NEWS RELEASE

NETSCOUT Defends Customers From Cyberattacks With Automated, Real-Time Traffic Analysis, Global Threat Intelligence, and ML-Based Mitigation

2023-09-19

Adaptive DDoS Protection for Arbor TMS Dramatically Improves Dynamic Distributed Attack Detection Including Carpet Bombing

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC**. (NASDAQ: NTCT), a leading provider of performance management, cybersecurity, and DDoS attack protection solutions, today launched Adaptive DDoS Protection for its **Arbor® Threat Mitigation System (TMS)** to dramatically improve detection of distributed attacks that dynamically change vectors and target numerous destination IP addresses at once.

NETSCOUT ASERT, the company's expert security research and DDoS attack mitigation team, has documented a significant increase in dynamic Distributed Denial-of-Service (DDoS) attacks using multiple vectors and techniques to launch botnet-based, direct-path, state exhaustion, and application-layer attacks designed to evade conventional static network and cloud-only-based DDoS defenses. Carpet-bombing attacks have risen by more than 110%. They are particularly challenging for SOC teams to mitigate using conventional means as these attacks target large swaths of IP addresses versus a single host and generate hundreds or thousands of alerts per attack.

“Direct path attacks are overtaking reflection/amplification as the most popular DDoS attack vector, and they are increasingly botnet-driven, multi-vector, and dynamically adjusted in real-time,” said Patrick Donegan, founder and principal analyst, HardenStance. “No company knows more about DDoS attacks than NETSCOUT. ASERT analyzes highly curated data from its ATLAS Intelligence Feed (AIF) and uses ML-based algorithms to recommend changes to attack countermeasures to stop DDoS attacks. Automating this functionality to bring intelligence into its Adaptive DDoS Protection functionality makes Arbor TMS even more compelling in mitigating DDoS attacks.”

Adaptive DDoS Protection analyzes traffic in real-time and automatically implements threat intelligence-driven mitigations and countermeasures to block dynamic DDoS attacks as they evolve. Adaptive DDoS Protection gives SOC teams a scalable, always-on, stateless packet processing solution that uses unmatched visibility into more than 50% of all internet traffic, real-time global DDoS attack threat intelligence, and decades of DDoS mitigation experience to automatically detect, adapt to, and mitigate dynamic DDoS attacks.

Defending Against Carpet Bombing

Carpet bombing attacks are one of the most devastating distributed attacks bad actors can initiate since they target large ranges of IP addresses simultaneously, generating thousands of attack alerts that are impossible for SOC teams to manage. Through Adaptive DDoS Protection, NETSCOUT has introduced a new way to understand DDoS traffic at the network level across all subnets to detect and report on carpet bombing attacks in one, easy-to-understand alert. NETSCOUT’s ML-based Precise Protection Prefix technology automatically determines the specific IP ranges targeted by the attack. It then automatically redirects those to Arbor TMS for mitigation, even as the attack moves around the network to different targets. This Adaptive DDoS Protection capability dramatically improves the detection and mitigation of carpet-bombing attacks.

“Defending a network requires as much knowledge about your adversary as possible,” said Scott Iekel-Johnson, AVP, DDoS and Threat Intelligence at NETSCOUT. “We have embedded our global threat intelligence and decades of attack mitigation experience into this product. It’s like having an ASERT analyst at your side 24/7. Our Adaptive

DDoS Protection finds attacks that other solutions miss through dynamic detection and intelligent redirection to enable Arbor TMS to mitigate DDoS attacks better than any other solution on the market."

To learn more about Adaptive DDoS Protection for Arbor TMS, visit our **website**.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance and availability disruptions through the company's 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, Twitter, or Facebook.

Editorial Contacts:

Maribel Lopez
Manager, Marketing & Corporate Communications
+1 781 362 4330
maribel.lopez@netscout.com

Chris Shattuck
Finn Partners for NETSCOUT
+1 404 502 6755
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC