



Achieving 360 Degree Network Visibility with Nimsoft

Table of Contents

Introduction	3
Complete IT Infrastructure Monitoring	4
Cloud-Based Networks	5
Comprehensive Network Coverage	6
Networks and Devices.....	6
Automated Network Topology Creation and Root Cause Analysis	6
Flexible Topology Views.....	7
Easy Topology Customization.....	7
Root Cause Analysis.....	8
Sophisticated Dashboards and Reporting	9
Real-Time Dashboards of IT and Business Services.....	9
Real-Time Alarm Console	9
Performance Trend Reporting	9
SLA Creation, Monitoring, and Reporting	9
Flexible, Reliable Notification	10
Integration with Third-party Network Management Systems.....	10
Conclusion	10

Executive Summary

360° network visibility is critical for ensuring continuous availability of networks, servers, and applications—anything less could have costly bottom-line implications. This paper details how the Nimsoft Monitoring Solution (NMS) equips network administrators with the vital insights they need to proactively and effectively govern IT infrastructures and ensure continuous availability of servers and applications—whether they are managed locally or in the cloud.

Introduction

Today's enterprise and service provider networks can be extremely complex and constantly changing. With so many interdependent systems, processes, and services—all of which are critical to business users—comprehensive, continuous monitoring is essential. How do administrators gain a 360°, real-time, and intuitive view of their IT infrastructure, so they can effectively govern these complex ecosystems?

As part of the Nimsoft Unified Monitoring™ architecture, the Nimsoft Monitoring Solution (NMS) delivers the visibility needed to monitor and manage performance across all IT environments, including public and private clouds, SaaS deployments, distributed networks, and internal datacenters.

NMS represents a comprehensive, easy-to-use solution that enables network administrators to deliver the highest levels of service quality. Business users benefit from dashboards that provide a real-time view of the availability and performance of mission critical applications and services. Comprehensive reporting provides IT management with a deep understanding of network, application, server, and database performance.

NMS features:

- **Complete IT infrastructure monitoring.** NMS allows administrators to efficiently monitor and optimize performance and availability of their IT infrastructure.
- **Comprehensive network coverage.** NMS monitors access and response times for all network devices, servers, applications, and service ports.
- **Automated network topology creation.** NMS automates the entire process of defining an extensive topology—delivering intuitive, visual diagrams of the entire IP network, including layer 2 and 3 traffic.
- **Advanced root-cause analysis.** NMS offers root-cause analysis capabilities that enable fast detection of the source of a network issue, and that eliminate the false alarms that may otherwise result from devices “downstream” from a downed system.
- **Sophisticated dashboards and reporting.** NMS makes it easy to leverage the data gathered to gain valuable and timely insights, featuring flexible graphical dashboards and performance and SLA reporting.

NMS makes it faster and easier for administrators to identify and address a host of issues:

