DATA SHEET

ATLAS Intelligence Feed

REAL-TIME INTERNET TRAFFIC INTELLIGENCE WORKING WITH ARBOR SOLUTIONS TO PROTECT YOUR DATA CENTER.

Leverage the global threat analysis of the Arbor Security Engineering & Research Team (ASERT) and the ATLAS® Intelligence Feed (AIF) to provide automated, up-to-date protection against the growing threat of distributed denial of service (DDoS) attacks.

With the advent of "do-it-yourself" DDoS attack tools and "botnets for hire," launching a DDoS attack today is easier than ever. Those unfortunate enough to be attacked can face lost revenue, stiff fines, negative media attention, brand tarnishment and other negative impacts. Therefore, it's imperative that you and/or your service provider have the ability to detect and stop the latest DDoS attacks before they impact your business. Data center operators and network security teams can rely upon the expertise of Arbor Networks® and the Pravail™ Availability Protection System (APS) to detect and stop DDoS attacks that threaten the availability of their data centers and services.

> **"Arbor Networks' research is utterly indispensable for anyone who wants to understand the network security landscape, how it is evolving and what the implications may be."**
>
> Ethan Zuckerman, Harvard University Berkman Center for Internet & Society

Expert, Up-to-Date, Automated Protection

The Arbor Security Engineering & Response Team (ASERT) is a recognized industry expert when it comes to Internet threat analysis. ASERT's primary focus is on botnets, which account for a majority of the DDoS attacks on the Internet today. On a daily basis, ASERT gathers approximately 5,000 malware samples from the Internet and other sources. The malware samples are then run through an automated threat analysis system, where they are classified. Unique attacks are stored in a database of over 2.5 million such analyses. When a new botnet or application-layer attack is detected, an attack signature is created, distributed and installed in Arbor's Pravail APS product; this automated service is known as the ATLAS Intelligence Feed (AIF).

AIF allows network security personnel to:

- Stay abreast of the latest attacks by leveraging the daily Internet threat analysis and expertise of ASERT.
- Save time by eliminating the need to manually update security products with the latest attack detection signatures.
- Quickly stop DDoS attacks before they impact critical business services.

Key Features and Benefits

Up-to-Date Protection

Take advantage of ASERT's daily Internet threat analysis and expertise for the latest botnet and application-layer DDoS attack detection signatures.

Automatic Protection

Eliminate time-consuming manual updates by automatically receiving and installing new DDoS attack signatures in Pravail APS.

Botnet and Application-Layer Attack Protection

Detect and stop botnet-derived, application-layer DDoS attacks before they impact critical business services.

Comprehensive Data Center Protection

The combination of AIF-derived botnet and application-layer attack signatures plus the ability to detect other types of DDoS attacks (i.e., floods, malformed packets, connection exhaustion) makes Pravail APS a comprehensive DDoS protection solution for the Internet-facing data center.

ARBOR® NETWORKS

Arbor Pravail APS

Proven DDoS protection is now available to enterprises. The Pravail Availability Protection System (APS) uses the same packet engine technology trusted by many of the world's ISPs to secure the Internet data center (IDC) edge from threats against availability—specifically, protection against botnet-derived, application-layer DDoS attacks.

With Pravail APS, your data center security team can:

- Detect and block emerging application-layer DDoS attacks.
- Deploy a turnkey solution to stop availability threats immediately.
- Prevent illegitimate botnet communications by leveraging real-time intelligence from Arbor's Active Threat Level Analysis System (ATLAS®).
- Mitigate volumetric attacks by coordinating with Cloud Signaling℠-enabled service providers.

ATLAS and Arbor's Threat Analysis Ecosystem

Arbor's Active Threat Level Analysis System (ATLAS) is the world's first globally scoped threat analysis network. A number of ISPs have authorized Arbor to deploy specially designed probes that gather DDoS attack information on their dark-IP networks. ASERT gathers and analyzes information from the ATLAS probes plus "anonymous" alert and DDoS statistics from Arbor's Peakflow® SP solutions that are deployed in a majority of the world's ISP networks. Some of ASERT's analysis can be seen in research documents and blog postings. In addition, every 24 hours data is published to a public security portal located at atlas.arbor.net. This ATLAS data is also used to create the ATLAS Intelligence Feed (AIF), which contains the latest botnet and application-layer DDoS attack signatures for the Arbor Pravail APS product—thus completing Arbor's threat analysis ecosystem.

Arbor Threat Analysis Ecosystem

Stop Emerging Application-Layer Threats

According to Arbor's sixth annual *Worldwide Infrastructure Security Report*, 77% of respondents have experienced an application-layer attack, with HTTP-based attacks accounting for 85% of those attacks. A well-publicized example came from a group of WikiLeaks supporters called Anonymous, who used a combination of social networks, botnets and "do-it-yourself" attack tools to launch application-layer DDoS attacks against their victims. The ATLAS Intelligence Feed can protect services running in data centers by detecting and stopping botnets and application-layer DDoS attacks including:

- DDoS botnet attacks such as BlackEnergy and Darkness
- Voluntary botnet attacks such as LOIC and HOIC
- "Slow HTTP" attacks such as Slowloris and Pyloris

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

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for next-generation data centers and carrier networks. Arbor's proven solutions help grow and protect our customers' networks, businesses and brands. Arbor's unparalleled, privileged relationships with worldwide service providers and global network operators provides unequalled insight into and perspective on Internet security and traffic trends via ATLAS—a unique collaborative effort with 100+ network operators across the globe sharing real-time security, traffic and routing information that informs numerous business decisions.

For technical insight into the latest security threats and Internet traffic trends, please visit our Web site at arbornetworks.com and our blog at asert.arbornetworks.com.

ARBOR® NETWORKS

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 6299 0695

www.arbornetworks.com

DS/AIF/EN/0911