NETSCOUT

NEWS RELEASE

NETSCOUT Enables Deep Packet Visibility for Business Assurance

2016-11-15

nGenius Packet Flow Switches Deliver New Capabilities for Service Assurance and Cybersecurity

WESTFORD, Mass.--(BUSINESS WIRE)--Nov. 15, 2016-- **NETSCOUT SYSTEMS, INC.** (NASDAQ:NTCT), a leading provider of business assurance – a powerful combination of service assurance, cybersecurity, and business intelligence solutions – today announced capabilities in its nGenius® **Packet Flow Switches** (PFS) that deliver deeper packet visibility. nGenius PFS enable customers to continuously monitor and secure real-time traffic across all business services, regardless of underlying protocols, in both physical and virtual environments. By seamlessly integrating the nGenius PFS with the nGeniusONE® **Service Assurance platform**, customers benefit from a solution that reveals additional packet details, thus extracting more intelligence from the traffic flow. With expanded security capabilities such as hybrid port mode, organizations gain additional flexibility that ease transitions from passive to active security deployments. nGenius PFS enable unified visibility for both service assurance and cybersecurity, as part of a business assurance solution that reduces performance and security risks.

“The ongoing innovations that NETSCOUT is building in their nGenius Packet Flow Switches address the needs for deeper packet visibility and security with our customers,” said John Carson, managing director, Phoenix Datacom, a leading UK-based reseller and integrator of network-based testing, analysis and security solutions to major telecommunications service providers, government agencies and enterprises. “With NETSCOUT, we can help customers see more in their networks, and secure their infrastructure to deliver a complete business assurance solution.”

“Unified packet visibility solves the problem of disparate monitoring infrastructures for service assurance and network security that lead to operational inefficiency and risk,” said Zeus Kerravala, founder and principal analyst, ZK Research. “The steps that NETSCOUT has taken with the integration of its cybersecurity, service assurance and

packet visibility capabilities are critical in helping organizations gain deeper packet visibility and obtain a holistic view of their infrastructure and services."

According to the **Network Monitoring Report** (2016) from IHS Technology, NETSCOUT leads the service provider segment for network monitoring switches, complementing its strong position in the enterprise market. NETSCOUT packet flow switches fortify and advance such leadership with additional new capabilities that create deep visibility into packet flows, so monitoring tools can see more from the network. These new capabilities leverage internal development initiatives along with integration of key features and functionality acquired as part of the Company's last year's acquisition of the Danaher Communications Business. nGenius Packet Flow Switches provide service assurance through capabilities such as:

- Flexibility in forwarded traffic: In virtualized environments, users can choose to either de-encapsulate packets, forward it on encapsulated, or do both. This flexibility allows monitoring tools to see more, as needed. Additionally, tight integration with NETSCOUT **InfiniStream**® probes allow the probes to use the information in the encapsulation headers to provide deeper visibility into the packet data, such as port and time stamp information.
- Traffic origination visibility: Through integration with the nGeniusONE Service Assurance platform, PFS mode on the packet flow switch allows monitoring tools to see from which links on the network a particular packet flow originates through customizable VLAN tagging. The packet flow switch can set custom VLAN Tag ID values, as traffic is forwarded to monitoring tools. This enables the tools to inspect traffic based on origin, which is critical in multi-tenant environments.
- Visibility into tunneled packet flows: With generic stripping (de-encapsulation), nGenius Packet Flow Switches support network environments that utilize a variety of tunneling protocols (e.g. GRE, ERSPAN, GTP, MPLS) by giving monitoring tools the visibility into these packet flows. Packets can be de-encapsulated from tunnels and inspected, so monitoring tools can see things that were previously hidden within these protocols.

