Arbor Networks, the cyber security division of NETSCOUT, 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 risks 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.
Overview

To investigate and respond to today’s orchestrated attack campaigns, security teams need instant access to real-time threat data and an archive of both threat indicators and traffic data from across their whole network.

Too often, today’s incident response tools are failing enterprise security teams because deployments cannot provide both broad and deep information across the network, users wait hours for results, expert users are required and, in many cases, the data required has already been aged out of the product.

Arbor Networks understands that security teams who investigate and respond to advanced threats need access to both real-time and historical threat and traffic data — at the speed-of-thought. Arbor Networks Spectrum™ provides this visibility and access, enabling the discovery of new threats and providing innovative workflows and visualisations that enable security teams to validate and investigate any threat on their network in minutes — not hours.

Arbor Networks Spectrum delivers a new approach to incident response with a purpose-built platform:

Unlike other solutions, which rely on logs or events for their sources of data, Arbor Spectrum uses the network. The network is at the heart of modern business, and attackers cannot avoid it (without physical access) in the way that they can evade detection/prevention solutions. All perimeter incursions are visible on the network, if we look in the right way.

- Fast and easy access to a complete network threat and traffic archive. Traffic and threat indicator visualizations that users quickly understand host behavior over time.
- Workflows that empower security teams to easily pivot from threat discovery to incident investigation to forensics, all within the same user-interface.
- Multiple threat intelligence sources for detection: Arbor ATLAS® Intelligence Feed; Emerging Threats Pro; third-party user specified policy.
- Flexible deployment options that allow enterprises to easily and cost-effectively cover their entire network
- Efficient use of storage to preserve the rich layer 7 traffic data for the last month or more.

Arbor Spectrum provides:

Packet + Flow
Arbor Spectrum utilizes an innovative architecture that combines the analysis and archive of packets and flow within a single solution. While packet analysis and archive provides deep intelligence at critical points on the network, flow data, such as NetFlow, provides the broad, cost-effective visibility needed to cover the entire network. Arbor Spectrum can support packet-only deployments, flow-only deployments or a combination of the two.

By combining the analysis and archive of both packet and flow data, Arbor Spectrum provides security teams with a unique insight into their business, allowing threats and suspicious behaviors to be investigated no matter where they occur within the enterprise network.

Real-Time Traffic Analysis and Threat Detection
Arbor Spectrum delivers high-performance packet and flow analysis in real-time to identify attack campaign threats. For both packet and flow analysis, Arbor Spectrum can apply both proprietary Arbor and user supplied intelligence to identify threat indicators within your network. The ATLAS Intelligence Feed is powered by ASERT.

ASERT uses a combination of Arbor’s global analysis of more than one-third of the world’s Internet traffic, advanced malware research, botnet infiltration and a global network of honeypots to generate a high-fidelity feed of global threat data. For packet analysis, the ATLAS Intelligence Feed combines URL, domain and IP reputation to identify threat indicators based on a match with known bad actor or current attack campaign infrastructure. For flow analysis, the ATLAS Intelligence Feed applies IP reputation to consumed flow records.
In addition to the ATLAS Intelligence Feed, Arbor Spectrum also uses the industry-leading Snort and Suricata security policies from Emerging Threats Pro LLC for deep packet inspection and the identification of malware, vulnerability exploits and other indicators. Users can also apply their own custom Snort policies for analysis. Arbor Spectrum applies these policies with an internal Suricata engine.

Arbor Spectrum also includes “built-in” system rules that analyze flow and packets for network-based indicators such as port scans, host scans and long-lived sessions.

In 2016, Arbor intends to enhance the platform to analyze both packets and flow with additional third-party and user-defined security intelligence. Users will be able to import security content that follows the Structured Threat Information eXpression (STIX) standard. Users will also be able to define business specific policies that enable the detection of unusual or inappropriate network communications.

**Unique Visualizations and Workflows**

The Arbor Spectrum user-interface is designed to provide security analysts and incident responders with workflows that speed up key parts of the incident response process. The user-interface allows the user to interactively navigate, search and pivot through both threat-indicator and traffic data, giving them the visibility they need to discover, investigate and respond to threats.

The user interface, in release 2.1, includes five modules:

- Indicator prioritization overview of threats detected using ATLAS Intelligence or other sources, and specific network activity
- Hunting, to provide visibility into threat indicators detected across the network over time
- Host-Dossier to give a complete picture of host threat and traffic activity
- Connections to provide a detailed view of network conversations matching a specific filter
- Investigations to aggregate related indicators, host profiles and network connections into a single view of an advanced threat

**Scalable, High Performance Traffic Archive**

Arbor Spectrum provides security teams with fast access to a rich traffic archive derived from packets and/or flow without the need for complex deployments involving hundreds of terabytes of storage. The platform architecture maintains rich traffic data over an extended period of time — often weeks or months longer than that offered by traditional network forensic products. This innovative approach to network forensics is designed for ultra-fast search of the archive. This empowers security analysts to execute complex queries over long periods of time within seconds — not hours.

For flow analysis and archive, the 64 TB AT-2300 appliance maintains a traffic archive of 6 months or more while collecting up to 100,000 flows per second.

