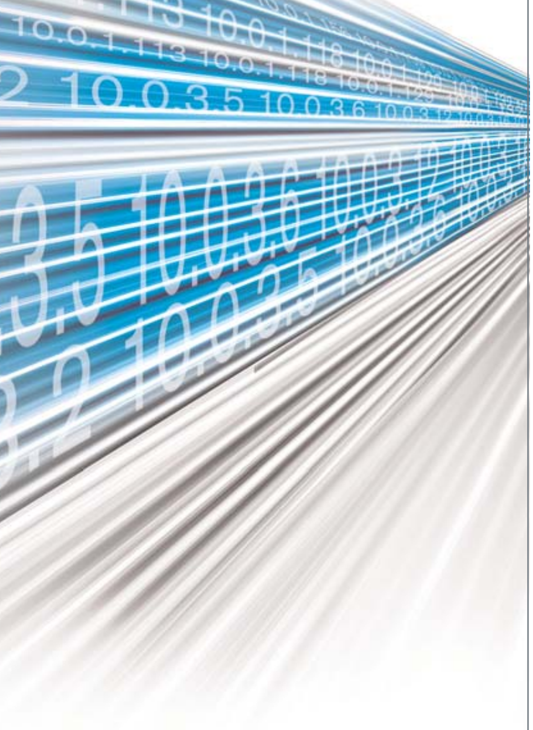


DATA SHEET

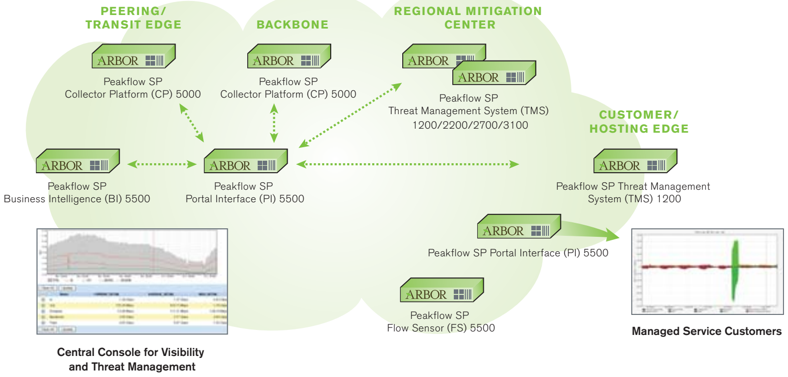
Arbor Peakflow SP

PERVASIVE NETWORK VISIBILITY, SECURITY AND PROFITABLE MANAGED SERVICES

Today's service providers face intense competition, high churn rates, lean operations, and a proliferation of network traffic, applications and security threats—creating challenges that threaten the availability of networks and services. These widespread challenges are confronting Internet service providers (ISPs), application service providers (ASPs), hosting providers and large enterprises alike. To address these challenges, service providers need cost-effective, pervasive and intelligent visibility into network and application traffic, combined with the ability to quickly recognize and mitigate security threats.

The Arbor Networks® Peakflow® SP ("Peakflow SP") solution is a network-wide infrastructure security and traffic-monitoring platform that addresses these critical requirements, scaling with your network and customer base. By leveraging IP flow technologies, it provides pervasive network and application visibility–enabling you to proactively identify threats, improve network performance and make more informed business decisions. The de facto standard and security platform of choice for a 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 engineering, customers and new IP services.
- **Secure Your Network:** Real-time detection, mitigation and comprehensive reporting of network anomalies enable you to minimize their adverse impact on both your network and your customers' networks.
- **Grow Your Network:** Leverage the same Arbor Peakflow SP platform used for network visibility and security to deliver differentiated, profitable, in-cloud DDoS managed services.


PEERING/ TRANSIT EDGE
BACKBONE
REGIONAL MITIGATION CENTER
CUSTOMER/ HOSTING EDGE
ARBOR
Peakflow SP Collector Platform (CP) 5000
Peakflow SP Collector Platform (CP) 5000
Peakflow SP Threat Management System (TMS) 1200/2200/2700/3100
Peakflow SP Business Intelligence (BI) 5500
Peakflow SP Portal Interface (PI) 5500
Peakflow SP Threat Management System (TMS) 1200
Peakflow SP Portal Interface (PI) 5500
Peakflow SP Flow Sensor (FS) 5500
Central Console for Visibility and Threat Management
Managed Service Customers

Peakflow SP Architecture

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

Key Features and Benefits

Business Intelligence

Gain insight into all network entities to make more intelligent business decisions.

