

# NETSCOUT Helps Make Zero Trust Architectures More Achievable

2025-07-17

Omnis Network Security Solution Enables All Five Key Steps to Zero Trust Architecture Maturity and Supports the NIST Playbook to Reduce Cybersecurity Risks

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT), a leading provider of observability, AIOps, cybersecurity, and DDoS attack protection solutions, today announced how its solutions align with National Institute of Standards and Technology (NIST) initiatives designed to help U.S. federal agencies adopt standards and best practices tied to zero-trust security frameworks that aim to protect data and resources across hybrid environments with high-availability needs.

Ever since NIST published **NIST SP 800-207** in 2020, setting forth Zero Trust Architecture (ZTA) as a means to combat both internal and external threats, the adoption of ZTA has accelerated, driven by a risk-based approach to cybersecurity. However, even NIST has acknowledged that building and implementing ZTA is a complex undertaking.

NETSCOUT's **Omnis Network Security Solution** enables all five key steps to ZTA maturity, including: identifying and continuously monitoring all critical services, mapping all transaction flows across an organization's entire digital infrastructure, verifying that micro perimeters are behaving as expected and detecting when a perimeter has been crossed, providing metadata and layer 7 visibility into all applications, and providing visibility throughout the dwell time of an incident with full context to restore normal operation with the shortest downtime.

"We're proud to collaborate with trusted technology leaders across our robust partner ecosystem to deliver mission-ready solutions," said Chris Wilkinson, executive vice president of sales at Four Inc., a leading public sector IT distributor. "NETSCOUT's proven ability to strengthen Zero Trust Architectures and accelerate adoption—

securely, efficiently, and at scale—makes them a critical pillar of our cybersecurity strategy for both DoD and civilian agencies in addition to SLED environments.”

“As the U.S. federal government actively modernizes its IT infrastructure, the need for Zero Trust Architecture to strengthen security postures becomes increasingly critical to protect sensitive information from the rise in cyberattacks,” said Karl Schaub, chief solutions architect, NETSCOUT. “We have established trusted relationships with federal agencies to address their observability and cybersecurity needs by embracing a zero-trust approach and working collaboratively with our partners to deliver robust and highly scalable solutions.”

NETSCOUT’s **Omnis Cyber Intelligence**, a key component of the Omnis Network Security solution and **FIPS and Common Criteria certified**, helps government agencies achieve zero-trust maturity through a highly scalable and cost-effective network detection and response (NDR) solution. The solution provides comprehensive network visibility into north-south and east-west traffic, enhances threat detection and investigation workflows, improves collaboration between NetOps and SecOps, and enables faster incident detection and response.

Omnis Cyber Intelligence’s Adaptive Threat Analytics continuously captures and stores all metadata and packets, independent of detected threats, and features seamless bi-directional integration with SIEM/SOAR/EDR/XDR platforms. This enables security teams to investigate alerts or validate zero-trust policies, thereby reducing response times and cybersecurity risks. The solution is fully integrated with other cybersecurity and observability solutions from Palo Alto Networks, Splunk, ServiceNow, VMware, and others.

Visit our website to learn more about how NETSCOUT supports **zero trust security architecture** or explore more about the **Omnis Cyber Intelligence** 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](https://www.netscout.com) or follow @NETSCOUT on **LinkedIn**, **X**, or **Facebook**.

©2025 NETSCOUT SYSTEMS, INC. All rights reserved. Third-party trademarks mentioned are the property of their respective owners.

## 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