

# Active Threat Feed (ATF)

## PROTECTION AND VISIBILITY FOR THE ENTERPRISE NETWORK

### Service Benefits

- Up to date, immediate threat detection via ATF policies that are automatically synced with Arbor Peakflow systems deployed across the globe.
- Rapid, pre-signature, mitigation strategy reduces attack proliferation and business operational costs.
- Leverages the 24x7 global vigilance and analysis performed by Arbor Networks' ASERT to optimize time and expense of internal security team.
- Improves internal network protection through partnerships with leading service providers.

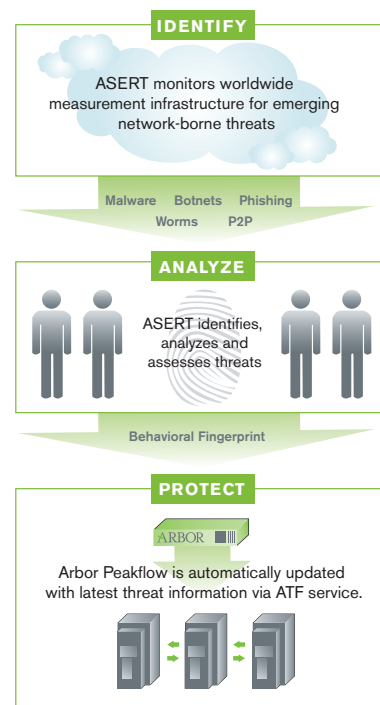
### Service Capabilities

- Scoping and analysis of high-visibility threats.
- Composite threat modeling without manual alert analysis.
- False positive reduction of zero-day threat detection.
- Acceptable-use policy (AUP) definition via application traffic profiling.

Every day network operators and security engineers battle emerging attacks, propagating worms and other threats as they struggle with an increasing workload and costs associated with network administration. To effectively protect their networks, they must understand the true nature of the threats facing them and implement the technologies and processes which best counter these threats.

The powerful combination of the Arbor Security Engineering and Response Team (ASERT) and Active Threat Feed (ATF) service addresses these challenges by delivering to customers the industry's only global, 24x7 behavioral-based threat update service. ASERT, a team of renowned security researchers, leverages the world-wide presence provided by the deployment of Arbor Peakflow products in many of the world's services provider networks. Along with data from other sources, (both public and proprietary), ASERT creates traffic behavioral "fingerprints" for known or unknown emerging threats, before signatures can be created for IDS/IPS or Anti-Virus products. These fingerprints, along with comprehensive information and mitigation strategies to thwart the attack, are then distributed to subscribing Arbor Peakflow X customers via the Active Threat Feed (ATF) service. The objective is simple—optimize already stressed enterprise information security teams by leveraging Arbor Networks' ASERT and ATF services to detect and mitigate known or emerging threats before they impact critical business services.

### How ATF Works



### Why ATF?

ATF offers Arbor customers real-time threat detection by feeding continuously updated behavioral fingerprints to the Arbor Peakflow® platform. ATF fingerprints inspect network traffic flows and classify a series of seemingly unrelated events as a composite threat. This helps security administrators instantly identify worms, botnets, and malware at a glance rather than having to correlate a series of disparate alerts or wait for the latest signature to be added to their IDS/IPS or Anti-Virus products.

Each ATF fingerprint details the identified threat by including packet-level analysis, a description of the representative traffic the fingerprint looks for and affected hardware and software platforms. Additionally, ATF details mitigation strategies, which may include host and/or network-based configuration changes, host security updates and application or OS patching requirements. Combined with Arbor Peakflow's "Show Relationships" feature, administrators can specifically identify affected hosts within the network and generate appropriate rules for security devices protecting the network, such as firewalls, routers or switches.

