

# Arbor Peakflow SP

## PERVASIVE NETWORK VISIBILITY, SECURITY AND MANAGED SERVICES

Whether you're an Internet service provider (ISP), application/hosting service provider (ASP) or large enterprise, you face growing competition, higher bandwidth consumption and mounting network security threats. At the same time, you're undoubtedly struggling with lower revenues and tighter budgets given today's economic realities. In other words, you're being asked to do more with less. To address these challenges, you need a solution that simultaneously provides: cost-effective, pervasive and intelligent visibility into network and application traffic; the ability to quickly recognize and mitigate security threats; and the potential to deliver revenue-generating managed services.

The Arbor Networks® Peakflow® SP solution ("Peakflow SP") is a network-wide infrastructure security and traffic-monitoring platform that addresses these three critical requirements and allows you to scale with your growing network and customer base. By leveraging IP flow and deep packet inspection (DPI) technologies, it provides pervasive network and application visibility—enabling you to proactively identify threats, improve network and service performance and make more informed business decisions. The de facto security standard for the majority of the world's leading service providers, Peakflow SP combines the following functionality in one integrated, comprehensive solution:

- **Know Your Network:** Pervasive visibility into network, application and routing traffic allows you to make sound decisions about transit partners, network architecture, customers and new IP services.
- **Secure Your Network:** Real-time detection, mitigation and comprehensive reporting of security events enable you to minimize their adverse impact on your network, your services and your customers.
- **Grow Your Network:** Leverage the same Arbor Peakflow SP platform used for network visibility and security to deliver differentiated, profitable, in-cloud distributed denial of service (DDoS) managed services.

### Key Features and Benefits

#### Scalable and Cost-Effective Visibility

Leverage IP flow and deep packet inspection (DPI) technologies to gain pervasive, cost-effective network and application-layer visibility to reduce costs, optimize services and protect infrastructure.

#### Intelligent Traffic Engineering

Correlate data to highlight critical network and application traffic, reduce peering costs, improve traffic engineering and perform network troubleshooting.

#### Comprehensive Threat Management

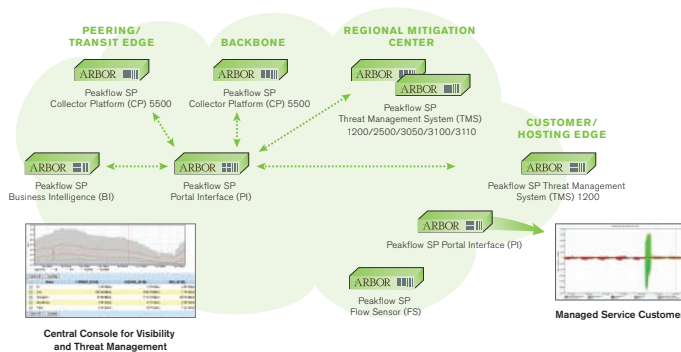
Gain complete threat detection, surgical mitigation and reporting capabilities to protect and maintain your network, reduce costs and avoid lost revenue due to unavailable IP services.

#### Service Visibility, Performance and Protection

Gain visibility into critical network services, monitor their key performance metrics and detect and mitigate threats—allowing you to maintain service availability and customer satisfaction.

#### Managed Service Enabler

Leverage the same Arbor Peakflow SP platform used for network visibility and security to easily provision, deliver and maintain differentiated, profitable, in-cloud DDoS managed services.



#### Peakflow SP Architecture

Consists of five types of appliances: 1) Peakflow SP Collector Platform (CP) appliances in the peering edge or backbone; 2) Peakflow SP Flow Sensor (FS) appliances in the customer aggregation edge; 3) Peakflow SP Business Intelligence (BI) appliances to increase scalability and add redundancy for managing critical business objects; 4) Peakflow SP Portal Interface (PI) appliances to increase the scale, redundancy and profitability of Arbor-based managed services; and 5) Peakflow SP Threat Management System (TMS) appliances deployed in any part of the network to surgically mitigate network threats.

