

# **Securing and Monitoring BYOD Networks using NetFlow**

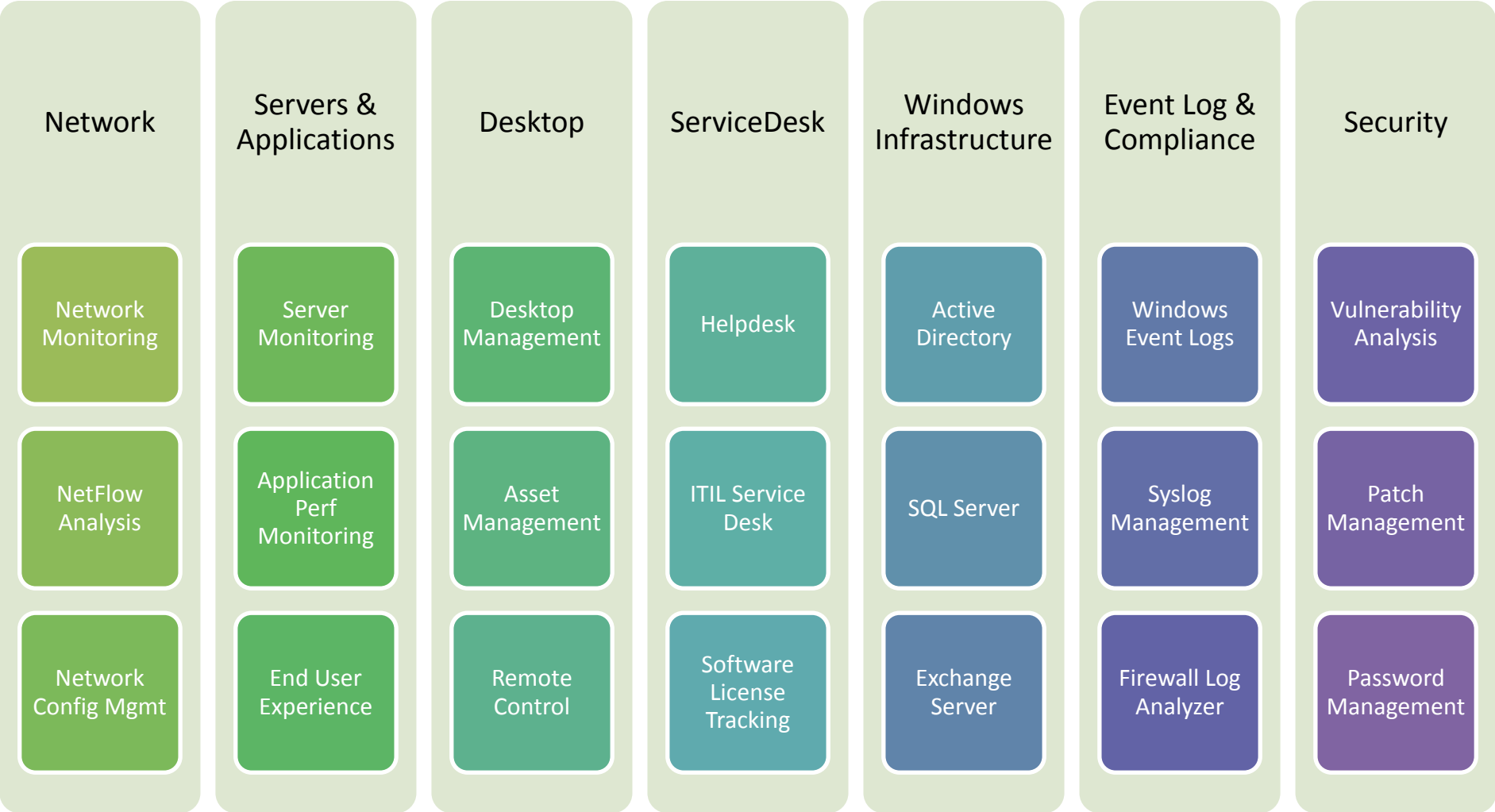
**How NetFlow can help with Security Analysis,  
Application Detection and Traffic Monitoring**

