NETSCOUT

NEWS RELEASE

NETSCOUT Strengthens Operational Resilience of Critical Infrastructure Against AI-Driven, Internet-Scale DDoS Attacks

2026-07-24

Improving Operational Resilience with the Ability to Distribute and Scale DDoS Defenses Across the Entire Security Footprint

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT® (NASDAQ: NTCT), a leading provider of observability, AIOps, cybersecurity, and DDoS attack protection solutions, today announced continued investments in infrastructure and technology to double its Arbor® Cloud DDoS attack mitigation capacity to 33 Tbps, which is aimed at keeping critical digital services available during DDoS attacks, protecting revenue-generating digital operations, supporting always-on AI-driven businesses, and maintaining customer trust.

This capacity enhancement, coupled with NETSCOUT's recent acquisition of DDoS network and infrastructure, reinforces the company's commitment to delivering industry-leading cloud-based DDoS defense at global scale. By fully owning and securing end-to-end control over the platform, NETSCOUT has a clear path to scale innovative, resilient services for customers worldwide. Unlike cloud mitigation services that merely add bandwidth, Arbor Cloud combines global mitigation capacity with global threat intelligence, drawing on NETSCOUT's unparalleled visibility into real-world internet attack activity. Spanning 16 global scrubbing centers, this significant increase in capacity equips customers with the ability to defend against the growing scale, frequency, and sophistication of DDoS attacks by consistently balancing mitigation capacity across all attack vectors in their environments.

According to **Markets and Markets**, the DDoS protection market size is expected to continue to grow, driven by increasingly sophisticated attacks and accelerated cloud adoption. Today, multi-vector attacks are the norm. Bad actors are launching more simultaneous attacks as well as quick hit and run attacks, forcing shorter response times

from defenders. In addition, mega-botnets like Aisuru and Kimwolf have raised the ceiling on attack sizes with a few attacks approaching or exceeding 30 Tbps. Enterprises and service providers have a compelling need right now to improve the protection levels of their critical digital infrastructure.

“With the increased use of AI, threat actors are targeting organizations whose defenses are vulnerable to the new, more complex DDoS attacks designed to take down critical infrastructure,” stated Carlos Morales, SVP and general manager, Arbor Cloud, NETSCOUT. “As enterprises increasingly rely on AI-powered applications and cloud-native services, while at the same time, attack size and complexity continue to rise, implementing automated and proactive defenses for uninterrupted availability has become a business risk imperative. Arbor Cloud plays a key role in achieving that objective.”

Increasing Arbor Cloud capacity provides significant advantages, including:

- Greater intelligent mitigation capacity - absorbs and blocks larger volumetric and more sophisticated attacks without losing effectiveness.
- Multiple threat mitigation - handles multiple concurrent targets (e.g., from carpet bombing attacks) or multiple attack vectors simultaneously.
- Consistent operational performance – protects critical infrastructure, ensuring capacity does not become a constraint as attack size and frequency increase.
- Faster stabilization post spikes – acts as a shield wall preventing attacks from reaching customer infrastructure and creating collateral damage that lasts well beyond when the actual attack subsides.
- Operational confidence – provides added assurance for mission-critical sectors, like financial services, hospitals, retail, and the public sector, which require that protection remains available when legitimate traffic surges and cyberattacks occur simultaneously.

Arbor Cloud plays a critical role as part of NETSCOUT’s multi-layered, adaptive DDoS protection, combining on-premises DDoS defense with cloud-based traffic scrubbing services that are tightly integrated via automated cloud signaling. This hybrid design stops attacks as close to the source as possible while seamlessly absorbing loud volumetric attacks in the cloud. Offering comprehensive global protection, Arbor Cloud is supported by a 24x7 Security Operations Center staffed by NETSCOUT’s DDoS protection experts. The capacity expansion is expected to be fully completed by the end of August 2026.

This investment reinforces NETSCOUT’s long-standing leadership in DDoS protection by combining one of the world’s largest dedicated DDoS mitigation networks with decades of cyber defense expertise, industry-leading threat intelligence, and global Internet visibility. As digital infrastructures continue to evolve rapidly, and AI accelerates both innovation and cyber threats, NETSCOUT remains committed to providing organizations with the scale, intelligence, and operational resilience required to confidently protect what matters most.

Resources:

- Reference the latest NETSCOUT **DDoS Threat Intelligence Report**.
- Learn more about **Arbor Cloud DDoS Protection**.

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