## Real-Time Global Threat Analysis—From One Console

Arbor's Network Security, Engineering and Response Team (ASERT) leverages Arbor's trusted relationship with a majority of the world's Internet service providers to gain unique insight into global threat activity. As a result, ASERT delivers multiple benefits back to the industry and Arbor customers under a broad initiative known as the Active Threat Level Analysis System (ATLAS). Below are some of the ATLAS deliverables that manifest themselves in the Peakflow SP solution:

### ATLAS Security Portal

The ATLAS security portal (located at <http://atlas.arbor.net>) provides a real-time view into global threat activity. This information is easily accessible from within the Peakflow SP console, allowing service providers to see how worldwide threat activity may be impacting their network.

### Fingerprints

As ASERT analyzes global threat activity, it creates "fingerprints" that are the network behavioral patterns of attacks. These fingerprints are automatically distributed to Peakflow SP customers via the Active Threat Feed (ATF) service—allowing Peakflow SP TMS to detect and surgically mitigate attacks that match these fingerprints.

### Fingerprint Sharing Alliance

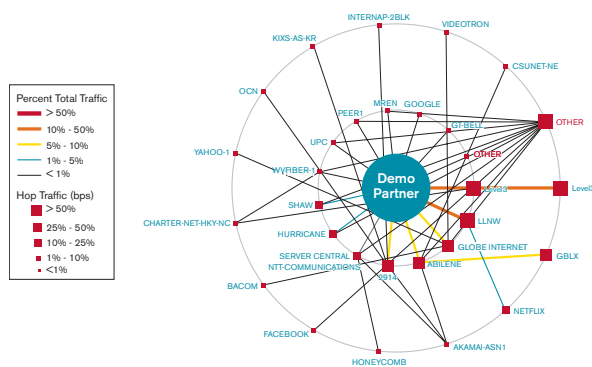
The distributed nature of DDoS attacks requires ISPs to work with each other to stop these events. To help facilitate this collaboration, Arbor created the Fingerprint Sharing Alliance (FSA), which allows service providers to easily share fingerprints among their Peakflow SP deployments.

## The Power, Scalability and Availability You Need

Arbor Peakflow SP is a solution for network-wide, non-intrusive reporting, anomaly detection and intelligent mitigation. Peakflow SP learns normal traffic and routing behavior across hundreds of routers and thousands of interfaces, and correlates the traffic patterns with the topology data to build logical data models. Armed with this information, Peakflow SP notifies your operations staff and customers of significant changes to the network, whether they are due to a DDoS attack, misconfiguration, equipment failure or the long-term effects of shifting traffic. Peakflow SP provides a single, comprehensive solution with the intelligence, scalability and availability necessary to effectively tackle these threats to network integrity.

## Intelligent Traffic Engineering, Capacity Planning and Network Troubleshooting

Arbor Peakflow SP dramatically improves traffic engineering and capacity planning by correlating real-time topology information with traffic data. Peakflow SP allows network operators to optimize their network and reduce costs by providing detailed visibility into the traffic that is leaving or entering their networks via peering or transit links. Peakflow SP provides insight into critical information such as BGP routing, MPLS VPNs, QoS and applications such as DNS, VoIP and P2P—enabling network operators to automatically recognize hot spots and engineer the network for lower costs, higher performance and new services. Peakflow SP and Peakflow SP Threat Management System ("Peakflow SP TMS") can also perform real-time analysis of services, applications and packets to quickly restore services and reduce mean time to repair (MTTR).



## Service Visibility, Performance and Protection

To your customers, your network is only as good as the applications and IP services that run on it. The diversity of customer applications ranging from triple-play services (e.g., data, voice and video) to Over The Top (OTT) applications (e.g., IM, Skype and YouTube) makes service optimization even more challenging. Using flow and payload analyses, Arbor Peakflow SP and Peakflow SP TMS can automatically recognize over 90 applications; alternatively, you can define custom applications. To help ensure customer satisfaction and optimal performance of applications such as HTTP, VoIP and DNS, Peakflow SP and Peakflow SP TMS provide insight into key metrics such as jitter, latency, network round-trip times, delay and packet loss. Additionally, Peakflow SP TMS enables a unique set of application-layer attack detection and surgical mitigation capabilities that allow service providers to protect business-critical IP services—thus maintaining availability, reducing support costs and optimizing business services.

