Arbor Networks Introduces Pravail® Security Analytics for Advanced Threat Detection, Incident Response and Security Forensics

*Test-drive the powerful new Pravail Security Analytics solution with a **free trial***

BURLINGTON, Mass., March 18, 2014 – Arbor Networks Inc., a leading provider of DDoS and advanced threat protection solutions for enterprise and service provider networks, today introduced Pravail Security Analytics for advanced threat detection, incident response and security forensics. The technology delivering this solution was developed by Packetloop, a Sydney, Australia-based innovator in the field of Big Data Security Analytics that was acquired by Arbor in September 2013.

"Arbor is able to offer enterprise security teams the richest set of data regarding the activities happening on their network. Pravail Security Analytics is a powerful solution that will allow our customers to see attacks on their global networks faster and in more detail than seen before. We're focused on bringing meaningful context to massive amounts of data so that security teams can focus on the critical few, react faster and identify the threats lurking within their network environment before they impact the business," said Arbor Networks President Matthew Moynahan.

Global Attack Intelligence for Local Protection

The attack intelligence that keeps Pravail Security Analytics at the cutting edge of network security comes from Arbor's ATLAS® Active Threat Level Analysis System. ATLAS is a collaboration with nearly 300 service providers who share anonymous data with Arbor, up to 70TB/sec of global Internet traffic. This collective view delivers globally scoped insight into the attack landscape. This data set is analyzed by Arbor's security research team who then develops detection methodologies; and creates fingerprints that identify threats and malicious activity occurring within the enterprise.

Reveal Attacks Hidden within Your Global Network

Today's breed of attacker is not looking to be a short-term and visible nuisance. They use stealthy and sophisticated methods to penetrate an organization's perimeter and the indicators of compromise are often impossible to identify before it's too late. In order to really understand subtle, advanced targeted attacks, enterprises need a complete record of all network traffic. By analyzing data very quickly, Pravail Security Analytics can be used for real-time attack response decisions, and by storing the data for future reviews, it can be looped to identify previously undetected attacks using the latest threat intelligence.

Rapid Deployment, On-Premise or In the Cloud

Pravail Security Analytics uses big data technologies that lower the barrier to entry for organizations looking to deploy and operate world-class security analytics. An organization can securely upload packet captures to Pravail Security Analytics in the Cloud and be analyzing their data within minutes of a threat being identified. For organizations that cannot upload their packet captures for compliance or regulatory reasons, Pravail Security Analytics can also be deployed as an on-premise solution using distributed Collector appliances. The Collector appliances can be used to scale out storage or processing capabilities for high speed capture points, or for deployment into multiple locations to provide distributed coverage. Most importantly, the Collector appliances operate in real-time, streaming the security analytics data to the Controller for analysis with virtually no delay. This means security analysts can track attacks live, as they happen, or perform post hoc analysis with stored and uploaded packet captures.

By using Controllers and Collectors, Pravail Security Analytics can support three flexible deployment architectures:

- **Pravail Security Analytics Cloud** - where the Controller is the Pravail Security Analytics cloud platform. Data is uploaded in the form of packet captures and processed in the cloud.
- **On-Premise Collector to Cloud Controller** - A collector is deployed on your network and processes real-time network streams. The results are encrypted and streamed to the cloud where they are analyzed.
- **On-Premise Collector to On-Premise Controller** - in this model nothing leaves your network. Data is collected and processed within your network and streamed to a Controller within your network.

The technology in the Collectors can scale to meet network speeds, length of packet capture retention (for looping) and real-time processing speed. This means that full real-time functionality of Pravail Security Analytics is available for network speeds in excess of 10Gbps. Big Data Security Analytics on a grand scale. Collectors are available in multiple physical appliance form factors as well as Virtual Machines. Controllers can also be scaled but aren't as heavily utilized as Collectors. They store all the metadata and make it available for analysis and can scale to support decades of processed data. At this time Controllers are only available in a physical appliance or of course by leveraging the cloud platform.

A **production demonstration** of the Cloud solution is available that leverages pre-existing data sets. This enables the user to test drive the solution and see its powerful capabilities firsthand. A **free trial** of the Cloud solution is also available, enabling users to quickly analyze their own network packet captures for threats, anomalies and misuse. The free trial allows users to upload up to 1GB of their data for thirty days.

General availability of the Pravail Security Analytics on-premise Collector solution is planned for April 30, 2014.

“Organizations are looking for solutions that help them deal with the problem of advanced threats hidden within their networks," said John Grady, research manager for Security Products at IDC. "Arbor’s Pravail Security Analytics is a powerful platform for the security analyst, processing huge amounts of data and providing actionable intelligence through intuitive visualizations that reveal threats in both real-time and historical data sets. Arbor now has a unique combination of NetFlow, packet capture and global threat intelligence from their ATLAS infrastructure to address today's dynamic threats that evade signature-based solutions.”

About Arbor Networks

Arbor Networks, Inc. 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’s advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market leading analytics for dynamic incident response, historical analysis, visualization and forensics. 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 risk to their business.

To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor’s research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.

Trademark Notice: Arbor Networks, Peakflow, ArbOS, How Networks Grow, ATLAS, Pravail, Arbor Optima, Cloud Signaling, the Arbor Networks logo and Arbor Networks: Smart. Available. Secure. are all trademarks of Arbor Networks, Inc. All other brand names may be trademarks of their respective owners.