**Don Thomas Jacob**

**Technical Marketing Engineer**

**ManageEngine NetFlow Analyzer**





ManageEngine is an IT management vendor focused on bringing a complete IT management portfolio to all types of enterprises

- **What is BYOD**
- **Audience Poll**
- **Reasons for Concern**
- **Limitations of BYOD Solutions**
- **What is NetFlow**
- **Why NetFlow for BYOD Networks**
- **Questions**

## Define: BYOD (Bring Your Own Device)



*“ The practice of allowing employees to bring their own computing devices like smartphones, laptops or PDA to the workplace for use and connectivity on the corporate network. ”*

# Define: BYOD (Bring Your Own Device)

*“ The practice of allowing employees to bring their own computing devices like smartphones, laptops or PDA to the workplace for use and connectivity on the corporate network. ”*

- **Cost Savings**
  - Device/Hardware cost transferred to employee
- **Free up your IT Team**
  - Ownership on the employee – Devices handled better
  - Reduce the time spend by IT team on end-user device support and troubleshooting
- **Employee Satisfaction**
  - Flexibility to work when & where as needed, on ones own chosen device
- **Increased Productivity**
  - Telecommuting and flexible working hours increase productivity

## BYOD Reach

An Aberdeen study in July 2011 found 75% organizations are permitting BYOD for business purposes

Gartner study says that by 2014, 90 percent of organizations will support corporate applications on personal devices

<http://www.gartner.com/it/page.jsp?id=1480514>

Cisco is adopting a "Any Service, Any Device, Anywhere" architecture which will evolve to a "Virtual Enterprise" – An enterprise which is location and service independent

[http://www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/any\\_device\\_white\\_paper.pdf](http://www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/any_device_white_paper.pdf)

## POLL

**What is your organization's decision regarding BYOD implementation?**

- BYOD allowed for all device types including laptops
- BYOD permitted only for smartphones/tablets
- Planning to implement
- Currently not considering

## **BYOD: Reasons for Concern**



# Reasons for Concern

## Nascent Mobile Device Management (MDM)

- No established MDM policies and monitoring solutions
- No multi-platform or IPv6 support, may not be user friendly, etc.

## Different devices, Different Operating Systems

- Patch management and Compliance issues

## Lack of Visibility

- Where is the device in the network?
- What is it accessing?

## Applications - Unverified and Untrusted

- Security issues, Malwares and Bandwidth Issues

## Vanishing Network Perimeter

- Remote connections, Security concerns



## Personal Work @ Work

- Tendency to use BYOD for personal purposes



- Exponential growth in HD Video and social media
- Live Streaming of highly popular NCAA men's college basketball tournament was made available on Android devices
- Non-business related traffic volume increases

