DATA SHEET

Arbor Peakflow X

NETWORK AND DATA CENTER VISIBILITY, PROTECTION AND COMPLIANCE

Today's networks and Internet data centers are not just the conduit through which all business flows. They are also the connection to a large and growing array of security threats that originate both outside your environment, and from within.

The Arbor Peakflow® X solution ("Peakflow X") was purpose-built to meet the demands of the largest enterprises and data center operators, addressing a wide range of external and internal security threats while maintaining business continuity. It constructs a system-wide view of the entire network and data center, auto-learning host behaviors to determine who talks to whom, and how.

> **"Peakflow X is a product that allows us to leverage and augment prior investments in network infrastructure equipment, network analysis and network security products."**
>
> David Arbo, Director
> of Network Security,
> American President Lines

Using this data in conjunction with real-time security information provided through Arbor's subscription-based Active Threat Feed (ATF) service, Peakflow X generates actionable insight that lets you:

- **Gain** unmatched cost-effective, enterprise-wide network visibility.
- **Stop** existing and emerging internal network and data center threats, such as distributed denial of service (DDoS) attacks, botnet armies, viruses and phishing solicitations.
- **Determine** if application performance anomalies are causing network performance problems or impacting other applications or services.
- **Control** user access and eliminate insider misuse.
- **Comply** with government and industry regulations (i.e., PCI, HIPAA, etc.)
- **Deliver** virtualized IP VPN and data center managed security services.

Real-Time Network Behavior Analysis

Peakflow X quantifies normal network behavior by analyzing IP flow statistics from network devices (e.g., Cisco Systems' NetFlow, Juniper Networks' cflowd, Extreme Networks' and Foundry Networks' sFlow and industry-standard IPFIX) and raw packet data. It uses this information to create baseline definitions of normal network behavior, and in real-time, compares traffic against these baselines by performing network behavior analysis (NBA). NBA is used to identify virulent zero-day attacks and other developing threats that do not yet have signatures—and therefore, can easily slip by other security appliances, such as intrusion prevention systems and firewalls.

Application Intelligence

The Peakflow X Application Intelligence collector extends the visibility of Peakflow X up to the application layer, providing a single, integrated solution to optimize network and application performance. The collector provides visibility into the performance of critical applications by conducting behavioral analysis on both network and application traffic. This insight enables you to maximize the performance, reliability and security of key business applications by quickly resolving network issues; avoid over-provisioning your network to meet application demands; and expand application usage across geographically dispersed networks without risking bandwidth or security issues.

Key Features and Benefits

Network-Wide Visibility and Application Intelligence
Leverage both IP flow (e.g., NetFlow) and deep packet inspection (DPI) to enable pervasive, cost-effective visibility and performance analysis of your network traffic and data center applications.

Network Behavioral Analysis
Identify the normal behavior of traffic including Voice over Internet Protocol (VoIP) and P2P, and be alerted to abnormalities due to misconfigurations or malicious activity.

Comprehensive Threat Analysis and Zero-Day Protection
Rely on the behavioral analysis capabilities of Peakflow X and the industry leading global threat analysis of Arbor's Security Engineering and Response Team (ASERT) to detect zero-day threats missed by outdated signature-based security tools (e.g., IDS/IPS, antivirus software).

Compliance Assurance
Ease the burden associated with meeting internal use policies or governmental/industry regulations, such as HIPAA, PCI, EU Data Retention Directive, NERC, ITIL and ISO 17799.

Virtual Managed Security Services
Leverage the benefits of cloud computing and virtualization (e.g., VMWare ESX/ESXi) to deliver cost-effective IP VPN or data center managed security services with Peakflow X Virtual.

ARBOR®
NETWORKS

ATLAS Integration

The Active Threat Level Analysis System (ATLAS®) from Arbor Networks is the world's first globally scoped threat analysis network. With ATLAS data integrated into Peakflow X, enterprises can gain contextualized intelligence into threat activity on a global and local perspective.

Comprehensive Threat Intelligence

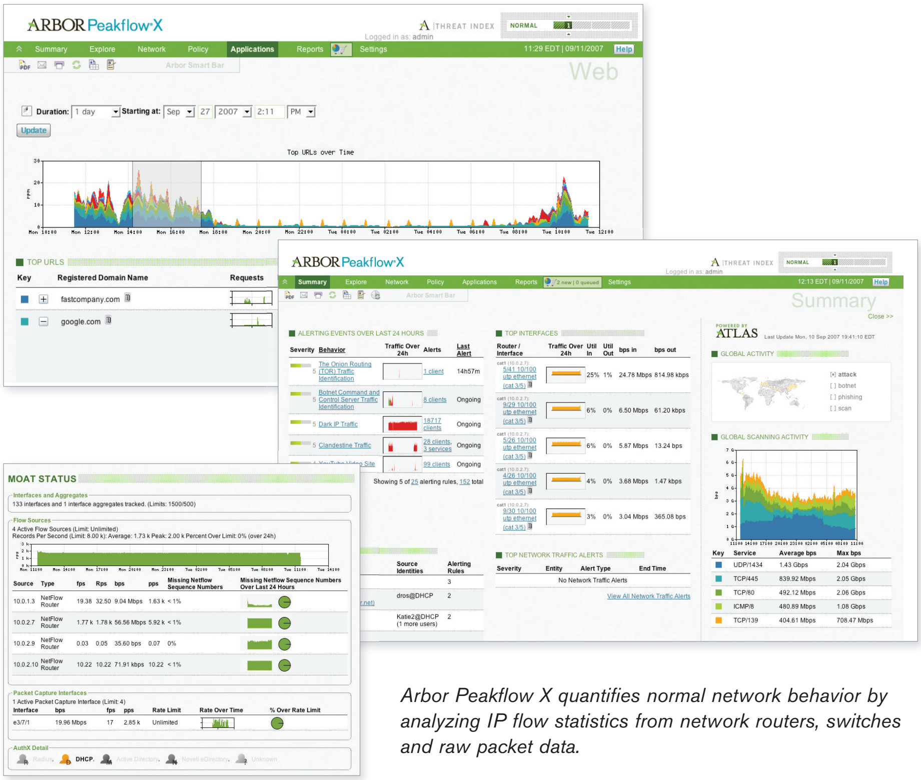
Leverage holistic intelligence to detect, understand and mitigate the pervasiveness of threats that are impacting or may impact a network infrastructure.

Enhanced Resource Allocation

Reduce or eliminate the manual collection and analysis of global security threats, and focus on proactive measures to constantly be one step ahead of the next threat.

Intelligent Threat Mitigation

Rely on ATLAS to analyze threat propagation trends and deliver greater visibility into malware and other Internet threats—enabling you to drive software patching prioritization, AV signature deployment and firewall/IDS tuning.



Key		Registered Domain Name	Requests
🟦	⊞	fastcompany.com	
🟦	⊟	google.com	

Severity	Behavior	Traffic Over 24h	Alerts	Last Alert
5	The Onion Routing (TOR) Traffic Identification		1 client	14h57m
5	Botnet Command and Control Server Traffic Identification		8 clients	Ongoing
5	Dark IP Traffic		18717 clients	Ongoing
5	Clandestine Traffic		28 clients, 3 services	Ongoing
4	YouTube Video Site		99 clients	Ongoing

Showing 5 of 25 alerting rules, 152 total

Router / Interface	Traffic Over 24h	Util In	Util Out	bps in	bps out
cat1 (10.0.2.7): 5/41 10/100 utp ethernet (cat 3/5)		25%	1%	24.78 Mbps	814.98 kbps
cat1 (10.0.2.7): 9/29 10/100 utp ethernet (cat 3/5)		6%	0%	6.50 Mbps	61.20 kbps
cat1 (10.0.2.7): 5/26 10/100 utp ethernet (cat 3/5)		6%	0%	5.87 Mbps	13.24 bps
cat1 (10.0.2.7): 4/26 10/100 utp ethernet (cat 3/5)		4%	0%	3.68 Mbps	1.47 kbps
cat1 (10.0.2.7): 9/30 10/100 utp ethernet (cat 3/5)		3%	0%	3.04 Mbps	365.08 bps

