usually set at high water marks and consequently don't detect problems until they are critical, even though users can be affected well before that time. Or, they are set too low and inundate IT with alerts that just get ignored.

The problem with end user complaints to the help desk is that by the time they call and IT is made aware of the situation, things have reached a certain level of urgency—users are impacted, the business is affected, and IT must go into crisis mode to resolve the issue.

Imagine this situation... what if the vice president of sales called the help desk to complain of poor VoIP quality while he was talking to a key account? When IT does not have advanced warning of problems, all the help desk operator can respond with is, "Oh, you're having a problem? We'll get right on it."

While reactive troubleshooting is a valid and integral component of managing service delivery—after all you can't possibly predict and prevent all service delivery issues—using only this "break and fix" approach can be costly to IT and the business. Minimizing the number of incidents and being aware of issues as they are occurring can go a long way to improving end user productivity and satisfaction. In addition, constant firefighting can leave IT with little time for problem avoidance and overall network efficiency and evolution initiatives.

#### **Preemptive Problem Resolution**

Increasing visibility into the service delivery environment allows users to move from the responsive or reactive model to a more preemptive paradigm. Implementing tools and technologies that provide end-to-end visibility for capacity planning, tuning and optimizing the service delivery environment can improve the perspective of the IT team while at the same time more effectively support the business.

End-to-end visibility enables the IT organization to:

- Proactively combat network congestion by reporting on bandwidth growth and forecasting capacity shortfalls
- Understand and report on which applications consume your network resources in order to postpone upgrades and justify growth and policy decisions
- Tune traffic to optimize resources by identifying over- and under-utilized segments for redistribution and load balancing
- Baseline and monitor current traffic patterns to ensure all applications can be supported, even during peak activity periods
- Baseline application responsiveness to set meaningful thresholds that properly reflect service levels

These activities enable IT to better understand the total service delivery environment and to preemptively take action to avoid many common problems that can often impact end user performance.

Let's revisit the previous example except this time the IT team has implemented proactive monitoring of key performance indicators (KPIs) for critical business applications, including VoIP. By monitoring the KPIs on VoIP and setting appropriate thresholds that trigger at the point just prior to when user performance is impacted, the IT team receives notification response time for the VoIP application is degraded.

Based on this information the IT team quickly moves to diagnose the reason for the change by examining the conversations, hosts, and worst performing servers to find the root cause. While examining the problem, the condition continues to worsen and begins to impact performance. At the same time, the Sales VP is unable to talk with his customer and calls the help desk. Now, instead of getting an unsatisfactory response from the IT team, the help desk operator can respond with, "Yes sir, we are aware of the problem and we should have it fixed momentarily." Although the end user is still impacted, the length of time that the business is affected is shortened because the IT team was able to start working earlier in the process.

**Prevent Problems with Predictive Intelligence**

The third approach to managing service delivery builds on the preemptive management methodology to provide predictive capabilities that provide sufficient notice, enabling the IT organization to actually diagnose and fix the problem before user performance is significantly impacted.

This is done through the use of:

- Dashboard views that provide easy-to-interpret status of service health
- Key performance indicators that correlate user experience with network and application health to more closely align IT operations with business priorities
- Automated anomaly detection that provides early notification of potential problems before they turn into full-blown service meltdowns.

Understanding the connection between network elements, applications and the users in the context of "IT services" via a service-aware dashboard is fundamental to the success of the business. IT professionals who view the service delivery environment and the business as interdependent have also realized that if the service delivery environment falters or fails, the business suffers.

Let's take a final look at the VoIP problem the Sales VP was having... In this instance, the network manager receives an automated analytics alert that indicates there is significantly more jitter (a KPI metric) than normal for the VoIP service. Even though the jitter hasn't yet reached the point where threshold-based alerts are triggered, the analytics engine is able to detect these more subtle changes and flags it as a potential or brewing problem. Because the network manager received notification so early in the cycle, he was able to diagnose and fix the issue before his users noticed anything unusual.

