NETSCOUT

NEWS RELEASE

NETSCOUT Improves Customer's Digital Resilience and Security Posture

2024-09-12

Omnis Cyber Intelligence's New MITRE ATT&CK ® Aligned Behavioral Analytics Helps Stop Ransomware, Improve Remediation, and Meet Compliance Needs

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT), a leading provider of performance management, cybersecurity, and DDoS attack protection solutions, today announced updates to its advanced, scalable deep packet inspection-based Omnis Cyber Intelligence Network Detection and Response (NDR) platform. New MITRE ATT&CK behavioral analytics enable earlier detection of advanced threats like ransomware, suspicious traffic, or unauthorized access attempts while improving remediation to help meet industry and country compliance requirements.

"Digital resilience allows enterprises to continuously operate and quickly leverage digital opportunities to serve their customers, especially during economically challenging times," stated Fernando Montenegro, senior principal analyst, Omdia. "A mature cyber strategy is key to digital resilience, and comprehensive security controls require organizations to deploy technology such as Omnis Cyber Intelligence to continuously monitor their networks, so they can react to and mitigate threats early before they impact their operations."

New Omnis Cyber Intelligence enhancements include:

- Tighter alignment with ATT&CK – A new security events dashboard that can easily be toggled to show events aligned to ATT&CK tactics and techniques, enabling security teams to quickly prioritize, investigate, and remediate threats.
- Expanded behavioral analytics – Expanding behavioral analytics at the source allows for the early detection of advanced multi-staged attacks, such as ransomware and unusual network traffic, before major impact occurs.

- Malicious file detection – Known malicious file detection has been added to the Omnis Cyber Intelligence list of multi-dimensional threat detections, enabling it to detect known and unknown zero-day threats.
- Host IP address enrichment – Along with IP address, host and machine name identification has been added to alerts, enabling SecOps teams to accurately identify, investigate, and remediate threats.
- Open Integration Framework – A new open framework that can quickly integrate with third-party solutions such as firewalls, endpoint detection (EDR), and SIEM/SOAR/XDR platforms enables real-time response to incidents, such as blocking malicious IP addresses with firewalls or isolating compromised endpoints.

As organizations seek out new effective and efficient methods to comply with industry or government regulations, such as the EU's **Digital Operational Resilience Act (DORA)** , which goes into effect on January 17, 2025, they are learning that the network continues to play a strategic role for success. Omnis Cyber Intelligence's continuous, scalable deep packet inspection-based network monitoring, tighter alignment with ATT&CK, expanded behavioral analytics, and new open architecture for ecosystem integration helps organizations meet these important compliance requirements and strengthen their digital resiliency.

"NETSCOUT helps its customers strengthen their digital resilience by enabling easier detection, faster response, and more effective recovery from cyber threats," stated Jerry Mancini, senior director, office of the CTO, NETSCOUT. "The new functionality we've added to our Omnis Cyber Intelligence platform helps organizations improve their security posture and better react to an ever-changing threat landscape while supporting compliance and reporting needs."

Visit our website to learn more about how NETSCOUT is **transforming network security** and helping organizations meet compliance requirements.

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