For packet analysis and archive, Arbor Spectrum saves off a complete PCAP for every session where a threat indicator identified by AIF, ET Pro or custom Snort policies is seen. This PCAP is easily accessible from the Spectrum user-interface to allow the user to share and view the PCAP in external tools, such as Wireshark, next to the automatically generated decode provided within the Arbor Spectrum interface itself.

Where captured packets do not trigger a threat indicator, Arbor Spectrum applies an efficient use of storage to archive essential elements of the traffic. This includes the first 1,000 bytes, key layer 3/4 traffic data and layer-7 metadata for each session. For the 2.0 release, the extracted/stored data includes:

- Start time and duration of the connection
- Quality of service value
- Protocol
- Size of the traffic streams in packets and bytes (in each direction)
- IP addresses, ports, and TCP flags for the source and destination
- IP address of the collector that received the traffic
- Requested DNS hostnames
- HTTP URL
- Complete HTTP headers
- First 1000 bytes of session

---

1 Sarbanes-Oxley Compliance Disclaimer: Functionality and features described within will be provided only when and if available and are not commitments on the part of Arbor Networks.
Arbor Spectrum: Traffic Analysis and Archive

In the near future, Arbor intends to enhance the platform to provide users with direct access to the first 1,000 bytes of each session with the option to download a reconstructed PCAP of that traffic.

Platform enhancements may also extend the rich traffic data archive to include:

- File hashes
- Stream entropy
- TLS/SSL server certificate
- TLS/SSL common name, subject name, issuer name
- TLS/SSL certificate fingerprint
- FTP user name and password
- FTP data checksum
- SMTP meta-data

Through this efficient approach to network forensics, a single AT-2300 appliance can maintain a month or more of archived information when processing more than 5 Gbps of traffic. Arbor's approach also allows for users to search this data and get results up to 10x faster than with any other network forensic product.

When analyzing archived traffic for new threats (new policies), Arbor Spectrum won't have to replay every packet; it will focus only the data applicable to the policy. For most Snort and Suricata signatures that require payload analysis, the first 1,000 bytes of the session (as stored by Arbor Spectrum) provide the necessary traffic for this retrospective analysis.

Future PCAP Options

In 2016, Arbor intends to enhance the platform with additional workflows for analyzing and archiving full PCAPs. First, users will be able to upload PCAPs to a packet collector for analysis and archive — just as if the traffic was collected and analyzed in real-time.

To empower the real-time tracking of threats throughout the network, Arbor intends to provide users with the workflow and functionality to initiate a full packet capture for selected hosts or connections via the existing packet collectors. The platform will provide a full decode of the PCAP — as well as providing an easy means to quickly and easily download the PCAP for analysis in external tools, such as Wireshark.

---

2 Sarbanes-Oxley Compliance Disclaimer: Functionality and features described within will be provided only when and if available and are not commitments on the part of Arbor Networks.

3 Ibid.
A Scalable Deployment Architecture

Arbor Spectrum can provide full security visibility into the entire network cost-effectively and quickly, giving the user the ability to access network traffic and threat indicator information over extended time-periods at the speed-of-thought. Spectrum allows the user to investigate threats quickly and easily, allowing the timeline of an attack campaign to be quickly determined and lateral movement of a threat inside network understood, so that the correct response can be taken before the attacker achieves their goal.

For Medium to Large Enterprises

Arbor recommends a pervasive deployment analyzing both packets and flows throughout the network. Packet collectors should be deployed at the Internet and data-center edge as well as the network core. Flow provides a cost-effective method to gain broad visibility into the network. Flow generation should be enabled in the Internet edge routers as well as the core and aggregation edge routers, and the flow should be exported to Spectrum flow collectors. The following is an example of an enterprise deployment:

For Data Centers

The same methodology applies. Packets should be captured from the Internet edge and the core/aggregation edge, and they can also be captured deeper from the top of the rack (TOR) or end of row (EOR). Flow should be exported from all routers and switches that provide support for this functionality, to give the broadest view. The following is an example:
The controller appliance provides the graphical, web-based user-interface and manages the packet and flow collectors. In release 2.0 a single controller can support up to five packet collectors and five flow collectors. Each collector is single purpose i.e. a packet collectors or flow collector.

Multiple capture interfaces on each collector (1 Gigabit Ethernet and/or 10 Gigabit Ethernet) receive packet or flow traffic from sources within the monitored network. The sources for packet traffic are network taps or mirror ports. The source devices for flow are routers, switches or probes.

Because flow can be a very cost-effective means to gain broad visibility across a network, a customer can start with flow-based visibility and add packet visibility, for greater depth, as they grow their solution. This architecture can provide a more cost-effective deployment strategy over comprehensive packet capture throughout the network. Packet captures are surgically deployed at key network points.

In 2H2016, Arbor will provide virtual software licenses for the Spectrum controller and collector functions. This will provide additional flexibility and the potential to use Spectrum more easily within NFV environments. In release 2.0 Spectrum controller and collector licenses can only be used on Arbor appliances.

---

**Summary**

**Incident Response At The Speed Of Thought**

Arbor Spectrum, leveraging flexible deployment options, provides broad and deep security visibility into the enterprise network and beyond. As a result, security teams can investigate and respond to threats accessing both real-time and historical threat and traffic data — at the speed-of-thought. Only Arbor Spectrum provides network truths, enabling the discovery of new threats and providing innovative workflows and visualizations that enable security teams to quickly validate and investigate any threat on their network.