ATLAS Intelligence Feed (AIF) for NETSCOUT Arbor Edge Defense (AED)

HIGHLIGHTS

Threat Intelligence Designed for the Network Perimeter

ATLAS® Intelligence Feed (AIF) for NETSCOUT® Arbor Edge Defense (AED) is a subscription-based service that is specifically designed to maximize the functionality of the AED and enable it to be a first and last line or smart, automated perimeter defense.

Features and Benefits:

Automated and Accurate Inbound DDoS Attack Mitigation

Protect the availability of networks and services by updating AED with highly curated threat intelligence that enables it to block inbound DDoS attacks automatically and with accuracy.

Blocking of Inbound Scanning or Brute Force Attacks

Reduce load on firewalls by offloading detection and blocking of inbound scanning activity and brute force password attacks (e.g. SSH, telnet, SMB etc.) to AED.

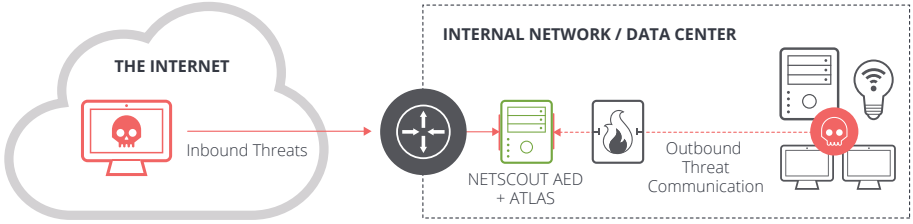
Block Outbound IoCs Missed by Security Stack

AED's deployment outside the firewall and continuous update of IoCs enable it to be a last line of defense by blocking outbound traffic from compromised internal devices that has been missed by the security stack.

Intelligent Warning Service

Rely upon ATLAS/ASERT worldwide botnet monitoring along with expanded contextual intelligence, for a proactive, intelligent warning of active DDoS attacks targeting your organization.

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.



Deployed between the Internet router and firewall, NETSCOUT Arbor Edge Defense (AED) acts as a first and last line of smart, automated, perimeter defense. Fueling NETSCOUT AED's high performing, stateless packet processing engine, is NETSCOUT's ATLAS Intelligence Feed (AIF) which is created via 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, 15+ 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 –** Enrichment, Deep Behavioral Analysis, Recursive Introspection & Extraction, and Validation processes built up over years of operational experience provide extensive allow-list generation ensuring legitimate internet infrastructure such as DNS is never blocked.

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 AED, enables you to quickly address advanced attacks, whether they be DDoS-related or part of a larger advanced threat campaign against your organization.

ATLAS Intelligence Feed in NETSCOUT Arbor Edge Defense

There are two versions of the ATLAS Intelligence Feed for AED – AIF Standard and AIF Advanced. The table below outlines the different threat intelligence categories supported by each version.

Category (Direction)	Description	AIF Standard	AIF Advanced
DDoS Reputation (Inbound)	• **Active Attackers:** Block IP addresses actively participating in DDoS attacks around the globe (e.g. Open NTP, DNS, RDP servers participating in Reflection/Amplification attacks). • **Known Attack Bots/Tools:** Block traffic matching known botnets, or attack tools (e.g. Mirai botnet, Slow Loris attack tool).	✓	✓
Internet Infrastructure (Inbound)	• **Search Crawlers:** Up-to-date list of IP address blocks associated with legitimate search engine bots used to reduce false positives. • **Dynamic IP Geolocation:** Up to date, accurate country information automatically applied to dashboards, reports and packets decodes.	✓	✓
Cyber Threats (Inbound and Outbound)	• **Malware IoCs:** Block IP addresses, domains or URLs associated with known malware, APTs, or botnet command and control. For all blocked IoCs, additional contextual intelligence related to the IoC such as hash values, DNS resolutions, activity in specific industries is provided. • **Scans and Brute Force Attacks:** Block inbound scanning and known brute force attempts (e.g. SSH, Telnet, SMB).	–	✓

Intelligent Warning System

The ATLAS Intelligence Feed subscription (Standard or Advanced version) provides more than just an intelligence threat feed. Another important component of AIF subscription is the Intelligent Warning System. Behind NETSCOUT's ATLAS Intelligence Feed is the state-of-art Honeypot and Botnet monitoring system operated by ATLAS Security and Engineering Research Team (ASERT). When ASERT identifies or is alerted to a active threat targeting an Arbor Edge Defense customer with an AIF subscription, the customer will be notified and provided vital information (e.g. attack type, target IP address, domain, URL, ASN and CnC details) to prepare/mitigate the attack if it was to occur.

Additional Contextual Threat Intelligence

Another valuable component of the ATLAS Intelligence Feed is the ability to provide additional contextual threat intelligence. When an IoC is detected and/or blocked with NETSCOUT AED, any additional information that exists in the vast NETSCOUT ATLAS Threat Intelligence database will automatically be provided. This additional contextual threat intelligence (e.g. malware samples, hashes, DNS resolutions and endpoint IoCs) enables cybersecurity teams to determine the risk to their organization; and/or using their arsenal of other security tools, proactively hunt for signs of compromise, eradicate and ultimately avoid the data breach.

LEARN MORE

For more information about NETSCOUT AED visit:

https://www.netscout.com/product/netscout-aed

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_018_EN-2101 06/2021