Adaptive Network Intelligence

netDeFlect

Protecting DR and BCP

Esphion
March 2005

ESPHION

Agenda

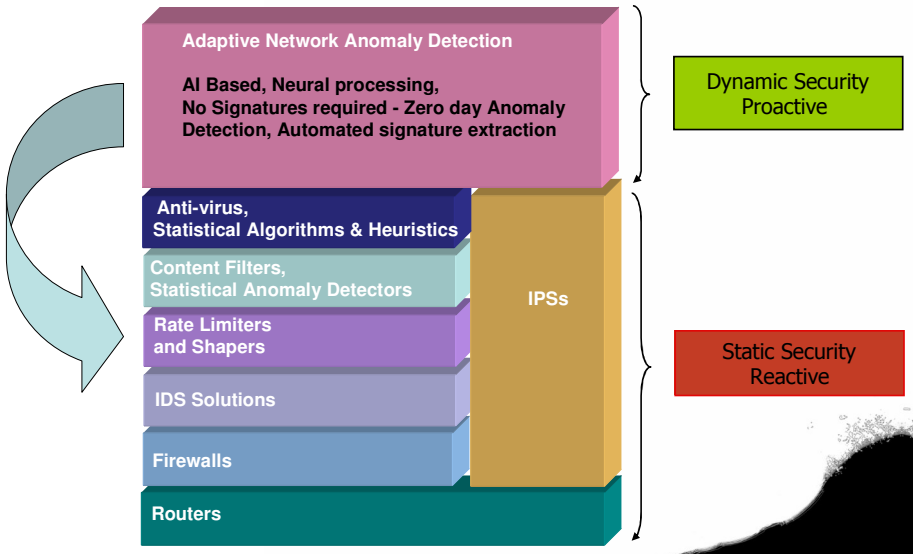
- Static security
- Anomalies and rules
- Neural technology (ANN)
- Esphion's Solution
- Anomalous Traffic
- Signature generation
- Deployment
- Existing Technology
- Reporting

ESPHION

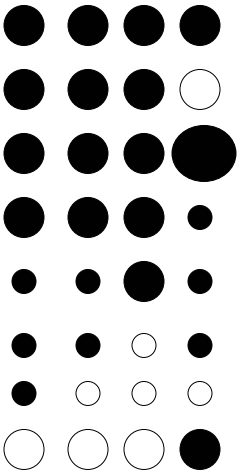
Router's, Firewalls, IDS, IPS Static Technology

- Current technologies rely on known factors
- Rule based
- Filter based
- Signatures
- In Line
- Protect Networks from known events

Dynamic Security Overlay



Anomalies and Rules !



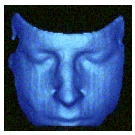
•**Rules**

•IF one is WHITE
•IF one is BIG
•IF one is SMALL
•IF three are SMALL
•IF all are SMALL and one is WHITE
•IF all are SMALL and one is BLACK
•IF one is BLACK
•IF……..
•..

What is the Rule for this ?

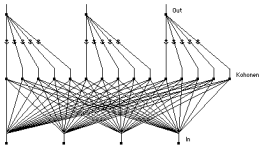
ESPHION

What is a Neural Network?



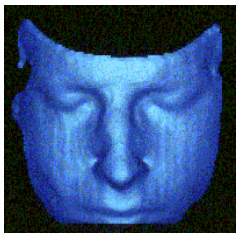
- Neural networks are based on the processing ability and memory abstraction of the human brain to identify patterns of behavior of interest.

- Neural networks are used where:
  - We can not use fixed mathematical solutions to complex evolving problems
  - We can get lots of examples of the behavior we require
  - Where we need to pick out structure from existing data and patterns of behaviors
  - Where huge volumes of data need to be processed in real, or near-real time.



