

MEASURE VISUALIZE PROTECT



OSSIR

8 Novembre 2005



Arbor Networks: Security Industry Leader

Arbor's Peakflow products ensure the security and operational integrity of the world's most critical networks

Solid Financial Base

- Sales have more than doubled each year; 130% in '04

Solid Market Base

- Worldwide over 100 customers including tier 1 service providers, MSOs, enterprises and mid-tier enterprise

Solid Technology Base

- Solutions based on 5 years of academic research at the Univ. of Michigan; 16 patents (pending)

Strategic Partnerships include:



Technology
Developer
Partner



MEASURE VISUALIZE PROTECT



Arbor Solutions

peakflow® | SP *for service providers*

Infrastructure security, intelligent traffic analysis,
managed DoS protection

peakflow™ | X *for large enterprises*

Internal Network Security: Actively defend against
worms, segment and harden networks, eliminate
insider misuse, simplify compliance

Peakflow|SP: Innovative Technologies

Relational Network Modeling

Peakflow|SP measures normal network traffic, correlates it with topology information to build intelligent data-models, and presents the data in flexible, real-time, business-centric reports

Network Anomaly Detection


Peakflow|SP detects both known and zero-day network anomalies without requiring signature updates and with minimal network configuration

Intelligent Mitigation Management

Peakflow|SP provides the ability to react quickly in the face of emerging threats via access rule generation, blackhole integration, sinkholing, and mitigation devices, all in a single, integrated management console

Peakflow|SP: Innovative Products

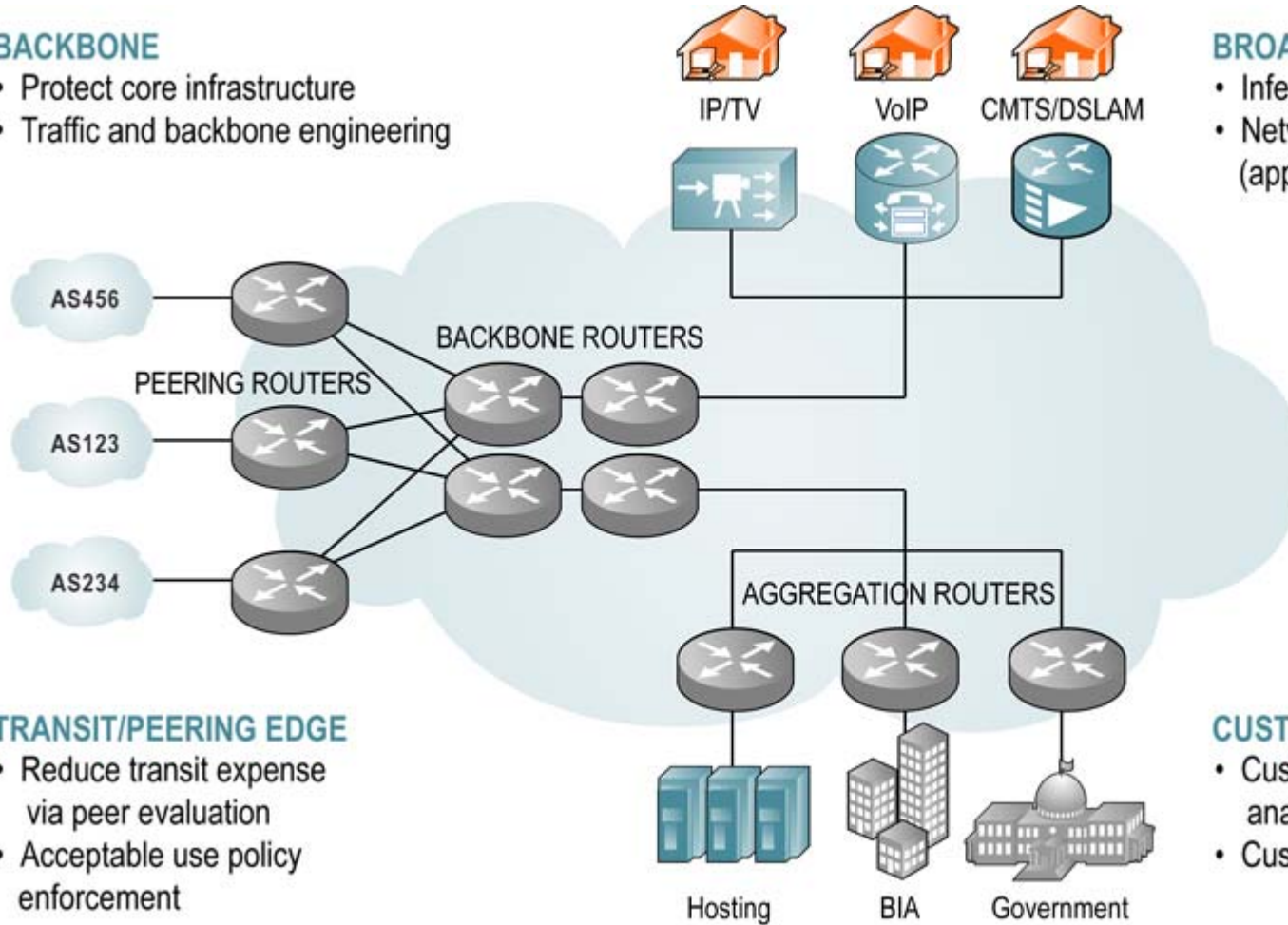
Device	Features	Licensing
MS Managed Services	ALL Traffic & Routing (TR) Features ALL Infrastructure Security (IS) Features Customer Facing Portal	“Right-to-Resell” MS Services & Customer-based Licensing
CP Converged Platform	ALL Traffic & Routing (TR) Features ALL Infrastructure Security (IS) Features	Router-based Licensing
TR Traffic & Routing	Network-wide Traffic Reporting Routing, Peering, Transit Management Route Analytics	Router-based Licensing
IS Infrastructure Security	Network-wide Anomaly Detection Classification, Notification, Traceback, Reaction Post-mortem via Flexible Anomaly Reporting	Router-based Licensing

Device Specifications	
	Chassis: 2RU rack height (3.35”/8.9 cm), 36 lbs/16.3 kg
	Power: -38 to -75 VDC, Redundant AC/DC power
	Ports: 2 GigE, 1 Serial Console, 6 Optional PCI slots (Copper or Fiber)
	Performance: Configured for NetFlow (OC-48) and packets (GigE)
	Compliance: NEBS Level 3 certified (AC or DC), ETSI

Peakflow|SP Use Cases: Value Throughout the Network

BACKBONE

- Protect core infrastructure
- Traffic and backbone engineering



BROADBAND EDGE

- Infected host cleanup
- Network abuse (applications, top talkers)