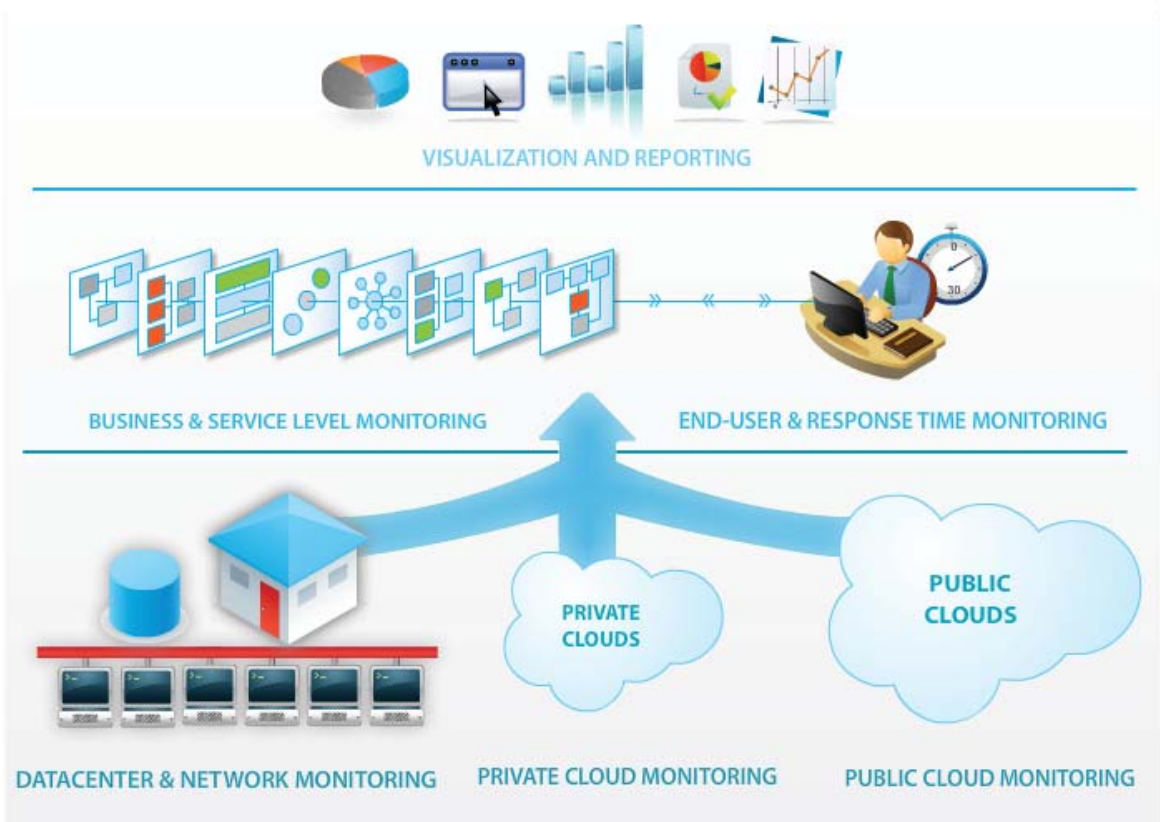
- **Broken network and application connectivity links**
- **Excessive network latency**
- **Network device degradation and failure**
- **Network interface degradation and failure**
- **Excessive bandwidth utilization**

In the following pages, we detail each of these capabilities.

Complete IT Infrastructure Monitoring

Nimsoft Unified Monitoring provides a flexible architecture for comprehensive monitoring of any device—whether it resides in a local datacenter or in the cloud. Leveraging the Unified Monitoring architecture, NMS allows administrators to efficiently monitor and optimize performance and availability of their IT infrastructure including:

- **Cloud.** NMS enables IT managers to monitor private and public cloud instances on the same dashboard, eliminating the need for multiple monitoring solutions.
- **Virtualization.** NMS enables administrators to monitor and fully optimize their virtual environments, featuring solutions for all major server virtualization vendors, including VMware, Microsoft, Citrix, IBM, and Sun.
- **Applications.** With NMS, organizations can monitor all their critical applications, including: Microsoft Exchange, Active Directory, and IIS; Lotus Notes; SharePoint; VoIP; Citrix; WebSphere; and many others.
- **Servers.** NMS offers monitoring support for iSeries AS400, Netware, Linux, Windows, and UNIX servers—all from a single, easy-to-use console.
- **Databases.** NMS provides real time and comprehensive database health check monitoring for Oracle, Microsoft SQL Server, Sybase, MySQL, DB2, Informix, and more.
- **Networks.** NMS delivers comprehensive monitoring coverage of the entire network infrastructure, including Cisco IPSLA and QoS; DNS, DHCP, and TCP; SNMP; routers and switches; and traffic.