**BANDWIDTH Issues / Poor Business Application Performance**

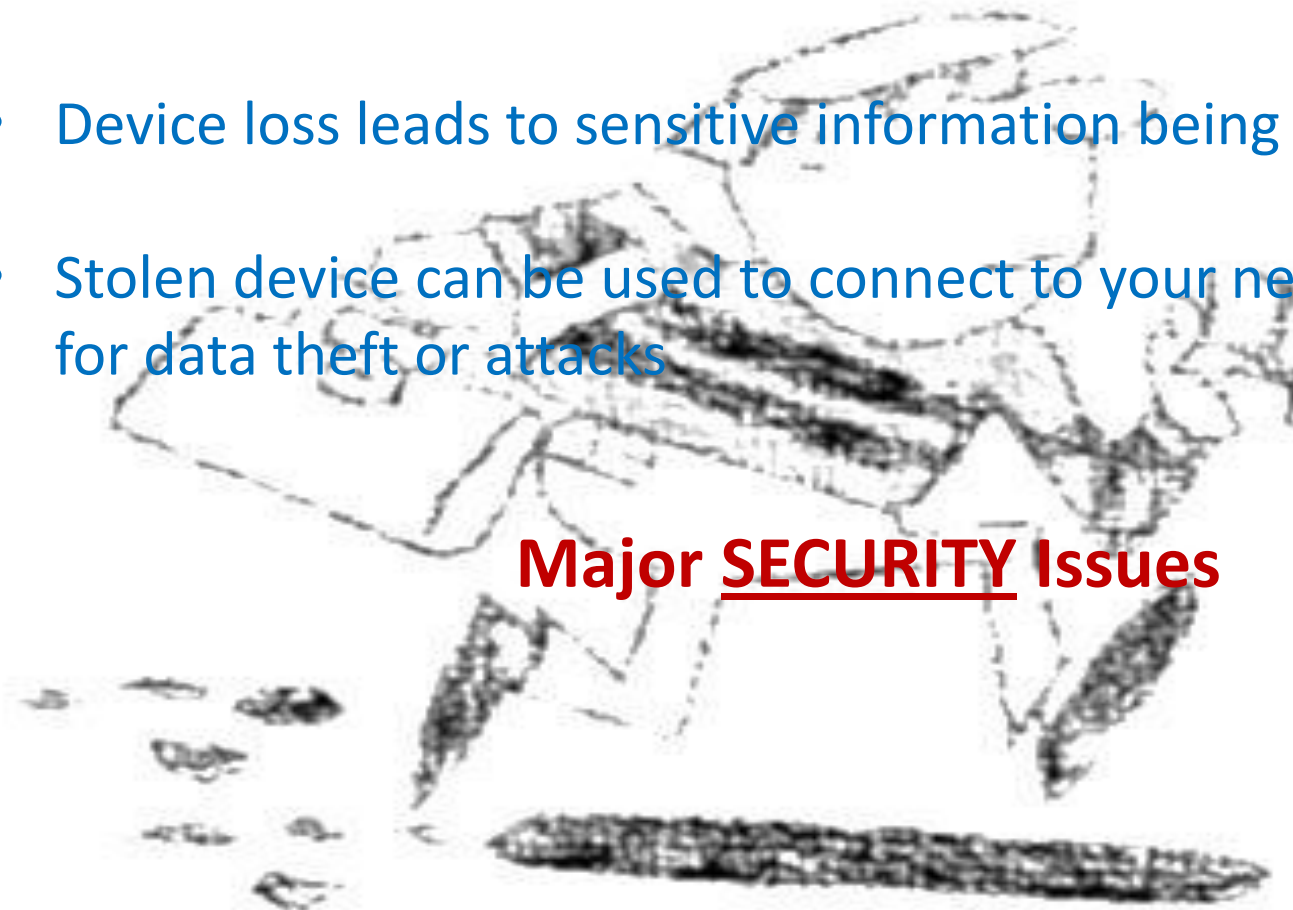
## Device Loss = Data Loss



## Device Loss = Data Loss

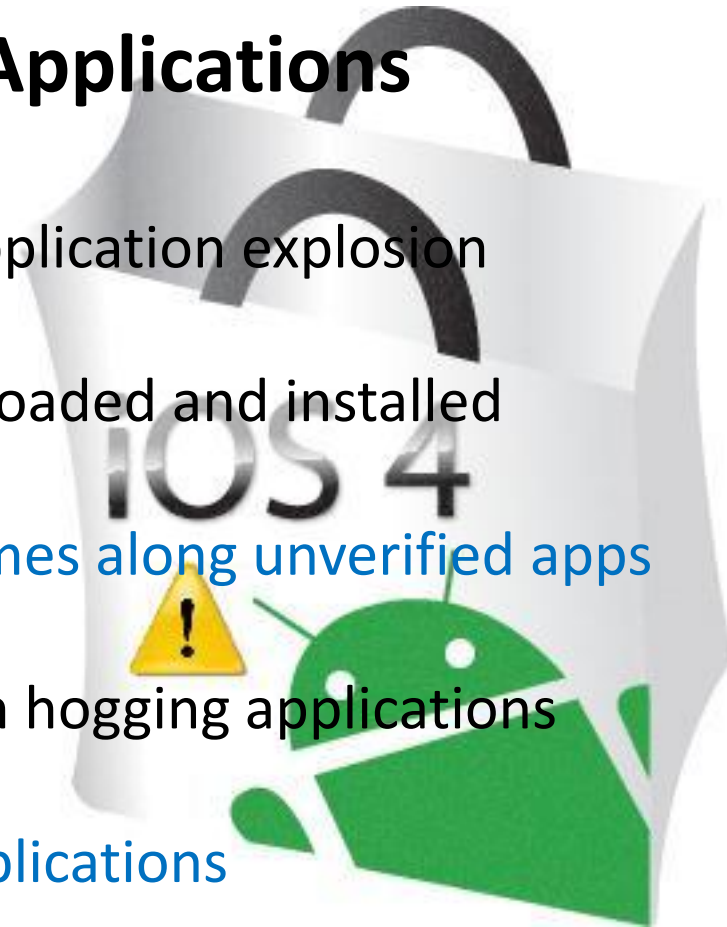
- Biggest threat is when BYOD leaves the enterprise network
- Business data / internal emails stored on device
- Device loss leads to sensitive information being left in the open
- Stolen device can be used to connect to your network remotely for data theft or attacks