**Terminology**

**Key Performance Indicators**

Key performance indicators or KPIs refer to the metrics that allow IT professionals to ensure that users are able to access the network services and applications they need in order to support their company in meeting business goals. KPIs provide essential information for:

- Monitoring response time and understanding if the response time falls within acceptable parameters
- Generating alarms against certain error codes, providing visibility into HTML errors for Web-based applications
- Determining if client or server errors exist and looking at the success rate for applications or services, providing IT with an indication of where potential problems may exist
- Providing an understanding of the quality of voice or multicast applications by evaluating packet loss measurements

NetScout defines key performance indicators for both data and voice applications, but how the data is presented and interpreted varies between data and voice applications as shown in Figure 1.

Data Applications	Voice Applications	
Slow Responses	High Jitter	How often an application exceeds and acceptable responsiveness threshold
Timeout	Max Jitter	How often an application is not available
User Events		Application-specific client errors
Packet Loss	Packet Loss	An indication of dropped packets in IP multicast applications and voice applications

**Figure 1**

In the case of our sales VP, he goes on to close the deal and is blissfully unaware that there was even a problem brewing. That's the capability that predictive analysis provides—preventing service delivery issues before they affect the business. And, fewer calls to the help desk.

**Optimizing Services**

There are several business challenges that most, if not all, of today's CIOs struggle with on a regular basis. They include aligning IT operations more closely with business goals and priorities, enhancing cross-team collaboration, and improving IT productivity and effectiveness. Of course, the ultimate end goal of IT is to optimize service delivery availability and performance to ensure the business functions as efficiently as possible.

### Creating Business Services that More Closely Align IT Operations with Business Priorities

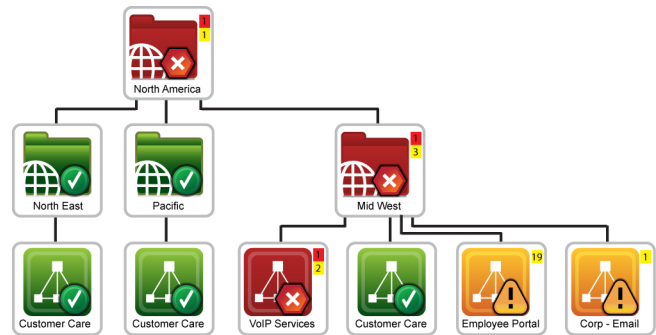
There are a handful of applications or services that are essential to driving any business. If you are a manufacturer, critical applications might include customer relationship management (CRM), supply chain management (SCM) or manufacturing execution systems (MES). For a retailer, the essential services probably include point of sale (POS), human resource management or accounting software, among others, and hospitals rely on applications like electronic billing and medical records management, and picture archiving and communications systems (PACS). Some services are limited to certain geographies such as mid-west fabrication, or HQ payroll. The point is that the applications and services that drive a business vary by company and industry, but all companies have several applications or services that can bring it to a virtual standstill when they are inaccessible. Ensuring that IT minimizes downtime by prioritizing degradations and outages of these essential services and applications over less critical services helps align IT operations more closely with business goals and keeps the organization running at maximum efficiency.

One of the ways in which IT can more closely align with business priorities is to monitor the actual business services rather than the individual applications and protocols that comprise the service. For example, monitoring a single business service called “converged VoIP” can provide much more meaningful and actionable observations than monitoring the individual VoIP-related protocols (SIP, SCCP, RTP, etc.) necessary to set up and maintain a digital phone call (Refer to Figure 3). The idea behind creating and monitoring service views is that both IT staff and business managers can immediately understand the status of essential services, which enables them to prioritize actions based on that service’s impact on the business.

### Enhancing Collaboration

Creating key business services and monitoring their status with at-a-glance dashboard views improves visibility into the health of these critical services. Unified views support an end-to-end workflow consistent with how service delivery behaves—this improves cross-functional collaboration and enables process improvements.

