NETSCOUT

NEWS RELEASE

Arbor Cloud DDoS Managed Service Wins Best Enterprise Security Solution at 2017 Computing Security Awards

2017-10-18

BURLINGTON, Mass.--(BUSINESS WIRE)--Oct. 18, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), announced today that the **Arbor Cloud** DDoS managed service was named Best Enterprise Security Solution at the prestigious **2017 Computing Security Awards** held last week in London. This is the third major industry award recognizing Arbor Cloud for excellence in distributed denial-of-service (DDoS) protection in the past four weeks. Arbor Cloud was also named **Best Cloud Product** at the Cloud Excellence Awards sponsored by Computing Magazine, and **Best Managed Service** at the CyberSecurity Breakthrough Awards.

“Once again this is tremendous recognition for the DDoS managed service that Arbor has built. The volume and sophistication of DDoS attacks continues to increase, and for many businesses, a managed service is their best option. With Arbor Cloud, smaller organizations can be protected by the same technology and people that defend the world’s largest organizations. Our message is, you don’t have to compromise any longer on something as important as the availability of your business,” said Theresa Abbamondi, Arbor Networks Director of Product Management for Arbor Cloud & Services.

Arbor Cloud: Affordable, Fully Managed DDoS Protection

Arbor Cloud offers enterprise customers’ affordable, fully managed DDoS protection powered by the industry’s leading technology and backed by its most experienced incident responders. Arbor Cloud can be deployed as cloud only, hybrid - where the customer manages the on-premise solution - or fully managed, with Arbor handling all aspects of a best practice multi-layered defense.

Arbor Networks® APS can be deployed as an appliance or virtual solution, delivering visibility into traffic entering

the network, providing always-on DDoS attack detection and mitigation up to 40Gbps. Arbor's patented **Cloud Signaling** capability tightly integrates this on-premise protection with cloud-based defenses, automating a key component of DDoS defense and 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.

Why Does Arbor Cloud Keep Winning Awards?

Industry Leading Scale: Arbor Cloud has 4Tbps of mitigation capacity dedicated to DDoS protection. By distributing capacity globally, attacks can be mitigated more quickly and 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.

Automated Threat Intelligence: 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.

Custom Workflows: The Arbor Cloud team takes the time to understand customer processes and has the flexibility to work within them. With many vendors, even good ones, it's their way or no way.

Customer-focused Reporting: Arbor Cloud also offers complete transparency of operations, including a view into blocked hosts and even packets, offering the flexibility enterprises need to alter attack countermeasures and thresholds. Arbor takes a proactive, consultative approach that leverages global threat intelligence as the basis for recommendations to improve customer's security posture, and supplies executive-level reporting that demonstrates ROI and key metrics for the C-suite.

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 the benefits and features of 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, 2017 and NETSCOUT's subsequent Quarterly Report 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.

Trademark Notice: Arbor Networks, the Arbor Networks logo and ATLAS are all trademarks of Arbor Networks, Inc. All other brands may be the trademarks of their respective owners.

View source version on businesswire.com: **http://www.businesswire.com/news/home/20171018005153/en/**

Source: Arbor Networks Inc.

Arbor Networks
Kevin Whalen, 781-362-4377
kwhalen@arbor.net