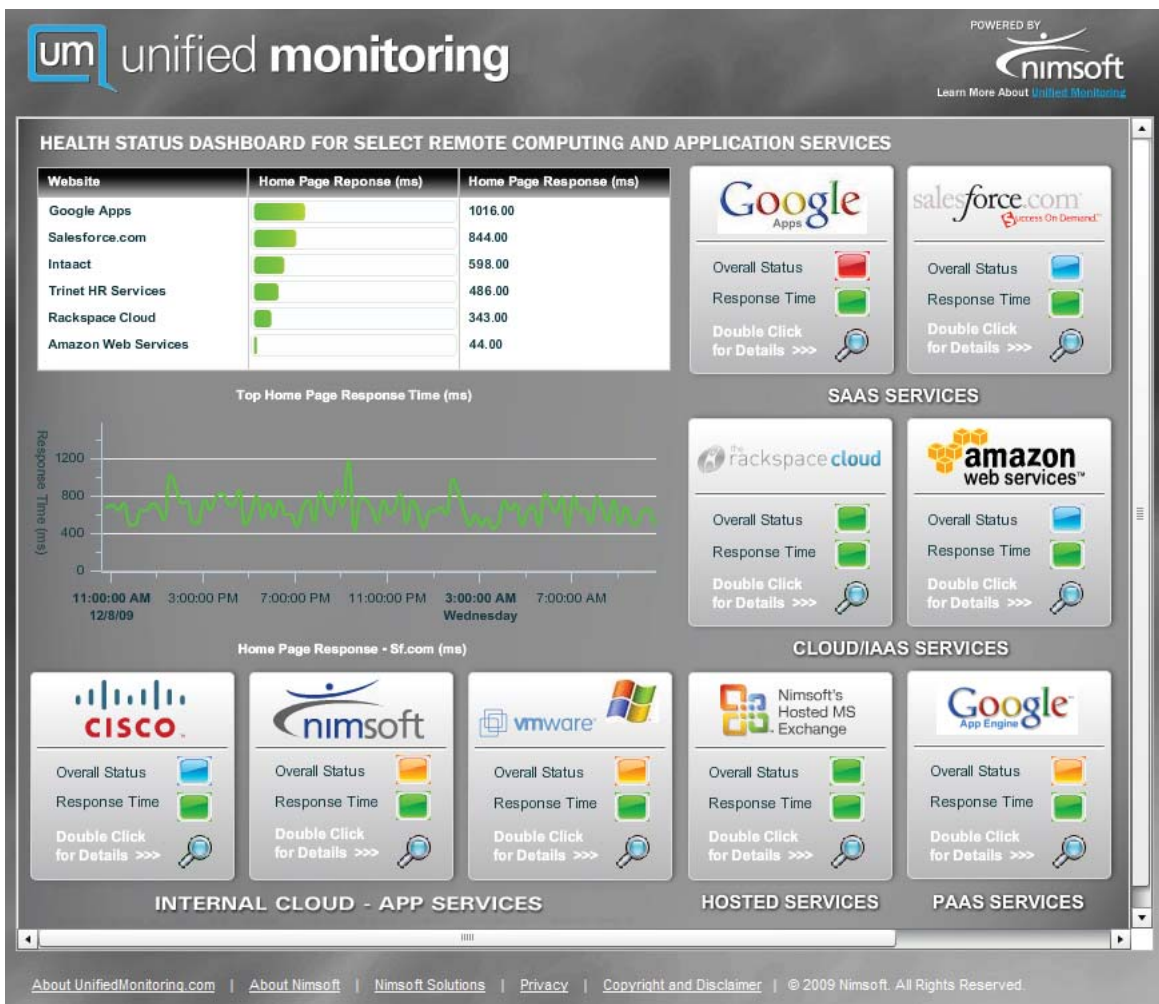


Today's business applications are running on SaaS, cloud, and managed environments, as well as in virtualized environments and the legacy datacenter. NMS delivers the visibility needed to monitor and manage performance across all these environments.

Cloud-Based Networks

NMS scales and extends to monitor the evolving, internal datacenter, including private clouds. Further, NMS enables IT managers to monitor these public cloud deployments:

- **Infrastructure as a Service (IaaS).** NMS provides complete monitoring of the key performance benchmarks of public IaaS services, including Amazon and Rackspace.
- **Platform as a Service (PaaS).** With Nimsoft, administrators can monitor the availability and performance of PaaS services, such as Microsoft Azure or Google App Engine.
- **Software as a Service (SaaS).** NMS offers the availability and performance measurement capabilities users need to understand and manage their key SaaS services, including cloud offerings like Salesforce CRM and Netsuite.



NMS provides detailed performance metrics of all of the components of a business service, regardless of whether it is located internally in the data center or externally in the cloud.

Comprehensive Network Coverage

Networks and Devices

NMS features a broad set of capabilities that enable organizations to monitor all the network connections and devices across their internal network, including the following:

- **Network and application connectivity.** NMS features connectivity monitoring for routers, switches, servers, applications, printers, and practically any other network-enabled device. NMS features a specialized probe that uses the ping command (ICMP ECHO) to verify network connectivity between the host where the probe resides and the targeted remote system. The probe can also test connectivity to TCP-based services, including Telnet and HTTP, as well as any other application with a designated service port.
- **Interface traffic.** NMS offers capabilities for monitoring the network interfaces on PCs, Windows and UNIX servers, routers, switches, and other SNMP-enabled devices.
- **Cisco devices.** NMS can use SNMP to proactively monitor and collect performance data from Cisco routers and switches. NMS also support Cisco IPSLA configurations, monitoring such protocols and services as DHCP, DNS, ICMP, FTP, HTTP, SNA, UDP, and TCP. Finally, NMS enables administrators to monitor and analyze trends on a number of Cisco QoS metrics.
- **SNMP.** NMS can monitor any standard or proprietary MIB object from any SNMP-compliant device. NMS can also monitor all SNMP-enabled routers, switches, servers, and printers. It can report on a variety of error conditions in the form of SNMP “traps”, and it can monitor networks to provide views of all SNMP traps generated on the network.
- **Syslog.** NMS can monitor any device that uses the well-known Syslog format, including routers, switches, firewalls, and UNIX servers.