Using role-based access and authentication puts these business service views into the hands of IT staff and business service owners who are not normally users of service delivery management solutions, providing focused, relevant information



**Figure 2: Creating and monitoring business services by aggregating related applications and network services into a single icon provides a business-relevant view that enables immediate understanding of overall service performance. This helps prioritize actions based on the impact to the business.**

Service	Application	Network Services (Protocol)
E-Mail	Microsoft Office Outlook, web-based e-mail	SMTP, POP, MIME and IMAP
E-Commerce	Electronic Data Interchange (EDI)	HTTP/HTTPS, SSL, DNS
Voice	Softphone, IP Phone	SIP/RTP, SCCP, H.323, Skype

**Figure 3**

## Defining Services, Network Services and Applications

NetScout defines and refers to “services”, “network services” and “applications” distinctly and specifically, with each having a particular meaning. Examples are listed in figure 2.

**Service** – the combination of network services and applications that work in unison over the network infrastructure to deliver a business function to the end user.

**Application** – software-based tools that are operated by means of a computer or internet protocol-based device, which supports or improves the user’s ability to meet business goals.

**Network service** – commonly referred to as a protocol, provides the foundation of a network computing environment. Network services are primarily installed on one or more servers to provide a shared resource to client computers into the exact services that these groups are interested in and responsible for, as well as one-click, contextual drill down into all relevant supporting details and reports.

Business service views bridge the network and application silos as well as technology and business worlds by providing consistent and unified views that:

- Provide management with easy-to-interpret summaries of the performance of business services necessary to running the business
- Give business managers and application managers focused visibility into the performance of the applications essential to their job and bringing up only focused, relevant troubleshooting information on drill down
- Facilitate help desk handoff to the right team on the first try through the use of detailed alerting and root cause analysis, streamlining troubleshooting
- Provide the networking team with visibility to instantly laser in on problem areas by focusing on the key applications or services that drive the business and leaving issues affecting non-business critical applications to be investigated when time permits

#### **Improving IT Productivity & Effectiveness**

IT managers are especially concerned with how to get more work accomplished with the same, or even less, staff. Streamlining the problem resolution processes is one effective way to improve IT productivity. By reducing the time spent on problem identification and root cause analysis, the IT staff can complete more events in the same amount of time or it can free up personnel for problem avoidance and planning activities.

Contextual drill down to progressively deeper levels of detail—starting from top-level service health views based on key performance indications, to traffic flows, to in-depth packet level analysis—streamlines and focuses the problem resolution process. The result of this highly efficient, top-down workflow is accelerated problem isolation across the entire IT organization.

#### **Leveraging the nGenius architecture**

The nGenius® Service Delivery Manager is a software application that resides on the nGenius Performance Manager server and applies its patented, statistical behavior modeling and anomaly detection to the same packet flow data collected by nGenius Probes and nGenius InfiniStream® data sources strategically deployed throughout the network.

The nGenius Service Delivery Manager dashboard views provide early notification of abnormal changes in traffic behavior that may indicate emerging issues, giving IT organizations a real chance of catching issues at their earliest stage of development when there is an opportunity to prevent service-affecting performance degradations or system outages.

The nGenius Service Delivery Manager software helps an IT organization evolve from a proactive mode of addressing business- impacting issues to a predictive and preventative model by delivering:

- At-a-glance, dashboard views of the health of the unified service delivery environment, bridging the gap between network and application management, and simplifying and assuring service delivery
- Advanced health metrics (KPIs) to monitor responsiveness, errors and packet loss, enabling preemptive problem detection from an end user experience perspective
- Intelligent alerting that forecasts changes in behavior when preemptive actions have the chance to prevent service degradations and outages; also provides root cause analysis to streamline problem diagnosis
- Identification of service delivery threats such as BotNets, spyware and other types of attacks
- Verifies compliance and alerts on violations to defined IT policies such as use of restricted applications or unauthorized access to a subnet or specific server
- Virtual network flow maps that graphically illustrate each application's flows across the network to help pinpoint where problems are occurring
- Workflow-based drill down from top-level service health, to traffic flows, to in-depth packet-level analysis, enabling streamlined problem isolation across the entire IT organization
- Support for Web-enabled mobile devices for anytime, anyplace access to real-time service delivery management data
- Self-monitoring of the nGenius instrumentation, their associated processes, and interface alarms to quickly diagnose and resolve any issues with the nGenius solution itself

#### **Managing service delivery with the nGenius Service Delivery Manager software**

The nGenius Service Delivery Manager software addresses the challenges of real-time service delivery management by providing an at-a-glance status of business service health using a simplified, Web-based dashboard that monitors business services, not simply individual applications or protocols. By aggregating related applications and protocols to provide business-relevant views of services, the nGenius Service Dashboard view can be used across the IT organization to immediately understand service health and more closely align the operating environment with critical business services and priorities.

