Data Sheet

ATLAS® INTELLIGENCE FEED

A smarter response to security and availability threats.

Given the influx of threats coming at your business from every possible angle, entry-point and vector, what's really needed to stay ahead of attackers? Context. That context can help you gauge risk, prioritize your security operations team's time, and move on to the next threat (among many) at hand. The right security intelligence fuels the creation of mechanisms to recognize and block network-based attacks—some of the time. However, effective security intelligence not only identifies attacks, but understands and catalogs the attack infrastructure, methods and other indicators so that broader, more proactive measures can be taken with confidence.

Addressing Advanced Threats

The ATLAS Intelligence Feed, or AIF, from Arbor Networks arms customers with policies and countermeasures that enable them to quickly address attacks as part of an advanced threat or DDoS attack. The AIF is a service of the Arbor Security Engineering and Response Team (ASERT) and enables customers to directly benefit from the depth and breadth of Arbor's research capability.

Arbor Networks has a strong portfolio of products designed for both enterprise and service provider networks—all of which benefit from the consumption of AIF. As new attack information is discovered, the AIF is updated and changes are delivered automatically to Arbor products via a subscription over a secured SSL connection arming them with the latest threat intelligence to thwart modern day DDoS attacks or advanced threats. The best way to protect your organization is to have the most up-to-date intelligence from the broadest view, enriched by seasoned experts. This is the ATLAS Intelligence Feed.

Dynamics of an Effective Threat Intelligence Feed

Effective threat intelligence requires three things:

- A continuous source of real world network traffic and threat data
- A robust infrastructure for gathering and analyzing network traffic and threat data;
- And a dedicated team to manage all the above and to add a "human intelligence" aspect to the analysis.

However, truly great threat intelligence goes beyond simply collecting and analyzing attack data. It should make a marked improvement over existing staff and processes through seamless integration into your security program—meaning that the information must be actionable. The risk from each threat should be clear and the actions to be taken should be evident.

—

Key Features & Benefits

Dynamic Updates for Accurate Protection

The AIF is updated with the latest threat information to maintain the most accurate detection policies across all Arbor Networks products.

Campaign-Based Attack Identification

By combining attack data from multiple sources and focusing on malware characteristics, AIF identifies not only singular points of compromise, but related attacks as part of a campaign.

Fast Attack Response

The AIF policies provide valuable context to each attack, enabling a faster, more informed response.

Threat Validity and Prioritization

In addition, to collecting and analyzing threat data, ASERT goes a step further to validate that threats are both real and current.

ARBOR®
NETWORKS
The Security Division of NETSCOUT

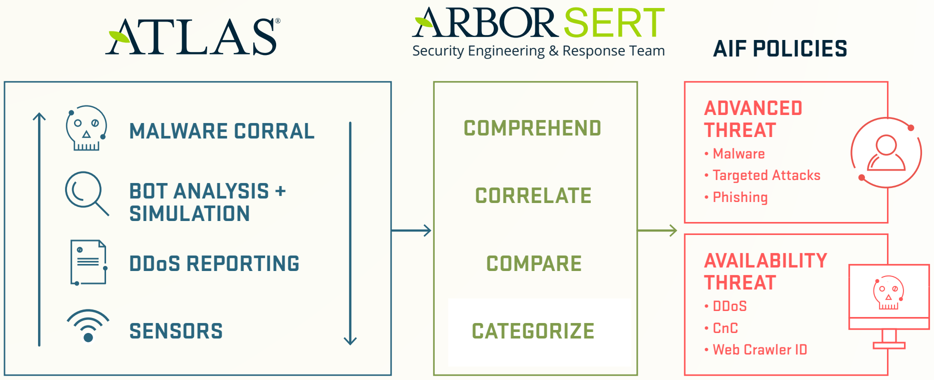

Figure 1 *ATLAS uses a variety of tools and processes to collect and analyze threat data. The team focuses on the capabilities and potential of attacks, pulling out multiple indicators of an attack campaign. These indicators are delivered to Arbor products via the ATLAS Intelligence Feed.*

Arbor's world class team of security researchers are dedicated to discovering and analyzing emerging internet threats and developing targeted defenses. Arbor uses a sophisticated combination of attack data collection, partner information and analysis tools to create AIF policies that not only detect threats, but also provide the context required for informed mitigation decisions.

One of the key technologies behind the AIF is Arbor's dynamic reputation intelligence. Reputation intelligence gives validity to the threat indicators that make up AIF policies. As ASERT collects traffic and threat information, it can piece together various elements of the threat—including what other types of compromise a particular malware might be capable of. However, to avoid taking action on a threat that hasn't yet materialized, reputation intelligence provides clear, demonstrable proof of when and how long a particular IP, DNS or URL has been compromised. Attack validation is added to relevant AIF policies through confidence scoring. This type of attack validation is provided to each AIF policy delivered to Arbor's products in the form of confidence scoring, so users can be certain that a threat identified by the product is significant and real.

Applying ATLAS Intelligence

Each product within the Arbor Networks' portfolio is designed to consume the AIF—though they all use different parts of the feed to inform different actions within the products. Some of the products analyze NetFlow and some of the products look at network packets. Policies within the AIF will include relevant information for each product.

Arbor Networks® APS

Beyond blocking availability threats based on bandwidth thresholds, the APS uses the AIF policies to identify multiple types of DDoS attacks including 'low and slow' attacks aimed at the application layer. In addition, the AIF helps the APS detect and stop certain categories of botnets from compromising the network. By stopping these availability and botnet threats from entering the network, it enables other security devices to do the jobs they were intended to do.

Arbor Networks® Spectrum

ATLAS security intelligence within Spectrum enables organizations to dig deeply into attack events for forensic analysis. The attack indicators present in the AIF help identify what the attack is/was capable of in the network and where it spread. In addition, organizations can overlay this threat information with traffic going to and from the most critical assets, with the context and information to escalate events for further investigation.

How Does the AIF Protect Organizations from DDoS and Botnets?

The AIF has been proven effective by many Arbor Networks customers at blocking the latest targeted, complex and sophisticated attacks.

To more accurately detect threats to the network, the AIF:

- Identifies threats regardless of attack volume; no waiting for an attack to reach a volume threshold before defending.
- Uses multiple levels of protection aligning with confidence levels.
- Applies attack intelligence contributed from advanced controlled detonation of millions of malware samples.
- Includes reverse engineering of specific malware as well as all malware related to a botnet.
- Actively monitoring Internet threats around the clock utilizing Arbor's global sensors network.
- Historical tracking of botnets, their locations and attack methods over time.
- ATLAS is a collaborative project with more than 300 customers who have agreed to share anonymous traffic data totaling approximately one-third of all Internet traffic.

Arbor Networks® SP

Security intelligence from the AIF provides SP customers with the ability to quickly detect large scale DDoS attacks before they cause service outage internally or to customers.

Arbor Networks® TMS

AIF policies in the TMS give organizations detailed information about DDoS attacks to quickly and confidently begin blocking them. This accuracy is critical in blocking malicious attacks that can result in costly downtime. The AIF provides this same level of protection to the Cisco ASR 9000 vDDoS Protection product.

Breaking Down the Intelligence Feed

There are two subscriptions available for the AIF—Standard and Advanced. With two subscriptions, customers can choose the level of attack detection and/or protection that fits their needs.

AIF Standard

With the standard feed customers can detect and/or address some of the most prevalent attacks targeting business today, including malware, botnets and DDoS attacks. The policies and countermeasures are updated to with new attack information to provide broad, accurate detection. Examples of the policies and countermeasures included this feed are included below.

	Threat Policy Types		APS	Spectrum	SP	TMS+
Command & Control	• Peer to Peer • HTTP • IRC		✓	✓	✓	
DDoS Reputation Threats	• Attacker • Target		✓	✓	✓	
Malware	• Webshell • Ransomware • RAT • Fake Anti Virus • Banking • Virtual Currency • Spyware • Drive By • Social Network	• DDoS Bot • Dropper • Ad Fraud • Worm • Credential Theft • Backdoor • Exploit Kit • Point of Sale • Other	✓	✓	✓	
IP Geo Location	• Identification by country for sources of inbound traffic • Identification by country for destinations of outbound traffic		✓	✓	✓*	✓*
DDoS RegEx	• Identifies DDoS attackers based upon IP address indicators from ATLAS • Identifies DDoS targets based on indicators from ATLAS HTTP Flooder		✓			✓
Web Crawler Identification	Identify inbound connections to web services from known search engines		✓			
ET Pro	IDS Signatures			✓		

Figure 2 *Example threats identified using the AIF Standard feed. All countermeasures and policies are continuously updated, so above list may change at any time.*

—

How Arbor Networks is Uniquely Positioned to Address Advanced Threats

Arbor has a long history in botnet research and DDoS mitigation.

As DDoS has evolved from a simple diversionary tactic to a feature of malware and botnets used in cybercrime and APT attacks, Arbor has expanded its ASERT team and research capabilities to identify and analyze additional threat types. ASERT's approach to threat intelligence now includes several factors that not only help identify threats but to confirm their pervasivness and severity, these include:

- Reputation monitoring and active tracking of attack campaigns based on real world indicators from the Red Sky Alliance.
- A rich malware analysis backend system comprised of both external partner technology along with internally built analysis and processes.

ASERT uses this threat data and analysis to develop the AIF, which is used by Arbor customers to detect events occurring in, on and around the network. The combination of this microview (on the network) and the macroview of internet traffic (delivered via the ATLAS portal), gives customers a distinct advantage for addressing advanced threats.

—

[*] IP-Geo Location updated in SP, TMS and Cisco ASR 9000 DDoS Protection products via product patch.

[+] The AIF policies used in TMS are the same for the Cisco ASR 9000 DDoS Protection.

AIF Advanced

The Advanced AIF is designed for organizations that are concerned with stealthy, more subtle attacks. With a subscription to this feed, customers get all of the countermeasures and policies included in the Standard feed, as well as additional policies for uncovering attack behaviors indicative of ongoing, campaign-style attacks—those that are highly customized to a specific business and are difficult to detect because they may appear legitimate. Examples of countermeasures and policies included in this subscription are included below.

	Threat Policy Types	APS	Spectrum	SP	TMS
Location-Based Threats	• Traffic Anonymization Services • TOR • Proxies • Sinkholes • Scanners • Other	✓	✓		
Email Threats	• Spam • Phishing	✓	✓		
Targeted Attacks	• APT • Hactivism • RAT • Watering Hole • Rootkits	✓	✓		
Mobile	• Mobile C&C • Spyware • Malicious Apps	✓	✓		

Figure 3 *Example threats identified using the AIF feed. Countermeasures and policies are continuously updated, so the above list may change at any given time. Policies in the Advanced subscription are currently not available to SP, TMS or Cisco ASR 9000 DDoS Protection customers.*

ARBOR®
NETWORKS
The Security Division of NETSCOUT

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 6664 3140

Latin & Central America
T +52 55 4624 4842

www.arbornetworks.com