ESPHION

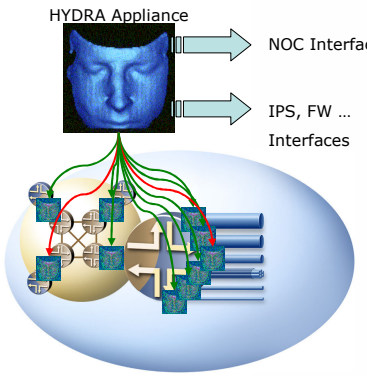
Neural networks



- **1940's** first neural network model
- **1950's** Rosenblatt's "perceptron" capable of learning
- **1980's** renewed interest – faster machines, self generating NN's - competitive learning models, multilayer networks.
- **1990's** Commercial, Banks – OCR –Image compression, Data mining speech recognition, Weather forecast.
- **2000's** ???

ESPHION

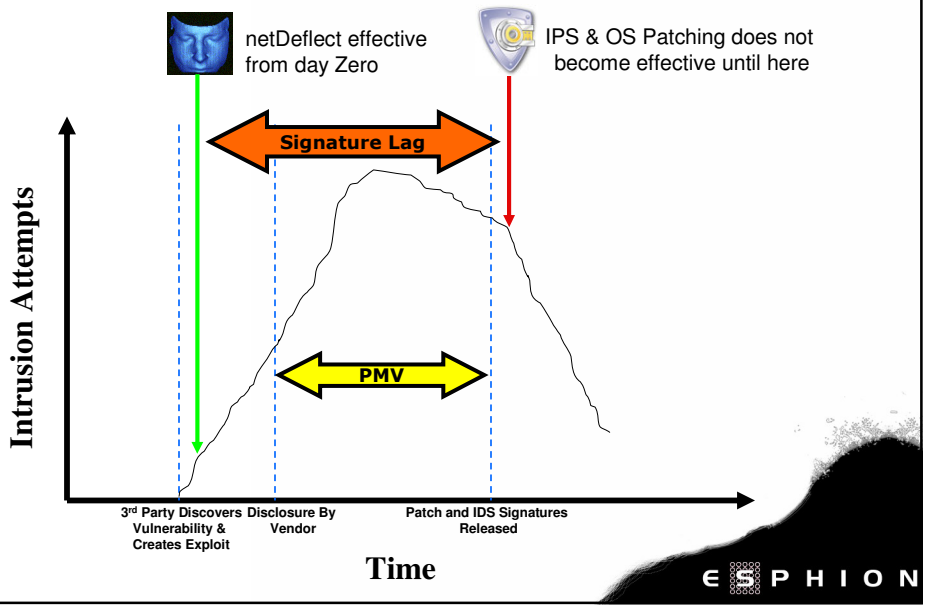
Esphion's Solutions
netDeFlect – adaptive Security



- Distributed adaptive solution that automatically detects and diagnoses unknown threats in real-time without ***signatures***
- Self learning ***neural networks***: maximize the ability to adapt to changing network conditions without ongoing re-configuration and maintenance
- Creates - *within seconds* - 'signatures' from anomalous network traffic for use by in-line IPS tailored to the traffic on a specific network.
- Compliments existing reactive security solutions (IPS) – delivers layered 'best practice' security solution

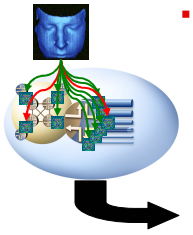
ESPHION

Zero Day Attack's

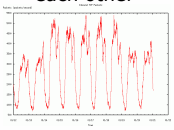


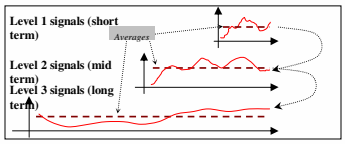
ESPHION

How it works - netDeFlect's Anomaly Detection and Diagnosis Technology

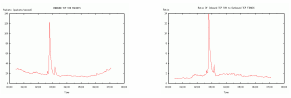


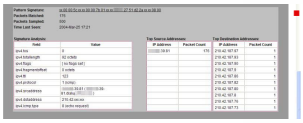
- Extensive data collected directly from the network, e.g.
  - Number of packets of particular types
  - Ratio of particular packet types compared to each other





Patent Pending Neural Network analysis used to detect anomalous deviations in traffic profiles