In each of the areas above, NMS leverages all vital monitoring metrics generated, ensuring network administrators can harness the comprehensive and deep network coverage they need to monitor and manage network performance effectively.

Automated Network Topology Creation and Root Cause Analysis

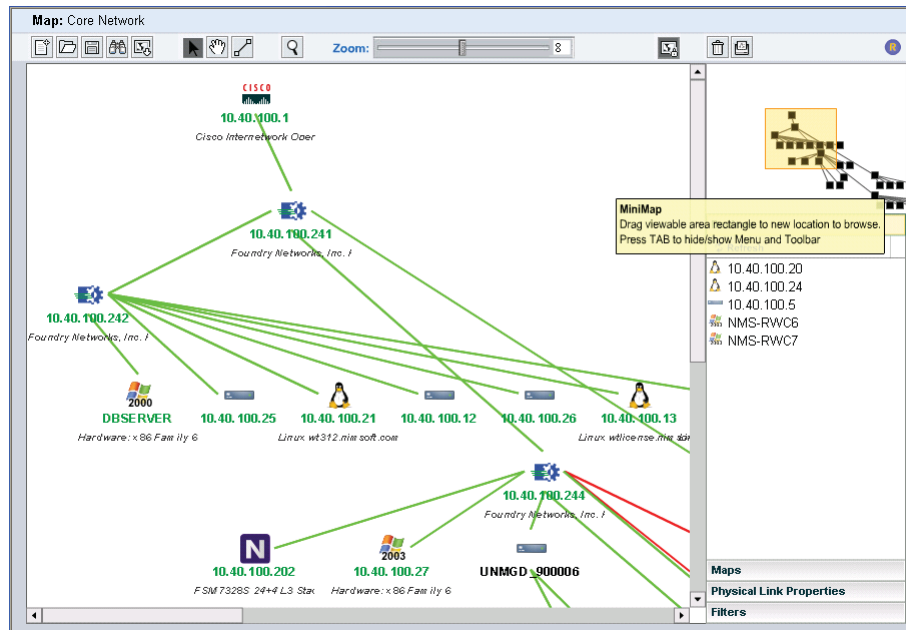
NMS features the Nimsoft RCA and Topology Manager—a simple, yet powerful additional module. RCA and Topology Manager automates the process of network topology definition and produces intuitive, visual diagrams of the entire network. With RCA and Topology Manager, administrators can gain a unified, real-time view of their dynamic, distributed networks and more effectively optimize performance and availability. RCA and Topology Manager offers the following capabilities:

- Automated discovery of node connectivity and dependency relationships.
- Complete mapping of large, complex networks.
- Flexible topology customization, featuring drag-and-drop modification and graphic integration.
- Regeneration capabilities incorporate recent network changes, ensuring topologies remain current.

RCA and Topology manager offers these features:

- **Root cause analysis through real-time polling and topology maps.**
- **Monitoring intelligence that eliminates false alarms and streamlines troubleshooting.**
- **Multi-tenant functionality for segregating and viewing large networks.**

With RCA and Topology Manager, administrators get visual clarity into network relationships so they can more rapidly perform network enhancements, additions, and repairs. RCA and Topology Manager discovers physical connectivity and dependency relationships among all network devices and servers on a network—including distributed networks and “non-managed” devices such as hubs, “dumb” switches, and non-SNMP devices.



Nimsoft RCA and Toplogy Manager automatically creates and updates network topologies, making it easy for administrators to view and manage their complex networks.

This solution provides an intuitive user interface for viewing the hierarchical structure of large, complex networks, and it automatically regenerates topologies to reflect any changes that have been made to the network—so administrators are always assured of getting current views of the network.