TRANSIT/PEERING EDGE

- Reduce transit expense via peer evaluation
- Acceptable use policy enforcement

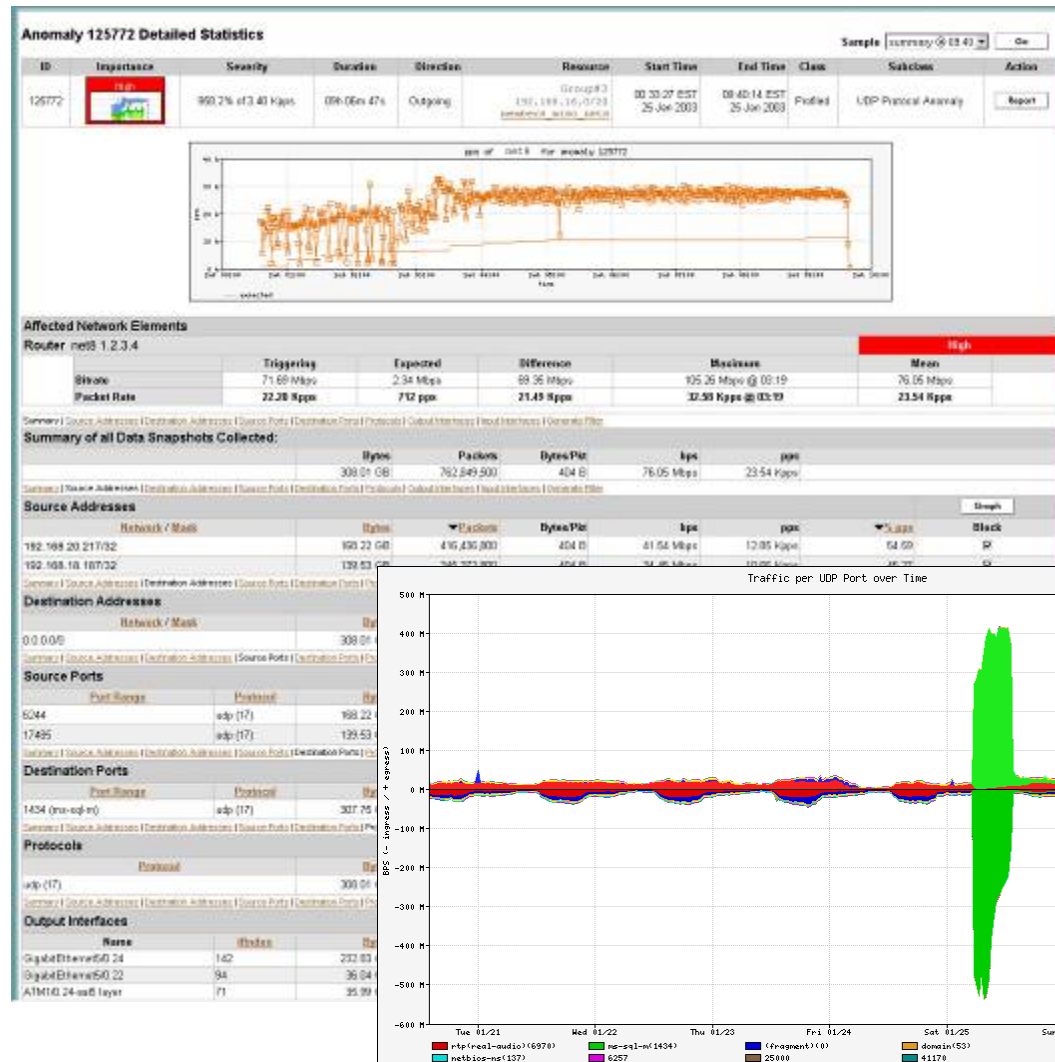
CUSTOMER EDGE

- Customer & marketing analysis
- Customer portal

Protect Core Network Infrastructure

Ensures operational integrity for the world's largest service providers.

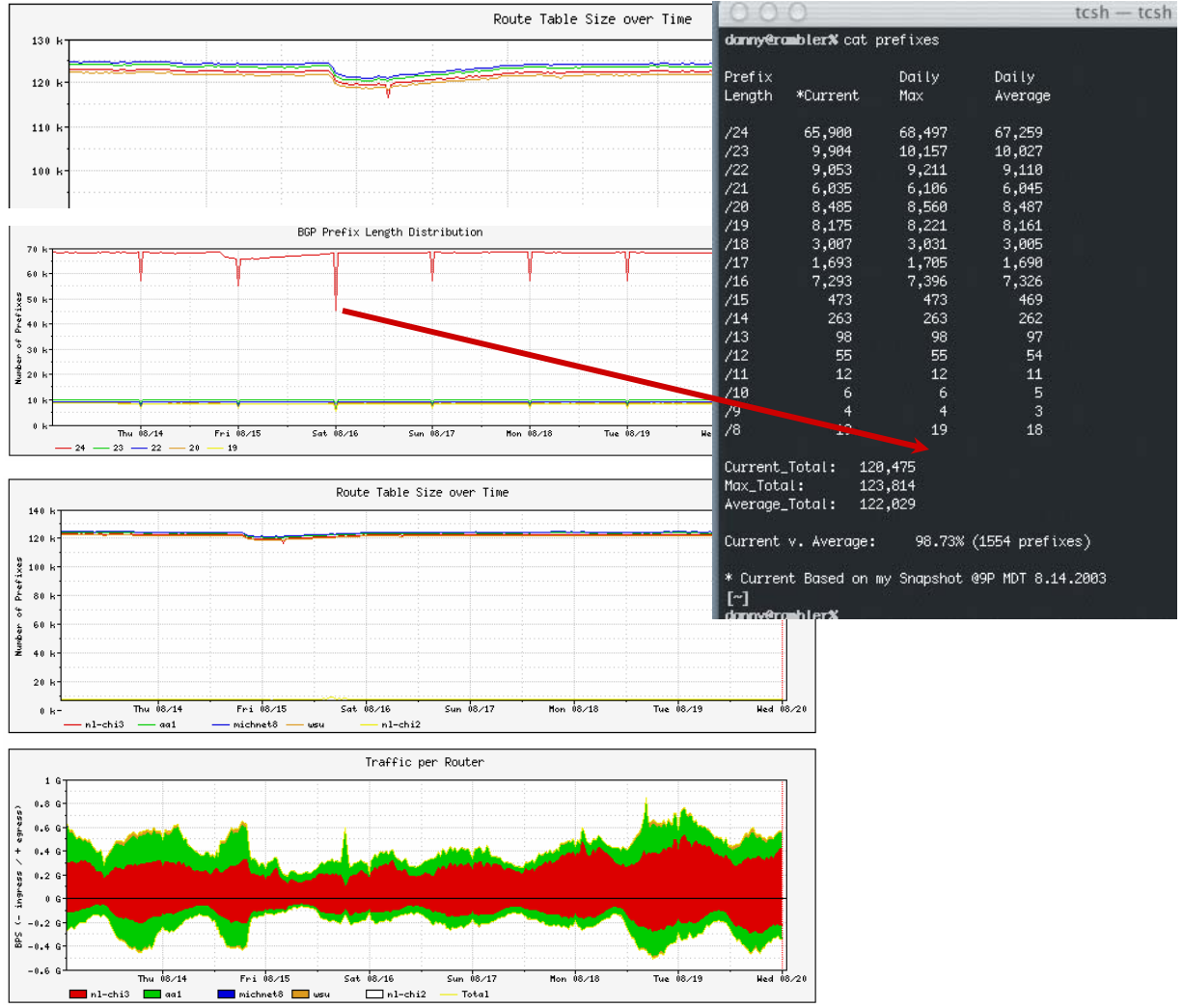
"Peakflow SP alerted us to the SQL worm well before we received the first customer-call, allowing us to focus on remediating the affected servers."



Real-Time, Network-Wide Engineering

Empowers operators by providing real-time, network-wide traffic reports for significant events.

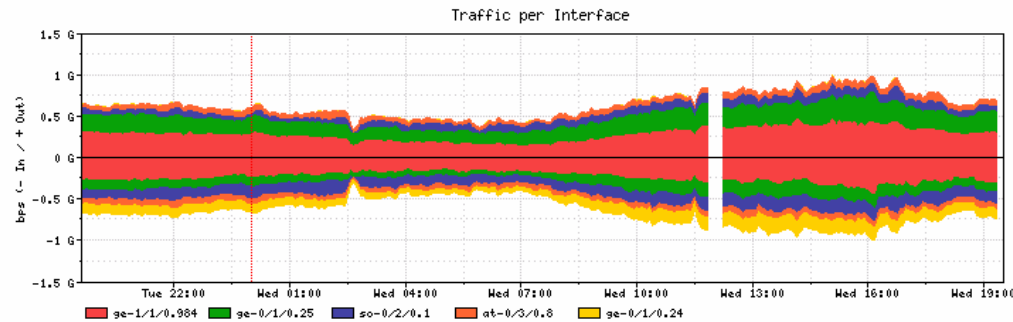
“Peakflow’s real-time awareness of behavior across our entire network equips us to close the expensive gap between the onset of an attack and its resolution”



Intelligent Capacity Planning

Perform intelligent capacity and “hot-spot” planning based on business realities.

“By using Peakflow SP, we are able to expand our traffic monitoring and planning analysis, which will ultimately mean better service for our customers.”



[Download](#) | [Email](#)

Showing 46 of 85 Items (39 have no data)

Interface Usage Alerts							
Clear All	ID	Start Time	Stop Time	Reported By	Alert Type	Information	
<input type="checkbox"/>	60655	Wed Dec 15 16:55:01	Wed Dec 15 16:55:01	hete	Iface Usage	High usage for Interface Serial2/0 on Router calvin3: 60.66 Mbps (134.66% of 45.05 Mbps)	
<input checked="" type="checkbox"/>	ge-1/1/0.984 vlan UM c	60638	Wed Dec 15 16:15:01	Wed Dec 15 16:15:01	shete	Iface Usage	High usage for Interface Serial1/0.3 on Router Issu: 79.36 Mbps (176.36% of 45.00 Mbps)
<input checked="" type="checkbox"/>	ge-0/1/0.25 vlan CHI-	60034	Mon Dec 13 1:15:00	Mon Dec 13 1:15:00	shete	Iface Usage	High usage for Interface FastEthernet0/0 on Router umd2: 98.92 Mbps (98.92% of 100.00 Mbps)
<input checked="" type="checkbox"/>	so-0/2/0.1 pvc to Ak	59692	Sun Dec 12 1:15:00	Sun Dec 12 1:15:00	shete	Iface Usage	High usage for Interface FastEthernet0/0 on Router umd2: 101.09 Mbps (101.09% of 100.00 Mbps)
<input checked="" type="checkbox"/>	at-0/3/0.8 pvc to MS	59663	Sat Dec 11 19:30:00	Sat Dec 11 19:30:00	shete	Iface Usage	High usage for Interface Serial1/0.3 on Router Issu: 64.64 Mbps (143.65% of 45.00 Mbps)
	59489	Sat Dec 11 1:15:01	Sat Dec 11 1:15:01	shete	Iface Usage	High usage for Interface FastEthernet0/0 on Router umd2: 105.42 Mbps (105.42% of 100.00 Mbps)	
	59488	Sat Dec 11 0:45:00	Sat Dec 11 0:45:00	shete	Iface Usage	High usage for Interface FastEthernet0/0 on Router mtu2: 116.83 Mbps (116.83% of 100.00 Mbps)	
	59262	Fri Dec 10 1:15:00	Fri Dec 10 1:15:00	shete	Iface Usage	High usage for Interface FastEthernet0/0 on Router mtu2: 96.98 Mbps (96.98% of 100.00 Mbps)	
	59256	Fri Dec 10 0:45:00	Fri Dec 10 0:45:00	shete	Iface Usage	High usage for Interface FastEthernet0/0 on Router mtu2: 105.10 Mbps (105.1% of 100.00 Mbps)	
	59063	Wed Dec 8 18:00:00	Wed Dec 8 18:00:00	itte	Iface Usage	High usage for Interface Hssi4/0 on Router fsu2: 52.07 Mbps (115.6% of 45.05 Mbps)	
	58875	Tue Dec 7 10:15:01	Tue Dec 7 10:15:01	itte	Iface Usage	High usage for Interface Hssi4/0 on Router fsu2: 43.81 Mbps (97.27% of 45.05 Mbps)	
	58834	Mon Dec 6 19:15:00	Mon Dec 6 19:15:00	itte	Iface Usage	High usage for Interface Hssi4/0 on Router fsu2: 45.01 Mbps (99.92% of 45.05 Mbps)	
	58832	Mon Dec 6 18:50:00	Mon Dec 6 18:50:00	itte	Iface Usage	High usage for Interface Hssi4/0 on Router fsu2: 43.02 Mbps (95.51% of 45.05 Mbps)	
	58799	Mon Dec 6 10:45:00	Mon Dec 6 10:45:00	itte	Iface Usage	High usage for Interface Hssi4/0 on Router fsu2: 45.22 Mbps (100.4% of 45.05 Mbps)	
	58770	Mon Dec 6 5:15:00	Mon Dec 6 5:15:00	shete	Iface Usage	High usage for Interface FastEthernet0/0 on Router oakland4: 99.15 Mbps (99.15% of 100.00 Mbps)	
	58612	Sun Dec 5 1:10:00	Sun Dec 5 1:10:00	itte	Iface Usage	High usage for Interface Hssi4/0 on Router fsu2: 48.20 Mbps (107.0% of 45.05 Mbps)	

MEASURE VISUALIZE PROTECT

Peering Evaluation and Visualization

Reduce transit expense by monitoring peers and potential peers.

“With Peakflow SP, we have an accurate, network-wide perspective of all transit and peer traffic, providing us more insight and control over our business.”



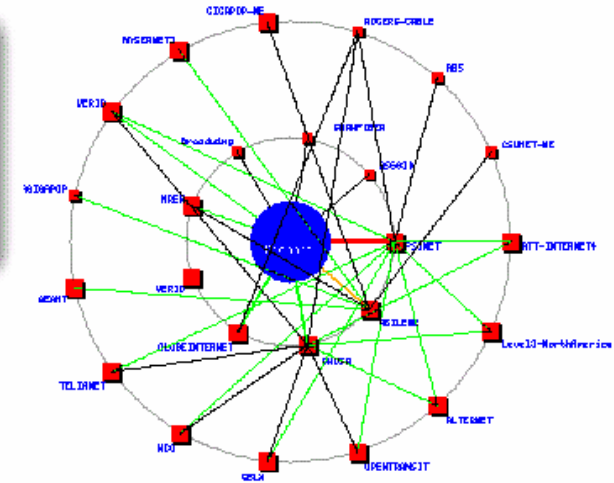
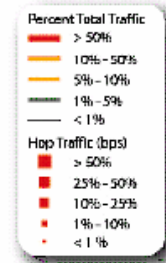
merit
System > Alerts > Network > Router > Peer > Customer > Profile >

Peering Evaluation

Click on ASN to view breakdown by Peer.

Period: Today

Rank	ASN	Name
1	174	PSINET
2	11537	ABILENE
3	3561	CWUSA
4	7018	ATT-INTERNET4
5	3355	Level3-NorthAmerica
6	701	ALTERNET
7	2914	VERIO
8	6453	GLOBEINTERNET
9	3549	GBLX
10	22335	MREN
11	1668	ATDN
12	7132	SBIS
13	22909	CIPS-OSP1
14	5511	OPENTRANSIT
15	7911	WCG
16	3754	NYSENET3
17	5779	Y-BR-SERV
18	6478	ATT-INTERNET3
19	8075	MICROSOFT
20	21844	THEPLANET
21	577	BELL
22	20965	GEANT
23	1239	SPRINT
24	4134	CHINANET
25	1299	TELIANET



merit
System > Alerts > Network > Router > Peer > Customer > Profile > Interface > Mitigation > Query > Administration >

Peering Evaluation AS7018

[Summary | Breakdown by Peer]

Period: Today

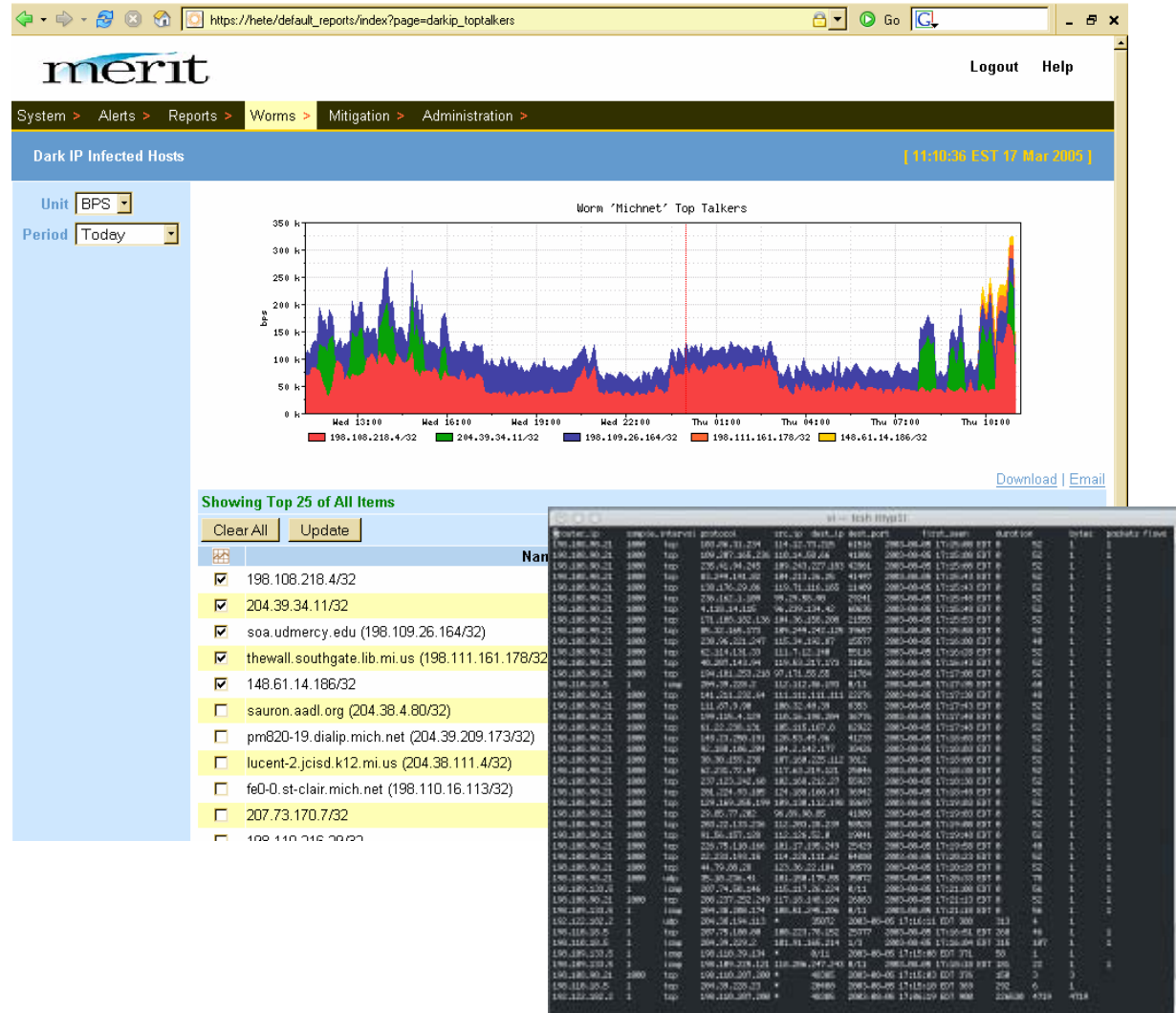
Showing 6 Items

AS	Peers Carrying Traffic from/to AS7018	Into Network	Out of Network	Sum
Concast (AS174)		63.00 Mbps	110.00 Mbps	173.00 Mbps
Comcast (AS3561)		15.31 Mbps	9.51 Mbps	24.82 Mbps
Concast (AS22909)		947.00 Kbps	0.00 bps	947.00 Kbps
Internet2 (AS11537)		54.00 Kbps	0.00 bps	54.00 Kbps
Global NAP's (AS1784)		44.00 Kbps	0.00 bps	44.00 Kbps
MREN (AS22335)		1.54 Kbps	0.00 bps	1.54 Kbps

Infected Host Cleanup

Analyze Dark IP Space to identify and remove infected hosts

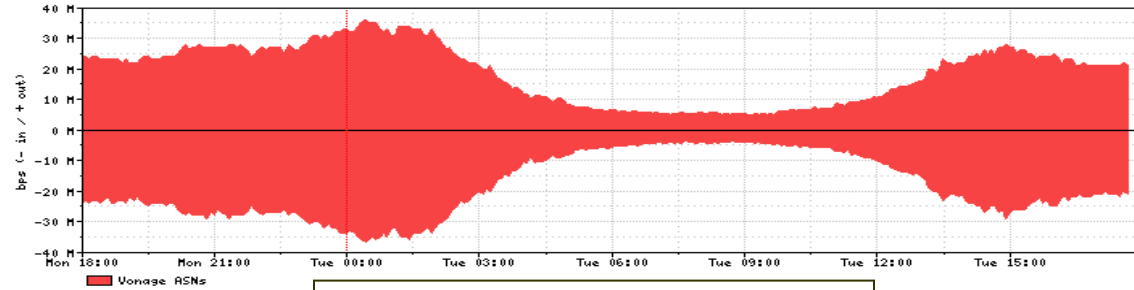
"Given the help desk expense we would have otherwise incurred [with worm clean-up], Peakflow has already paid for itself."



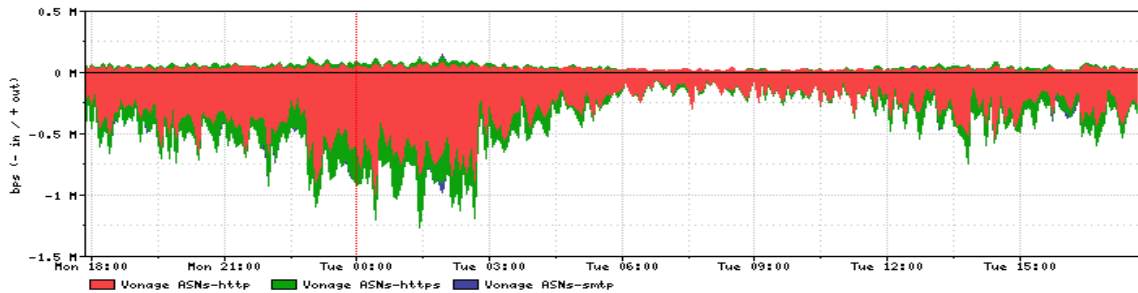
Converged Applications Analysis

Monitor traffic utilization of critical services including voice, video, and data.

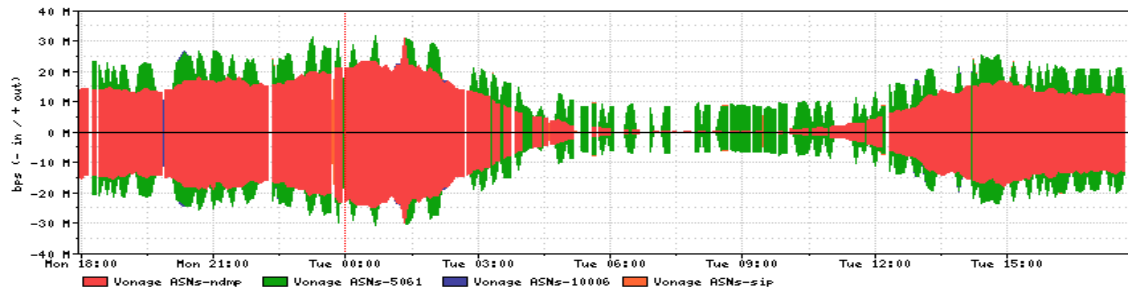
“We now have ability to monitor network and service utilization in real-time and with a high degree of granularity.”



Total Vonage Traffic on Network



Amount of Control Traffic

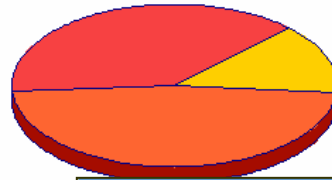


Amount of Data Traffic

Network and Bandwidth Abuse

Detect and track subscribers violating acceptable use policies.

Profile 'abovenet' Top Talkers



- 141.217.220.154/32
- 146.9.3.79/32
- 141.217.220.216/32
- 155.139.50.90/32
- 155.139.67.35/32

Top Talkers Reports

Top Talker Flows						
Router	Protocol	Src IP	Src Port	Dst IP	Dst Port	Bytes
nl-chi3	tcp	206.16.1.243	80	161.57.214.84	1996	1500
nl-chi3	tcp	206.16.1.243	80	161.57.214.84	1996	1500

Showing Top 200 of All Items

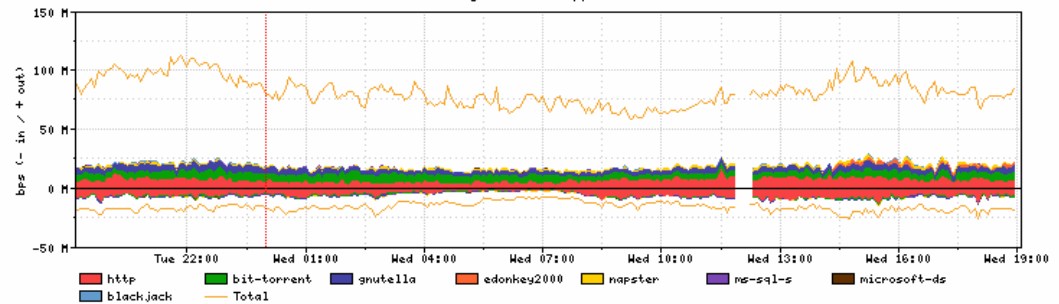
Clear All Update

Current / Average / Max / PC35

Name	In	Out	Sum	Details
<input checked="" type="checkbox"/> 141.217.220.154/32	0.00 bps	62.00 Kbps	62.00 Kbps	Details
<input checked="" type="checkbox"/> 146.9.3.79/32	0.00 bps	45.00 Kbps	45.00 Kbps	Details
<input checked="" type="checkbox"/> 141.217.220.216/32	0.00 bps	12.97 Kbps	12.97 Kbps	Details
<input checked="" type="checkbox"/> 155.139.50.90/32	555.00 bps	0.00 bps	555.00 bps	Details
<input checked="" type="checkbox"/> 155.139.67.35/32	411.00 bps	0.00 bps	411.00 bps	Details

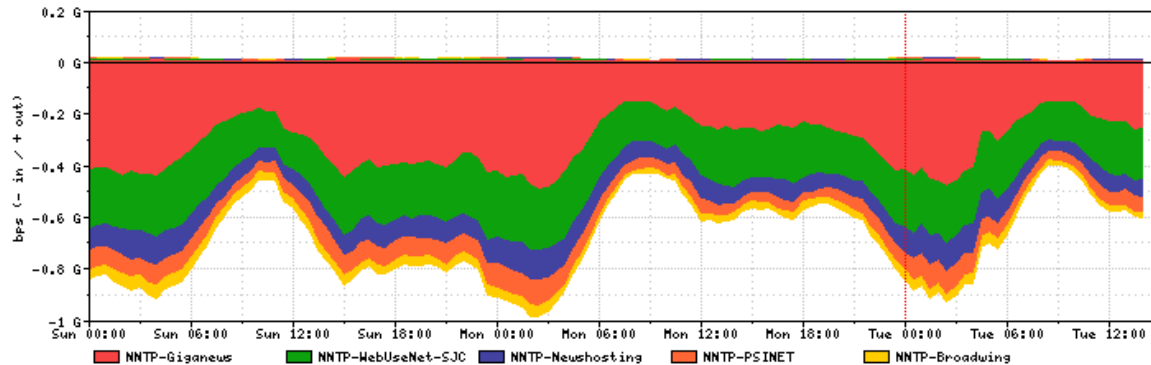
Application Breakdown Reports

'Teleglobe' TCP Applications



Evaluate Potential Market Offerings

Evaluate new service offering for customers in order to recognize cost savings and generate new revenue streams.



Showing Top 200 of All Items

IP	Name	ASN	In	Out	Sum
<input checked="" type="checkbox"/>	NNTP-Giganeus	30094	510.00 Mbps	9.77 Mbps	519.76 Mbps
<input checked="" type="checkbox"/>	NNTP-WebUseNet-SJC	18607	266.00 Mbps	5.39 Mbps	271.39 Mbps
<input checked="" type="checkbox"/>	NNTP-NewsHosting	20798	136.00 Mbps	2.25 Mbps	138.25 Mbps
<input checked="" type="checkbox"/>	NNTP-PSINET	174	107.00 Mbps	1.99 Mbps	108.99 Mbps
<input checked="" type="checkbox"/>	NNTP-Broadwing	6395	57.00 Mbps	1.06 Mbps	58.06 Mbps
<input type="checkbox"/>	NNTP-AS-ELDOSALES	11588	62.00 Mbps	989.00 Kbps	62.99 Mbps
<input type="checkbox"/>	NNTP-HIBBLE	26234	42.00 Mbps	712.00 Kbps	42.71 Mbps
<input type="checkbox"/>	NNTP-NOVIA	4306	35.00 Mbps	561.00 Kbps	35.56 Mbps
<input type="checkbox"/>	NNTP-NET-SUPERNEWS	11697	15.67 Mbps	301.00 Kbps	15.97 Mbps
<input type="checkbox"/>	NNTP-VERIO	2914	11.63 Mbps	551.00 Kbps	12.19 Mbps
<input type="checkbox"/>	NNTP-BAND-X-US-1	18695	12.05 Mbps	455.00 Kbps	12.51 Mbps
<input type="checkbox"/>	NNTP-IADFW	4278	8.33 Mbps	160.00 Kbps	8.49 Mbps
<input type="checkbox"/>	NNTP-Hostcentric	11388	11.68 Mbps	222.00 Kbps	11.90 Mbps
<input type="checkbox"/>	NNTP-VOICENET	3932	9.29 Mbps	153.00 Kbps	9.44 Mbps
<input type="checkbox"/>	NNTP-LLHW	22622	9.81 Mbps	311.00 Kbps	10.13 Mbps
<input type="checkbox"/>	NNTP-5731	5731	7.76 Mbps	311.00 Kbps	8.07 Mbps
<input type="checkbox"/>	NNTP-ALTOPIA	6456	5.09 Mbps	285.00 Kbps	5.37 Mbps
<input type="checkbox"/>	NNTP-PRODIGY	1698	4.55 Mbps	95.00 Kbps	4.65 Mbps
<input type="checkbox"/>	NNTP-GOLDENGATE	7753	5.50 Mbps	96.00 Kbps	5.60 Mbps
<input type="checkbox"/>	NNTP-INFB	14116	2.71 Mbps	45.00 Kbps	2.75 Mbps
<input type="checkbox"/>	NNTP-BAIS-RSTN	6350	3.14 Mbps	70.00 Kbps	3.21 Mbps

News Services

Network-based Security Offerings

Create on-net security offerings via a customizable portal

“Rapid growth in the managed security services (MSS) market is forcing vendors to offer increasingly comprehensive bundles to keep pace while customer premises-based equipment (CPE) moves to in-the-cloud network-based security”



merit Logout Help

Status Alerts > Traffic > Administration >

UM Network Status [19:49:16 EST 15 Dec 2004]

Alert Snapshot

Alert Totals	High	Medium	Low
Ongoing [0]:	0	0	0
Recent [128]:	16	1	111
Last 24 Hours [27]:	5	1	21

Customer Traffic Summary

Top Ongoing Alerts

No alerts found

For technical assistance: [Search](#) [Quick Links...](#)

merit NETWORK INC.

Home MichNet Networking R&D Learning Systems

About Us Services Resources News Events

Overview Board of Directors Bylaws Staff History Directions

Welcome to the MichNet Customer Portal!

Please authenticate

Username:

Password:

POWERED BY **ARBOR NETWORKS**

News: [Merit to Support ProQuest Research via Internet2](#), [Merit to Provide Internet Service to State of Michigan](#)

Events: [NANOG49IN, Jan. 30-31](#), [Merit Calendar of Events](#)

Merit Networks, Inc. 4051 Plymouth Road 734.764.0430
 5200 Lakeside, Skokie, IL 60077
 State 2000
 Fax: 708.461.0027

Practical Route Analytics

Leverage BGP route analytics to troubleshoot network problems, validate policy changes, improve application performance, etc.

“Route analytics technologies will become an integral part of any network management system deployed at companies and service providers alike by 2008.”



Diff Routing Table

Report
Start 08:42:55 PM EST 03/20/05
End 07:42:55 AM EST 03/21/05

Summary

Unchanged	154516
New	311
Changed	1797
Deaggregated	3
Deleted	219

Origin ASN Start=154703, End=154798 (Net=95)

BGP Instability Analysis

Report
Start 08:44:48 PM EST 03/20/05
End 07:44:48 AM EST 03/21/05

Summary

Withdraw	5115
Announce	56148
Number Unique Prefixes	20

Top Origin ASNs			Top BGP Prefixes		
ASN	Number of Updates	Percentage	Prefix	Number of Updates	Percentage
AS22488	2544	4.53	193.255.236.0/23	16	0.03
AS12455	1682	3.00	61.94.176.0/24	9	0.02
AS7018	1264	2.25	194.116.232.0/23	8	0.01
AS17557	1090	1.94	220.67.244.0/22	5	0.01
AS7843	1014	1.81	207.193.32.0/23	5	0.01
AS14654	702	1.25	202.63.219.0/24	4	0.01
AS8795	606	1.08	195.251.118.0/24	3	0.01
AS4795	597	1.06	68.208.214.0/23	3	0.01
AS24219	568	1.01	67.33.7.0/24	3	0.01
AS21351	565	1.01	61.11.4.0/24	3	0.01
AS20096	507	0.90	68.208.56.0/22	3	0.01
AS705	476	0.85	62.3.64.0/18	3	0.01
AS7893	443	0.79	66.18.0.0/20	3	0.01
AS3464	403	0.72	80.69.96.0/20	3	0.01
AS5668	391	0.70	80.67.128.0/20	2	0.00
AS6386	369	0.66	13.12.0.0/16	2	0.00
AS19773	366	0.65	213.152.69.0/24	2	0.00
AS724	349	0.62	202.88.36.0/24	2	0.00
AS6746	343	0.61	208.219.171.0/24	2	0.00
AS22024	340	0.61	157.253.0.0/16	1	0.00

BGP Route Analytics from *Inside* the Network and from *Outside* the Network (External RouteViews)

Worm Detection, Tracking & Cleanup

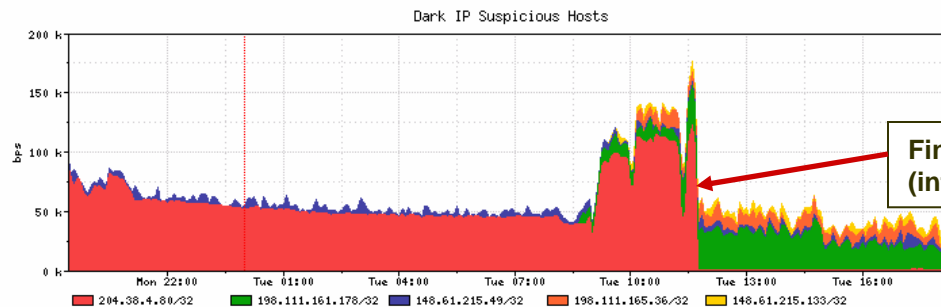
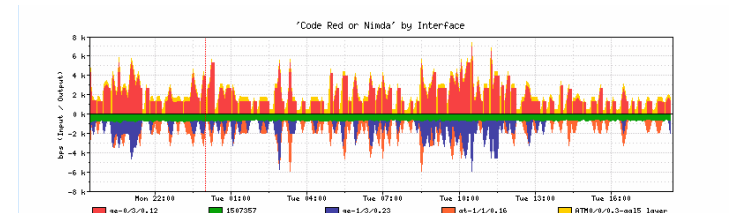
Instantly detect, track, contain, and cleanup worms

"Within minutes, Peakflow detected the anomalous traffic created by the worm, provided filters to mitigate the effects and pinpointed the affected servers. Thanks to Peakflow, Rackspace was able to maintain its record of 24 months of 100 percent network uptime."



Detect Worm Activity (W32/Sasser alert)

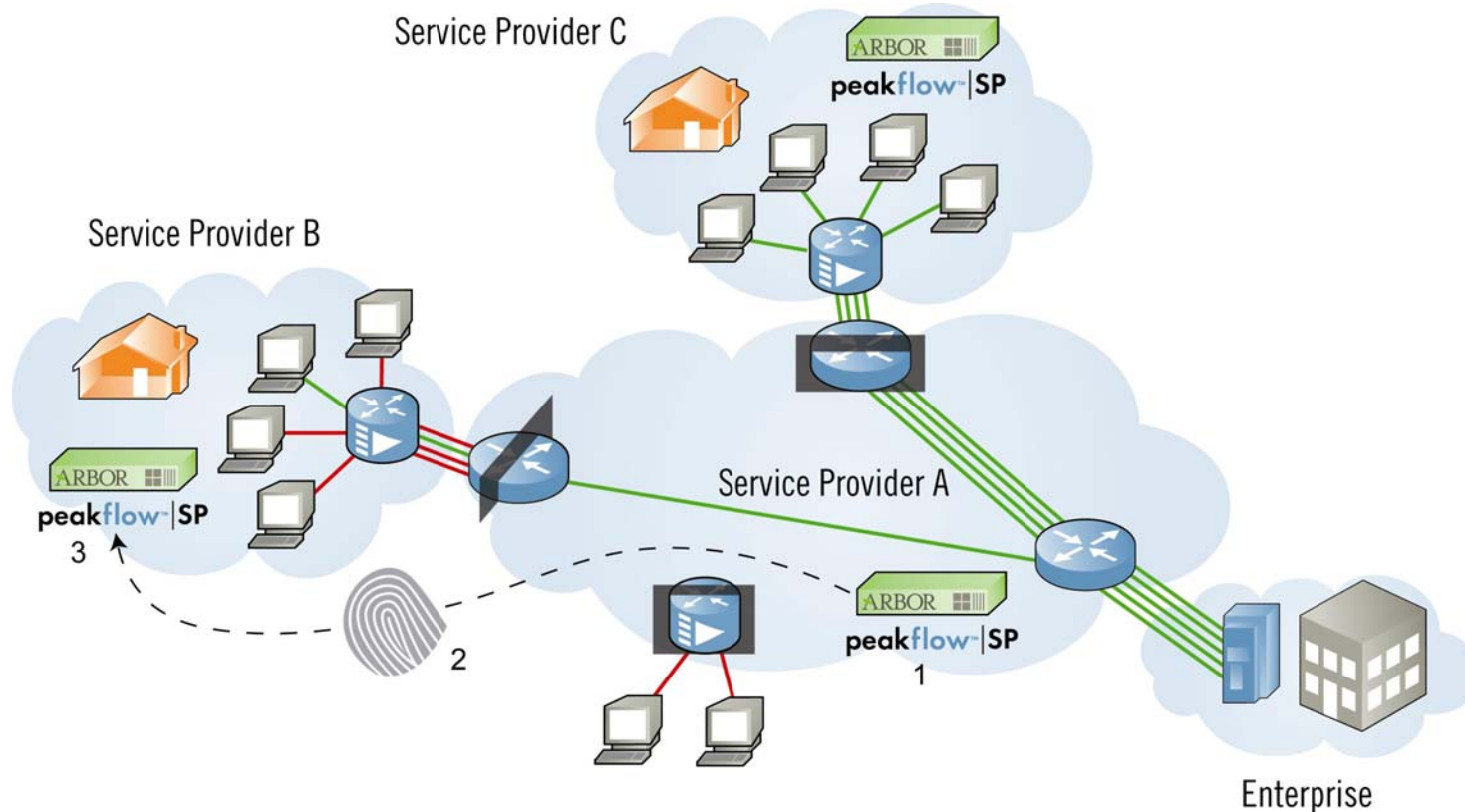
Track Specific Worm Traffic (Per Interface, Customer, Profile)



Fingerprint Sharing Alliance

- The Fingerprint Sharing Alliance has recognizable benefits for participating providers:
 - Increase in total network availability and recognize cost savings
 - Automate a formally manual response process
 - Decrease MTTR (response/repair)
 - Increasing traceback scope beyond single administrative domain
 - Conduct collaborative responses
 - Lower wasted bandwidth by filtering closer to the real ingress points
 - Reduce the number of compromised hosts from networks
 - Leverage a common language to improve communication between diverse network operators

Fingerprint Sharing Example



1. Using Peakflow SP, Service Provider A detects and mitigates a DDoS attack.
2. Service Provider A automatically sends the attack “fingerprint” to the relevant upstream providers affected by the attack.
3. After securely receiving the fingerprint, the information is used by the upstream ISP to traceback, analyze, and mitigate the attack, thereby identifying and removing compromised hosts as close to the internet ingress point as possible.

Intelligent Mitigation Management

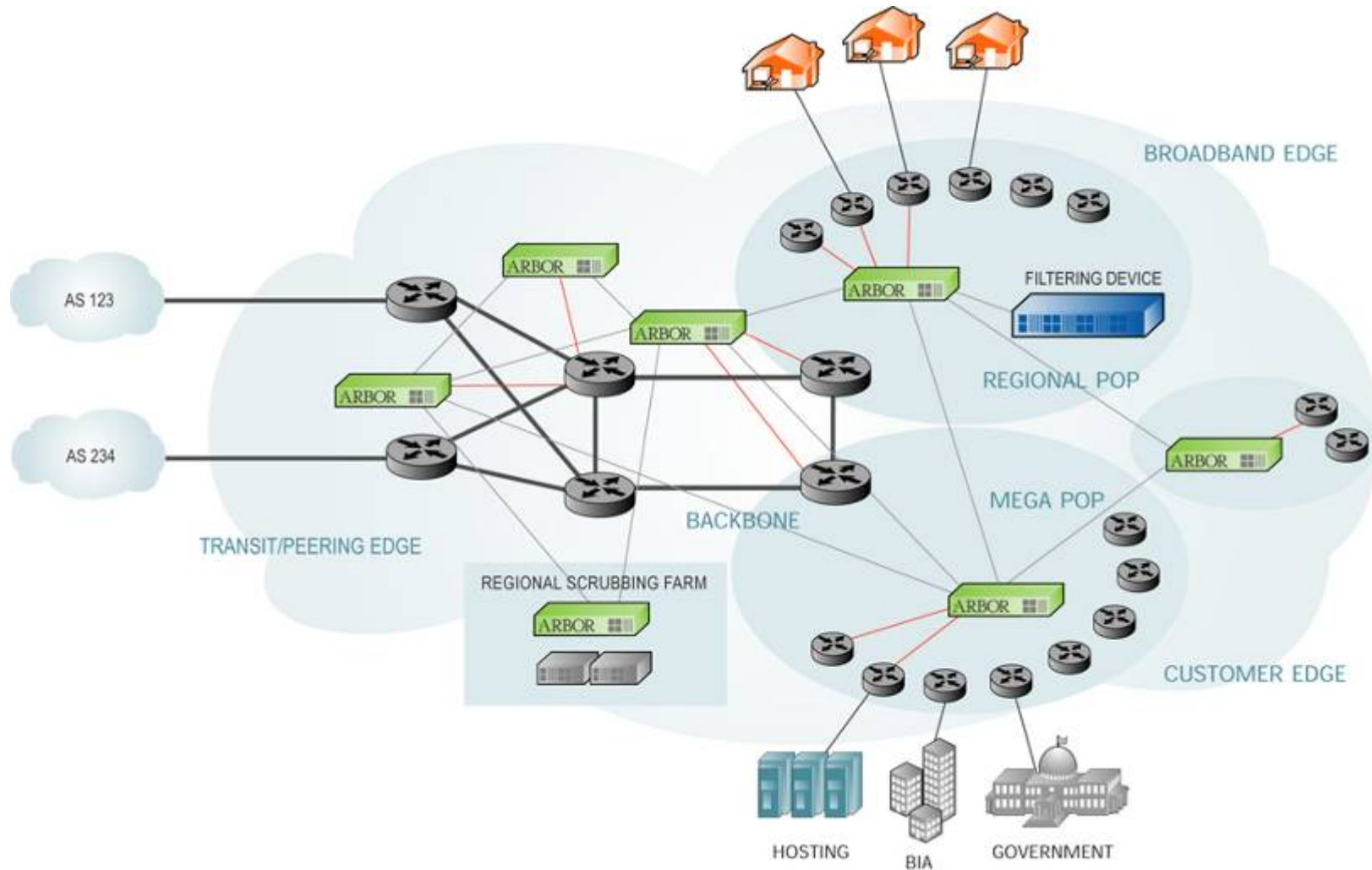
Peakflow SP not only supports today's remediation options ...

- Filtering/ACLs
- Rate-Limiting
- BGP Blackholing
- Off-Ramping/Sinkholing
- Dedicated Filtering Device

... but provides the intelligence necessary to know which one to choose and how to configure it.

[> more](#)

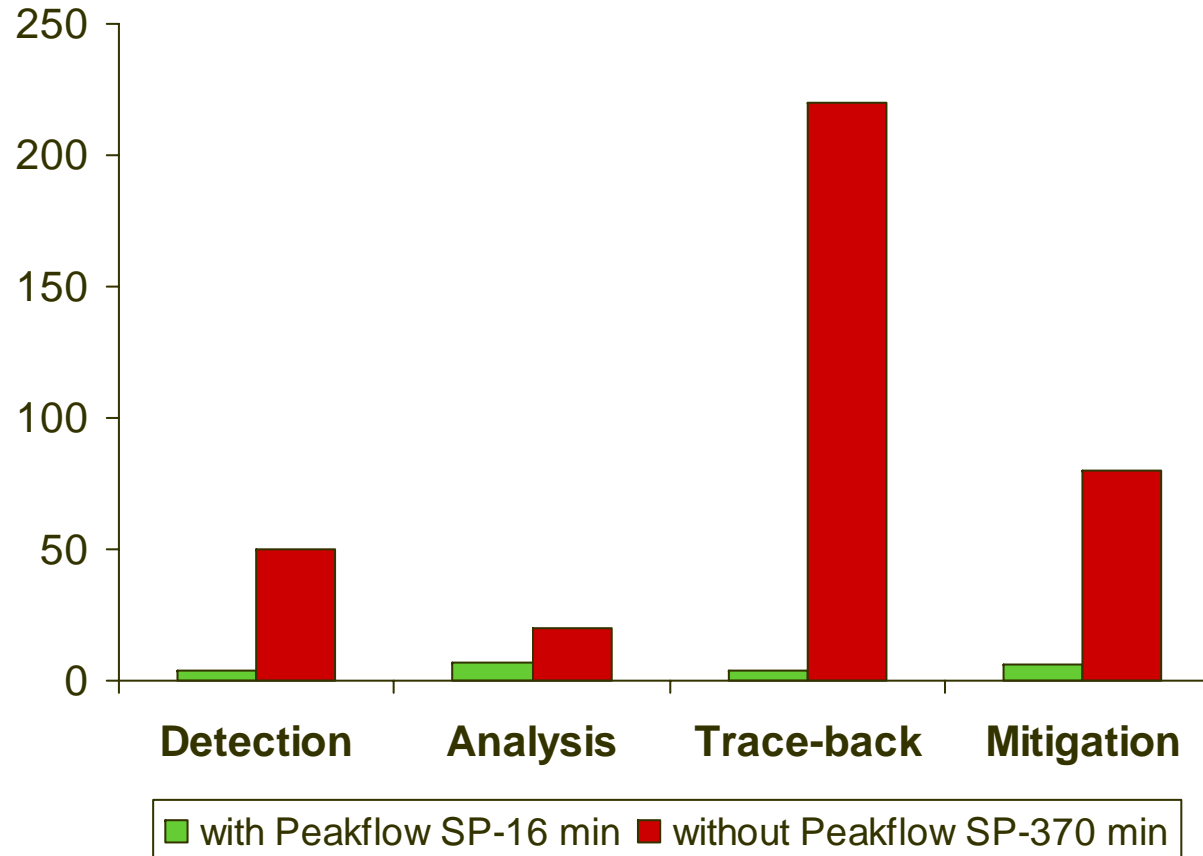
Peakflow|SP: Standard Architecture



Results at Global Tier-1 ISP

Improved Security Response with Peakflow SP

Average time spent during a DoS attack in minutes



Next Steps

- Product Demonstration
- Schedule Trial to Demonstrate Value
 - Protecting Key Customers and Critical Service Delivery Infrastructure
 - Protecting Peering and Regional Infrastructure
- Action Items

Thank you

MEASURE VISUALIZE PROTECT



www.arbornetworks.com
