Peakflow® Solution

Pervasive network visibility and threat management

Internet service providers, Mobile Network Operators, Cloud/Mass Hosting providers and large enterprises face the common challenge of meeting increasing user demand for more services and higher availability. Operations staff, engineering and management need the network intelligence and tools to deal in real time with events that impact availability. They also need to make the right network engineering and capacity planning decisions to ensure smooth, efficient operations in the future as they meet growing demand for services.
The Peakflow solution ("Peakflow") is the de facto standard for network intelligence and infrastructure availability. Peakflow protects service availability for more Internet Service Providers, more cloud providers and more enterprises than all other solutions combined.

Key Features and Benefits

Protect Network Infrastructure
Detect and stop DDoS attacks before they impact availability and performance of fixed or mobile network infrastructure.

Protect Services
Safeguard critical services such as DNS, voice, video, Web, ecommerce and email from targeted attacks.

Mobile Packet Core Visibility & Threat Detection
Gain visibility into GTP traffic and detect threats before they impact mobile network performance.

Optimize Network Resources
Use traffic visibility and comprehensive reports for better traffic engineering and faster, more effective troubleshooting. Reduce transit costs, improve utilization and intelligently plan for growth.

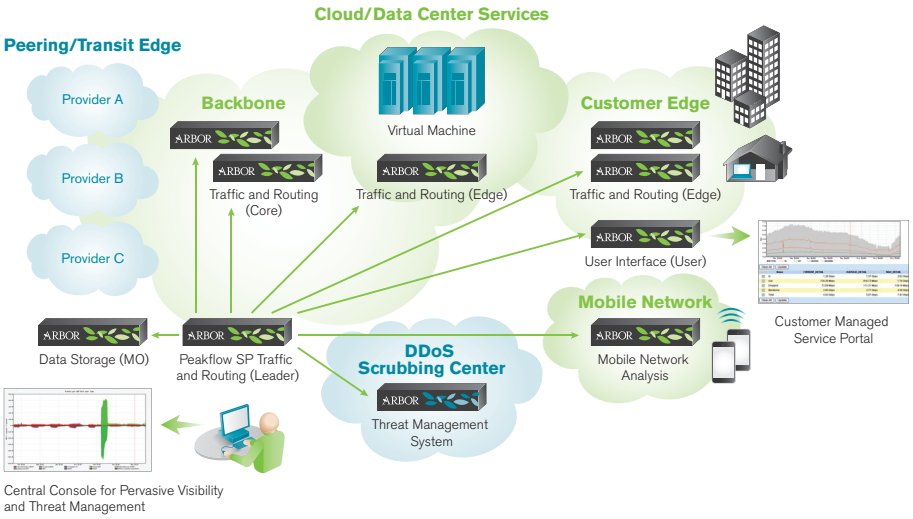
Launch Managed Security Services
Leverage the same Peakflow platform used for network visibility and security to easily provision, deliver and maintain differentiated, profitable, in-cloud DDoS Protection services.

Flexible Licensing
Peakflow's Flex Licensing unlocks new performance and scalability improvements and enables a more optimized, less expensive deployment.

The Power of Network Intelligence

Peakflow collects, aggregates and analyzes packets, NetFlow, SNMP and BGP routes from across the network. It transforms masses of data into actionable intelligence that supports day-to-day operational excellence and sound planning for the future. The Peakflow solution is based on the following principles:

- **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 Infrastructure:** Real-time detection and mitigation of security events enable you to prevent adverse impact on your network, your data centers, your services and your customers.
- **Grow Your Business:** Leverage the same Peakflow platform used for network visibility and security to deliver differentiated, profitable, in-cloud distributed denial of service (DDoS) protection services.



Peakflow SP architecture

1) Core Traffic and Routing analysis in Peering/Transit edge and/or Backbone; 2) Edge Traffic and Routing analysis at Customer edge and Data Center; 3) Mobile Network Analysis in Mobile Packet Core; 4) Data Storage to increase scalability and add redundancy; 5) User Interface for customer portals; 6) Surgical mitigation of network threats in DDoS Scrubbing Centers.

ARBOR® NETWORKS

Real-Time Global Threat Analysis, From One Console

The Arbor Security Engineering and Response Team (ASERT) leverages Arbor's trusted relationships with a majority of the world's Internet Service Providers to gain unique insight into global threat activity. ASERT delivers multiple benefits to the industry and Arbor customers under an initiative called the Active Threat Level Analysis System (ATLAS). These benefits include:

ATLAS® Security Portal

The ATLAS security portal (located at 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.

