Arbor Networks® Spectrum

Epic Range, Faster Proof

Unite a macro view of internet traffic with a micro view of internal network traffic to detect and confirm the most damaging threats as they happen.

KEY FEATURES

- High confidence campaign indicators with ATLAS Intelligence
- Unique work flows to rapidly surface and connect threat indicators and suspicious activity
- High performance network traffic archive. Access to months of network data at your finger tips
- Search and pivot months of network data in seconds
- Deployed in less than a day. Appliance and virtual form factors.

DETECT

- View of relevant indicators to start investigating
- Detect new threats with ATLAS Intelligence indicators
- Import STIX feeds to apply shared threat intelligence
- Retrospective analysis to search archive for newly identified indicators

ATLAS Intelligence Indicators

ATLAS is the world's largest data set of live Internet traffic telemetry (approximately one-third of all Internet traffic). ATLAS allows Arbor to monitor attack activity levels across the Internet and then further distills those attack traffic patterns into highly vetted Intelligence Indicators on an hourly basis into Spectrum.

Advanced malware is no longer the most dangerous enemy in the world of advanced threats. The new enemy is human orchestrated. It's the attack campaign — a series of hidden events engineered to create chaos.

Conquering advanced threat campaigns demands a secret weapon — traffic. By uniting a comprehensive macro view of internet traffic with a micro view of traffic on your network, Arbor Spectrum reveals previously invisible clues while providing insight, speed and perspective that boosts the effectiveness of your entire security team.

- **Epic Range:** Spectrum provides complete network visibility paired with thoroughly vetted ATLAS (Automated Threat Level Analysis System) threat intelligence distilled from one-third of all global internet traffic.
- **Faster Proof:** Reach conclusions that matter — faster — with Arbor Spectrum's real-time flow and packet analysis. Activated by rapid search and easy pivots into months of past activity, any other security solution.

How Arbor Spectrum Works

Spectrum leverages Arbor's global visibility with ATLAS unique threat intelligence and your own threat data and traffic patterns to detect, investigate and prove the most damaging threats.

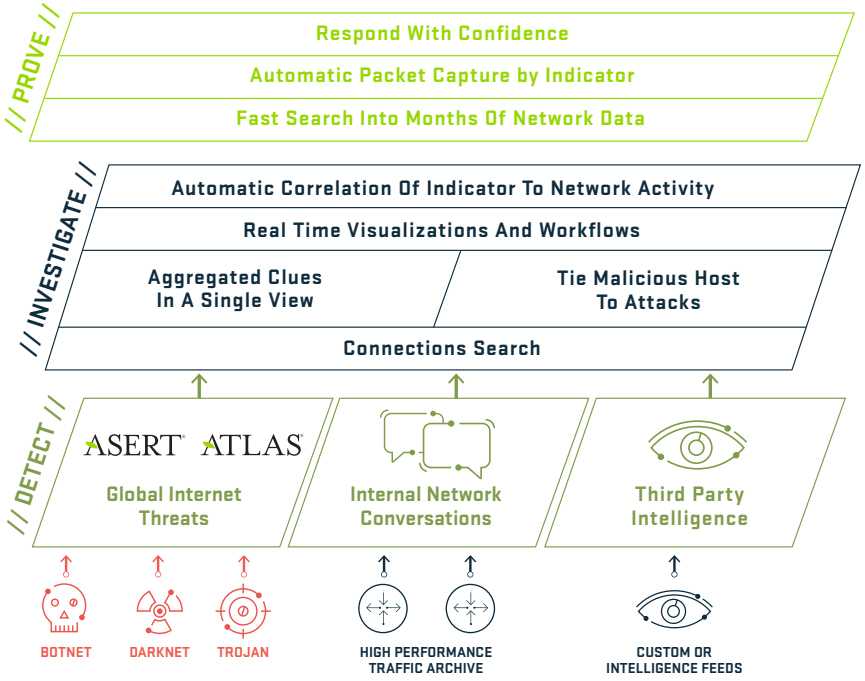

Figure 1: How Arbor Spectrum Works

ARBOR NETWORKS
The Security Division of NETSCOUT

INVESTIGATE

Indicator Prioritization

Real time visual representation of trends in new indicators (threat targets, sources).

