NETSCOUT

NEWS RELEASE

Arbor Networks Extends Global Leadership Position in On-Premise DDoS Protection, According to IHS Technology

2017-06-06

On-Premise Protection is First Line of Defense Against Today's Advanced DDoS Attacks

BURLINGTON, Mass.--(BUSINESS WIRE)--Jun. 6, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), was identified once again as the top supplier of distributed denial-of-service (DDoS) mitigation appliances overall, as well as in the Carrier, Enterprise and Mobile market segments, according to a new report from IHS Technology, formerly Infonetics Research.

"Arbor continues to lead the market because they are continuously innovating and moving into fast-growing markets. They are well positioned to benefit from all of the macro trends driving growth in the DDoS mitigation product market," said Jeff Wilson, senior research director, cybersecurity technology for IHS Markit. "Arbor now offers many price points and capacity options for on-premises protection, from low cost sub-100Mbps virtual solutions to 160Gbps carrier-class appliances. With the Arbor Cloud managed service, Arbor is leading the industry in best practice hybrid defense."

DDoS Market Drivers

According to Wilson, "Without a doubt, the number one driver for the DDoS prevention market is the attacks themselves." Wilson goes on to say, "The rise of botnets and easy-to-use tools for launching attacks means that there are more DDoS attacks pushing greater volumes of traffic, initiated by a wider variety of attackers than ever before. There is no indication that the pace of innovation in the creation of attacks and the ingenuity that drives the distribution of those threats will ever slow down, and so prevention solutions need to continue to evolve as well."

Arbor's On-Premise DDoS Solutions

Arbor APS provides always-on, in-line protection from network and application layer DDoS attacks and some advanced threats. Arbor APS inspects traffic entering or leaving the network, analyzes it, and drops traffic that is determined to be part of a DDoS attack or from an identified DDoS attacker. Via Cloud Signaling, Arbor APS delivers intelligent integration between on-premises and in-cloud DDoS attack protection. Arbor APS is further enhanced by threat intelligence via the ATLAS Intelligence Feed (AIF). Developed by Arbor's Security Engineering and Response Team (ASERT), the AIF includes geolocation data and automates the identification of attacks against infrastructure and services from known botnets and malware while ensuring that updates for new threats are automatically delivered without software upgrades.

Arbor TMS is a vital component of the Arbor Networks SP solution. Arbor Networks TMS surgically removes DDoS attack traffic from the network without disrupting key network services. It also provides comprehensive, real-time visibility into network applications, proactively monitoring denial of service attacks so customers can maintain service performance. Arbor TMS can be deployed in-line to provide "always on" protection.

Arbor TMS supports a mitigation architecture called diversion/reinjection. Arbor TMS removes only the malicious traffic and forwards the legitimate traffic to its intended destination. This is highly advantageous for service providers, large enterprises and large hosting/cloud providers. It enables a single, centrally located Arbor TMS to protect multiple links and multiple data centers. The result is more efficient use of mitigation capacity and fully non-intrusive security. Other in-line devices may inspect all traffic all the time on the links they monitor. Arbor TMS only needs to inspect traffic that is redirected to it in response to an attack on a specific target.

Supporting Resources

- IHS Technology Report: **IHS Technology DDoS Prevention Appliances Biannual Market Tracker: Regional, H1 2017**
- Press Release: **Arbor Networks Further Automates DDoS Attack Mitigation for MSSPs and Enterprise Customers**
- DDoS Threat Landscape: **Arbor's 12th annual Worldwide Infrastructure Security Report**
- Arbor's DDoS protection portfolio works for all types of businesses, **learn how**.

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.

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.

Results based on IHS Markit, Technology Group, IHS Markit Technology DDoS Prevention Appliances Biannual Market Tracker: Regional, H1 2017. Results are not an endorsement of Arbor Networks, Inc. Any reliance on these results is at the third party's own risk. Visit **technology.ihs.com** for more details.

View source version on businesswire.com: **http://www.businesswire.com/news/home/20170606005471/en/**

Source: Arbor Networks Inc.

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