NETSCOUT

NEWS RELEASE

Arbor Networks New Arbor SP Insight Big Data Analytics Extension to SP Deployments Raises the Bar for Network Visibility

2016-12-06

Enables Deeper and Wider Network Insights for Faster, More Informed Business Decisions

BURLINGTON, Mass.--(BUSINESS WIRE)--Dec. 6, 2016-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), today announced Arbor SP Insight, a new software-based extension to its Arbor Networks SP platform (Arbor SP) that dramatically expands and enhances network operators' traffic analytics and distributed denial-of-service (DDoS) attack forensics capabilities.

The majority of the world's internet service providers, along with data center operators and large network operators, rely on Arbor Networks' SP platform for network-wide visibility, DDoS detection, traffic engineering and advanced peering and transit analysis. Arbor SP helps these customers maintain peak service performance and availability, intelligently expand their network capacity, understand their operational costs and uncover new service opportunities.

With the launch of Arbor SP Insight, operators can further enhance their network visibility and make more informed operational, security and business decisions faster than ever before. Arbor SP Insight adds powerful new visual analytics and a big data repository to Arbor SP while preserving Arbor's unique flow annotations and enrichment – giving users an infinitely searchable photographic memory of their traffic data with essential network context. Arbor SP Insight's all-new interactive user interface tightly integrates with existing Arbor SP workflows for a near-zero learning curve and unified user experience, so users have the power and freedom to explore their data and reach conclusions faster and more intuitively.

"For years, service providers and global network operators have relied on Arbor SP for traffic visibility, capacity

planning, and peering relationships, not to mention DDoS protection, and for these folks, the network is the business," said Rik Turner, senior analyst at Ovum. "With the big data analytics capabilities of Arbor SP Insight, customers will now be able to understand what's happening on their network like never before. We expect the ability to customize searches and report functionality within Arbor SP Insight to have an impact across the entire organization, from the C-suite to services and marketing teams, and of course, network and security operations."

Network Performance Optimization

Arbor SP Insight enables service providers and global network operators to research impaired network performance events and reduce time to resolution of future events by quickly conducting wide-ranging and fine-grained root cause analysis on large sets of un-aggregated traffic data. Customers can also perform 'What if' analysis on their peering and transit traffic, driving new discoveries and proactive capacity planning and backbone engineering decisions that reduce costs and increase revenues.

DDoS Attack Forensics

Arbor's unique flow annotations and enrichment create crucial context by matching Arbor SP Insight's memory to Arbor SP's knowledge of network topology, customers and traffic patterns – enabling users to conduct agile, multi-dimensional searches of their raw and enriched data with unlimited filtering, the ability to maintain granularity over time, detailed retrospective drill-downs and effortless pivots from graphical to tabular visualizations – all while maintaining state on the event and period of interest.

"Arbor SP Insight transforms an Arbor SP deployment into a rich data lake users can explore at the speed of thought to improve their overall network visibility, application and service performance. Arbor SP Insight's flexible, unlimited and multi-dimensional analytics engine can answer a multitude of business questions, and uncover new insights about traffic and the underlying network. It stores all network flows, both raw and annotated, for as long as the customer needs to retain them for real-time or historical, unstructured analysis. You are limited only by your own imagination and the amount of disk space you allocate," said Talbot Hack, Arbor Networks Director of Product Management for DDoS & ISP Network Visibility.

About Arbor Networks

Arbor Networks, the security division of NETSCOUT, **netscout.com**, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor Networks Spectrum™ advanced threat solution delivers complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of attack campaigns, malware and malicious insiders. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to

provide a richer picture into networks and more security context so customers can solve problems faster and reduce the risks to their business.

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 of Arbor SP Insight and the Arbor Networks' SP platform, 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/20161206005154/en/**

Source: Arbor Networks Inc.

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