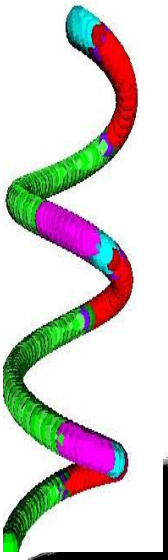


Patented Anomaly diagnosis technology produces
- Automated Capture of anomalous traffic
- Standardized signature of anomaly created
- Worm scanning activity revealed
- Critical Information output to network operation for action

ESPHION

Anomalous Traffic: Worms

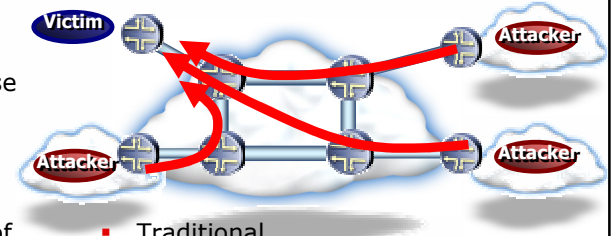
- Designed to Intrude by Stealth
  - Objective is to Secure Unlawful Access, Theft, Vandalism, Extortion
- Worms attack the hosts / computers on a network
  - Take advantage of vulnerability's in OS's and/or application's.
  - The network is typically NOT the target.
  - Do NOT need intervention to perform the infection or replication.
  - Automatically looks for new systems to infect (Self Propagating)
- Worms are most often identified through Symptoms of infection
  - instability of infected host, increased CPU load
  - Network Scanning activity seeking - new hosts to infect
  - Well written Worms are not detected!!!!!
- Networks are impacted as a 'side-effect'
  - rapidly spreading worms may cause huge traffic increases
  - overload billing systems



ESPHION

Anomalous Traffic: DDoS
(Distributed Denial of Services)

- Extortionate activity NOT aimed to 'intrude', but only to 'deny access'
- For most enterprises and individuals, defense is not possible

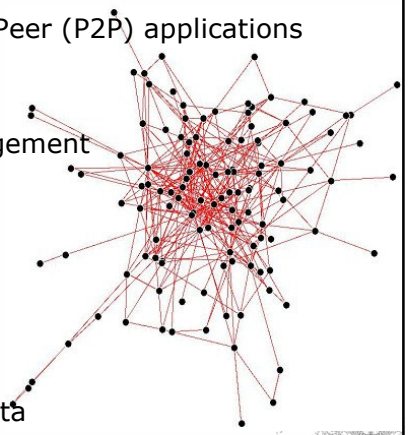


- Often Tens of ,000's of compromised PC's used to send network traffic (Flood) to a targeted company.
  - DDoS may affect multiple levels of network infrastructure
  - filling the network links
  - exhausting router forwarding capability
  - overloading Ethernet switches
  - Exhausting IDS / Firewall memory and resources overloading of servers
- Traditional (Firewall/IDS) Methods of Detection and Filtering are Limited
  - Target typically notices only when services cease to function.
  - Providers notice when their customers (The targets) call and complain
  - Flood Traffic may look like 'normal' network traffic

ESPHION

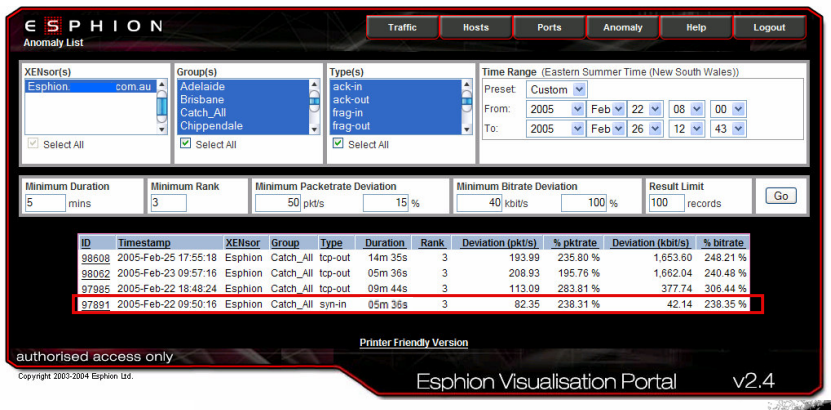
Anomalous Traffic: Network Abuse (MISUSE)

