NETSCOUT

NEWS RELEASE

NETSCOUT Announces Omnis AIF for Smarter Automated DDoS Attack Blocking

2022-07-12

Innovative Intelligence-Based Approach Uses Unique Global Visibility and Automated AI Analytics Engine to Speed DDoS Attack Response and Reduce Operational Overhead

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC**., (NASDAQ: NTCT), a leading provider of cybersecurity, service assurance, and business analytics solutions, today announced that it has launched a new, innovative AI-based solution enabling its customers to automatically and instantaneously block a large proportion of DDoS attacks thus simplifying operations and minimizing risk to their businesses.

The solution leverages NETSCOUT's ATLAS® network, an unmatched source of visibility into DDoS attack activity on the Internet. Multiple ATLAS datasets are analyzed, curated, and correlated using artificial intelligence. This automated intelligent pipeline is developed using NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) expertise to identify botnet members and other network infrastructure that is actively participating in DDoS attacks.

This intelligence is continuously updated and shared in real-time with NETSCOUT's industry-leading Arbor Threat Mitigation System (TMS) and Omnis® AED Smart DDoS attack protection solutions via the Omnis ATLAS Intelligence Feed (AIF). This new Omnis AIF content enables TMS and AED to know, in advance, the IP addresses of devices across the Internet that are being used to launch DDoS attacks, resulting in the ability to instantly block up to 90% of attack traffic, without further analysis, during an attack.

This data provides TMS and AED with the intelligence needed to automatically stop botnet-generated DDoS attacks, including reflection/amplification, direct-path TCP state exhaustion, application-layer, and encrypted attacks. The analysis behind Omnis AIF is based on NETSCOUT's unique, global DDoS attack visibility extending to more than

one-third of all Internet traffic and millions of DDoS attacks. This global intelligence can then be applied automatically for local protection.

"This is an innovative way to block DDoS attacks," stated Darren Anstee, chief technology officer for security at NETSCOUT. "Omnis AIF, which incorporates the new DDoS reputation feed, takes an intelligence-based approach providing customers with faster, more comprehensive, and more automated solutions. Our approach is different because we leverage global observations in DDoS attack activity to drive local automation and response. As a result, we can dramatically lower the risk of business impact due to DDoS attack for our customers."

With this intelligence-based approach, customers will experience less business impact from legitimate blocked traffic and spend less time analyzing DDoS attacks.

Visit our website to learn more about Omnis **AIF**, **AED**, or **TMS**.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) protects the connected world from cyberattacks and performance disruptions through advanced network detection and response and pervasive network visibility. Powered by our pioneering deep packet inspection at scale, we serve 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.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20220712005341/en/**

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.