NETSCOUT

NEWS RELEASE

NETSCOUT Expands Automated Threat Detection and Response Capabilities

2025-07-15

Adaptive Threat Analytics Provides the Essential Knowledge to Accelerate Cybersecurity Responses

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT), a leading provider of observability, AIOps, cybersecurity, and DDoS attack protection solutions, today announced Adaptive Threat Analytics, a new enhancement to its **Omnis Cyber Intelligence** Network Detection and Response (NDR) solution, designed to improve incident response and reduce risk. Adaptive Threat Analytics enables security teams to investigate, hunt, and respond to cyber threats more rapidly.

Cybersecurity professionals face a challenge in the race against time to detect and respond appropriately to cyber threats before it is too late. Alert fatigue, increasing alert volume, fragmented visibility from siloed tools, and cunning AI-enabled adversaries create a compelling need for a faster and more effective response plan. **McKinsey & Company** noted last year that despite a decline in response time to cyber-related risks in recent years, organizations still take an average of 73 days to contain an incident.

In the threat detection and incident response process, comprehensive north-south and east-west network visibility plays a critical role in all phases, but none more so than the ‘Analyze’ phase between ’Detection’ and ‘Response.’ Adaptive Threat Analytics utilizes continuous network packet capture and local storage of metadata and packets independent of detections, built-in packet decodes, and a flexible ad hoc querying language, enabling more rapid threat investigation and proactive hunting. This provides SOC analysts with the specific knowledge needed to determine and execute the proper response more efficiently.

“Network environments continue to become more disparate and complex. Bad actors exploit this broadened attack surface, making it difficult for security teams to respond quickly and accurately,” said John Grady, principal analyst,

cybersecurity, at Enterprise Strategy Group. Due to this, continuous, unified, packet-based visibility into north-south and east-west traffic has become essential for effective and efficient threat detection and incident response."

Omnis Cyber Intelligence's AI-driven correlation stitches disparate events into cohesive, high-fidelity incidents, providing a holistic, actionable view of the entire attack chain. It delivers superior scalability and cost-effective NDR capabilities across complex IT environments and easily integrates into your cybersecurity ecosystems, such as your SIEM, SOAR, or XDR.

"Security teams often lack the specific knowledge to understand exactly what happened to be able to choose the best response," stated Jerry Mancini, senior director, Office of the CTO, NETSCOUT. "Omnis Cyber Intelligence with Adaptive Threat Analytics provides 'big picture' data before, during, and after an event that helps teams and organizations move from triage uncertainty and tuning to specific knowledge essential for reducing the mean time to resolution."

Visit our website to learn more about how NETSCOUT's **Adaptive Threat Analytics** is accelerating incident response with faster analyses and investigations.

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