- Not-used for-business / Peer to Peer (P2P) applications
  - Traffic Volumes
  - Content Liability
  - Work and private data management
- Web and Game Servers
  - UDP traffic.
  - Streaming Content
- Non-sanctioned Applications
  - Chat Relay's
  - Re-mailers, Spam hosts
  - Non-sanctioned storage of data
- Non-sanctioned Network Access
  - Wireless Networking
  - Internally configured Firewall Bypass dial-in



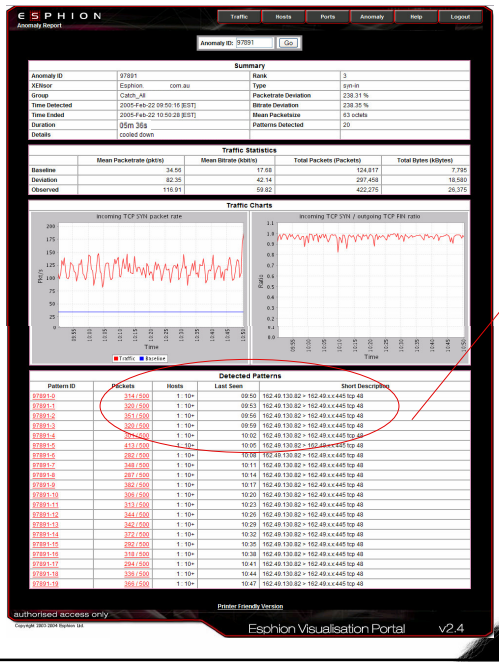
ESPHION

netDeFlect Visualisation Portal



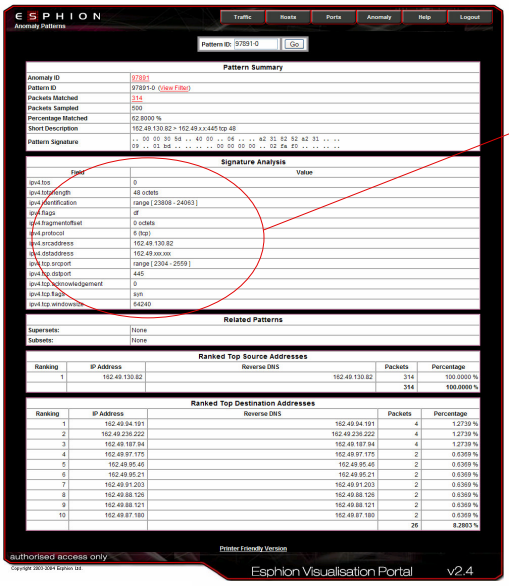
ESPHION

netDeFlect Anomaly Report



netDeFlect Detected Patterns shows single host scanning multiple target machines on customer subnet.

netDeFlect Output/Views



netDeFlect Packet Analysis produces instant filter information that can now be applied to customer affected Firewalls/ IDS's/Router ACL's

- may also be used in patch mgmt processes & services

-Providing information

-Port No

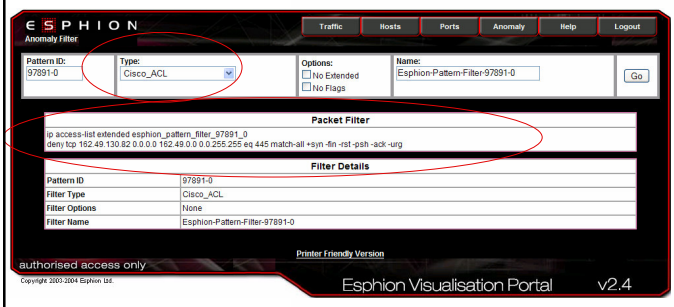
-Packet size

-Protocol type

-Source & destination IP Address's

-Signatures

netDeFlect ACL Generation



netDeFlect produces automatic ACL's and Rules that can be directly applied to complimentary security devices…..