ATF and AIF

Using ATLAS global monitoring, Arbor researchers discover emerging network layer and application layer attacks and develop appropriate defenses. These defenses are automatically uploaded to Peakflow systems via the ATLAS Threat Feed and the ATLAS Intelligence Feed.

Cloud Signaling™ Technology

Arbor's latest advance in DDoS defense provides automated and coordinated response to attacks that threaten to both overwhelm network bandwidth capacity and data center services.

Peakflow SP Traffic and Routing, User Interface, and Data Storage roles. Each can optionally be deployed on the Peakflow SP 6000 appliance depicted enclosure.

Peakflow SP tells network operators:

- Where traffic on their network is coming from and going to.
- What routes the traffic takes.
- What interfaces and devices are most heavily used.
- Who are the top talkers on the network.
- What are the short- and long-term trends.
- What is the traffic forecast.

This reporting is extremely valuable to network operators. It enables efficient and cost-effective network engineering that allows operators to make better decisions concerning peering and transit agreements, identify overused or underused devices and circuits, and gain insight into customer usage trends and requirements. Peakflow is non-intrusive on the network. They leverage network telemetry provided by routers and switches to deliver key intelligence without relying on inline probes or taps.

Anomaly Detection

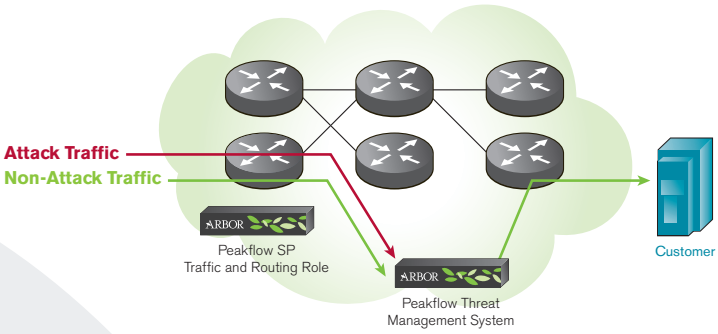
A core value of Peakflow is its ability to generate alerts to anomalies on the network. These anomalies can be indicative of malicious traffic (e.g. DDoS attacks), device failures, unusual demand spikes, GTP signaling storms or misconfigurations. These alerts enable operators to spot problems quickly, rapidly identify the root cause and take corrective action.

Denial of Service Protection

The Peakflow Threat Management System mitigates DDoS attacks by surgically removing attack traffic while allowing non-attack traffic to pass normally. It can be deployed inline for "always on" protection. However, unlike other products, it does not have to be deployed inline.

Peakflow Threat Management System supports a mitigation architecture called "diversion/reinjection." In this mode, traffic is redirected to Peakflow Threat Management System via routing updates issued by the Peakflow SP Traffic and Routing role. Peakflow Threat Management System then removes only the attack traffic from the packet stream and forwards legitimate traffic to its intended destination.

This is highly advantageous for service providers, large enterprises and large hosting/cloud providers. It enables a single Peakflow Threat Management System to protect multiple data centers from a central location and allows a much more efficient use of mitigation capacity. Inline devices must inspect all traffic all the time on every monitored link. Peakflow Threat Management System only needs to inspect traffic that is redirected to it—a small subset of the overall traffic flowing through larger networks.



Peakflow Threat Management System surgical mitigation

The Solution for Profitable Managed DDoS Services

Peakflow reduces the operational complexity and cost of deploying 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. Peakflow is used by more managed services providers to deliver DDoS protection services than all other solutions combined.

Mobile Packet Core Visibility and Anomaly Detection

Arbor's Peakflow Mobile Network Analysis is a fully integrated extension of Peakflow SP, providing network operators with unified visibility and threat management across their fixed and mobile networks from a single console.

Peakflow Mobile Network Analysis provides real-time and historical analytics into critical 3G (HSPA) and 4G (LTE) GTP-C message flows, improving understanding of signaling patterns and unwanted traffic activity in the mobile core as the basis for securing it.

Peakflow Mobile Network Analysis also detects and alerts on malicious and non-malicious GTP-C traffic anomalies, providing early warning of threats to network and service performance and availability.

Management and Scale

Peakflow provides the industry's most comprehensive and flexible reporting and management system for network visibility and security. It is designed for use in multiple contexts—including enterprise, hosting/cloud provider and service provider environments. Features include the ability to monitor, report and protect up to 20,000 managed objects (e.g., customers, IP address ranges, interfaces, routes and services); support for 550,000 network interfaces; extensive reporting and drill-down capability; report customization; plus the definition of flexible and customizable management roles.

Businesses That Use Peakflow

Power Requirements	Service Benefits
Internet Service Providers (ISPs, MSOs)	Wireline ISPs use Peakflow for network visibility and anti-DDoS functionality to improve network engineering; better manage peering and transit relationships; keep bad or unwanted traffic from consuming network capacity; provide MPLS visibility to customers; and prevent DDoS attacks from affecting end customers.
Mobile Network Operators (MNOs)	Mobile providers use Peakflow to protect core infrastructure (GGSNs) and core services (AAA, DNS) from DDoS and resource-exhausting attacks from the Internet and from subscribers.
Hosting and Cloud Providers (IaaS, PaaS, or SaaS)	Hosting and cloud providers use Peakflow to improve traffic engineering; keep unwanted traffic from affecting overall service levels; and protect core and customer operations from DDoS attacks.
Enterprises	Enterprises use Peakflow to defend online operations against DDoS attacks—protecting online retail, SaaS, gaming, media and entertainment—and financial services.
Managed Security Services Providers (MSSPs)	Pure-play MSSPs, hosting providers and ISPs all use Peakflow to provide DDoS protection as a managed service.

Proven, Comprehensive Threat Detection and Mitigation

The Peakflow solution is deployed more widely than all other solutions combined. The reason is clear: It provides valuable business intelligence, network visibility and protection from events that threaten service availability.

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.

Use IP Location to gain visibility and block traffic from unwanted sources. Defend against Web-based threats or anomalies by using mechanisms to detect and mitigate HTTP-specific attacks.

Protect and manage DNS services. Advanced DNS protections and reporting in the Peakflow platform ensure availability of these critical services.

Protect critical VoIP services from automated scripts or botnets that exploit packet per second and malformed request floods.

Protect SSL based services (web, email, file transfer) from attacks on SSL infrastructure.

Control flash crowds and misbehaving hosts. Peakflow provides the tools to detect and manage demand spikes in order to ensure continuous service availability.

"We've been growing with the Peakflow product set since the beginning when we were a small ISP to now as a global service provider. Working with Arbor has been an absolute pleasure over the last five years. I would not hesitate recommending the product to anyone who runs an IP network—either on a local or global scale."

Christiaan Keet, Network Services Director, Easynet Global Services

Peakflow Deployment Scale

Mitigation Capacity	4 Tbps
BGP Routes (Unique)	3,750,000,000
Flows Per Second (Non-sampled)	30,000,000
Routers	5,000
Monitored Interfaces	200,000
Total Interfaces	550,000
Managed Objects	20,000
Collection Appliances	150
Peakflow Threat Management System Appliances	100
Pravail APS Appliances (Cloud Signaling)	200
Users	700

