Arbor Networks Spectrum with NETSCOUT ISNG

HIGHLIGHTS

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

The attack landscape has changed. Attack tools such as malware, typically used to initially compromise a network, are no longer the weapons of choice. Today's attackers access user accounts and manipulate well known IT applications or operating systems, bypassing conventional perimeter security defenses. The Mean Time to Detect an attack is typically greater than 150 days yet the time it takes for their adversary to initially compromise a network is under 10 minutes.

Arbor Networks Spectrum™ can dramatically increase the entire security team's Mean Time to Know when an attacker is already inside, and take swift action to eject or contain them. Not only does it provide deep visibility into network activity and quickly surfaces high-priority issues, but through automating and orchestrating key incident response and security operations workflows, security teams can scale up – accomplishing far more with existing staff and resources.

Epic Range

Arbor Spectrum provides complete network visibility paired with high fidelity ATLAS (Active Threat Level Analysis System) threat intelligence distilled from one-third of all global internet traffic. The combination of ATLAS visibility and ATLAS intelligence policies, which are continuously updated with the latest threat intelligence, give customers the highest fidelity view into the threats that are happening in, on or around their networks.

Faster Proof

Reach conclusions that matter – faster – with Arbor Spectrum's real-time, high performance traffic archive, now integrated with NETSCOUT's industry leading network and application meta data collection and analysis technology, ISNG with Adaptive Service Intelligence™ (ASI) Technology to give unprecedented pervasive visibility into,and analysis of, protocol, application and network data. Built-in investigation workflows, rapid search and easy pivots into months of past network and user activity, turns days and hours of work into seconds.

How Arbor Spectrum Works

Arbor 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 threat. Arbor Spectrum leverages NETSCOUT ISNG with ASI technology and/ or Arbor Spectrum Flow Collection, with Active Directory to surface internal network activity.

Model shown: ISNG 9895.

Detect

Spectrum goes beyond reporting of individual network anomalies by using threat detections that include multiple indicators of activity to help you find the most critical problems and suspicious events in your network.

Spectrum monitors your network for specific activities and compiles related, significant events. Detections are triggered when certain combinations of activities occur.

By correlating events, Spectrum decreases or eliminates the need to look at individual indicators, and produces fewer false positives.

Spectrum creates the following types of detections:

- First Connection with an Unapproved Host.
- First Connection on an Unapproved Port or Service.
- Network Scanning Activity by a potentially compromised Host.
- Unapproved Access with a High Level of Outflow.
- Host with an ATLAS Indicator and other Event.

Custom Flow Policies

- Allow creation of user-defined rules to monitor traffic for unexpected behavior. Rules are defined by one or more of source IP, destination IP, protocol, destination port.

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 Arbor Spectrum.

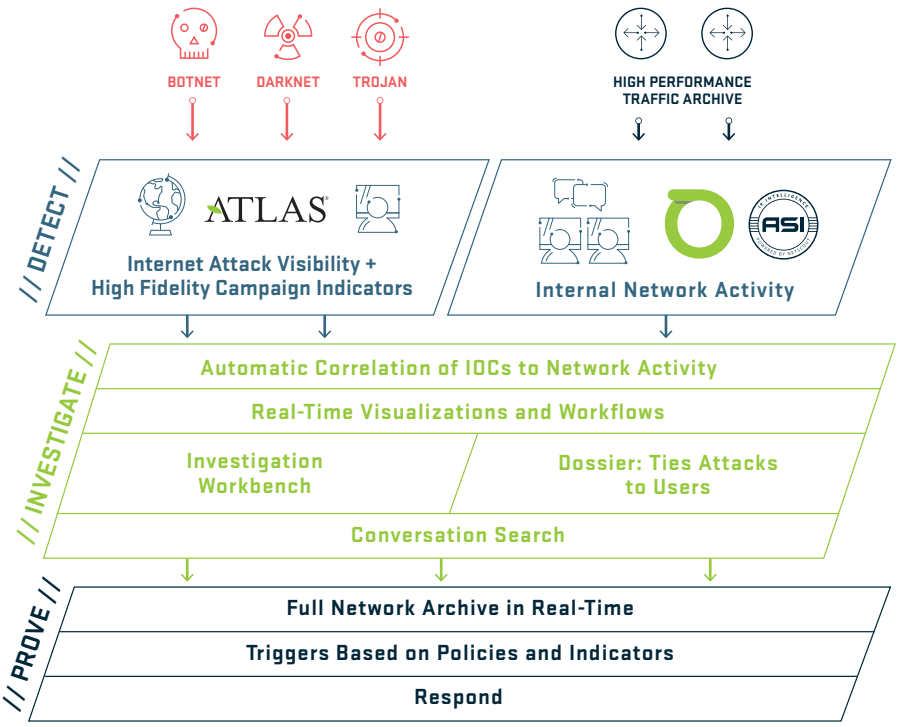

Figure 1: How Arbor Spectrum Works.

