

NETSCOUT's Arbor Cloud Expands DDoS Protection Across Asia

2018-10-24

Distributed Architecture Allows for Greater Scale While Also Addressing Emerging Data Privacy Considerations for Cloud Services

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.** (NASDAQ: NTCT), a leading provider of service assurance, security, and business analytics, today announced that it has expanded attack mitigation scrubbing centers for its Arbor Cloud DDoS managed service in Japan and Singapore while also opening a new scrubbing facility in Australia. Additionally, the Company has added new regional resources to its security research organization, the ATLAS Security Engineering & Response Team (ASERT).

By distributing mitigation capacity across more scrubbing centers in Asia, attacks can be mitigated faster and with greater efficiency since they will be closer to the source. This distributed model enables customer traffic to stay in-region and, in some cases, in-country. The **Arbor Cloud** scrubbing centers in Tokyo, Singapore, and Sydney strategically expand coverage that is in closer geographic proximity to many of its largest customers and prospects in the Asia Pacific region. Not only does this allow for quicker remediation, it provides additional value by addressing emerging data privacy considerations on cloud service providers.

Building on NETSCOUT's Position as Frost & Sullivan's Asia Pacific 'Anti-DDoS Solutions Vendor of the Year'

These investments by NETSCOUT follow a **recent announcement** from Frost & Sullivan, one of the foremost technology research firms tracking the DDoS market, naming Arbor as the best 'Anti-DDoS Solutions Vendor' in Asia

Pacific for the third consecutive year.

“NETSCOUT’s Arbor solutions provide customers with comprehensive, high-performing and cost-effective solutions to help them protect against volumetric and sophisticated DDoS attacks. Vast global intelligence, outstanding expertise in DDoS attack management, extensive network partners around the world, and commitment to automation and innovation allow NETSCOUT to outshine competitors and gain greater popularity among organizations in the region, particularly telcos, governments, and enterprises that run critical information infrastructure,” said Vu Anh Tien, Industry Analyst, Cybersecurity Practice at Frost & Sullivan.

ASERT’s Unique Global Perspective

ASERT’s global view into the threat landscape and attack trends reflects the substantial investment in the **ATLAS** infrastructure, a collaborative project with hundreds of network operators who have agreed to share anonymous traffic data covering approximately one-third of all internet traffic. From this unique vantage point, ASERT develops campaign-oriented threat intelligence for customers, complete with the context and confidence information required to detect and stop specific threats and enhance security posture over time. ASERT shares operationally viable intelligence with international Computer Emergency Response Teams (CERTs) and with network operators around the world via intelligence briefs and security content feeds.

NETSCOUT’s Arbor Cloud: Affordable, Fully-Managed DDoS Protection Service

NETSCOUT’s **Arbor Cloud** offers enterprise customers a fully-managed, best-practice distributed denial-of-service (DDoS) defense service that integrates on-premise DDoS protection and cloud-based mitigation for best practice defense of its users during a network attack. When used in combination with Arbor Edge Defense, NETSCOUT’s solution for identifying incoming DDoS attacks and outbound communication from compromised hosts at the network edge, enterprises can continue to deliver critical online services. In addition, **NETSCOUT’s Arbor DDoS solutions** are deployed in the world’s largest service provider networks. NETSCOUT has worked closely with many of these customers, helping them leverage their existing Arbor deployments to launch and support revenue-generating DDoS managed services. Arbor Cloud enables these customers to scale existing, or in some cases launch new cloud-based DDoS security services by giving them access to NETSCOUT’s 9 Tbps of total mitigation capacity.

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's Arbor Cloud 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 slowdowns or downturns in economic conditions generally and in the market for advanced network and service assurance solutions specifically; the volatile foreign exchange environment; the Company's relationships with strategic partners and resellers; dependence upon broad-based acceptance of the Company's network performance management solutions; the presence of competitors with greater financial resources than ours and their strategic response to our products; our ability to retain key executives and employees; and lower than expected demand for the Company's products and services. 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/20181024005260/en/): <https://www.businesswire.com/news/home/20181024005260/en/>

NETSCOUT

Kevin Whalen, 781-362-4377

Sr. Director, Corporate & Marketing Communications

kevin.whelen@netscout.com

Source: NETSCOUT SYSTEMS, INC.