ARBOR® NETWORKS

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

DS/PEAKFLOWSOLUTION/EN/0214-LETTER

Peakflow Platforms

Role / Description	Appliance-Based License	Flex License
TRAFFIC AND ROUTING	**Peakflow SP Collector Platform (CP) appliance: CP 6000-5, CP 6000-2 or Peakflow SP Flow Sensor (FS): FS 6000-15**	**SP-6000 appliance**
Peakflow SP Collector Platform (CP): • Collects flow data in a Peakflow SP deployment Peakflow SP Flow Sensor (FS): • Performs collection/analysis functions of the CP appliance except for BGP peering analysis	For core backbone and peering routers: • CP 6000-5 collects 200k flows/sec from 5 routers. • CP 6000-2 collects 200k flows/sec from 2 routers. For smaller customer edge routers: • FS 6000 collects 200k flows/sec from 15 routers.	• Collects 200k flows/sec from 32 core routers or 100 edge routers
USER INTERFACE	**Peakflow SP Portal Interface (PI) appliance: PI 6000-25**	**SP-6000 appliance**
• Dedicated management platform for Peakflow SP deployments • Offloads management and reporting from the CP appliance • Designed for managed services by supporting customer portals, portal API and more concurrent users	• Required for Peakflow SP deployments with 5 or more CP appliances • PI leader device supports up to 25 concurrent users or up to 125 per deployment • PI supports up to 200 Pravail® appliances for Cloud Signaling™	• User Interface for Peakflow SP Flex licensing deployments • Supports up to 100 concurrent users or 700 per deployment • Supports up to 200 Pravail® appliances for Cloud Signaling™
DATA STORAGE	**Peakflow SP Business Intelligence (BI) appliance: BI 6000-500**	**SP-6000 appliance**
• Dedicated management platform for creating monitored and protected managed objects (customers, networks, resources) • Increases the scale of a Peakflow SP deployment without having to add CP appliances	• Supports up to 500 Managed Objects (MOs) • 20 BI appliances in a Peakflow SP deployment enable up to 10,000 managed objects	• Supports up to 1000 Managed Objects (MOs) • 20 BI and/or Data Storage appliances in a Peakflow SP deployment enable up to 20,000 managed objects with Flex licensing
MOBILE CORE ANALYSIS	**Peakflow Mobile Network Analysis**	
• Real-time and historical analysis of critical 3G (HSPA) and 4G (LTE) GTP-C message flows. • Detects and alerts on malicious and non-malicious GTP-C traffic anomalies	• Fully integrated into Peakflow SP UI • License increments include 25K, 50K or 100K GTP-C messages/sec • System supports up to 1M GTP-C messages/sec	
MITIGATION	**Peakflow Threat Management System**	
• Provides deep packet inspection (DPI), application intelligence and surgical mitigation of attacks	• Threat Management System 4000 for up to 40 Gbps and 40 Mpps mitigation • Threat Management System 2300 for up to 10 Gbps and 10 Mpps mitigation • 100 Threat Management System appliances in a deployment can mitigate up to 4 Tbps • Available as an embedded router blade on the Alcatel Lucent 7750 SR or Cisco CRS routers	

Peakflow SP 6000 Appliance Specifications

Features	Description		
Power Requirements	Redundant dual power sources; **AC:** 100-127V/200-240V, 50 to 60Hz, 6/3A; **DC:** -48 to -72V, 13A max		
Physical Dimensions	**Chassis:** 2U rack height; **Weight:** 39 lbs (17.7 kg); **Height:** 3.45 inches (8.76 cm); **Width:** 17.14 inches (43.54 cm); **Depth:** 20 inches (50.8 cm); Standard 19 inches and 23 inches rack mountable		
Hard Drives	Dual solid state drives running RAID 1		
Network Interfaces	No add-in network interfaces; or 4 x 1 GigE (SFP for copper, GigE SX, or GigE LX); or 8 x 1 GigE (SFP for copper, GigE SX, or GigE LX); or 2 x 10 GigE (SFP+ for SR or LR); or 2 x 10 GigE (SFP+ for SR or LR) and 4 x 1 GigE (SFP for copper, GigE SX, or GigE LX)		
Environmental	**Operating temperature:** 41° to 104°F (5° to 40°C); **Relative humidity (operating):** 5 to 85%, (non-operating) 95% at 73° to 104°F (23° to 40°C)		
Operating System	ArbOS is Arbor's proprietary, embedded operating system, based on Linux.		
Regulatory Compliance	RoHS 2002/95/EC, IEC/EN/UL 60950-1 2nd ed., E2006/95/EC, 2001/95/EC, FCC Part 15 Subpart B Class A, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, IC ICES-003 Class A, ETSI EN 300 386, ETS 300-019-2-1, ETS 300-019-2-2, ETS 300-019-2-3, ETS 753, CISPR 22 Class A, CISPR 24, Gost, BSMI, VCCI Class A, KCC Class A, UL Mark, CE Mark, ETSI, NEBS-3 (DC), NEBS-1 (AC)		
Virtual Machine Requirements	**Hypervisor:** VMware vSphere v5.0, 5.1 and 5.5; **vCPUs:** 4 to 32; **Network interfaces:** 1 to 10; **Memory:** 8 or 16 GB; **Storage:** 100 GB min.	**Hypervisor:** Xen Cloud Platform v1.6.10-61809c; **vCPUs:** 4 to 15; **Network interfaces:** 1 to 10; **Memory:** 8 or 16 GB; **Storage:** 100 GB min.	**Hypervisor:** KVM QEMU v1.4.2; vCPUs: 4 to 32; **Network interfaces:** 1 to 10; **Memory:** 8 or 16 GB; **Storage:** 100 GB min.