

### PRESS CONTACTS:

#### Connect Public Relations

Spencer Parkinson  
spencerp@connectpr.com  
(801) 373-7888 x119

#### Network Instruments, LLC

Stephen Brown  
sbrown@networkinstruments.com  
(952) 358-3820

### Network Instruments® Introduces Comprehensive Forensics at FOSE

*New Version of Observer® Offers Security Forensics, High-Level Reporting, IPv6 Support, and Expansion of VoIP and Application Analysis*

Minneapolis, MN – March 13, 2007 – Minneapolis, MN – Network Instruments, a leading provider of innovative analysis solutions for in-depth network intelligence and continuous availability, today announced it will be featuring its recently released GigaStor™ appliance with integrated security forensics at FOSE on March 20 –22, at the Washington Convention Center in booth 2144. The GigaStor provides comprehensive forensic analysis to quickly identify and resolve network, application, and security issues, allowing network and security teams to work together on quick problem resolution.

When troubleshooting large government networks, managers from security and network teams often do not have the visibility required to quickly isolate and resolve issues. This can result in time wasted by attempting to replicate the network issue or fighting with other network teams over the cause of the issue.

To facilitate fast problem resolution, Network Instruments has expanded the retrospective network analysis capabilities of GigaStor to identify security breaches. GigaStor operates like a security camera, recording everything traversing the network for future analysis. With security forensics, GigaStor determines whether a security breach occurred by comparing the historical traffic against a list of thousands of known attacks and anomalies. If a breach is identified, GigaStor provides drill-down analysis to determine the source and time of the occurrence.

“GigaStor plays a critical role in helping government agencies quickly isolate network, security and application problems,” said Steven Bowen, federal territory manager for Network Instruments. “For our government customers, it’s about being able to troubleshoot any network issue before it affects the users. Having GigaStor’s comprehensive forensics means that you can simultaneously process for network, applications, and security issues, identify the problem, and take action.”

In addition to security forensics, Network Instruments has added other capabilities to answer the network management needs of government clients.

#### Observer Reporting Server

Observer Reporting Server provides high-level reporting on network and application activities across the enterprise. The Observer Reporting Server connects to multiple Observer Suite consoles and aggregates critical network performance metrics into an overall view of network health.

In addition to providing an easy-to-access view of network performance, reports can be segmented by individual business units, user groups, or infrastructure types. This allows network managers to quickly view bandwidth utilization or application use by department. If managers notice unexpectedly high bandwidth use from a department, they can quickly and seamlessly drill down on the report to the individual link or user detail using the Reporting Server and Observer. Root cause and Expert analysis can then be performed using Observer.

#### Expanded Native IPv6 Support

In line with a recent government mandate requiring that all government agencies support IPv6 by 2008, Observer now tracks, reports, and monitors IPv6 traffic. Past versions of Observer have decoded IPv6. Whereas, all Observer data is now listed with the appropriate IPv6 address displayed and, more importantly, IPv6 has been pulled through and integrated with all Observer features, including Forensics, Application Analysis, Expert, and VoIP Analysis.

#### VoIP Expansion

According to a recently released Network Instruments survey, 45 percent of network engineers indicated they have VoIP running on their network. The adoption of VoIP will continue to increase during 2007 with 30 percent of respondents planning to implement the technology in the next 12 months. Network Instruments continues to invest and expand the Observer VoIP offering to provide greater support to the countless engineers that use Observer to monitor and optimize VoIP traffic. Observer now includes support for Avaya CCMS and Nortel UNISim protocols as well as providing long-term trending for call detail records (CDR).

### **Application Analysis**

Many organizations use Observer for monitoring application performance and isolating application problems. It provides true application response time, allowing network managers to prioritize, configure, and optimize application performance. Observer now offers integrated support for Microsoft Networking (Server Message Block), in addition to Citrix, Oracle, VoIP, Microsoft Exchange, HTTP, DNS, SQL, FTP, POP3, Telnet, SMTP, and SNMP. Managers can also set triggers and alarms on any application metric, ensuring they know about application problems before users are affected.

### **Product Pricing**

Network Instruments has added many significant enhancements to GigaStor and the Observer product family, and pricing remains the same. The GigaStor begins at \$20,000 for a two-port configuration. Observer Expert, with over 70 VoIP-specific metrics, Application Analysis, and IPv6 Support is \$2,895. Observer Suite, with an SNMP console and Web Reporting, is \$3,995. Additional product information is available at [www.networkinstruments.com](http://www.networkinstruments.com).

###

### **About Network Instruments**

Network Instruments provides in-depth network intelligence and continuous network availability through innovative analysis solutions. Enterprise network professionals depend on Network Instruments' Observer product line for unparalleled network visibility to efficiently solve network problems and manage deployments. By combining a powerful management console with high-performance analysis appliances, Observer simplifies problem resolution and optimizes network and application performance. The company continues to lead the industry in ROI with its advanced Distributed Network Analysis (NI-DNA™) architecture, which successfully integrates comprehensive analysis functionality across heterogeneous networks through a single monitoring interface. Network Instruments is headquartered in Minneapolis with sales offices worldwide and distributors in over 50 countries. For more information about the company, products, technology, NI-DNA, becoming a partner, and NI University please visit [www.networkinstruments.com](http://www.networkinstruments.com).