NEWS RELEASE

NETSCOUT Extends Adaptive DDoS Defense Protection to Address the Rising Business Cost of Weaponized Broadband and IoT Devices

2026-08-18

New Automated Outbound Protection Helps Service Providers Reduce Network Disruption, Infrastructure Costs and Internet-Wide Risk

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT® (NASDAQ: NTCT), a leading provider of observability, AIOps, cybersecurity, and DDoS attack protection solutions, today announced an extension of its Adaptive DDoS Protection (ADP) solution enabling service providers to automatically detect and mitigate outbound DDoS attack traffic. By extending protection from the attack target towards its source, NETSCOUT helps operators prevent compromised subscriber devices from disrupting their own networks, consuming costly capacity and attacking customers and organizations across the internet.

Consumer broadband routers, cameras and other IoT devices are increasingly being weaponized by Turbo-Mirai class botnets capable of generating multi-terabit attacks. These outbound attacks have already caused costly service outages, reputational damage and customer loss, and damage to peering relationships risking a large increase in transit costs at service providers around the world. By detecting and mitigating malicious traffic generated by compromised device populations before it leaves their networks, service providers can reduce abuse complaints and infrastructure costs while protecting their own networks and services and helping lower subscriber churn and regulatory risk.

“The combination of higher-speed broadband connectivity and vulnerable IoT devices has been weaponized by a new class of massive DDoS botnets,” said Patrick Donegan, founder and principal analyst, HardenStance. “Source-side mitigation, or attack suppression as it’s sometimes known, is a critical part of the equation. NETSCOUT’s

approach, backed by its ATLAS Intelligence Feed (AIF) and ASERT analysts, gives service providers the tools they need to detect and stop attacks before they have an impact, protecting their customers and the broader internet from the large-scale DDoS attacks we have seen."

Using AI-powered threat intelligence and automated detection and mitigation, NETSCOUT's ADP solution, an addition to its **Arbor Sightline** and **Arbor Threat Mitigation System**:

- Automatically detects and mitigates ever evolving attacks through dynamic detection, intelligent redirection and adaptive mitigation.
- Extends these capabilities to outbound traffic, combining enhanced, customized detection with comprehensive threat intelligence tailored for each ISP.
- Uses NETSCOUT's proprietary AI/ML-powered DDoS detection to analyze massive volumes of outbound internet traffic to uncover attacks designed to hide within legitimate flows.
- Draws on unique global real-time intelligence of DDoS activity covering approximately half of all internet traffic to rapidly detect and mitigate DDoS attacks and pinpoint the responsible, compromised devices.

"We are extending DDoS defense from the target to the source," stated Darren Anstee, CTO, Security, NETSCOUT. "By using our internet-scale visibility to derive localized threat intelligence for our customers, NETSCOUT can identify and precisely suppress attacks at their origin, before they cause problems locally or at their target. This capability gives our customers a new level of comprehensive defense across their peering, transit, cloud and customer edges."

This expansion of capabilities demonstrates how NETSCOUT is applying its global threat visibility and proven ADP solution to meet emerging service provider challenges. By extending an established inbound DDoS workflow to outbound and cross-bound threats, NETSCOUT enables operators to improve network-resilience, cost-controls and revenue protection through its proven Arbor Sightline and Arbor TMS solutions.

Resources:

- Learn more about the expanded **Arbor Sightline** and the **Arbor Threat Mitigation System**.
- Understand the evolving tactics of botnet-driven DDoS from the latest NETSCOUT **DDoS Threat Intelligence Report**.

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. As a leading provider of network observability, AIOps, carrier service assurance, cybersecurity, and Distributed Denial-of-Service (DDoS) attack protection solutions, 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