The consolidated Service Dashboard combines KPI alerts and analytics alarms and directly correlates with end user experience to provide an understanding of how services compare to expected service levels. From a service delivery perspective, KPI metrics provide essential information for:

- Monitoring response time and understanding if the response time falls within acceptable parameters
- Determining if client or server errors exist and looking at the success rate for applications or services, providing IT with an indication of where potential problems may exist
- Providing an understanding of the quality of voice or multicast applications by evaluating packet loss measurements

The simple Web dashboard allows IT to quickly identify which applications and services have been experiencing problems and for how long. It also provides the basis for streamlining and accelerating the diagnosis process. One-click drill downs lead to contextually appropriate and relevant:

- Service Summaries—provide more in-depth data visualization for faster diagnosis of service delivery issues
- Flow Maps—graphically illustrate the application flow and its status across the enterprise to quickly isolate where in the network service delivery problems are occurring
- Alert Lists—display service-specific KPI and analytics alerts, as well as nGenius Performance Manager basic threshold alarms

**Automated anomaly detection prevents service delivery problems with predictive visibility**

The nGenius Service Deliver Manager combines KPI monitoring with automated anomaly detection to predict and prevent service delivery problems by allowing system users to be notified of abnormal changes in service traffic, even before they reach set thresholds. The benefits of using the advanced analytics technology are two-fold—It provides warning of emerging problems significantly sooner than static threshold-based methods and it recognizes anomalies that are too subtle to be detected manually due to the complexities of the modern IP network. The result of this early warning notification is that performance degradations and potential service delivery meltdowns can often be prevented or avoided before they become service affecting.

The nGenius analytics engine automates the analysis of network behavior and relationships to identify anomalous behavior. The system continuously learns network activity to build a baseline of “normal” behavior and then compares the current traffic to the historical model to identify changes in performance outside expected behavior ranges. It helps answer questions such as:

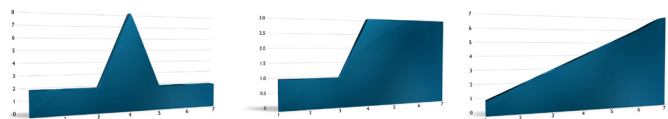
- Is the behavior typical for a Wednesday afternoon?
- How does this behavior compare to yesterday afternoon?
- How does this behavior compare to last Wednesday?

By comparing current network and application activities to its historical models, the analytics engine can detect rising and falling patterns for

- Physical and virtual link utilization
- Application utilization
- Application responsiveness as monitored by KPI metrics
- VoIP jitter

The analytics engine can identify different types of changes in behavior, as shown in figure 6, including:

- Spikes or sudden changes that are short lived. Spikes are often attributed to temporary issues like FTP downloads or backups at the wrong time of day, streaming music or video, illegal peer-to-peer file sharing, and so on.
- Shifts or sudden changes that are sustained and become the new “normal.” Shifts can be caused by the introduction of viruses and botnets, or by adding new applications and users to the network.
- Drifts or slow but steady changes are difficult to discover manually. They are typically caused by small, regular increases or decreases in normal behavior.



**Figure 5: The analytics engine in the nGenius Service Delivery Manager software can identify different changes in behavior, including “spikes,” “shifts” and “drifts.”**

**Action-oriented alerting accelerates problem identification and resolution**

Once anomalous behavior is detected, nGenius Service Delivery Manager simultaneously generates an intelligent alert that contains root cause analysis and updates the service dashboard to reflect the change in service status. Root cause analysis accelerates and streamlines problem diagnosis by correlating anomalous behavior to offending applications and links and by providing context about what was happening on the network at the time of the incident.