## ATF Fingerprint Groups

- Botnet Command & Control (C&C) Servers
- Dark Internet Protocol (IP) Addresses
- Host Scanning
- Instant Messaging (IM) Applications
- Internet Relay Chat (IRC) Applications
- Malicious Code
- Peer-to-peer (P2P) Application(s)
- Phishing Distribution Server(s)
- Port Scanning
- Remote Access Applications
- Tor Onion Routing
- US Embargoed Nation(s) Traffic
- Voice over IP (VoIP) Application(s)
- Vulnerability/Exploit Scanning
- Web-based Email Services



### Corporate Headquarters

6 Omni Way  
Chelmsford, Massachusetts 01824  
Toll Free USA +1 866 212 7267  
T +1 978 703 6600  
F +1 978 250 1905

### Europe

T +44 208 622 3108

### Asia Pacific

T +65 6327 7152

[www.arbornetworks.com](http://www.arbornetworks.com)

Copyright ©1999-2009 Arbor Networks, Inc.  
All rights reserved. Arbor Networks, the  
Arbor Networks logo, Peakflow and ATLAS  
are all trademarks of Arbor Networks, Inc.  
All other brands may be the trademarks  
of their respective owners.

DS/ATF/US/0307

## Arbor Security Engineering & Response Team (ASERT)

The creation of ATF fingerprints begins with cutting-edge security analysis, drawing upon up-to-the-minute security intelligence derived from a series of globally deployed attack sensors. ASERT is comprised of leading researchers, with each engineer having spent numerous years solving issues in exploit analysis, host-based Intrusion Prevention System (IPS) development, IDS signature development and malware reverse engineering. On a daily basis, ASERT engineers employ cutting-edge techniques, processes and methods to better identify the most damaging composite threats.

ATF fingerprints model composite threats by leveraging the pioneering flow-based analysis routines that form the core of all Arbor Peakflow appliances. "Flow," which is a data set generated by most of the world's routing and switching devices, captures, among other things, information on the source and destination IP addresses and ports, traffic protocols, used services and the logical interfaces. This enables ASERT to anticipate and track the relationships of multiple traffic flows and to model the sequences of actions that constitute a composite threat. By modeling a sequence of events that must occur in order for ATF to classify a threat, Arbor Peakflow helps security administrators instantaneously identify sophisticated worm propagation, while reducing the false positives associated with other behavior-based offerings.

## Distribution of ATF Fingerprints

Arbor Peakflow employs a secure HTTP connection to poll centralized ATF servers and pull down newly developed fingerprints. If any have been updated, Arbor Peakflow retrieves the fingerprint and updates existing policies where appropriate. This fingerprint delivery is protected with synchronized secure socket layer (SSL) certificates for both the client and the server to ensure that the expected endpoints are participating in the update process, thwarting attacks to the update process. The polling frequency can be configured from once an hour to once a week.

ATF fingerprints cover various categories of threats, ranging from botnet-infected hosts to application profiling (such as IRC), to host and port scanning, to use of peer to peer applications to spread malware to the exploitation of remote access applications to vulnerability scans. Together, these help administrators detect and mitigate the threats posed by unauthorized applications, new hosts and users, the use of unsecure protocols and networks and insider misuse.

## Summary

Arbor Networks' Active Threat Feed (ATF) service is the industry's only behavioral-based zero-day threat detection service. ATF automatically correlates an emerging threat's distinct behaviors and delivers this information in real-time to customers, reducing the cost and time required to identify and mitigate threats.

## About Arbor Networks

Arbor Networks is a leading provider of secure service control solutions for global business networks. Its customers include over 70 percent of the world's ISPs and many large enterprises. Arbor solutions deliver best-in-class network security and visibility, along with the power to improve profitability by deploying differentiated, revenue-generating services. By employing flow-based and deep packet inspection (DPI) technologies, Arbor solutions measure and protect the entire network—from the network core to the broadband edge. Arbor also maintains the world's first globally scoped threat analysis network—ATLAS—which uses technology embedded in the world's largest ISP networks to sense and report on comprehensive worldwide threat intelligence.