## Comprehensive Attack Detection, Surgical Mitigation and Reporting

Large-scale DDoS attacks affect not only the intended victim, but also other unfortunate customers who use the same shared network service. The Arbor Peakflow SP solution is a comprehensive threat management system that offers multiple methods of rapid attack detection and mitigation such as access control lists (ACL), BGP blackhole routing, BGP flow-spec and attack fingerprint sharing. Unfortunately, these mitigation methods also shut down all traffic destined for the victim's site—thus completing the DDoS attack. The combination of Peakflow SP and Peakflow SP TMS allows service providers to detect and surgically remove only the attack traffic while maintaining the legitimate business traffic.

Arbor's Security Engineering and Response Team (ASERT), a recognized industry leader in the area of global threat activity, creates fingerprints (network behavioral patterns of known or emerging threats) and distributes them to Peakflow SP customers via the Active Threat Feed (ATF) service. This allows network operators to conduct more granular attack detection and mitigation. After the attack has been thwarted, ISPs can easily produce reports that summarize the mitigation process for customers and/or management.

### The Solution for Profitable Managed DDoS Services

As the price of bandwidth declines and competition increases, IP-based services play a critical role in generating new revenue. It is crucial to leverage as much of the existing network infrastructure, tools and human resources as possible in order to deliver profitable, new in-cloud managed services. Arbor Peakflow SP is a strategic investment that allows product managers to leverage the same solution used for infrastructure visibility and security to deliver differentiated, in-cloud managed services such as DDoS protection.

Arbor Peakflow SP TMS plays a vital role in a Peakflow SP-based managed DDoS service. Peakflow SP TMS is an application-intelligent appliance for multi-service converged networks that speeds remediation by coupling high-level threat identification with packet-level analysis. Peakflow SP TMS allows providers to detect network and application-layer attacks and surgically scrub only the attack traffic while allowing non-attack traffic.

Peakflow SP is designed to reduce the operational complexity and cost of a managed DDoS service. Key features include templates/APIs for customized portals, redundancy, automated failover, data synchronization, "one-click" or auto-mitigation, customizable mitigation templates, real-time mitigation dashboards and comprehensive mitigation reports. These features simplify the provisioning and operational support of the managed DDoS service—increasing profitability and customer satisfaction.

### Optimized DDoS Protection

To optimize the deployment of DDoS mitigation, Peakflow SP TMS offers a variety of models and feature sets. The chart below outlines the various models, their features, performance capabilities and deployment scenarios.



Peakflow SP TMS deployment

### Multiple Methods of Threat Detection and Mitigation

The combination of Peakflow SP and Peakflow SP TMS allows service providers to protect critical IP services by leveraging the following methods of attack/anomaly detection and mitigation.

**Block known malicious hosts** by using white and black lists. The white list contains authorized hosts, while the black list contains zombies or compromised hosts whose traffic will be blocked.

**Block application-layer exploits** by using complex filters. Peakflow SP TMS provides payload visibility and filtering to prevent cloaked attacks from bringing down critical services.

**Defend against Web-based threats or anomalies** by using mechanisms to detect and mitigate HTTP-specific attacks. These mechanisms also help with managing flash-crowd scenarios.

**Shield DNS services from botnets** that mask, amplify and deliver exploits to DNS infrastructure and services. Arbor Peakflow solutions enable you to employ DNS-specific attack detection and mitigation capabilities.

**Protect critical VoIP services** from automated scripts or botnets that exploit packet per second and malformed request floods. Arbor Peakflow solutions enable you to employ VoIP/SIP-specific attack detection and mitigation capabilities.

**Control the zombie army** by using specialized, always on/always learning zombie detection mechanisms that ensure compromised hosts are not attacking mission-critical infrastructure.

**Enforce baseline protection** by building ongoing, always learning models of network behavior. This information can be leveraged to identify abnormal traffic and block it from the network at the time of attack.