User	Primary
IT Management	Functions as management summary; provides insight into business services status
NOC Operators/Network Engineers	Provides early warning of brewing problems to prevent business-impacting issues; Enables faster problem identification and resolution for more predictable business services
Application Developers	Provides early warning of brewing problems to prevent business-impacting issues; Enables faster problem identification and resolution for more predictable business services
Help Desk Operator	Helps assess problems for hand-off to the appropriate operations team on the first try
Business Managers	Gives business managers visibility into the performance of applications essential to running their business

**6 Figure 4: Visibility is critical to many parts of the organization. However, primary product usage depends on the role of the user.**

The evidentiary details include time, monitored interface/circuit, severity, and a description of the applications and the cause of the alert. Graphical chart views summarize the information captured when the alarm was triggered. Because the nGenius Service Delivery Manager software is seamlessly integrated with nGenius Performance Manager, users can click on the evidentiary graphs to drill down into nGenius Performance Manager for additional interactive troubleshooting views.

All alerts are posted to the nGenius alert list, which contains a summary panel and interactive filtering section in addition to the list of alerts. The alert list not only displays analytics and KPI alerts, but can also display other nGenius Performance Manager alarm types, such as power, device and basic threshold alarms, for consolidated event management.

The alert list groups related incidences together into a cascading alert to minimize the number of alerts IT staffs need to investigate, freeing them to spend more time focusing on other priorities.

In addition, nGenius alerting can be sent via email or SMS to deliver status updates to browser-based mobile devices for anywhere, anytime access or to third-party business service management (BSM) solutions for services-aware, consolidated fault and performance management with contextual drill down.

#### Integration with third-party business service management solutions

Just as with nGenius Performance Manager, nGenius Service Delivery Manager alerts can be forwarded to third-party business service management solutions for services-aware, consolidated fault and performance management. See Figure 6 for a list of supported BSM solutions.

NetScout Technology Partner	Solution
HP®	Network Management Center (NNM and NNMi) Business Availability Center (BAC) Operations Center
IBM®	Tivoli® NetCool®/OMNibus Tivoli NetView® Tivoli Enterprise Console (TEC)

Figure 6: Third-party BSM integration partners and solutions.

#### Service Summaries

In the nGenius Service Delivery Manager software, the consolidated service view provides a high-level perspective of how the services are running. These services are configured by the user to align with the needs of the business. If a particular service is regional, it can be defined as such. If multiple applications make up a single business service, again they are combined into a single entity. When a service is impacted, it will display as red on the dashboard to alert the administrator and accelerate the problem diagnosis and resolution process.

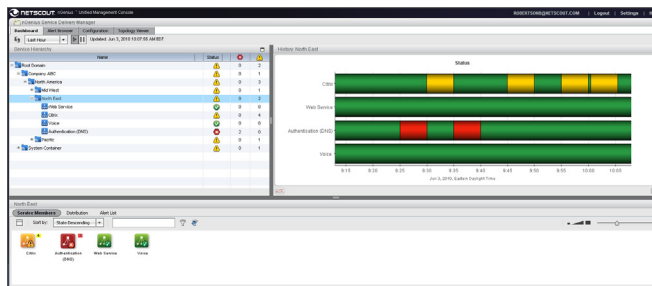


Figure 7: The consolidated services view provides an at-a-glance view of how services are performing.

One-click, contextual drill down into all relevant supporting service- or application-focused performance details and reports has the added benefit of bridging the network and application teams by providing consistent and unified views and simplifying and guiding access to this information.

Source	Available Charts
Application	<ul style="list-style-type: none"> <li>Response Time Distributions Over Time</li> <li>Number of Responses Over Time</li> <li>KPIs Over Time</li> <li>Worst Performing Servers Snapshot</li> <li>Worst Performing Locations Snapshot</li> <li>Service State Over Time</li> <li>Application Usage Over Time</li> </ul>
Interface	<ul style="list-style-type: none"> <li>Response Time Distributions Over Time</li> <li>Number of Responses Over Time</li> <li>KPIs Over Time</li> <li>Worst Performing Servers Snapshot</li> <li>Top AL Conversations Snapshot</li> <li>Application Usage Over Time</li> <li>Link Usage Over Time</li> </ul>
Server	<ul style="list-style-type: none"> <li>Server Response Time Over Time</li> <li>Number of Responses Over Time</li> <li>Number of Clients Over Time</li> <li>Worst Performing Flows Snapshot</li> <li>Top AL Host Usage Over Time</li> </ul>

Figure 8: The service summary charts and tables displayed for the selected application service and interface or server in question.