Scalable and Cost-Effective Visibility

Leverage IP flow technologies to optimize services, reduce costs and get pervasive, cost-effective network and application visibility.

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.

Operational Simplicity

Ease the provisioning, daily support and future expansion of DDoS managed services.

Intelligent Traffic Engineering

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

Managed Service Enabler

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

ARBOR®
NETWORKS

The Business Value of Managed Objects

One of Peakflow SP's greatest strengths is its ability to focus on critical network entities using a feature called managed objects. A managed object (MO) can be a specific network entity such as a peer, ASN, router, application, customer or type of traffic–or any Boolean combination of these entities. Managed objects allow network engineers, security architects and product managers to answer critical business questions. For example:

Network Engineer: "When will we need additional circuits between Chicago and Detroit?"

MO Definition: Chicago's routers AND Detroit's BGP subAS.

Security Architect: "What types of attacks are being sent to my VoIP infrastructure?"

MO Definition: CIDR blocks of SIP servers AND media gateways.

Product Manager: "How many of our subscribers in the New York metro area are using VoIP applications like Skype?"

MO Definition: APPID "skype" AND "New York" CIDR blocks.

High Availability for Managed Services

The Peakflow SP Portal Interface (PI) device provides fault tolerance and redundancy to keep managed services up and running. Deployed in a hierarchical fashion, these devices optimize service availability via:

Real-Time Data Synchronization: Peakflow SP PI devices are always in contact with the Peakflow SP deployment-polling data, analyzing events and synchronizing configuration changes with each other.

Automated Failover: One Peakflow SP PI device acts as the leader while another is the backup. In the event of leader-to-backup communication loss, an automated failover designates the backup as the new leader until communication is reestablished.

The Power, Scalability and Availability You Need

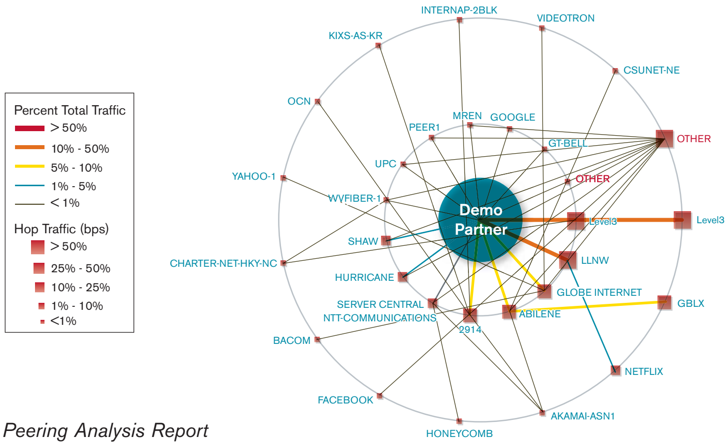
Arbor Peakflow SP is a solution for network-wide, non-intrusive relational modeling, anomaly detection and intelligent mitigation. Peakflow SP learns normal traffic and routing behavior across hundreds of routers and thousands of interfaces, and correlates the traffic patterns with the topology data 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 network integrity threats.

Intelligent Traffic Engineering and Capacity Planning

Arbor Peakflow SP dramatically improves traffic engineering, IP service performance and capacity planning by correlating real-time and historical topology information with traffic data. It provides insight into critical information such as transit/peering traffic, BGP routing, MPLS VPNs, QoS and applications such as DNS, VoIP and P2P—enabling network operators to engineer the network for lower costs, higher performance and new managed services.

Powerful Route Analytics

BGP connects the largest networks in the world. Arbor Peakflow SP provides multi-protocol BGP analysis to enable network operators to detect, isolate and repair BGP problems. Network operators can use Peakflow SP to perform route analysis and automatically be alerted to anomalies both inside their network domain and across the Internet.



Peering Analysis Report

A 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's 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 new, differentiated, revenue-generating, managed services such as DDoS protection.

The Arbor Peakflow SP Threat Management System (TMS) plays a vital role in a Peakflow SP-based managed DDoS service. Peakflow SP TMS is an application-intelligent device 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, "one-click" or auto-mitigation, customizable mitigation templates, mitigation and Peakflow SP TMS status reports. These features simplify the provisioning and operational support of the managed DDoS service—increasing profitability and customer satisfaction.

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 Peakflow SP solution is a comprehensive threat management system that offers multiple methods of attack detection and mitigation such as: access control lists (ACL), BGP black-hole routing, BGP flow-spec, attack fingerprint sharing, and support for other third-party packet scrubbing products. In order to reduce the cost of collateral damage, service providers often use such techniques to shut down all traffic destined for the victim's site—thus completing the DDoS attack. The combination of Arbor Peakflow SP and Peakflow SP TMS allows service providers to detect and surgically remove only the attack traffic while maintaining the legitimate business traffic. After the attack has been thwarted, ISPs can easily produce reports that summarize the mitigation process for customers and/or management.

