NETSCOUT

NEWS RELEASE

NETSCOUT Leverages AI/ML to Guard Critical IT Infrastructure and Minimize Business Risk

2024-12-19

Enhanced Capabilities Identify and Mitigate Dynamically Changing, AI-Enabled 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 updates to its industry-leading Arbor Edge Defense (AED) and Arbor Enterprise Manager (AEM) products as part of its Adaptive DDoS Protection Solution to combat AI-enabled DDoS threats and protect critical IT infrastructure. **NETSCOUT's DDoS Threat Intelligence Report** noted that application-layer and volumetric attacks have increased by over 43% and 30%, respectively. DDoS-for-hire services have also increased in number and sophistication, making attacks easier to launch. The Cybersecurity & Infrastructure Security Agency (CISA) also recently released a **cybersecurity advisory** that validated the need for better controls to prevent and detect malicious activity, reinforcing enterprises' need for protective solutions to minimize business risk.

"According to recent IDC research, IT environment complexity is often the top challenge to an organization's mitigation efforts, especially as attackers continually modulate their attack vectors using AI to challenge defenses," said Chris Rodriguez, Research Director, Security & Trust, IDC. "Organizations need to invest in proactive, adaptive measures to protect their environments like those provided by NETSCOUT's Adaptive DDoS Protection solution. Reactive or static mitigation that lacks sophisticated intelligence creates unnecessary risk and opens the door for costly damage to business productivity and reputation."

NETSCOUT employs artificial intelligence (AI) and machine learning (ML) technology in its ATLAS Threat Intelligence Feed and in a unique set of capabilities for adaptive DDoS protection. The NETSCOUT ATLAS global threat intelligence system monitors over 550 Tbps of Internet traffic in real-time across over 500 ISPs and 2000-plus enterprise sites from over 100 countries. The AI/ML algorithms run in the ATLAS cloud infrastructure as part of a

product-independent data collection and analysis pipeline that can be updated anytime without requiring product software or customer site updates.

AI/ML technology is also used in the latest AED and AEM releases to create a repeatable closed-loop DDoS attack analysis and mitigation process that automatically identifies changing attack vectors and provides recommendations specific to those attack vectors for attack mitigation, with the option to automatically apply those recommendations. NETSCOUT's AI/ML-powered ATLAS Threat Intelligence and Adaptive DDoS Protection solution utilizing AED and AEM automates DDoS attack detection and protection workflows to reduce downtime costs and provide better protection for business-critical services whether they reside on-premises or live in the public cloud.

"Adaptive DDoS Protection provides customers with a sophisticated feature set designed to stop the ever-evolving threats to critical IT infrastructure, which has increased by **55% over the last four years**," said Scott Iekel-Johnson, AVP, DDoS and Threat Intelligence at NETSCOUT. "We're continually adding new capabilities to our solution to help organizations protect assets anywhere, including on-premises, in a private data center, or a public cloud through a single solution."

Additional enhancements include holistic management and visibility into blocking non-DDoS threats, a new appliance that supports up to 200 Gbps of DDoS attack mitigation capacity and high-performance decryption, and Virtual AED's extended support for Microsoft Azure public cloud environments, in addition to AWS Cloud, for unified hybrid-cloud DDoS attack protection.

Visit our **website** to learn more about AED, AEM and NETSCOUT's Adaptive DDoS Protection Solution.

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