Arbor Networks SA

Visualizations and fast workflows combined with ATLAS® Intelligence to find and validate attacks at the speed of thought, anywhere within the network.

Key Features and Benefits

- Explore and understand attacks across the entire network
- Upload network packet captures from anywhere in the network, not just where you have a security enforcement point, to get an unprecedented view of attack risk across your entire global network.
- Visualization of real time attack trends to quickly find indicators of attack and build an attack timeline in minutes.
- Identify and validate an attack in minutes with interactive zoom and pivot, search and confirm an attack with a threat decode.
- Use unique "looping" capability to use new threat details to identify attacks in past network traffic activity.
- Confirm indicators of attack with ATLAS intelligence (ATLAS has visibility into the attack data of One-Third of the world's Internet traffic).
- Use custom feeds or intelligence to find and validate attacks in minutes.
- Simple deployment to start analyzing within hours of set up.

The most devastating advanced attacks are those that operate "under the radar" and create lot of damage before they are detected. In order to effectively—and quickly—identify these attacks, organizations become familiar with the traffic patterns in their network and be able to spot possible indicators of attack as soon as they occur.

Arbor Networks® SA solution gives organizations an unprecedented and detailed view of attacks in any captured network traffic, allowing users to analyze data at the speed of their thoughts versus waiting for long queries. Powerful visualizations display data from multiple perspectives (attacker, target, location or attack type)—enabling security analysts to quickly assess the security posture of the organization. Once an indicator of compromise has been identified, SA provides the analyst with actionable intelligence, allowing confirmation of the details and extent of the attack. Further, SA provides a look back in time, re-evaluating existing data with new attack information to ensure a complete picture of compromise.

Using SA On-Premise, organizations have the ability to:

- Identify indicators of attack in network traffic patterns in real time.
- Investigate and explore attacks without having any data leave the network.
- Analyze and process data faster and with more accuracy.
- Create attack timelines for threats that may have compromised the system months before discovery.
- Pinpoint attacker location by country or city or ISP (ASN).
- Scrutinize target hosts to uncover where infections may have spread.

SA On-Premise Specifications

SA On-Premise solution is deployed using a Controller appliance and distributed Collectors. The Collectors are available as appliances enabling organizations to scale out storage or processing capabilities for high speed capture points, or for deployment into multiple locations to provide distributed coverage. The Controller is used to store and analyze the security analytics data as well as manage the Collectors.

ARBOR® NETWORKS

Why Arbor?

Deepest Level of Network Traffic Information Visibility

SA uses packet capture to give organizations the richest set of data regarding the activities happening on the network. This level of activity awareness is unmatched by products that simply sit at the perimeter logging events.

Security Based on Real Attack Data

Threat intelligence at the cutting edge of network security comes from multiple sources, including real attack data derived from the ATLAS® Active Threat Level Analysis System. Using this system, Arbor monitors Internet traffic to detect new threats that are targeting the network. This data is analyzed by security experts distilled into analytics or detection policies.

Fueled by World-Class Research

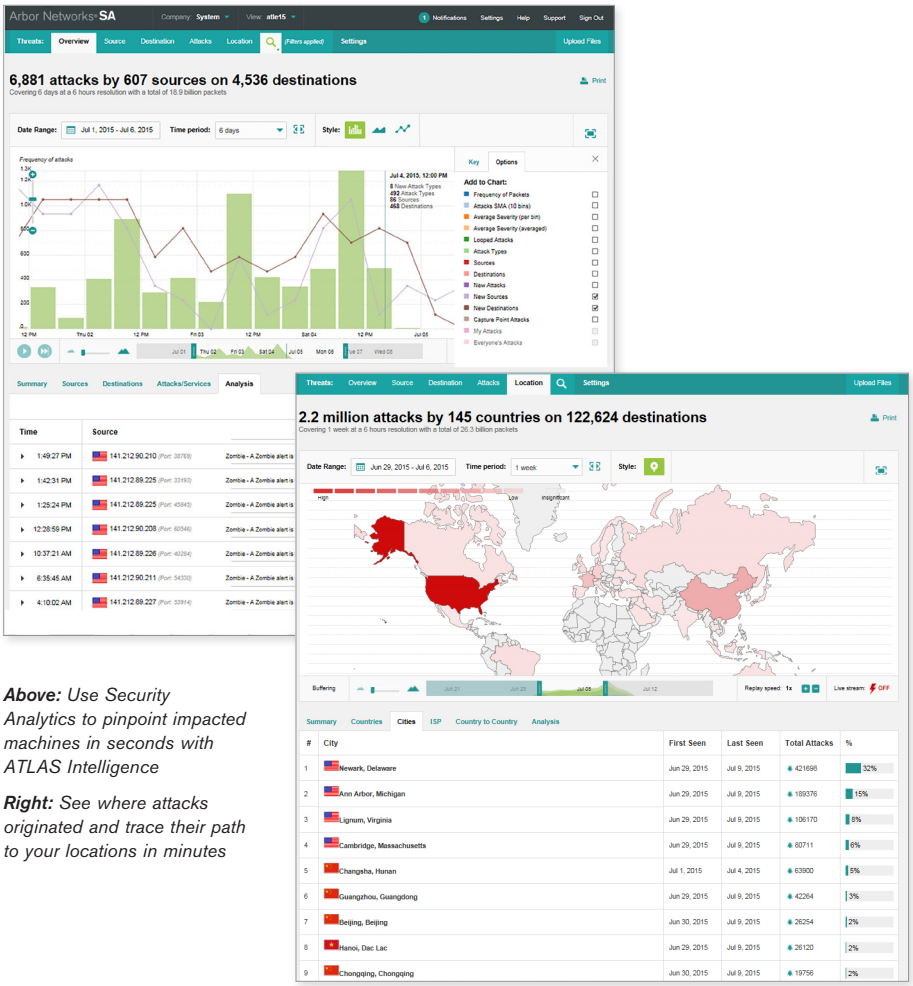
Arbor maintains a dedicated team of security professionals to continuously analyze the threat landscape to ensure the SA product family is up-to-date against the latest advanced threats. ASERT is a renowned group of researchers and engineers that monitors data from ATLAS, and other sources, to create "fingerprints" that identify threats and malicious activity occurring within the network.