Investigate

Indicator Prioritization

Real-time visual representation of trends in new indicators and network activity. Can be mapped into groups (including user assets, business function, location).

Investigations Module

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

REST API for Extensibility

The Spectrum application programming interface (API) allows you to access Spectrum functionality and extend it for your own use. The Spectrum API is accessible via an HTTP REST interface using JSON.

- Endpoints include:
- Connections Search queries
- Feeds
- Whitelists
- Indicators
- Domains and Domain controllers
- Groups

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 upload a PCAP into Arbor Spectrum.

Integration with Leading SIEM Platforms

Sends captured data into SIEM platforms including HP Arcsight, IBM QRadar, Splunk Enterprise Security.

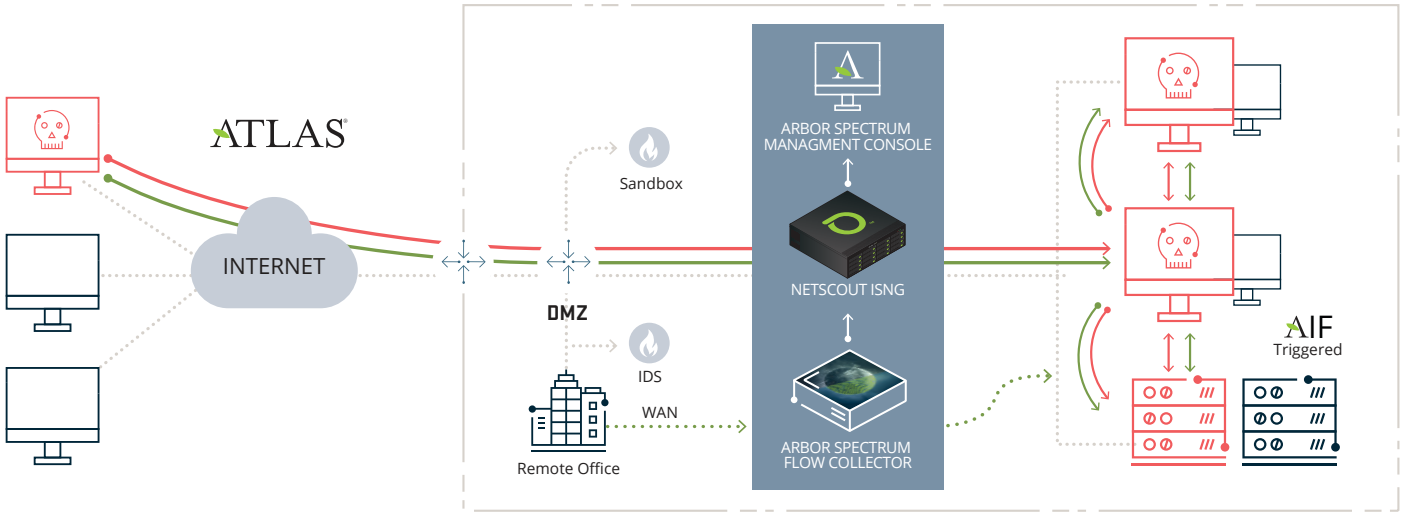

Figure 2: Arbor Spectrum with NETSCOUT ISNG Deployment.

Spectrum can now be deployed as a single collector that acts as both a management interface or a single packet or flow collector. It can also be deployed where the console can manage multiple packet and flow collectors.

Preferred NETSCOUT ISNG Models

ISNG Model	No. Interfaces	Interface Type	Storage	Cores	RAM
ISNG 9895	4	4-port 10G/1G	96 TB	36	256 GB
ISNG 9795	4	4-port 10G/1G	64 TB	24	128 GB
ISNG 4895	4	4-port 10G/1G	32 TB	36	256 GB
ISNG 4795	4	4-port 10G/1G	24 TB	24	128 GB

Arbor Spectrum Management Console and Flow Collector Models

	2200	2300
Deployment Options	Platform Console, Packet Collector or Flow Collector	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)	100,000	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 Arbor 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 GB / Data: 1–40 TB (maximum tested; designed to scale beyond 40 TB)	
Network Interfaces	1-2	3-15	1-15
Max Flows Per Second	n/a	n/a	250,000 FPS
Max Packet Inspection	n/a	Up to 2 Gbps	n/a

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

"No security product is a silver bullet, but Arbor Spectrum has given us true end-to-end visibility we never had before, and other solutions do not give."

"We are very happy with the solution and service from Arbor Spectrum. It has helped us reduce our Mean Time To Detect considerably."

Lead Security Engineer, Large Financial

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECPDS_001-1701 01/2018