Now:-

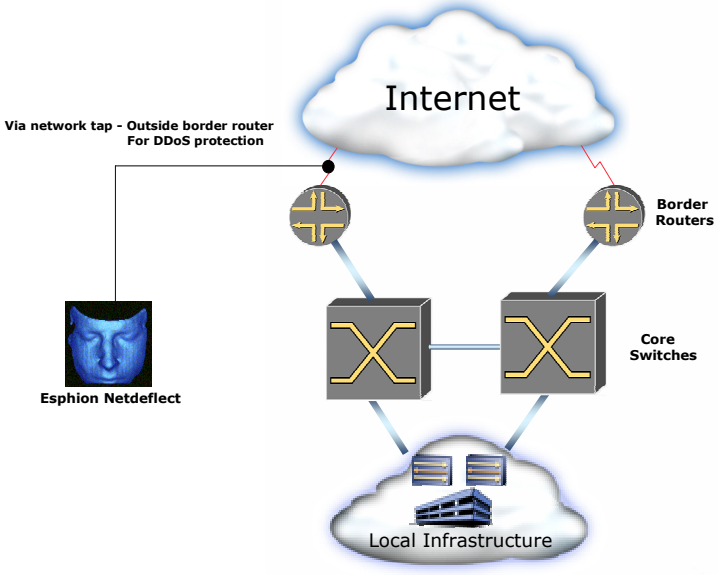
Cisco ACL's, Fortinet, SNORT

Near Deliverables:-

PIX, CheckPoint, Symantec…

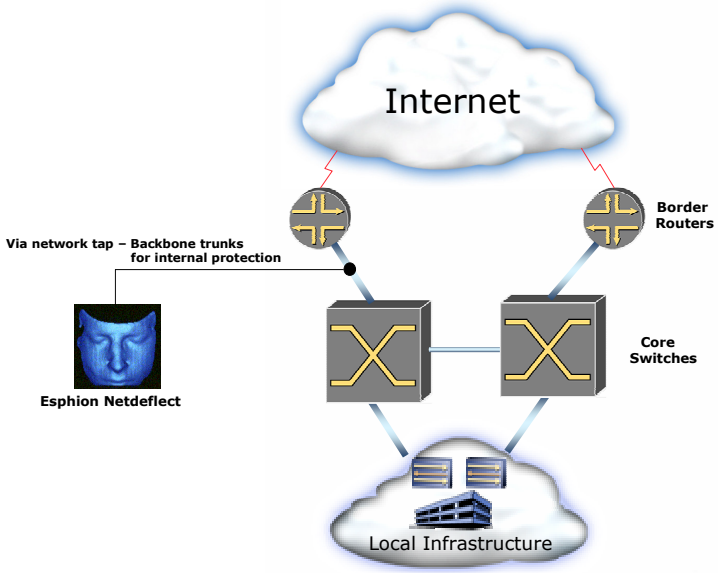
ESPHION

Standalone Deployments

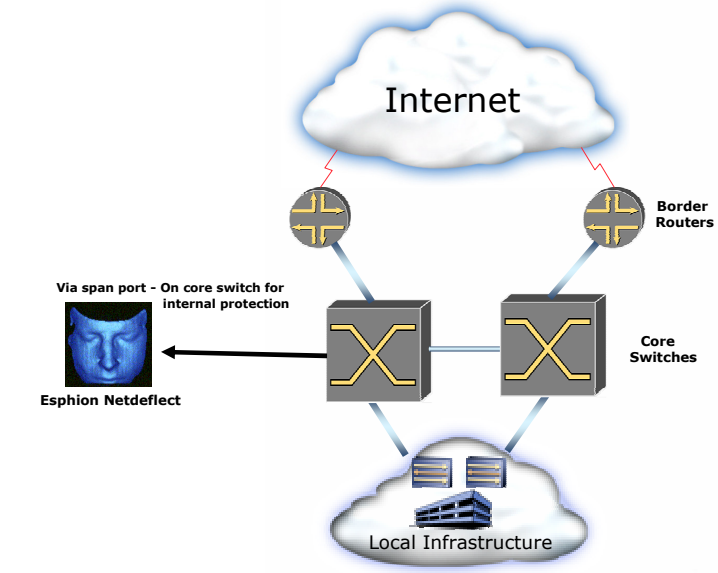


ESPHION

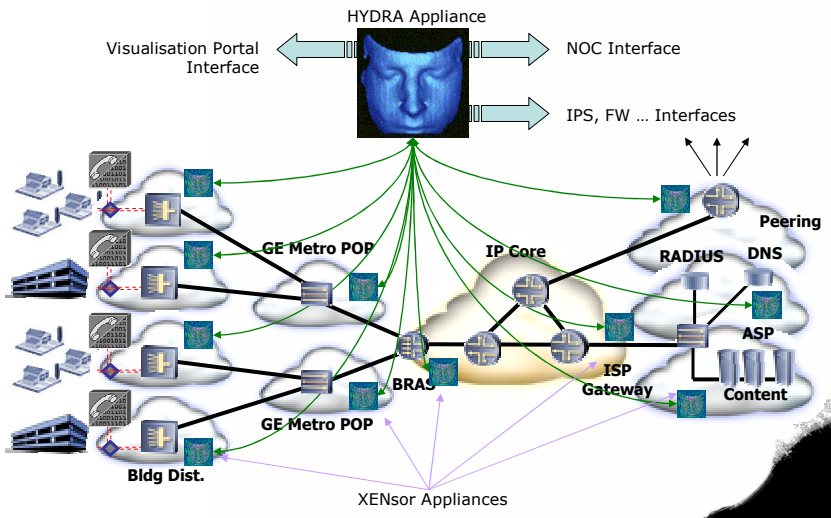
Standalone Deployments



Standalone Deployment

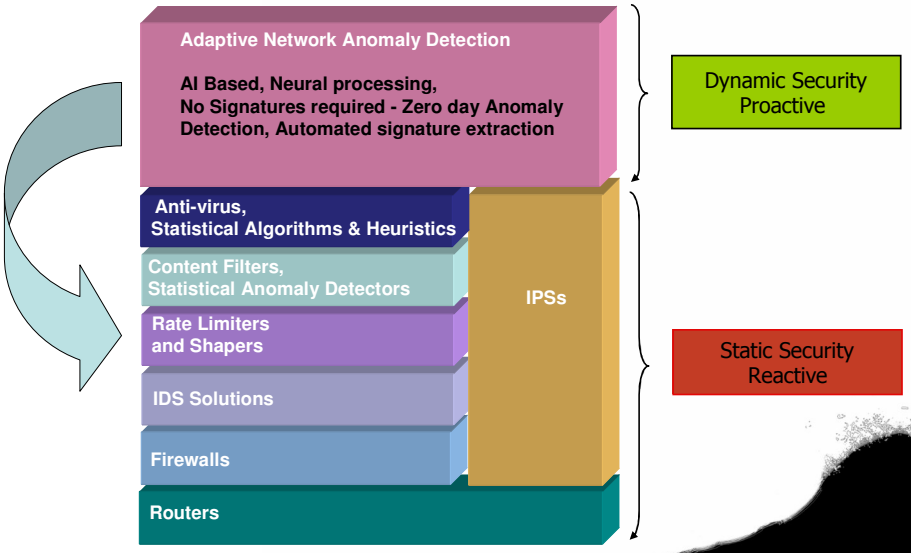


Typical distributed deployment



ESPHION