Each summary page displays different charts depending on whether it is associated with an application service, an interface, or a server. See Figure 8 for a list the charts and tables displayed for the selected application service and interface or server.

Service summary charts providing additional analysis capabilities through the ability to:

- Toggle between a logarithmic and linear y-axis
- Add forecast lines to charts
- Toggle between chart and table formats

In addition, most charts and tables provide one-click drill down to corresponding views in the Performance Manager console for continued troubleshooting by viewing additional charts, tables, and packet details.

### Services flow maps

The nGenius Service Delivery Manager service map shows the virtualized flow topology for a selected application service by displaying the nGenius Probes, InfiniStream appliances, and server groups that have detected the specific application under scrutiny. The service map can be displayed graphically or in grid format for very large networks to provide an indication of the segments where anomalies occurred.

Selecting and clicking on a specific interface icon launches an application and interface-specific view of the service summary or alert list and provides contextual drill down to the nGenius Performance Manager console for additional analysis.

### nGenius self-management capabilities

The nGenius Service Delivery Manager status dashboard contains icons for specialized services that monitor and report on the nGenius performance management environment itself.

The status of these processes indicate the health of the nGenius servers or data source devices and provides the information necessary to quickly diagnose and resolve any operational issues within the nGenius system, streamlining the process and reducing total cost of operation.

### Summary

The nGenius Service Delivery Manager software leverages your underlying investment in nGenius technology to address today's modern-day challenges of real-time service delivery management. The dashboard views provide early notification of abnormal changes in traffic behavior that may indicate emerging issues to give IT organizations a real chance of catching issues at their earliest stage of development when there is an opportunity to prevent service-affecting performance degradations or system outages.

The nGenius Service Delivery Manager software helps IT organizations assure the availability and performance of their service delivery environment by:

- Defining monitored services to align with the needs of the business and track the services that are important
- Reducing end user calls to the help desk by identifying and addressing problems significantly sooner—before they become business-affecting meltdowns
- Accelerating the problem resolution process by quickly pinpointing the area and root cause of problems
- Minimizing the impact an outage or degradation has on your critical business services and applications and therefore minimize its impact on your bottom line
- Optimizing the availability, performance, and effectiveness of your critical business services and applications

Additionally, the nGenius Service Delivery Manager software provides unified, end-to-end service views that transform performance data into actionable information for NOC operators, service managers, network engineers, application managers, IT management and business managers alike, providing the additional benefits of:

- Enhancing cross-team collaboration
- Increasing operational efficiency and productivity
- Decreasing network operational costs

### Ordering Information

The nGenius Service Delivery Manager software is installed with nGenius Performance Manager but is enabled through a separate license. The number of licenses required on the nGenius Service Delivery Manager software must match the number of licenses installed for nGenius Performance Manager for each server instance.

### For More information

**For more information please visit [www.netscout.com](http://www.netscout.com) or contact NetScout sales at 800-309-4804 or +1 978-614-4000**

© 2009-2010 NetScout Systems, Inc. All rights reserved. NetScout, nGenius and InfiniStream are registered trademarks and the NetScout logo is a trademark of NetScout Systems, Inc. and/or its affiliates in the United States and/or other countries. HP is a registered trademark of Hewlett-Packard Development, IBM, Tivoli, NetCool and NetView are registered trademarks of IBM Corporation. All other brands and product names, and registered and unregistered trademarks are the sole property of their respective owners. NetScout Systems, Inc. reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, and service and support programs.



#### 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

One Canada Square 29th floor  
Canary Wharf  
London E14 5DY  
United Kingdom  
Phone: +44 207 712 1672

#### Asia/Pacific Headquarters

Room 105, 17F/B, No. 167  
TunHwa N. Road  
Taipei, Taiwan  
Phone: +886 2 2717 1999