Highly Scalable Solution to Accommodate Growth or Change in the Data Center

The SA solution can be easily scaled to accommodate the changing needs in the enterprise. As networks grow and more information flows through the systems, the platform can adjust by adding Collectors to increase processing capability or storage for data retention.

"I would use this interface to quickly find attacks every day of the week compared to the IDS we have in house."

North American Industrial



Above: *Use Security Analytics to pinpoint impacted machines in seconds with ATLAS Intelligence*

Right: *See where attacks originated and trace their path to your locations in minutes*

SA Controller

All deployments of the SA On-Premise solution must include at least one Controller, as it's the primary device for security analysts to interact with. The Controller is responsible for:

- Running the Web Interface and User Interface of the application.
- Receive PCAP uploads and assign them to a collector for storage and processing.
- Storage of the security analytics metadata including:
- Deep Packet Inspection (DPI) results for all packets relating to an attack.
- Queries against the meta data.
- Management of the threat intelligence feeds and custom feeds.
- Issuing the command to Loop stored data on the Collectors (automatic and customer initiated).
- Mitigation and containment with Arbor Networks® APS blacklists

SA Collectors

The Collector appliance processes network streams (Live Capture Points) or Packet Capture files (Non-Live Capture Points), sending metrics and metadata to the Controller for storage, visualization and querying. It uses a mirrored copy of the traffic taken from either a network tap or via a mirror port on a network appliance (switch or load balancer) and adds no latency to the network flow. The Collector is responsible for the following functions in SA:

- Writing PCAP files to disk (for uploaded PCAPs).
- Writing real time streams to disk in the form of PCAPs.
- Analyze real time streams for matches against enabled attack signatures. For discovered attacks, perform analysis of PCAP data and extraction of security analytics metadata including:
  - Metrics
  - Counters
  - Deep packet inspection information.
  - Encapsulation and sending of security analytics metadata to the Controller
  - Looping existing stored data against delta changes to rules (feeds and custom signatures) to find previously undetected attacks.
  - Support for multiple network segments on a single packet collector

"We were able to set up and start analyzing attack traffic data using Arbor Networks SA within two hours of the appliances arriving on site."

Regional Telecommunications Provider

"We were able to identify trojan programs hidden on several PCs using several weeks of data. We were able to find this in minutes using Arbor Networks SA."

Global 2000 Organization

Features	6115
Security Analytics Data Storage (raw)	15 TB
Hard Drives	8 x 2 TB SATA 7200 RPM
Size	2 RU
Cluster Interface Options	4 port SFP options for 10/100/1000 Copper and GE SX/LZ Fiber
Management Interfaces	2 x XEON ES-2658; 2.1 Ghz/20 MB; 8 Core Processors
Memory	64GB
Power Supplies	Dual AC or DC Power

Features	6015	6064
Maximum Capture Points	1	1
Packet Capture Storage (Raw)	15 TB	64 TB
Hard Drives	8 x 2 TB SATA 7200 RPM	16 x 4 TB SATA 7200 RPM
Size	2 RU	3 RU
Capture Interface Options	4 Port SFP Options for 10/100/1000 Copper and GE SX/LX Fiber; 2 Port SFP+ Options for 10GE networks	
Managment Interface	2 x 10/100/1000 Copper	
Processor	2 x XEON ES-2658; 2.1 Ghz/20 MB; 8 Core Processors	
Power Supplies	Dual AC or DC Power	

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

DS/SA/EN/0815-LETTER