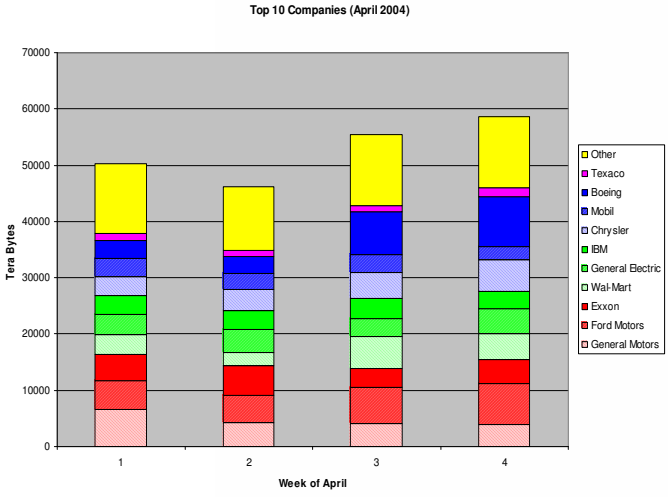
Dynamic Security Overlay



ESPHION

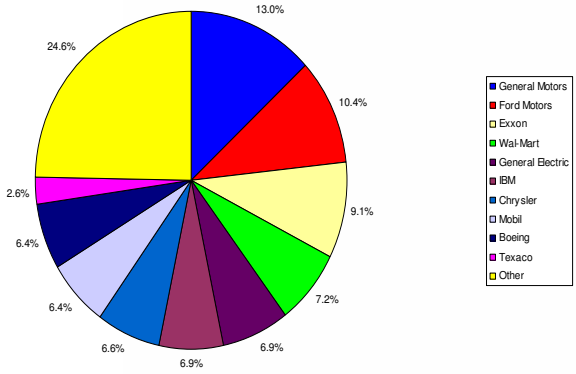
Real Time Traffic views from netDetail

Top 10 Users – Total Usage by week



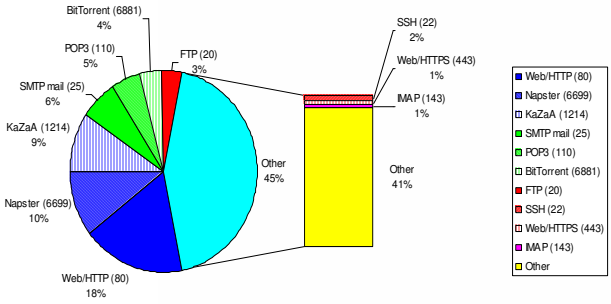
Top 10 Users by % used

Percentage Total Usage by Top 10 Customers (12 - 18 April 2004)

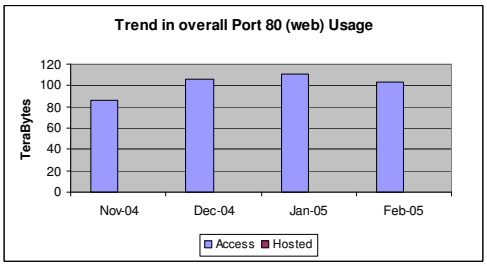


Top 10 Applications and % of Network used

