ATLAS Intelligence Feed (AIF)

for Arbor Threat Mitigation System (TMS)

HIGHLIGHTS

Actionable Threat Intelligence Designed for Full-stack DDoS Protection

ATLAS® Intelligence Feed (AIF) is a subscription-based service for Sightline and TMS, optimizing defenses to protect the network environments where deployed.

Key Features and Benefits

DDoS Attack Intelligence – NETSCOUT® Arbor Sightline and TMS are continually armed with highly curated, global DDoS attack intelligence from ASERT enabling you to automatically detect and stop known or emerging DDoS attacks.

TMS Mitigation Templates – Take advantage of ASERT's industry-leading experience in stopping DDoS attacks by frequently receiving predefined TMS mitigation templates.

Active Reflection/Amplification Attack Filters – TMS gets updated filter lists of active reflectors conducting Reflection/Amplification attacks as seen by ASERT / ATLAS global threat intelligence.

Working seamlessly together, your Arbor Sightline and Arbor Threat Mitigation System (TMS) already offer an industry-leading DDoS attack protection solution. But as the volume of network traffic and cyber threats continue to increase in frequency and sophistication, mature security teams will rely not only upon the latest cybersecurity technology (e.g., Arbor Sightline and TMS), but also highly curated threat intelligence that continuously arms these products enabling them to conduct more agile incident response and remediation.

NETSCOUT ATLAS Intelligence Feed (AIF) is a unique and powerful fusion 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 350 Arbor product deployments, private and public threat intelligence sources, sinkholes, botnet monitoring, darknet forum monitoring, honeypots, and sinkholes.
- **Process –** Supervised Machine Learning of ASERT's unmatched visibility of Internet attacks provides continual enrichment, deep behavioral analysis, recursive introspection & extraction, and validation.

Turning Massive Amounts of Internet Data into Actionable Threat Intelligence

ASERT continuously scans the Internet to identify all possible open reflectors for each type of reflection/amplification attack. The result is millions of abusable IP addresses. That huge amount of data is interesting, but not actionable. ASERT makes this intelligence useful and actionable by correlating it with the real-time, worldwide, DDoS attack data they get from ATLAS. For example, at any time, there are over 9 million abusable open NTP reflectors on the Internet. When correlating that to an ATLAS-derived list of reflectors actively conducting NTP Reflection/Amplification (R/A) attacks, the number of IP addresses is reduced to approximately 250 K. This much more manageable list of IP addresses is frequently sent to TMS via the ATAS Intelligence Feed where it is applied as a TMS filter that can be used to automatically and more intelligently block NTP R/A attacks. Only NETSCOUT has the ATLAS real-time DDoS attack data. Only NETSCOUT can provide this kind of DDoS intelligence to drive surgical, automated blocking for today's most common and most threatening DDoS attacks.

As new attack information is discovered, the ATLAS Intelligence Feed is updated, and changes are delivered automatically to your NETSCOUT Networks Sightline and Threat Mitigation System via a subscription service over a secured SSL connection.

Effective threat intelligence requires three things:

1. Continuous source of real-world network traffic and data;
2. Robust infrastructure for gathering and analyzing network traffic and threat data; and
3. Dedicated team to manage data and add the "human intelligence" to the analysis.

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 and seamlessly integrated into your security posture. ATLAS Intelligence Feed for Sightline and TMS allows you to enforce highly curated threat intelligence from industry renowned experts to protect you and your customers from the continuous onslaught of cyber attacks.

ATLAS Intelligence Feed

NETSCOUT's ATLAS Intelligence Feed (AIF) is a continuous feed of highly curated threat intelligence that enables you to automatically detect and mitigate all sorts of cyberthreats before they impact your or your customers. It consists of:

Category	Description
DDoS IP Reputation	Leveraging NETSCOUT ASERT's unmatched, global visibility into DDoS attack activity, AIF is automatically updated with over 1.5 Million IP reputation indicators of source/port combinations that are actively propagating specific DDoS attack vectors anywhere in the world. This DDoS IP Reputation data can be used to automatically and surgically block specific attack vectors, including all major Reflection/Amplification DDoS attack types such as Open NTP, SSDP, Chargen, RDP, and even DNS Reflection/Amplification, with minimal overblocking of legitimate sources compared to other approaches that block or rate limit all traffic for the attacking protocol or application. AIF also includes current hosts that are part of DDoS botnets, enabling AIF to automatically block many attacks launched by botnets, independent of any protocol or application used in the attack.
DDoS Attack Payload	AIF contains frequently updated DDoS attack signatures that Arbor TMS uses to inspect packet payloads and automatically mitigate application-layer DDoS attacks.
TMS Mitigation Templates	Take advantage of ASERT's industry-leading experience in stopping DDoS attacks by frequently receiving predefined TMS mitigation templates from AIF. These templates can be easily customized for your environment to stop the latest DDoS attacks or protect certain server types.

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

© 2025 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Omnis, Guardians of the Connected World, Adaptive Service Intelligence, Arbor, ATLAS, InfiniStream, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries.
Third-party trademarks mentioned are the property of their respective owners.

SECPDS_020_EN-2501 04/2025