Business assurance solutions must also reduce risk and streamline operations. nGenius Packet Flow Switches help organizations deploy inline security without worry, through security-optimized capabilities such as:

- Advanced inline aggregation: When aggregating traffic from multiple networks, VLAN tags are often utilized to identify the appropriate network source for returning inspected traffic. However, this creates issues for security systems that cannot process these tags. Additionally, in large-scale dynamic network environments with asymmetric routing, delivering packets back to the origination source is not possible. With nGenius Packet Flow Switches, discovery of the origination network by MAC address or Link Aggregation Group (LAG) alleviates the additional tagging requirement of other systems. So security systems can see all packet flows for inspection and analysis, and packets are returned to the source of origination on the network correctly.
- High frequency advanced health checks: nGenius Packet Flow Switches go beyond a simple interface (port

up/down) or “heartbeat” ping to see if security systems are on. With

L7 application-level functionality health checks, nGenius Packet Flow Switches ensure the security application or device is functioning as expected. Positive and negative health checks can be performed as frequently as every 100ms, ensuring that security systems function correctly; thus reducing time to detect security system failure. Used in combination in triggers, health checks enable automatic high-availability and fail over, to simplify operations and reduce security risk.

- Hybrid port support: Both passive (copies of traffic) and active (production) traffic can be sent to the same monitoring tool port, allowing security systems with a hybrid capability to receive the traffic on the same port. Systems that provide both active and passive capabilities, such as intrusion prevention (IPS) and intrusion detection (IDS), are gaining ground. The hybrid mode on nGenius Packet Flow Switches leads to better port utilization and efficient use of security systems, as now customers do not have to choose which mode to run the system in or run two systems (one active and one passive) in parallel.
- Scalable security systems: With the large amount of traffic that needs to be inspected from high-speed links (e.g. 40G) or aggregated from multiple links, the processing capability of each security system needs to be considered to prevent overload and potential failure on any one system. nGenius Packet Flow Switches support high capacity (up to 32 instances) session-aware load balancing, providing security visibility and reducing risk by preventing over-subscription and potential failure on any one system.

The new nGenius Packet Flow Switches capabilities provide deeper packet visibility while optimizing packets from the network to the monitoring tools and security systems. Additional integration with the nGeniusONE Service Assurance platform means organizations can deploy a business assurance solution that mitigates performance and security risks. Learn more about how nGenius Packet Flow Switches enable unified visibility for service assurance and security **here**.

About NETSCOUT SYSTEMS, INC.

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) is a leading provider of business assurance – a powerful combination of service assurance, cybersecurity, and business intelligence solutions – for today’s most demanding service provider, enterprise and government networks. NETSCOUT’s Adaptive Service Intelligence (ASI) technology continuously monitors the service delivery environment to identify performance issues and provides insight into network-based security threats, helping teams to quickly resolve issues that can cause business disruptions or impact user experience. NETSCOUT delivers unmatched service visibility and protects the digital infrastructure that supports our connected world. To learn more, visit **www.netscout.com** or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

Safe Harbor

Forward-looking statements in this release are made pursuant to the safe harbor provisions of Section 21E of the Securities Exchange Act of 1934 and other federal securities laws. Investors are cautioned that statements in this press release, which are not strictly historical statements, including without limitation, the statements related to the benefits of nGenius Packet Flow Switches, constitute forward-looking statements which involve risks and uncertainties. Actual results could differ materially from the forward-looking statements due to known and unknown risk, uncertainties, assumptions and other factors. Such factors include slowdowns or downturns in economic conditions generally and in the market for advanced network and service assurance solutions specifically; the volatile foreign exchange environment; the company's relationships with strategic partners and resellers; dependence upon broad-based acceptance of the company's network performance management solutions; the presence of competitors with greater financial resources than ours and their strategic response to our products; our ability to retain key executives and employees; lower than expected demand for the company's products and services; and the ability of NETSCOUT to successfully integrate the merged assets and the associated technology and achieve operational efficiencies. For a more detailed description of the risk factors associated with the company, please refer to the company's Annual Report on Form 10-K for the fiscal year ended March 31, 2016 and the company's subsequent Quarterly Reports on Form 10-Q, which are on file with the Securities and Exchange Commission. NETSCOUT assumes no obligation to update any forward-looking information contained in this press release or with respect to the announcements described herein.

©2016 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, InfiniStream, InfiniStreamNG, nGenius and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

View source version on businesswire.com: **http://www.businesswire.com/news/home/20161115005703/en/**

Source: NETSCOUT NETSCOUT SYSTEMS, INC.

NETSCOUT SYSTEMS, INC.
Donna Candelori, +1-408-571-5226
donna.candelori@NETSCOUT.com