**Major SECURITY Issues**



# Unverified and Greedy Applications

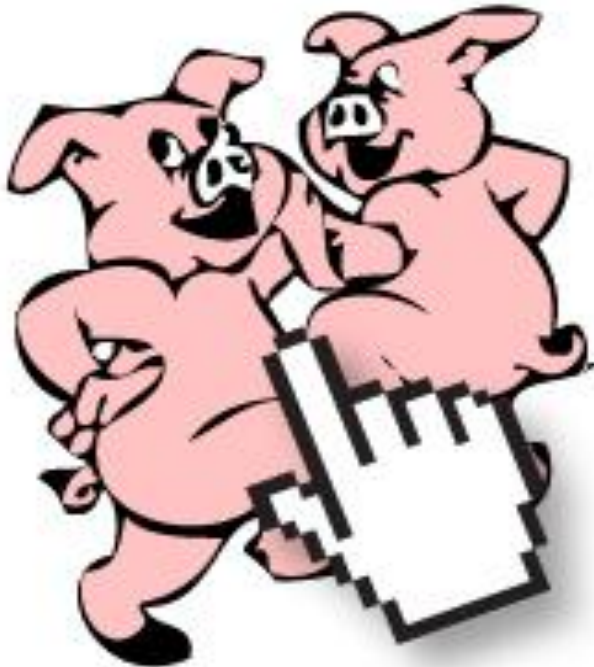
- Mobile device growth has lead to an application explosion
- New and unverified applications downloaded and installed
- Security threats and malwares risks comes along unverified apps
- Greedy Apps: Un-optimized, bandwidth hogging applications
- Bottlenecks due to traffic from junk applications



**SECURITY Issues & BANDWIDTH Bottlenecks**

## Inviting Network Threats

- BYOD users browse from unsecured Wi-Fi networks, visits untrusted sites or download from untrusted vendors
- “Dancing pigs over Security” – Users can be careless and devices outside the network perimeter are easier to attack and infect



## Inviting Network Threats

- BYOD users browse from unsecured Wi-Fi networks, visits untrusted sites or download from untrusted vendors
- “Dancing pigs over Security” – Users can be careless and devices outside the network perimeter are easier to attack and infect
- Huge increase in number of malwares targeting mobile software platforms like iOS and Android
- Infected device carried into the network – Malware enters LAN

**Network open to MALWARE**

# **Limitations of BYOD Solutions**



# Limitations of BYOD Solutions

## More Control on BYOD Devices & Web Traffic

**Limitation:** As good as having company issued device - BYOD advantage lost  
Vague and impractical solution - Genuine users will be effected

## Up-to-date Patch Management

**Limitation:** No multi-platform MDM or patch management solution available for the highly diverse mobile ecosystem

## Anti-Virus Software on Mobile Devices

**Limitation:** New age malware exploits zero-day vulnerabilities

## Multi Layered Security & Internal IDS

**Limitations:** Traditional, layered security solutions (firewall, proxy, content filtering, etc.) will fall short against new age threats  
Expensive to implement IDS/IPS in access layer to stop internal malware