Application-Layer Protection

To your customers, your network is only as good as the applications and IP services that run on it. From triple-play services (e.g., data, voice, video) to social networking applications (e.g., IM, Skype, iTunes), the growing diversity of customer applications makes service optimization even more challenging. The combination of Peakflow SP and Peakflow SP TMS provides a unique set of application-layer attack detection and surgical mitigation capabilities that allow service providers to protect business-critical IP services—allowing providers to maintain availability, reduce support costs and optimize business services.

Optimized DDoS Protection

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

Peakflow SP TMS Models	Form Factor	Attack Mitigation Performance and Features	Recommended Deployment Scenarios
Model 1200 	1 RU	- 1.5 Gbps - Not stackable - Deployment: Port Span, BGP Off-ramp, In-line	- Customer Dedicated Equipment - Smaller Aggregation and Edge POPs - Island Architectures
Model 2200 	2 RU	- 1.5 Gbps - Not stackable - Deployment: Port Span, BGP Off-ramp	- NEBS, ETSI Compliant Hardware - Same deployment scenarios as the 1200 but where NEBS is required
Model 2700 	2 RU	- 3-8 Gbps - Stackable - Deployment: Port Span, BGP Off-ramp, In-line	- Regional Scrubbing Center - Large Peering POPs - Major Network Gateways - Critical infrastructure
Model 3100 	3 RU	- 10 Gbps - Not Stackable - Deployment: Port Span, BGP Off-ramp	- Same deployment scenarios as the 2700, but in 10 Gbps environments

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 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 by using mechanisms to detect and mitigate *HTTP-specific attacks.* These mechanisms also help with managing Flashcrowd 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 assimiliate into our back office systems.”
>
> Urs Reutimann, Project Manager,
> sunrise

Peakflow SP Devices

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

Corporate Headquarters

430 Bedford Street
Lexington, Massachusetts 02420

Toll Free USA +1 866 212 7267
T +1 781 684 0900
F +1 781 768 3299

Europe

T +44 208 622 3108

Asia Pacific

T +65 6327 7152

www.arbornetworks.com

Arbor Peakflow SP Collector Platform (CP), Flow Sensor (FS), Business Intelligence (BI) and Portal Interface (PI) Device 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: 41° to 104°F (5° to 40°C)
Relative Humidity (Non-Operating): 95%, non-condensing at temperatures of 73° to 104°F (23° to 40°C)

Operating System
Our proprietary, embedded operating system is based on Whitebox Linux and is designed for maximum security.

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
Available upon request. NEBS solution available.

Arbor Peakflow SP Threat Management System (TMS) Device Specifications

Power Requirements
Redundant dual power sources

3100
AC: 100/240V, 50-60Hz, 460W nominal
DC: -48 to -68V; 460W nominal

2700
AC: 100/240V, 8.5A (50-60 Hz)
DC: -40 to -75V, 500W nominal

2200
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

Physical Dimensions
Standard 19 in and 23 in rack mountable

3100
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: 16.275 in (41.33 cm)

2700
Chassis: 2U rack height
Weight: 40 lbs (18.14 kg)
Height: 3.5 in (9 cm)
Width: 17 in (43 cm)
Depth: 24 in (61 cm)

2200
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)

Hard Drives
Dual hard drives running RAID 1

NICs

3100
2 x 10 GbE (SFP+)

2700
4 x 10/100/1000BaseT
4 x 1000BaseSX (fiber)
4 x 1000BaseLX (SFP+)

2200
2 x 10/100/1000BaseT (fiber option available)

1200
4 x 10/100/1000BaseT (fiber option available)

Stackability

2700
Max 3 TMS devices (3-8 Gbps of processing)

Environmental

3100
Operating: 32° to 1131°F (0° to +55°C)
Relative Humidity (Operating): 5 to 80% non-condensing

2700 and 2200
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

Regulatory Compliance

3100
UL 60950, IEC/EN 60950, FCC Part 15, Subpart B, Class A, CE Mark, NEBS GR-63-CORE and GR-1089-CORE Level 3, RoHS 6/6 Compliant

2700, 2200, 1200
FCC Part 15 Class A, IEC60950 3rd ed., CE, VCCI, BSMI, CISPR, ICES, CTick, MIC, CCC, (model 2200 NEBS)