Company Percentage Total Usage by Top 10 Applications by TCP Port (12-18 April 2004)

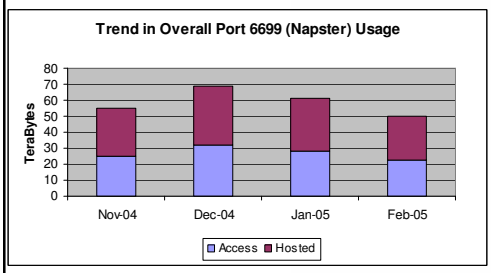


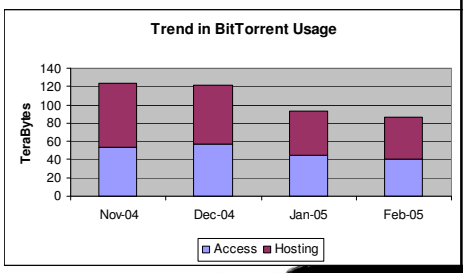
Sample Reports – Usage Trends Web, P2P



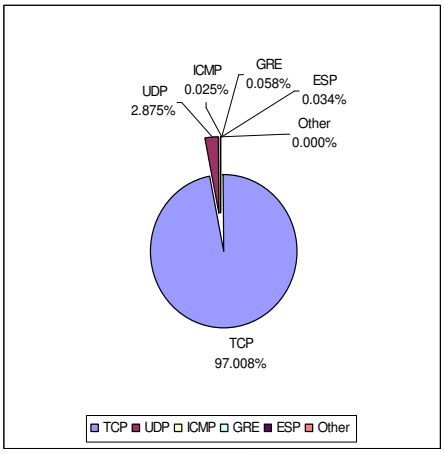
Notes:

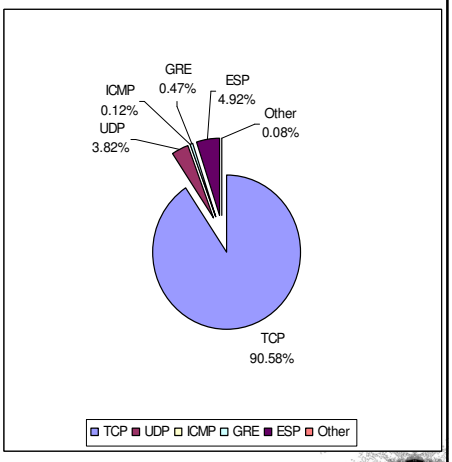
• Port 6881, 16881, 1881 and 6882 are used to represent BitTorrent. These ports contribute 95.5% of overall BitTorrent volume.





