

Arbor Networks Further Automates DDoS Attack Mitigation for MSSPs and Enterprise Customers

2017-06-06

Centralized Management and Enhanced Cloud Signaling Provides Automated Protection Against Known and Emerging Threats from the Data Center to the Cloud

BURLINGTON, Mass.--(BUSINESS WIRE)--Jun. 6, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), announced a new version of its on-premise, always-on, inline distributed denial-of-service (DDoS) detection and mitigation platform for enterprise customers, **Arbor Networks APS™**. Arbor APS v5.11 includes new features designed to ease the management of multiple APS devices and reduce the time to attack mitigation via improvements to its powerful and unique **Cloud Signaling** capability.

“Cloud Signaling has been a key innovation in enabling the industry-wide adoption of hybrid, or multi-layer DDoS defense as a best practice. Arbor understands the threat landscape and created an elegant way of linking on-premise and cloud-based mitigation. This tight connection is key to delivering protection from today's advanced DDoS attacks,” said Rob Ayoub, research director in IDC's Security Products program.

As DDoS attacks continue to dramatically rise in size, frequency and complexity, automation has become increasingly critical to protecting the network against these attacks. Arbor's Cloud Signaling capability automates key aspects of DDoS defense, tightly integrating on-premise and cloud-based mitigation. The fidelity of Arbor Cloud Signaling has been further enhanced as locally configured blacklists/whitelists on the Arbor APS are now embedded in the Cloud Signaling communication.

“Automation is a top priority for most organizations today. From a security perspective, that means they're stretched thin, using too many tools, chasing too many threats, with too little context. Arbor is really focused on being an operational asset for our customers by delivering solutions that help scale teams, enable faster time to

mitigation, and automate as many processes as possible without sacrificing effectiveness,” said Tom Lyons, Arbor’s vice president of product management.

The Arbor DDoS attack protection solution delivers intelligent integration between on-premises and in-cloud DDoS attack protection, backed 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.

Easier Management of Multi-APS Environments

This new management functionality benefits enterprises that manage the APS devices, as well as MSSPs that offer multi-layer or hybrid DDoS managed services to their customers. Arbor APS v5.11 includes a new console that greatly eases the management of multi-APS environments by providing centralized configuration and aggregated views of all DDoS attack activity. Each console can manage up to 50 APS devices.

Automating Key and Certificate Operations with Venafi

Arbor Networks has partnered with Venafi, the leader in machine identity protection, to make it easy to setup and maintain large scale SSL/TLS inspection required to stop sophisticated Layer 7 DDoS attacks hiding in encrypted traffic. Now the Arbor APS is continuously fed the most current SSL/TLS keys and certificates used across an enterprise to enable complete inspection and the ability to more quickly mitigate even the most sophisticated DDoS attacks.

“Sophisticated DDoS attacks are using the cloak of encryption to go undetected,” said Kevin Bocek, VP security strategy at Venafi. “With Arbor Networks integration now available for the Venafi Platform, customers can maximize visibility into encrypted traffic and protect themselves faster from DDoS attacks quickly becoming the norm. Protection is maintained with the help of Venafi continuously automating the entire SSL/TLS key and certificate lifecycle so Arbor Networks systems have the most current set of machine identities to perform inspection.”

Supporting Resources

- IHS Technology Report: **IHS Technology DDoS Prevention Appliances Biannual Market Tracker: Regional, H1 2017**
- Press Release: **Arbor Networks Extends Global Leadership Position in On-Premise DDoS Protection, According to IHS Technology**
- DDoS Threat Landscape: **Arbor’s 12th annual Worldwide Infrastructure Security Report**
- Video: Arbor’s DDoS protection portfolio works for all types of businesses, **learn how.**

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing all machine-to-machine connections and communications. Venafi protects all machine identity types by orchestrating cryptographic keys and digital certificates for SSL/TLS, IoT, mobile, code-signing, and SSH. Venafi provides global visibility of machine identities and the risks associated with them for the extended enterprise — on premise, mobile, virtual, cloud and IoT — at machine speed and scale. Venafi puts this intelligence into action with automated remediation that reduces the security and availability risks connected with weak or compromised machine identities while safeguarding the flow of information to trusted machines and preventing communication with machines that are not trusted.

With over 30 patents, Venafi delivers innovative solutions for the world's most demanding, security-conscious Global 2000 organizations, including the top five U.S. health insurers, the top five U.S. airlines, four of the top five U.S., U.K. and South African banks and four of the top five U.S. retailers. Venafi is backed by top-tier investors, including Foundation Capital, Intel Capital, Origin Partners, Pelion Venture Partners, QuestMark Partners, and Silver Lake Partners. For more information, visit www.venafi.com.

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](https://twitter.com/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.

View source version on businesswire.com: <http://www.businesswire.com/news/home/20170606005498/en/>

Source: Arbor Networks Inc.

Arbor Networks

Kevin Whalen, 781-362-4377

kwhalen@arbor.net