Investigations Module

Aggregate clues such related indicators, host profiles and network connections into a single view of an advanced threat.

Host Dossier with User ID/Activity Directory Integration

- Unique Host-Dossier workflows identify and track lateral movement within the network.
- A detailed view of network conversations between hosts and connection points of interest.

PROVE

Automatic Packet Capture of Any Indicator of Compromise

Enables disruptive and automated forensics by storing PCAPs of any identified indicator, making forensics scalable and cost effective.

Manual Packet Capture of Any Host or Conversation

Capability to trigger a PCAP of any host or conversation that is unearthed in a hunt or investigation.

ARBOR NETWORKS

The Security Division of NETSCOUT

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/SPECTRUM/EN/0416-LETTER

Spectrum Deployment

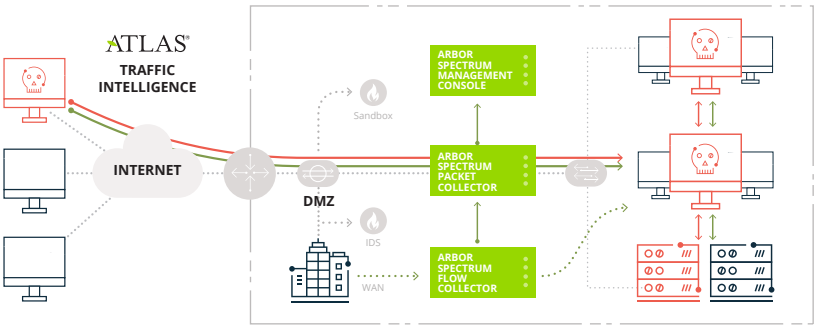

Figure 2: Spectrum Deployment

Appliance Models

	2200	2300
Deployment Options	Platform Console, Packet Collector or Flow Collector	Packet Collector or Flow Collector
Memory	64 GB	64 GB
Hard Drives	8 x 2 TB SATA 7200 RPM	16 x 4 TB SATA 7200 RPM
Storage Capacity	15 TB	64 TB
Traffic Archive	9.1 TB	44 TB
Max Flows Per Second (as a flow collector)	25,000	100,000
Max Packet Inspection (as a packet collector)	1.5 Gbps	5 Gbps
Capture Interface Options	4 Port SFP or 2 Port SFP+	
Management Interface	2 x 10/100/1000 Copper	
Processor	2 x XEON ES-2658; 2.1 Ghz/20 MB; 8 Core Processors	
Size	2 RU	3 RU
Power	Dual AC or DC **AC Unit:** 100-240 VAC, 47-63 Hz, 10-5A **DC Unit:** -40 to -72, 20-12A	Dual AC or DC **AC Unit:** 100-127/ 200-240VAC, 50/60Hz, 10/5 A **DC Unit:** -36 to -72, 31-15A
Relative Humidity	8 – 90% non-condensing	8 – 90% non-condensing
Heat Dissipation	@ 400 Watts, 1365 BTU/hr	@ 525 Watts, 1791 BTU/hr

Hardware Recommendations for Spectrum VM

Arbor makes the following hardware recommendations:

VM Deployments	Console	Packet Collector	Flow Collector
VMware Version Supported	vSphere Hypervisor software (formerly known as ESXi), version 5.5		
Core Allocation	8–32	8–32	8
Memory Allocation	16–64 GB	16 GB	16 GB
Disk Allocation	**OS:** 150 GB **Data:** 1–4 TB	**OS:** 150 / **Data:** 1–40 TB (maximum tested; designed to scale beyond 40 TB)	
Network Interfaces	1–2	3–15	1–15
Max Flows per Second			250,000 FPS
Max Packet Inspection		Up to 2 Gbps	

**Requirements and performance provided as documentation for production deployments. Spectrum supports other options for smaller scale proof of concept deployments.*