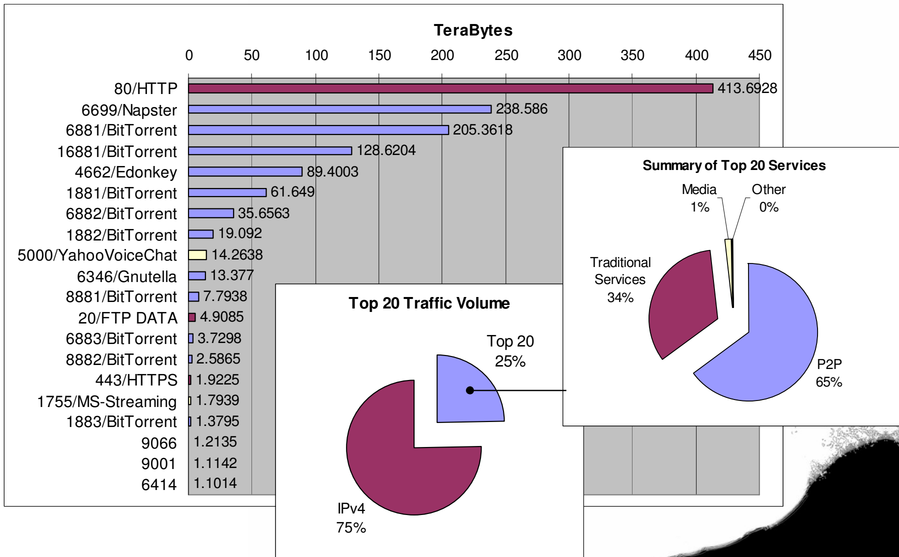
Sample Reports – Overall Traffic Usage





90-97% of traffic is TCP

Sample Reports – Traffic Volumes



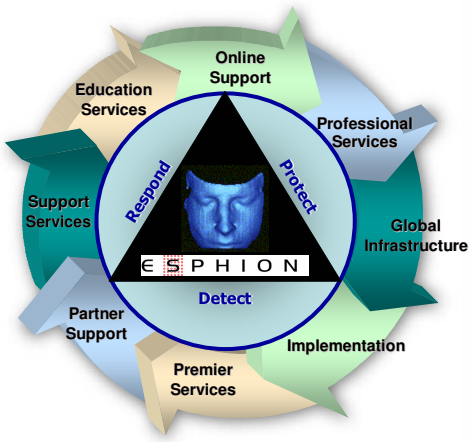
Anomaly Report for period: 12-18 April 2004

Total number of anomalous events	**200**
Inbound	60%
Outbound	40%
Total number critical events >15 minutes >30% degrade/total usage	90
Critical anomalous events alerted and mitigated	90

Anomalies by Classified Event	
Total anomalies attributed to worm scanning	**90**
Anomalies dues to worm scanning into your network	70%
Anomalies due to worm scanning originating from your network	30%
Total anomalies attributed to Denial of Service attacks	**40**
Denial of Service attack into your network	90%
Denial of Service attack out of your network	10%
Total anomalies attributed to P2P traffic	**50**
Inbound P2P traffic	40%
Outbound P2P traffic	60%
Total other/unattributed/unclassified anomalies	**20**
Inbound	40%
Outbound	60%

Estimated Bandwidth Consumed by Classified Anomalies	
Worm scanning	3GB
Denial of Service attacks	1GB
P2P traffic	30GB
Total other/unattributed/unclassified anomalies	70GB
Percentage of TOTAL consumption for the period	51.75%

Esphion Life-Cycle Services



ESPHION

THANK YOU

ESPHION

ESPHION