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.
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.

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.

<table>
<thead>
<tr>
<th>Category (Direction)</th>
<th>Description</th>
<th>AIF Standard</th>
<th>AIF Advanced</th>
</tr>
</thead>
</table>
| DDoS Reputation (Inbound) | • 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. | ✓ | ✓ |
| 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). | − | ✓ |