	Source Identities	Alerting Rules
		3
r.net)	dros@DHCP	2
	Katie2@DHCP (1 more users)	2

Severity	Entity	Alert Type	End Time
	No Network Traffic Alerts		

View All Network Traffic Alerts

Key	Service	Average bps	Max bps
🟦	UDP/1434	1.43 Gbps	2.04 Gbps
🟦	TCP/445	839.92 Mbps	2.05 Gbps
🟩	TCP/80	492.12 Mbps	2.06 Gbps
🟩	ICMP/8	480.89 Mbps	1.08 Gbps
🟧	TCP/139	404.61 Mbps	708.47 Mbps

133 interfaces and 1 interface aggregates tracked. (Limits: 1500/500)

4 Active Flow Sources (Limit: Unlimited)
Records Per Second (Limit: 8.00 k): Average: 1.73 k Peak: 2.00 k Percent Over Limit: 0% (over 24h)

Source	Type	fps	Rps	bps	pps	Missing Netflow Sequence Numbers	Missing Netflow Sequence Numbers Over Last 24 Hours
10.0.1.3	NetFlow Router	19.38	32.50	9.04 Mbps	1.63 k	< 1%	
10.0.2.7	NetFlow Router	1.77 k	1.78 k	56.56 Mbps	5.92 k	< 1%	
10.0.2.9	NetFlow Router	0.03	0.05	35.60 bps	0.07	0%	
10.0.2.10	NetFlow Router	10.22	10.22	71.91 kbps	10.22	< 1%	

1 Active Packet Capture Interface (Limit: 4)

Interface	bps	fps	pps	Rate Limit	Rate Over Time	% Over Rate Limit
e3/7/1	19.96 Mbps	17	2.85 k	Unlimited		

Arbor Peakflow X quantifies normal network behavior by analyzing IP flow statistics from network routers, switches and raw packet data.

Attack Detection and Mitigation Using Advanced IP Flow Analysis

Arbor's NBA capabilities for real-time threat detection are complemented by ATF. ATF augments layered defense strategies by validating IDS/IPS rules and detecting zero-day threats before signatures are created. Fingerprints speed the identification and resolution of a wide range of attacks, particularly multi-faceted blended threats.

Using IP flow information, the Peakflow X solution delivers:

- **Stateful Flow Reassembly:** Account and correct for multiple traffic flows generated by multiple appliances on a network, stateful flow reassembly (SFR) addresses real-world challenges that make raw IP flow monitors unreliable, including:
  - De-duplication of redundant flows.
  - Proper handling of data-channel connections from multiple protocols such as VoIP, FTP and RPC.
- **Compensation for Asymmetric Routing and Route Updates:** Gain an accurate view of the traffic at a high or granular level through a specific router.
- **Anomaly Detection Incorporating NBA:** Protect internal networks from employee misuse or worms, track the behavior of individual hosts or users, and identify anomalies.
- **Layer 2 Mitigation and Visibility:** Quickly view where a host is connected to the network and stop threats at the source. Peakflow X also enables the auto-discovery of enterprise switches and elimination of troubled hosts from the network without affecting other hosts.
- **Real-Time Risk Assessment:** Quickly pinpoint the biggest threats on your network by calculating a risk index that identifies which hosts or users are involved in multiple activities.
- **Flexible Identity Tracking:** In real-time, view the actual user name of the IP address accessing your servers at that moment, along with a history of identity login/logoff times.

Comprehensive Reporting

The Peakflow X solution features a wide range of standard and customizable graphical reports containing the actionable information you need to improve network operations and capacity planning. These reports provide insight into key metrics, such as top talkers, traffic statistics and a correlation of users, network hosts and services. IP quality of service (QoS) reports enable you to search and report traffic that is running at different QoS levels on the network and identify possible misconfigurations or traffic-level issues. Additionally, the comprehensive reports generated by Peakflow X help simplify auditing requirements for regulatory compliance.

Leverage the Benefits of Virtualization

"Cloud computing," "virtualization" and "software-as-a-service," these are all the latest industry buzz words that promise enterprises and service providers reduced capital and operating expenses, improved efficiency, service agility and business continuity. Peakflow X Virtual is a version of the Peakflow X software that runs on VMware's ESX and ESXi hypervisors. Peakflow X Virtual offers many of the same set of network visibility and security features as the appliance-based solution, but in a more cost-efficient manner by leveraging the benefits of a virtualized environment.

Ease the Burden of Meeting Industry Compliance

Many enterprises and data center operators struggle with meeting the internal use policies or industry and government regulations that are being imposed on them (e.g., PCI DSS, HIPAA, NERC CIP, EU Data Retention Directive, ITIL and ISO 17799, etc.). The robust real-time and historical reporting capabilities of Peakflow X track all network conversations, thereby easing the burden associated with gaining compliance. In addition, Peakflow X's extensible flow storage capabilities allow you to leverage the storage area networks (SANs) that exist in many of today's enterprises and data centers to archive virtually limitless amounts of raw IP flow-based data for forensic analysis and compliance monitoring.

A Platform for Managed Security Services

If you are a network or hosting service provider, you are undoubtedly facing increased competition and diminishing revenue due to the commoditization of network and hosting services. Therefore, it is imperative that you offer more IP-based services that can create new revenue opportunities for your company. Via IP flow analysis of PE or CPE edge routers, Peakflow X complements existing IP VPN- and CPE-based managed security solutions. With Peakflow X, you can:

- Provide your IP VPN customers visibility and security services with customized portals.
- Complement your existing CPE-based security services by utilizing the NBA capabilities in Peakflow X to ensure that customer internal use policies are met and detect threats that are unknown to your signature-based security solutions such as IDS/IPS or anti-virus.
- Leverage the historical reporting and offloading of raw IP flow data for post-event forensics services.
- Deliver anti-botnet or data loss prevention services.
- Offer a full suite of regulatory compliance services by utilizing the pervasive visibility and reporting features that provide the ability to audit all network and data center communications and security violations.

To make your Peakflow X-based managed security service even more profitable, you can deploy Peakflow X Virtual—a version of the product that runs on VMWare ESX and ESXi hypervisors. Peakflow X Virtual offers essentially the same features as the appliance-based product, but with the added benefits of virtualization and cloud computing that enable you to easily add new customers and reduce the operational expenses associated with your Peakflow X-based managed security service.

Arbor Networks Uniquely Leverages NetFlow

NetFlow is built into routers and switches from Cisco and other vendors, allowing these components to capture information about network traffic flows—streams of data that share a common source and destination and a common protocol.

NetFlow captures the source and destination IP address and port, the type of protocol the traffic uses, the type of service being provided and the logical interfaces for the flow. Peakflow X does not require the installation of hardware-based probes that can be expensive to purchase and maintain, cause network failures and slow network traffic if installed in-line with the flow of data.

An Enterprise-Class Solution

Peakflow X is the first and only product to deliver NetFlow data in an understandable and invaluable format for improving network visibility and security. In addition, by capturing Layer 2, Layer 3 and Layer 4 information, Peakflow X leverages this NetFlow data to provide deeper visibility into these critical network areas. As the size, speed and complexity of your network grows, so too must the capabilities of the Peakflow X solution. The Peakflow X controller platforms, including the Peakflow X Enterprise-Wide Controller, offer the performance needed to address your expanding network.

Customize and Integrate with Existing Tools

The valuable data gathered by the Peakflow X collectors and controllers can be integrated into existing network management and security portals via Web service APIs such as SOAP, XML and JSON.

Peakflow X Modes of Deployment

Arbor Peakflow X Enterprise-Wide Controller

2U rack mountable server manages up to 50 Peakflow X Collectors; aggregates and archives statistics; and creates a network-wide view.

Arbor Peakflow X Standard Controller

1U rack mountable server manages up to 25 Peakflow X Collectors; aggregates and archives statistics; and creates a network-wide view.

Arbor Peakflow X Standard Collector and Application Intelligence Collector

1U rack mountable server tracks GigE links; gathers IP flow data either directly from the router or by packet capture; identifies the anomalous traffic (including application traffic); and transfers data to the Peakflow X Controller.

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

Arbor Peakflow X Controller and Collector Specifications

Peakflow X Enterprise-Wide Controller

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
Standard 19 in and 23 in rack mountable

Hard Drives

Dual hard drives running RAID 1

Peakflow X Standard Controller and Collector

Power Requirements

Redundant dual power sources
AC: 100/127V, 6.3A, 200/240V, 3.2A (50-60 Hz)
DC: -48 to -60V, 12A max

Physical Dimensions

Controller and Collector:
Chassis: 1U rack height
Standard 19 in and 23 in rack mountable

Ports

Controller:
2 Copper Gigabit Ethernet Monitoring Ports
1 Copper Gigabit Ethernet NetFlow Port
1 Copper Gigabit Ethernet Management Port
Serial Console Port

Collector:
4 Copper Gigabit Ethernet Monitoring Ports
1 Copper Gigabit Ethernet NetFlow Port
1 Copper Gigabit Ethernet Management Port
Serial Console Port

Hard Drives

Dual hard drives running RAID 1

NICs

4 x 10/100/1000BaseT
Fiber option available

Insider Threat Detection

Learning Duration: Immediate to one week
Network Malware Detection: YES
Botnet Detection: YES
Phishing Detection: YES
Dark IP Detection: YES
Worm Detection: YES
Instant Messaging Detection: YES
Peer-to-Peer Detection: YES
DDoS/DoS Detection: YES
Relational Detection: YES
Statistical Anomaly Detection: YES
Automatically Updated Service: YES
Identify and Track by User Name: YES
Identify Hostname Using DHCP: YES

Active Threat Feed

Hourly Updates: YES
Detailed Threat Analysis: YES
Delivery Method: RSS Feed

ATLAS Integration

In-depth intelligence of threat activity on a global and local perspective: YES

Identity Tracking

Active Directory Support: YES
Novell eDirectory Support: YES
Identities Tracked: Over 100,000

Network Visibility

Devices Tracked: Hundreds of Thousands
Monitor & Record All Services: YES
Real-Time Traffic Visibility: YES
Custom & Standard Report Creation: YES
Scheduled Report Creation: YES

Network Worm Defense

Pre- and Post-Outbreak Quarantine: On Demand
Zero-Day Worm Detection: YES
Infected Host Discovery: YES

Stateful Flow Reassembly

Handles Asymmetric Routing: YES
Handles De-Duplication of Data: YES
Ephemeral Port Mapping: YES
Probe Detection: YES

Deployability

Cisco NetFlow (v5,7,9)
Juniper Networks cflowd
Extreme and Foundry Networks sFlow (v2,4,5)
Industry-Standard IPFIX
Flow Redirection Support: YES
Gigabit Packet Capture: YES
NTP Support: YES

Alert Management

SEM Support: YES
SNMP Support: YES (Custom MIB)
SNMP v2c: YES
SNMP v3: YES
SMTP: YES
Syslog: YES

Device Management

Multiple Users: YES
Web UI: HTTPS
CLI: SSHv1, SSHv2, Telnet & Serial Console
Communications Channels: 2048bit RSA Encrypted SSL
Radius Support: YES
TACACS+ Support: YES
SNMP Poll System & Alert Status: YES

Operating System

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

Device Security

- Hardened OS and network stack
- Fully encrypted communications channels
- Software packages are cryptographically signed, preventing Trojan code
- Built-in firewalling support, rejecting all packets by default (transparent to pings and port scans)