RCA and Topology Manager enables administrators to generate topologies maps automatically, based on a specified time period, and delivers a network topology that is accurate and current. As a result, it eliminates the time-consuming, error-prone process of manually detecting the interconnectivity of each node on a given network in order to build topologies. In addition, it delivers reports on the discovery process, generating such statistics as duration of run, current status, root topology node, number of bridges/hosts, any errors, and more.

Flexible Topology Views

RCA and Topology Manager equips administrators with a range of capabilities for tailoring topology views to specific environments. For example, the product offers “mini-map” navigation, drill-down capabilities, zoom controls, “accordion” menus, and a host of other features for navigating and viewing even the largest, most complex topologies.

Easy Topology Customization

RCA and Topology Manager provides a range of features for customizing existing topologies, enabling administrators to...

- Drag and drop elements on the canvas.
- Manually draw or edit dependencies and connections between entities.
- Integrate custom background images and diagrams.
- Leverage a library of geographic maps to tailor to specific locations.

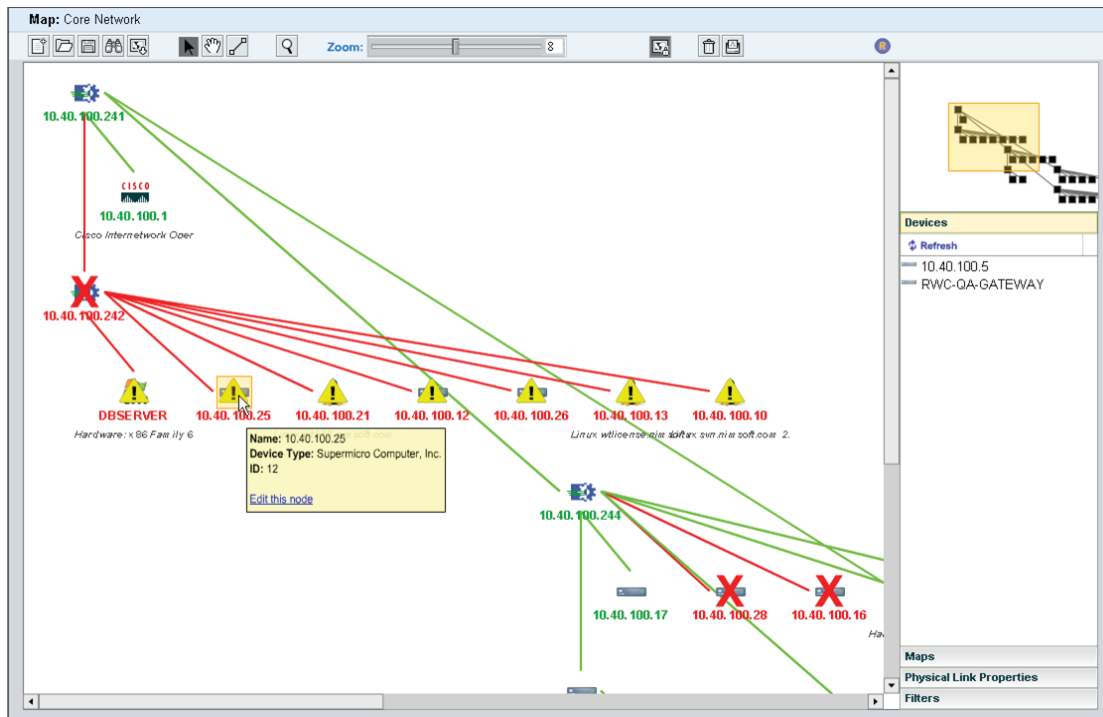
Root Cause Analysis

Within many enterprise networks today, one system outage can generate a flood of alarms, pages, and emails, as all the systems “downstream” from the impaired device may trigger a breach in monitored thresholds. The end result is that administrators have to sift through a lot of “noise” in order to identify the root cause of the issue.

RCA and Topology Manager offers sophisticated root-cause analysis (RCA) capabilities that simultaneously enable faster discovery of the source of a network issue—while significantly reducing unnecessary and redundant alarms.

RCA and Topology Manager offers the intelligence to identify the device that is the root cause of a network issue and determine which additional systems may be affected by the outage. As a result, RCA and Topology Manager eliminates the distraction of false or redundant alarms and delivers the insights administrators need to identify and address network issues in a timely manner.

Leveraging capabilities for real-time polling and a specified topology map, RCA and Topology Manager analyzes all paths from the monitoring station to an affected node to identify the root cause of an issue and to suppress notification of alerts for those nodes that may trigger alarms due to their relationship with the downed device. In addition, RCA and Topology Manager can be configured to take into account such factors as maintenance windows, the managed state of a device, and the detailed topology map to offer even better insights into network analysis and remediation.



