NETSCOUT

NEWS RELEASE

# NETSCOUT Takes Internet Scale Threat Protection to the Edge

2018-10-23

## New NETSCOUT Arbor Edge Defense Solution is the First and Last Line of Defense with Automated Detection and Blocking of Inbound and Outbound Threats

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.,** (NASDAQ: NTCT), a leading provider of service assurance, security, and business analytics, today introduced **NETSCOUT Arbor Edge Defense (AED)**, a new security solution that redefines the perimeter cyber security stack and serves as the first and last line of defense against multiple types of inbound and outbound threats.

“Data center and network architectures are becoming increasingly distributed, straining traditional perimeter enforcement points. At the same time, targeted campaigns are now backed by internet-scale intrusions like NotPetya. The unique combination of stateless filtering, rigorous curation of threat intelligence, and ingestion of third party feeds, allows NETSCOUT to block outbound threats with the same level of confidence as the inbound DDoS attacks they’ve been blocking for years,” said Jeff Wilson, IHS Markit research director for cybersecurity.

### Bringing Stateless Security to the Edge

NETSCOUT AED is an always-on, in-line solution which can be deployed as a physical appliance or virtual network function. It sits outside the firewall, between the enterprise or data center and the internet. A unique stateless packet processing engine provides efficient blocking of malicious traffic matching Indicators of Compromise (IoCs) without tracking any session state. As a result, NETSCOUT AED can make other perimeter defenses more effective by protecting them from DDoS attacks, and offloading the overhead associated with applying millions of IoCs to traffic streams.

NETSCOUT AED leverages the Company's proven market-leading DDoS technology that is already trusted by thousands of enterprises worldwide. As a result, it provides advanced packet-based protections against complex application-specific DDoS attacks and state-exhaustion techniques; as well as defenses against internet scale threats, neutralizing the malware families that make up the global botnet threat. Armed with millions of reputation-based IoCs, NETSCOUT's stateless packet processing engine can also detect and block outbound communication from internal compromised hosts that have been missed by other devices in the security stack; helping to stop further proliferation of malware and other tactics used within crimeware and advanced threat campaigns.

## Operationalizing Threat Intelligence

NETSCOUT has the unprecedented ability to enable security and network teams to connect and correlate unique intelligence on emerging internet threats and trends, with visibility into what is happening across their entire internal organization from a threat perspective. NETSCOUT's Active Threat Level Analysis System (ATLAS®), collects, prioritizes, and disseminates data on emerging threats based on our unique visibility into over one-third of all internet traffic. **The ATLAS Security Engineering & Response Team** (ASERT) is continuously and automatically delivering high fidelity threat intelligence via the **ATLAS Intelligence Feed**, enabling customers to not only block threats in real-time but enhance their defenses over time.

NETSCOUT believes that effective threat intelligence not only identifies attacks but also provides context to understand and catalogue attack infrastructure, methods, related indicators to enable faster security decisions can be taken with greater confidence. NETSCOUT AED supports standards such as STIX/TAXII for ingestion of third-party threat intelligence and provides a robust REST API to integrate threat detection and blocking telemetry, and contextual threat intelligence into existing SOC workflows and management tools.

"NETSCOUT AED provides a scalable, high-efficiency means of detecting and blocking traffic matching threat intelligence. Using both our own ATLAS Intelligence Feed (AIF) and third-party IoCs ingested via STIX/TAXII, we can detect and block many of today's threats while feeding information into other elements of the security stack via a robust set of APIs," said Darren Anstee, NETSCOUT's chief technology officer for security.

To learn more about NETSCOUT Arbor Edge Defense, visit our **blog**.

## About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver,

integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit **www.netscout.com** or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.

## Safe Harbor

Forward-looking statements in this release are made pursuant to the safe harbor provisions of Section 21E of the Securities Exchange Act of 1934 and other federal securities laws. Investors are cautioned that statements in this press release, which are not strictly historical statements, including without limitation, the statements related to the benefits and capabilities of NETSCOUT Arbor Edge Defense solution, constitute forward-looking statements which involve risks and uncertainties. Actual results could differ materially from the forward-looking statements due to known and unknown risk, uncertainties, assumptions and other factors. Such factors include ongoing development of NETSCOUT AED to adequately address current and future customer requirements in a timely manner. For a more detailed description of the risk factors associated with the Company, please refer to the Company's Annual Report on Form 10-K for the fiscal year ended March 31, 2018 and subsequent Quarterly Reports on Form 10-Q, which are on file with the Securities and Exchange Commission. NETSCOUT assumes no obligation to update any forward-looking information contained in this press release or with respect to the announcements described herein.

©2018 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20181023005695/en/**

NETSCOUT
Kevin Whalen, 781-362-4377
**kevin.whalen@netscout.com**

Source: NETSCOUT SYSTEMS, INC.