NEWS RELEASE

CORRECTING and REPLACING NETSCOUT Expands Capabilities to Support Enterprise Compliance Requirements in Cloud Environments

2025-10-30

Delivering essential visibility for compliance evidence, data protection and secure operations

WESTFORD, Mass.--(BUSINESS WIRE)-- Please replace the release with the following corrected version due to multiple revisions.

The updated release reads:

NETSCOUT EXPANDS CAPABILITIES TO SUPPORT ENTERPRISE COMPLIANCE REQUIREMENTS IN CLOUD ENVIRONMENTS

Delivering essential visibility for compliance evidence, data protection and secure operations

NETSCOUT® SYSTEMS, INC. (NASDAQ: NTCT), a leading provider of observability, AIOps, cybersecurity, and DDoS attack protection solutions, today announced it has extended continuous end-through-end monitoring to enhance attribution for audit controls and incident reports, prove zero-trust network policies, and shorten time to detect, contain, and document incidents. Enhanced monitoring is designed into its Omnis® KlearSight Sensor for Kubernetes to help address the complex compliance demands faced in Cloud environments related to both security and regulatory requirements.

With **93% of companies evaluating, piloting, or using Kubernetes** in production, organizations encounter significant challenges when it comes to monitoring at scale for observability and security purposes. NETSCOUT's continuous and comprehensive monitoring solutions provide real-time visibility into critical aspects such as

workloads, cluster configurations, network traffic, and API calls. This helps support the gathering of compliance evidence and keeping it more consistently up to date, enabling enterprises to meet regulatory standards and maintain robust security postures.

“When enterprises deploy Kubernetes for microservice application delivery, container dynamism can create compliance gaps which inhibit the ability to meet requirements for monitoring, auditability, and incident response,” stated John Grady, principal analyst, Omdia. “Enterprises need to capture the packet- and process-level activity needed for compliance reporting and investigations across their entire IT environment to manage risk, security, and ensure accountability against compliance standards.”

By supporting the need for visibility into Cloud-native environments like Kubernetes, these solutions help provide the information needed to demonstrate ongoing assurance that systems are secure, auditable, and resilient for regulatory frameworks and compliance requirements such as:

- Continuous monitoring and threat detection (e.g., DORA)
- Incident response and forensics (e.g., ISO 27001/27002)
- Data protection and privacy (e.g., GDPR, HIPAA)
- Configuration and vulnerability management (e.g., NIST 800-53, NIST 800-190)
- Audit and accountability (e.g., GDPR, ISO 27001, HIPAA and others).

Without clear visibility, enterprises can miss critical activity inside their Kubernetes environments, creating blind spots that increase the risk of non-compliance with security and regulatory standards that require continuous monitoring. Since containers often communicate with each other within a cluster, known as east-west traffic, organizations need network-level visibility, along with microservice, and container-aware telemetry to detect anomalies, lateral movement, and policy violations in real-time. These capabilities also provide detailed packet - and container-level evidence, which is critical for understanding what happened, where, and when.

“Continuous monitoring is more than a best practice; it’s a risk mitigator and compliance enabler,” stated Thor Wallace, Chief Information Officer, NETSCOUT. “Visibility into Kubernetes cloud environments is important because it provides the insights needed to ensure service levels and customer expectations are met, while also helping support our compliance efforts.”

Visit our **website** for more information about **InfiniStreamNG**, **Omnis® KlearSight Sensor for Kubernetes solution**.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance and availability disruptions through its unique visibility platform and solutions powered by its pioneering deep packet inspection at scale technology. NETSCOUT serves the world's largest enterprises, service providers, and public sector organizations. Learn more at **www.netscout.com** or follow @NETSCOUT on **LinkedIn**, **X**, or **Facebook**.

Editorial Contacts:

Chris Lucas
NETSCOUT Systems, Inc.
+1 978 614 4124
chris.lucas@netscout.com

Chris Shattuck
Finn Partners for NETSCOUT
+1 404 502 6755
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC