ATLAS® Intelligence Feed for Pravail®

A smarter response to advanced threats

Enterprise security teams are in a constant cat and mouse game with attackers who are organized and resourceful—trying to stay ahead of the latest attacks, while maintaining business continuity.

Advanced threats are highly targeted and often combine multi-dimensional and multi-phased attacks. Attackers seek unique vulnerabilities present within the network—whether unpatched systems, naïve users or rogue devices. Traditional perimeter devices look at what's coming into the network and provide only partial coverage against these attacks. Organizations need to quickly and accurately identify an attack or breach has occurred so that they can implement mitigation strategies before the organization is impacted.

Addressing Advanced Threats

The ATLAS® Intelligence Feeds (AIF) from Arbor Networks arms customers with policies and countermeasures that enable them to quickly address advanced threats. The AIF is a service of the Arbor Security Engineering and Response Team (ASERT) and enables Pravail customers to directly benefit from the depth and breadth of Arbor's research capability.

One of the key technologies behind AIF is Arbor's dynamic reputation feed. This feed is used with AIF to identify known bad sites—those operating as command and control servers or sites delivering drive by downloads. The reputation feed includes policies designed to keep network users from visiting those sites. Unlike other reputation service offerings, Arbor's feed is updated frequently to account for rapidly changing attacker behavior, which helps ensure more effective and accurate attack detection.

All AIF updates are delivered automatically to Pravail products via a subscription over a secured SSL connection. Customers can choose from two different subscriptions based on their needs.

- **AIF Basic:** Includes policies and countermeasures that detect activity associated with DDoS threats and botnet activity.
- **AIF Advanced:** Includes the basic service, as well as policies that identify location-based threats, targeted attacks or campaigns, and risks related to botnets, DDoS, financial fraud and mobile.

Dynamics of an Effective Security Feed

A security intelligence feed is only as good as the information used to create it. The changing nature of advanced threats requires a dedicated security research team with cutting-edge tools and processes for analyzing not only the underlying code of the attack, but the full architecture of how the attack is designed, weaponized and executed.

Key Features and Benefits

Up-to-Date Protection
AIF is continuously updated with the latest threat information to maintain the most accurate detection policies across all Pravail products.

Broad Attack Identification
AIF uses information from multiple resources, including real attack data from ATLAS, to help identify hundreds of thousands of attacks.

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

Research-based Reputation Analysis
Arbor's reputation feed for AIF is rapidly and constantly updated to better ensure that legitimate traffic is not flagged as malicious.

ARBOR® NETWORKS

How Arbor Networks is Uniquely Positioned to Address Advanced Threats

Arbor has a long history in botnet research and DDoS mitigation. However, as DDoS has moved from just a diversion to be a feature of malware and botnets used in cybercrime and APT attacks, Arbor has expended its ASERT team and research capabilities to tackle additional threat types.

There are several features that make ASERT uniquely capable of detecting millions of advanced threats including targeted attacks, campaigns, malware and mobile botnets. These features include:

- **Valuable partnerships** such as the Red Sky Alliance, which provides access to more than 23 million PCs being actively monitored for threat intelligence.
- **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.

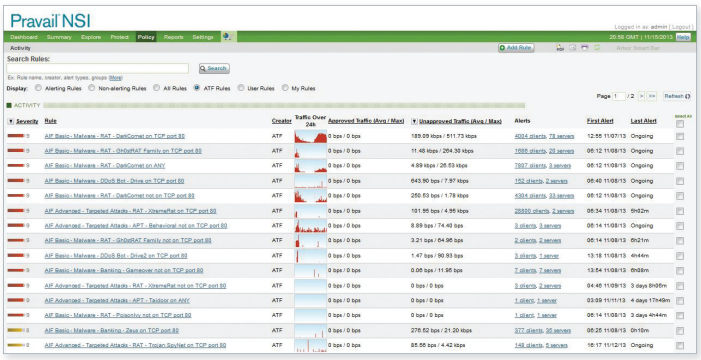
ASERT uses this threat data and analysis to develop the AIF feeds, which are used by Arbor's Pravail customers to detect events occurring in, on and around the network. The combination of this microview (on the network) and the macroview of global internet traffic (delivered via the ATLAS portal), gives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

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 provide detection of advanced threats but also the context required for informed mitigation decisions.

Current Attack Polices in AIF

AIF Categories	Policy Examples	Basic		Advanced	
		NSI	APS	NSI	APS
Command and Control	Peer to Peer	◉		◉	
	HTTP	◉		◉	
	IRC	◉		◉	
Malware	Ransomware	◉		◉	
	RAT	◉		◉	
	Fake AV	◉		◉	
	Banking	◉		◉	
	Virtual Currency	◉		◉	
	Spyware	◉		◉	
	Driveby	◉		◉	
	Social Network	◉		◉	
	DDoS Bot	◉		◉	
	Dropper	◉		◉	
	Adfraud	◉		◉	
	Worm	◉		◉	
	Credential Theft	◉		◉	
	Backdoor	◉		◉	
	Other	◉		◉	
DDoS	Attacker		◉		◉
	Target		◉		◉
Web Crawler Identification	ID Malicious Web Crawlers		◉		◉
IP Geo Location	Blacklist by Country		◉		◉
Location Based Threats	Traffic Anonymization			◉	
	Proxy			◉	
	Sinkholes			◉	
	Scanner			◉	
	Other			◉	
Email	Spam			◉	
	Phishing			◉	
Targeted Attacks	APT			◉	
	Hacktivism			◉	
	RAT			◉	
	Watering Hole			◉	
	Rootkit			◉	
Mobile	Mobile CNC			◉	
	Spyware			◉	
	Malicious App			◉	

Policies are constantly updated to reflect new categories and threats.



AIF Policies alert on events indicative of attack.

Critical assets for ASERT's AIF delivery include:

ATLAS

What separates Arbor from other vendors is how we leverage this pervasive service provider footprint to benefit all of our customers. ATLAS is a collaborative project with more than 275+ customers who have agreed to share anonymous traffic data with totaling an amazing 70 Tbps or approximately one-third of all Internet traffic. From this unique vantage point, Arbor is ideally positioned to deliver intelligence about DDoS, malware and botnets that threaten Internet infrastructure and network availability. Arbor customers enjoy a considerable competitive advantage by giving them both a micro view of their own network combined with a macro view of global Internet traffic; this is a powerful combination of network security intelligence that is unrivaled today.

Red Sky Alliance

Arbor Networks is a founding member of the Red Sky® Alliance—a private social network of trusted security experts that collaborate on the identification and neutralization of malware and other advanced threats. Red Sky members share actionable intelligence to effectively combat complex and stealthy attacks that often go undetected by traditional security defenses. The intelligence from the Red Sky Alliance complements Arbor's existing real-time security intelligence gathered via ATLAS®, providing an unparalleled level of visibility into both DDoS and advanced threats.

Actionable Detection Throughout the Attack Lifecycle

Advanced threats can be broken down into multiple attack stages. Each stage includes unique activity and indicators that can be used to identify and address the threat. Pravail products utilize AIF policies to alert administrators when these indicators are present and supply them with the relevant details that help enable mitigation and forensics.

Pre-Attack: Security Preparation

Arbor goes beyond traditional methods of attack data collection malware reverse engineering and focuses on the entire threat framework. By researching threats to this level, Arbor understands not only the nuances of the attack, but the behavior and style of the attacker to better predict what new attacks may surface.

All of this information is used to create or update AIF policies, enabling customers to directly benefit from the depth and breadth of Arbor's research capability. Armed with this information, customers can take proactive measures to help strengthen security defenses not only at the perimeter but throughout the network.

How Does AIF Protect Organizations From DDoS and Botnets?

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

To more accurately detect threats on the network, 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 honeypot network.
- ATLAS is a collaborative project with more than 275+ customers who have agreed to share anonymous traffic data totaling an amazing 70Tbps, or approximately one-third of all Internet traffic.

For More Information

The Pravail portfolio provides enterprises with proven perimeter and internal network security monitoring. The devices are kept up to date against the latest threats with an ongoing subscription to the ATLAS® Intelligence Feed (AIF), a research-driven feed of security policies designed to quickly and accurately identify threats based on attack activity, reputation and behavior.

For more information regarding ATLAS, ASERT, Pravail APS, Pravail NSI and the AIF service, visit Arbor's Web site at www.arbornetworks.com.

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

Europe
T +44 207 127 8147

Asia Pacific
T +65 68096226

www.arbornetworks.com

DS/AIFPRAVAIL/EN/1113-LETTER

During an Attack: Accurately Address the Threat

There are many types of advanced threats from availability threats to drive by downloads, spearphishing to amass hosts and gain a foothold into the network to malware that attempts exfiltrate sensitive data. In all cases, early detection is the gating factor between attacks that are merely annoying and those with catastrophic results.

Malware Infection

There are many types of advanced threats from availability threats to drive by downloads, spearphishing to amass hosts and gain a foothold into the network to malware that attempts to exfiltrate sensitive data. In all cases, early detection is the gating factor between attacks that are merely annoying and those with catastrophic results.

Botnets

With the AIF Pravail customers have several options for addressing botnets. Pravail APS can detect botnet activity at the perimeter and take action to block them from entering the network. Pravail NSI provides internal visibility into infected hosts that may be communicating outside the network with known command and control servers.

DDoS

The AIF automates the identification and mitigation of attacks against applications, infrastructure and services from known botnets. AIF automatically updates Pravail APS appliances with the latest defenses against new availability attacks and updates IP location data—all in real time. In addition, Arbor maintains policies in AIF that allow specific Web crawlers to access your site, but block those it detects as malicious.

Campaigns

Attackers may use social engineering techniques that target individuals or even entire industries. These carefully crafted attacks are designed to look legitimate and thus have a high likelihood of success. With AIF, Pravail can detect these attacks when/if they breach the network with information that enables security teams to address the event quickly—before data theft or fraud can cause damage.

Other Attacks

Using AIF, Pravail products can detect location-based threats such as sinkholes or proxies; credential theft attacks or remote access trojans. Not only does AIF provide alerts when these attack behaviors are present, it also provides critical details that help facilitate incident response.

Post Attack: Incident Response and Forensics

Once the threat has been addressed, it is important drill down into the attack to determine how the infection may have occurred so that steps can be taken to prevent similar attacks from happening again.

The Pravail portfolio provides the IP flow data and attack details needed to understand where attacks may have originated in the network, where they may have spread and what other systems could potentially be impacted. Identity tracking capabilities in Pravail NSI enable incident response and forensics in order to pinpoint which machines were compromised and determine how the system may be vulnerable. Pravail administrators can also run customized reports to show where attack activity has occurred and share the information with internal partners and management.