ATLAS Intelligence Feed (AIF)

for Arbor Sightline

HIGHLIGHTS

Local to Global Visibility Designed to see the Connected World

ATLAS Intelligence Feed® (AIF) for Arbor Sightline is an AIF subscription for Arbor Smart Visibility solutions. It enhances the traffic analytics, visibility, and threat detection provided by Sightline, Sentinel and Insight.

Features and Benefits

Infrastructure, Service, and OTT Visibility – Analyze and understand user intent by observing the behavior of the traffic from connected services, globally. Look beyond the IP and ASN of OTT traffic to identify and understand content and the underlying global services infrastructure being used to deliver it.

Threat Indicators – With AIF's frequently updated IP reputation lists Arbor Sightline can detect active botnet infestations / C&C communications, and other threats from malware running on computers, smart devices, or embedded devices such as DOCSIS cable modems.

Pervasive visibility is essential to network operational excellence. Identifying and isolating network impacts quickly requires comprehensive telemetry from across the network. But today's inter-connected networks aren't built to operate in a vacuum. They function to connect customers or subscribers to each other and to the broader Internet. The network has little definition or substance without understanding its place and how it's used in the broader Internet. That means maintaining high levels of service requires visibility not just within the network but from across the internet. That's why even with achieving visibility from every corner of the network, pervasive visibility requires incorporating a global perspective. And a global perspective requires comprehensive global intelligence.

Global intelligence from the ATLAS Intelligence Feed (AIF) provides Sightline customers with the ability to quickly detect large scale security attacks before they cause service outages internally or to your customers. AIF also identifies OTT services highly valued by subscribers and helps show the impact of those services on the network and their trends into the future. AIF expands your Sightline deployment to perform paralleled detection and analysis of all of your internet traffic via a unique and powerful combination of:

- **People –** NETSCOUT's ATLAS Security and Engineering Research Team (ASERT) is an industry renowned elite group of security researchers and Super Remediators that routinely collaborates with government CERTS and is an active part of a large cybersecurity community.
- **Collections –** Cohesively known as ATLAS, years of unparalleled global collection consisting of anonymized data sent from over hundreds of Arbor product deployments, private and public threat intelligence sources, sinkholes, botnet monitoring, darknet forum monitoring, and honeypots.
- **Process –** Enrichment, Deep Behavioral Analysis, Recursive Introspection & Extraction, and Validation.

By combining AIF with Arbor Sightline, Sentinel and Insight, your vision of network and traffic analytics extends your local view of network traffic to a global level. The benefit behind global visibility is observing user behavior and the threats that come with it from a wider lens and at a further distance. That way, you protect the uptime of your network from malicious attacks before they occur. You can see who is sending traffic, the context of that traffic, how much traffic flows to your network, and how network infrastructure plays a role in its dissemination. You have an unobstructed view of the flow of traffic from its origination to your internal network regardless of its discrete nature, therefore, providing your team with the preemptive countermeasures that protect your network from attacks while also ensuring the network optimally delivers high-value content and services for which subscribers are willing to pay a premium. AIF-Sightline powered by ATLAS is the global view to traffic analytics and visibility provided by Sightline, Sentinel, and Insight.

ATLAS Intelligence Feed for Arbor Sightline

By teaming Infrastructure and Service Visibility, your vision of network and traffic analytics extends your local view of network traffic to a global outlook. The benefit behind global visibility is observing user behavior and the threats that come with it from a wider lens at a further distance. That way, you protect the uptime of your network from malicious attacks before they occur. You can see who is sending traffic, what is the context of that traffic, how much traffic flows to your network and which network infrastructure plays a role in its dissemination. You have an unobstructed view of the flow of traffic from its origination to your internal network regardless of its discrete nature, therefore, providing your team with the preemptive countermeasure that protect your network from attacks. AIF-Sightline powered by ATLAS is the global view to traffic analytics and visibility provided by Sightline, Sentinel, and Insight.

The emergence of new content providers delivering OTT (over-the-top) services such as gaming, streaming media, and collaboration has grown dramatically. The proliferation of OTT and other services combined with cloud and CDN delivery has caused a transformation of the Internet backbone, causing a shift from a hierarchical design, to a flatter design centered around delivering content more regionally and directly – improving user experience and reducing costs. This de-coupling of content from content-owner renders traditional OTT traffic identification less effective, while visibility and optimization of traffic has become increasingly important. Arbor Sightline combines flow data and DNS lookups with ATLAS Intelligence to identify OTT services and the underlying delivery infrastructure, regardless of location. Classify traffic based on individual vendors, as groups, or as traffic types to fully understand the traffic flowing across the network.

As cyber threats continue to increase in frequency and sophistication, mature security teams will rely upon not only the latest cyber security technology, but also highly curated threat intelligence that arms these products enabling them to conduct more agile incident response and remediation- all to ultimately avoid the downtime or data breach which puts their organization in the news. Truly great threat intelligence goes beyond collecting and analyzing attack data. It should make a marked improvement over existing staff and processes. This information must be actionable through seamless integration into your security posture. The risk from each threat should be clear, and the actions to be taken should be evident. The ATLAS Intelligence Feed (AIF) from NETSCOUT®, in conjunction with NETSCOUT Arbor Sightline With Sentinel, enables you to quickly detect and address cyber threats within the network.

Category	Description
OTT Infrastructure and Service Visibility Traffic	Identify and categorize network flows to determine user intent and remove the ambiguity of hosted services. Classify traffic by criteria such as provider (AWS), owner (e.g. Netflix) or type (streaming media) regardless of its location to optimize network peering, improve user experience, and reduce costs.
Cyber Threat Detection (Note: Requires Sightline With Sentinel)	Detect and alert on threats across the global threat landscape including inbound and outbound command and control (C2) communications, automatic propagation of Internet of Things (IoT) botnets performing brute-forcing or exploitation of known vulnerabilities, download or exfiltration attempts from/to known adversary owned servers, illicit use of devices known to be reflectors/amplifiers to launch DDoS attacks, and known bot-compromised devices used to propagate or launch DDoS attacks. Detection of these types of activities are dependent on observing flow data and generating alerts from network-based Indicators of Compromise (IoCs) that NETSCOUT curates internally. This detection does not require packet re-assembly or full session data and should not take the place of other Intrusion Detection/ Prevention systems, but rather should be considered as an additional layer of security to catch threats missed by traditional security devices.

LEARN MORE

For more information about ATLAS Intelligence Feed Service visit:

www.netscout.com/global-threat-intelligence

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_019_EN-2201 02/2022