NETSCOUT

NEWS RELEASE

Arbor Cloud to Increase DDoS Attack Mitigation Capacity to 8Tbps

2017-06-13

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

BURLINGTON, Mass.--(BUSINESS WIRE)--Jun. 13, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), announced today that they have more than doubled the capacity of **Arbor Cloud** from 2Tbps to 4Tbps, and will have quadrupled capacity to 8Tbps by the end of 2017. The expansion effort includes upgrades of existing nodes and the introduction of more than a dozen new nodes in major traffic centers in North America, Europe, Asia and South America.

By distributing capacity across four times the number of scrubbing centers globally, attacks can be mitigated more quickly, closer to the source. This distributed model enables customer traffic to stay in-region and, in some cases, in-country. Not only does this allow for quicker remediation, it provides additional value by addressing emerging data privacy considerations on cloud service providers.

“In the aftermath of Mirai and with the continued innovation of IoT botnets, the stakes have changed. This capacity expansion reflects Arbor’s deep commitment to building the Arbor Cloud business for the long term. It allows us to not only support enterprises that recognize the need for DDoS protection, but also help our service provider customers who are leveraging their Arbor deployments to deliver revenue generating managed services themselves,” said Brian McCann, president of NETSCOUT’s Security Business unit.

“Arbor Networks has long been a leader in the DDoS mitigation market and this move shows the company’s commitment to the cloud and DDoS managed services going forward,” said Christina Richmond, program director for IDC's Security Services research practice. “Attack size is a significant concern for both service providers and for

the enterprise. Arbor Cloud serves both markets, and this distributed architecture and greater scale will help them meet customer demand for years to come."

Arbor Cloud for Enterprise: Affordable, Fully-Managed DDoS Protection Service

Arbor Cloud offers enterprise customers a fully-managed, best-practice distributed denial-of-service (DDoS) defense service that tightly integrates on-premise DDoS protection and cloud-based mitigation for best practice defense of its users during any network attack.

Arbor Cloud's on-premise component — **Arbor Networks® APS** — can be deployed as an appliance or virtual solution, delivering inline-visibility into traffic entering the network, and providing always-on DDoS attack detection and mitigation. The on-premise component can be managed by Arbor as part of a fully managed service, or by the customer. The Arbor APS is enhanced by threat intelligence via the ATLAS Intelligence Feed (AIF). Developed by Arbor's Security Engineering and Response Team (**ASERT**), the AIF includes geo-location data and automates the identification of attacks from known botnets and malware while ensuring that updates for new threats are automatically delivered without intrusive software upgrades. Working in unison with the AIF, Arbor APS can also block outbound threats, helping prevent data exfiltration. Finally, Arbor APS provides protection to existing infrastructure, such as firewalls and intrusion prevention systems (IPS), and to business-critical systems, which are frequent targets of DDoS attacks.

Arbor's patented **Cloud Signaling** capability tightly integrates on-premise protection with cloud-based defenses, significantly reducing the time needed to mitigate attacks. This hybrid, multi-layer defense is an industry best practice for DDoS protection services, ensuring that enterprise networks are protected no matter what type of advanced DDoS attack they are facing.

Arbor Cloud's on-demand, traffic-scrubbing service is staffed 24/7 by Arbor's DDoS security experts, providing complete transparency of operation, including a view into blocked hosts and traffic scrubbing performance, offering the flexibility enterprises need to alter attack countermeasures and thresholds.

Arbor Cloud for Service Providers

Arbor is pervasively deployed in the world's service provider networks. Arbor 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 quickly scale existing, or in some cases launch new cloud-based DDoS security services. Arbor is responding to customers and enabling them to meet end-user demand in an efficient and affordable way, without significant capital expenditures in network infrastructure or people. Arbor security experts will be on call 24/7 to support customers under attack and will handle all aspects of the service.

About Arbor Networks

Arbor Networks, the security division of **NETSCOUT**, is driven to protect the infrastructure and ecosystem of the internet. It is the principle upon which we were founded in 2000; and remains the common thread that runs through all that we do today. Arbor's approach is rooted in the study of network traffic. Arbor's suite of visibility, DDoS protection and advanced threat solutions provide customers with a micro view of their network enhanced by a macro view of global internet traffic and emerging threats through our ATLAS infrastructure. Sourced from more than 300 service provider customers, ATLAS delivers intelligence based on insight into approximately 1/3 of global internet traffic. Supported by Arbor's Security Engineering & Response Team (ASERT), smart workflows and rich user context, Arbor's network insights help customers see, understand and solve the most complex and consequential security challenges facing their organizations.

To learn more about Arbor products and services, please visit our website at **arbornetworks.com** or follow on Twitter **@ArborNetworks**. Arbor's research, analysis and insight is shared via the **ASERT blog**. For a global data visualization of DDoS attacks that leverages our ATLAS intelligence, visit the **Digital Attack Map**, a collaboration with Jigsaw, an incubator within Alphabet, Google's parent company (NASDAQ: GOOGL).

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 Arbor's portfolio of solutions, 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. For a more detailed description of the risk factors associated with NETSCOUT, please refer to NETSCOUT's Annual Report on Form 10-K for the fiscal year ended March 31, 2016 and NETSCOUT's 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.

View source version on businesswire.com: **http://www.businesswire.com/news/home/20170613005286/en/**

Source: Arbor Networks Inc.

Arbor Networks
Kevin Whalen, 781-362-4377

kwhalen@arbor.net