# What is NetFlow

# What is NetFlow

Technology developed by Cisco - Designed as a switching path

Is now the **Primary IP Traffic** accounting technology

Information on the WHO, WHAT, WHEN and WHERE of IP traffic

All major vendors now support flow export:

**NetFlow** - Cisco, Adtran, 3COM

**J-Flow** - Juniper

**IPFIX** - Nortel

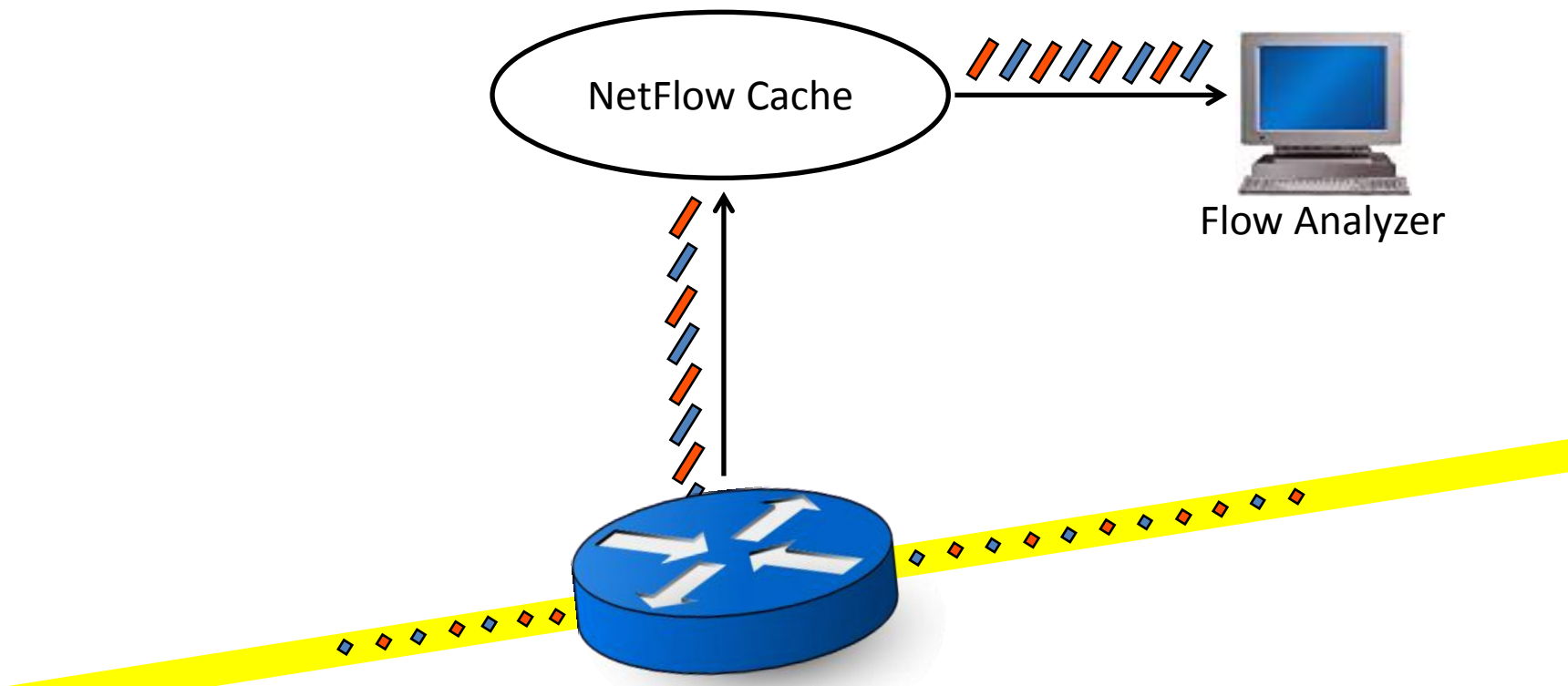
**sFlow** - Alcatel, HP, Brocade, Enterasys, Dell

