NETSCOUT

NEWS RELEASE

# NETSCOUT Continues to Innovate Its Arbor DDoS Protection With AI/ML to Reduce Cybersecurity and Business Risks

2025-02-25

AI/ML Powered Intelligence Feed and Adaptive DDoS Mitigation Essential for Defeating Rapidly Evolving DDoS Attacks

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT), a leading provider of performance management, cybersecurity, and DDoS attack protection solutions, today announced it enhanced its **Arbor® Threat Mitigation System (TMS)** Adaptive DDoS Protection solution with additional AI/ML functionality to better detect and block malicious traffic.

Distributed Denial of Service (DDoS) attacks targeting critical IT infrastructure and services have increased by 55% over the last four years. A perfect storm of AI-driven automation, evolving DDoS-for-hire services, augmented IoT botnets, and geopolitical conflicts have changed the threat landscape with more frequent, sophisticated attacks having the potential to do more damage more rapidly. To combat these attacks, organizations, enterprises and service providers require AI/ML-enabled solutions that can continually adapt to threats, using proactive, intelligence-driven security strategies to protect their networks.

“With AI-driven attacks, ransomware, and nation-state threats impacting corporate governance, financial performance, and customer trust, corporate boards expect their IT teams to be proactive in adapting to emerging threats like DDoS,” said Chris Steffen, Vice President of Research – Information Security, Enterprise Management Associates. “Implementing solutions that can adapt to threats helps minimize that risk.”

NETSCOUT utilizes a hybrid AI/ML strategy that combines AI/ML running at scale in the cloud, with supervision, to analyze data collected from an unprecedented 550 Tbps of Internet traffic (almost half of all Internet traffic), along

with AI/ML running in our software solutions to enable automated protection from these attacks. This provides a 'best of both worlds' approach – the computational scale of the cloud allows for large-scale analysis of threat data with supervision to ensure accuracy while AI/ML running in our software solutions enables them to leverage that pre-analyzed intelligence to make fast, accurate, automated decisions about what to detect and block.

The company's cloud-based AI/ML drives the creation of the **ATLAS Intelligence Feed**, which delivers unique capabilities in its Adaptive DDoS Protection solutions, arming them with the latest DDoS attack intelligence. The continuous analysis, which is updated multiple times per day, provides insight into the source IP addresses of devices actively conducting DDoS attacks on the internet, novel attack vectors, DDoS attack targets, and other intelligence. This enables Adaptive DDoS Protection to quickly and accurately detect even small direct-path attacks from sampled flow data and send the traffic to TMS for automated blocking.

The latest AI/ML-derived ATLAS Intelligence Feed iteration has been augmented with enhanced Geo-IP location functionality that maps IP addresses to geographic locations, enabling faster and more precise identification and blocking of malicious traffic. In addition, the ATLAS Intelligence Feed now includes NETSCOUT's ATLAS tracking of active DDoS campaigns, enabling Adaptive DDoS Protection to automatically detect and block attacks from over 65 known DDoS threat actors carrying out active attack campaigns against a range of targets, including NoName057 and RipperSec.

AI/ML technology has also been adopted as part of the Adaptive DDoS Protection solution. New in the latest release is AI/ML-powered source host misuse detection, which enables network operators to track misbehaving subscribers, infected hosts, compromised IoT devices, and other internal attack sources. This new capability makes it easier to detect and block outbound DDoS attacks that can impact service and infrastructure performance and availability as edge connectivity speeds increase. New TMS Source Mitigations enable network operators to redirect and surgically protect against threat activity from specific sources that may be targeting the entire network without requiring fully inline solutions on all network traffic.

## Service Provider Benefits

With updates to NETSCOUT's Adaptive DDoS Protection solution, service providers can better protect their critical infrastructures and the services they provide to their customers. Other key advantages include enhanced availability, reduced downtime costs, less aggravation, and new revenue-generating opportunities.

"With more sophisticated and frequent DDoS attacks, the risks have never been greater," said Scott Nichols, Chief Commercial Officer at Arelion. "Through our partnership with NETSCOUT, we're able to deliver industry-leading Adaptive DDoS protection to ensure the best experience possible for our customers."

Visit our website to learn more about NETSCOUT's **Arbor Adaptive DDoS Protection for Service Providers**.

## 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