RCA and Topology Manager offers the intelligence to identify not only the device that is the root cause of a network issue, but also which “downstream” systems will be affected.

Sophisticated Dashboards and Reporting

Real-Time Dashboards of IT and Business Services

NMS features dashboards that provide users with the real-time status of IT and critical business services.

Dashboards can be tailored to specific users, groups, and roles, and enable users to see practically any type of data in a single view—whether help desk call statistics, application performance metrics, IT resource utilization, geographical server location, database health, and much more. Dashboards are Web-enabled for remote accessibility and have access control features to ensure they are only accessed by authorized users.

Real-Time Alarm Console

NMS features a customizable Web-based alarm console that can be applied to create and customize user specific network monitoring dashboards. Alarm dashboards can show up-to-the-minute status of critical network links, bandwidth utilization, network latency, response times, and other critical network issues. NMS delivers the following network-specific console features:

- Network and application alerts can be viewed in real time.
- Network device auto layout and drag-and-drop host lists for device auto population.
- Layered views for drilling down through applications to underlying network devices and interfaces.
- Drop-down menus for configurable operations, providing point-and-click, context-sensitive access to third-party diagnostic tools.



Performance Trend Reporting

NMS offers robust performance reporting that allows businesses to track and analyze trends in network availability. NMS also tracks performance parameters such as network interface utilization, error rates, connectivity failures, latency, and any other technical items from a service level perspective. All network availability and performance data collected by NMS can be utilized for QoS and performance report generation.

NMS delivers sophisticated capabilities for turning this extensive monitoring data into intuitive insights that help users better understand and optimize infrastructure performance and service levels.

SLA Creation, Monitoring, and Reporting

NMS offers robust capabilities for SLA creation, monitoring, and reporting. QoS and performance data collected by NMS can be leveraged to calculate and report on service level compliance and breaches. All SLA and performance reports can be viewed in Web browsers.

Flexible, Reliable Notification

NMS provides flexible and reliable alert notification and data transport options. In cases where the network link between the probe and NMS management console is disabled, the probe will buffer alert and performance data locally until a failed network connection has been resolved. Further, NMS supports cellular communications for off-network alert notification and performance data transmission, which eliminates reliance upon a potentially broken network for data transport.

Integration with Third-party Network Management Systems

With NMS, alarm information generated can be converted to SNMP trap messages that are readable by any SNMP-based event manager.

Conclusion

Enterprise and service provider networks continue to grow increasingly complex and increasingly vital to business productivity, performance, and profits. The Nimsoft Unified Monitoring architecture provides scalability to monitor any IT environment, whether local, virtualized, or cloud based.

As part of Nimsoft Unified Monitoring, NMS delivers a comprehensive, flexible, easy-to-use solution that gives network administrators a complete 360° network view. This allows proactive monitoring and management of the entire network, ensuring optimal performance and reliability.

About Nimsoft

Nimsoft is the first provider of Unified Monitoring™ solutions for virtualized datacenters, hosted and managed services, cloud platforms, and SaaS resources. With a proven time to value measured in weeks, the Nimsoft Monitoring Solution™ (NMS) reduces an enterprise's total cost of ownership by up to 80 percent compared to legacy systems management vendors, while scaling and extending to places they just cannot go. The Nimsoft Unified Monitoring architecture eliminates the need to deploy a new monitoring solution for outsourced services, public or private clouds, or SaaS implementations. Nearly 1000 customers use Nimsoft Unified Monitoring solutions, including both mid-market and global organizations such as Amway Corporation, Barclays Capital, Casual Male, European Medicines Agency (EMA), Ladbrokes, TriNet, and hundreds of leading hosting, cloud, and managed service providers such as 1&1, CDW, Hitachi, and Rackspace. For more information, visit www.nimsoft.com or to see Nimsoft Unified Monitoring in action, visit the Nimsoft public portal at www.unifiedmonitoring.com.

National Toll Free

877 SLA MGMT (752.6468)
Phone: 650.570.5401
info@nimsoft.com
www.nimsoft.com

United Kingdom

+ 44 (0) 845 456 7091

Norway & Northern Europe

+ 47 22 62 71 60

Germany

+ 49 89 208 039100

Australia

+ 61 (0)2 9236 7216