“Arbor’s Peakflow SP enables us to secure the network, improve traffic engineering and offer managed DDoS protection, all on a platform that is easy to use and assimilate into our back office systems.”

Urs Reutimann, Project Manager,  
sunrise

## Peakflow SP Appliances



Arbor Peakflow SP Collector Platform (CP), Flow Sensor (FS), Business Intelligence (BI) and Portal Interface (PI). Each utilize the depicted enclosure.



### 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)

## Arbor Peakflow SP Collector Platform (CP), Flow Sensor (FS), Business Intelligence (BI) and Portal Interface (PI) Appliance Specifications

### Power Requirements

Redundant dual power sources  
AC: 100/240V, 8.5A (50-60 Hz)  
DC: -48 to -60V, 20.5A max

### Physical Dimensions

Chassis: 2U rack height  
Weight: 39 lbs (17.7 kg)  
Height: 3.45 in (8.76 cm)  
Width: 17.11 in (43.46 cm)  
Depth: 20 in (51 cm)  
Standard 19 in and 23 in rack mountable

### Hard Drives

Dual hard drives running RAID 1

### NICs

2 x 10/100/1000BaseT (fiber option available)

### Environmental

Operating: 32° to 104°F (0° to 40°C)  
Relative Humidity (Non-Operating): 95%, non-condensing at temperatures of 73° to 104°F (23° to 40°C)

### Operating System

ArbOS®, our proprietary, embedded operating system, is based on open source operating system technology such as Linux and Open BSD.

### Performance

Configured for NetFlow (OC-48) and packets (GigE)

### Compatibility

Flow Data: Supports Cisco NetFlow v5, v7, v9; Juniper cflowd  
Monitoring: Integrates with management consoles supporting SNMP v3  
Web-Based UI: IE 5-7.0 and Mozilla 1.2+ using SSL

### Regulatory Compliance

ETSI, NEBS and RoHS compliant

## Arbor Peakflow SP TMS Specifications

### Power Requirements

Redundant dual power sources

### 3050/3100/3110

AC: 100/240V, 50-60Hz, 460W nominal  
DC: -48 to -68V; 460W nominal

### 2500

AC: 100/240V, 8.5A (50-60 Hz)  
DC: -48 to -60V, 20.5A max

### 1200

AC: 100/240V, 8.5A (50-60 Hz)  
DC: -48 to -60V, 12A max

### Hard Drives

Dual hard drives running RAID 1

### Physical Dimensions

Standard 19 in and 23 in rack mountable

### 3050/3100/3110

Chassis: 3U rack height  
Weight: 33.5 lbs (15.2 kg)  
Height: 5.25 in (13.34 cm)  
Width: 19 in (44.8 cm)  
Depth: 16.28 in (41.33 cm)

### 2500

Chassis: 2U rack height  
Weight: 39 lbs (17.7 kg)  
Height: 3.45 in (8.76 cm)  
Width: 17.11 in (43.46 cm)  
Depth: 20 in (51 cm)

### 1200

Chassis: 1U rack height  
Weight: 25.41 lbs (11.52 kg)  
Height: 1.7 in (4.32 cm)  
Width: 16.93 in (43 cm)  
Depth: 20 in (51 cm)

### NICs

### 3100

2 x 10 GigE (SFP+)

### 3050/3110

2 x 10 GigE (SFP+)  
10 x 1 GigE

### 2500

2 x 10/100/1000BaseT (fiber option available)

### 1200

4 x 10/100/1000BaseT (fiber option available)

### Environmental

### 3050/3100/3110

Operating: 32° to 131°F (0° to +55°C)  
Relative Humidity (Operating): 5 to 80% non-condensing

### 2500

Operating: 32° to 104°F (0° to 40°C)  
Relative Humidity (Operating): 10 to 90% non-condensing

### 1200

Operating: 50° to 95°F (10° to 35°C)  
Relative Humidity (Operating): 12 to 90% non-condensing

### Operating System

### 1200/2500/3050/3100/3110

ArbOS®, our proprietary, embedded operating system, is based on open source operating system technology such as Linux and Open BSD.