## 7 unique fields define a flow

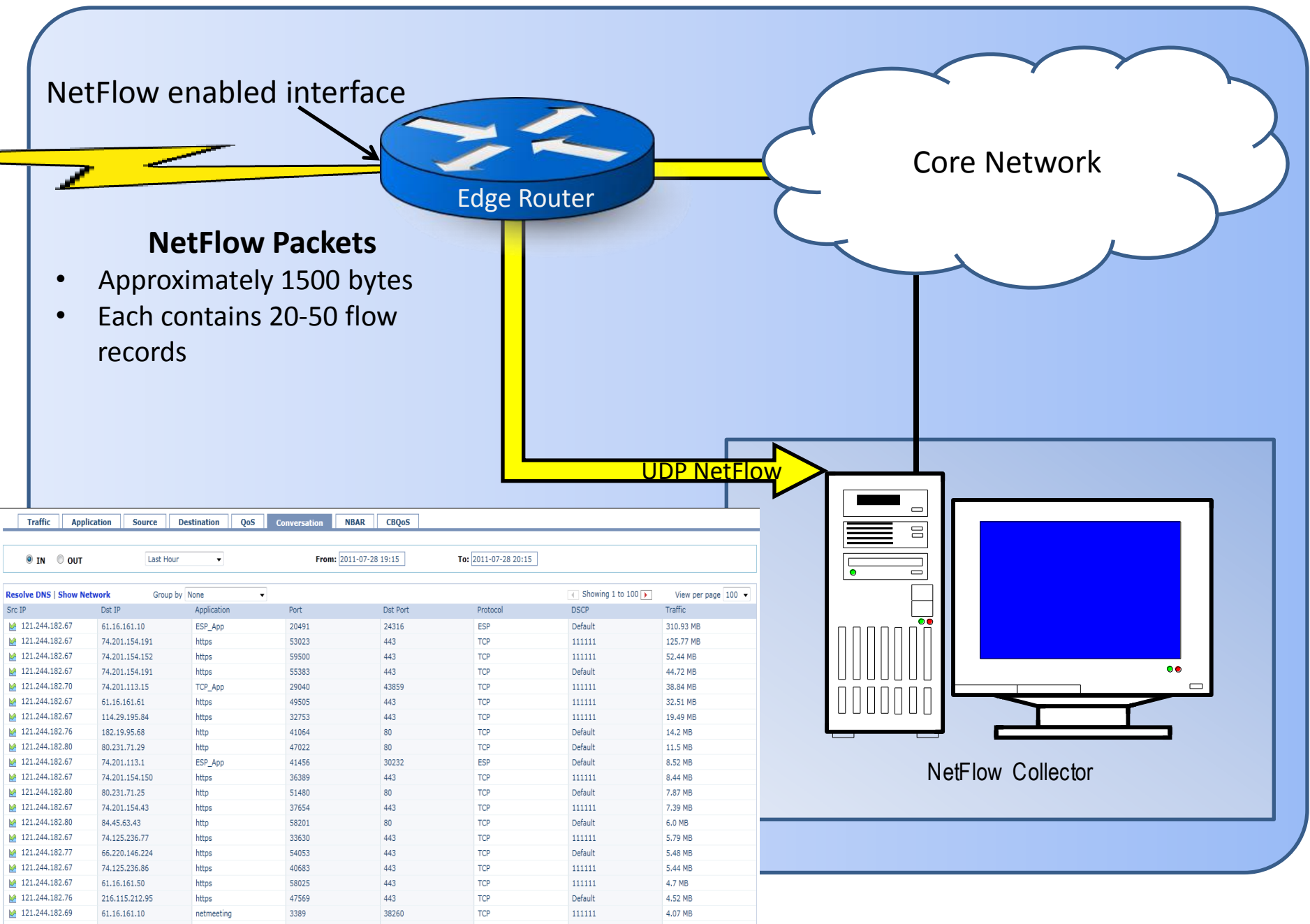


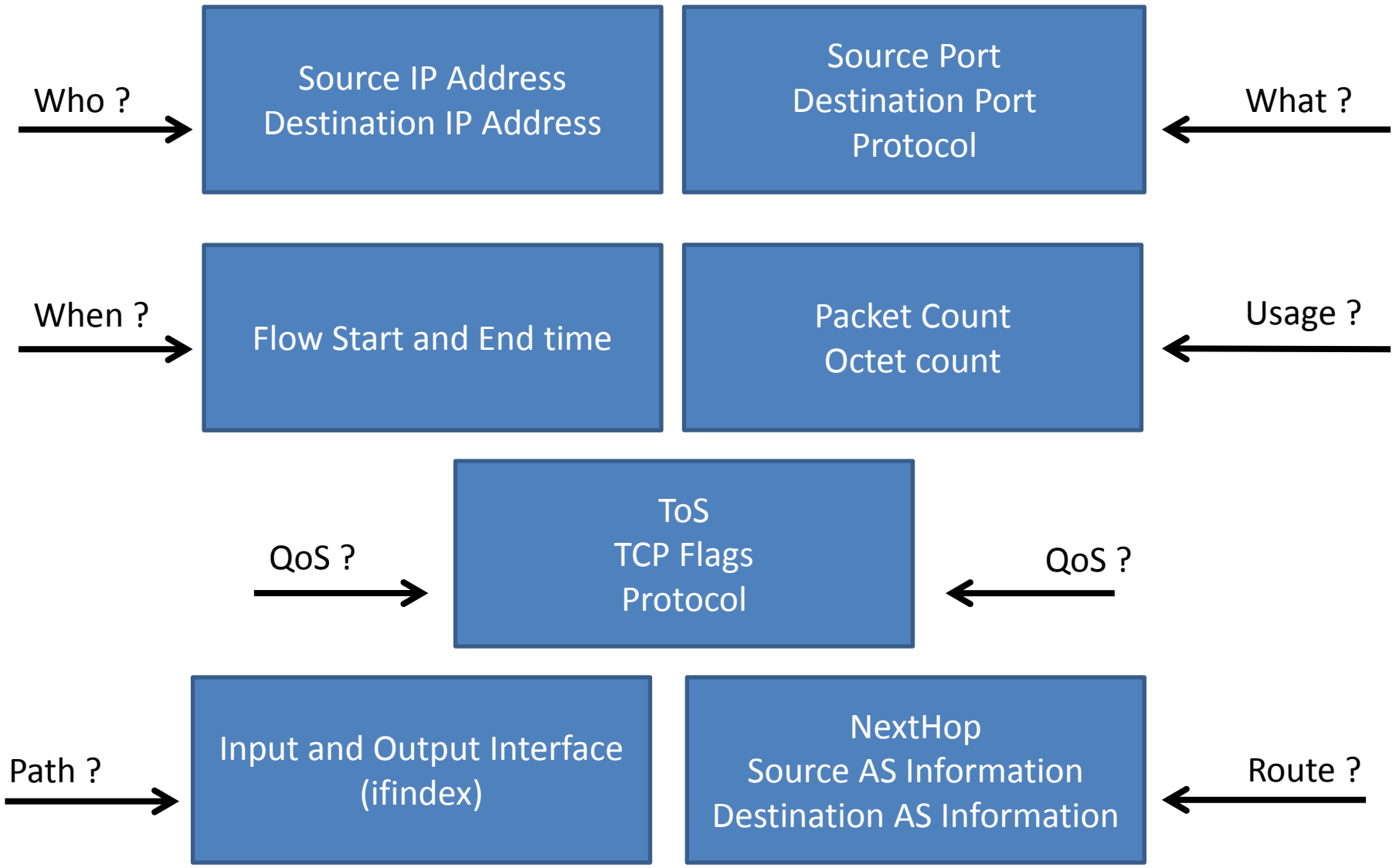
## How NetFlow Works

- Traffic passes through routing/switching device interface
- Flow created (remember the 7 fields) and stored in NetFlow cache
- Flows grouped and exported in UDP packets to collector based on active and inactive flow timeout



# What is NetFlow



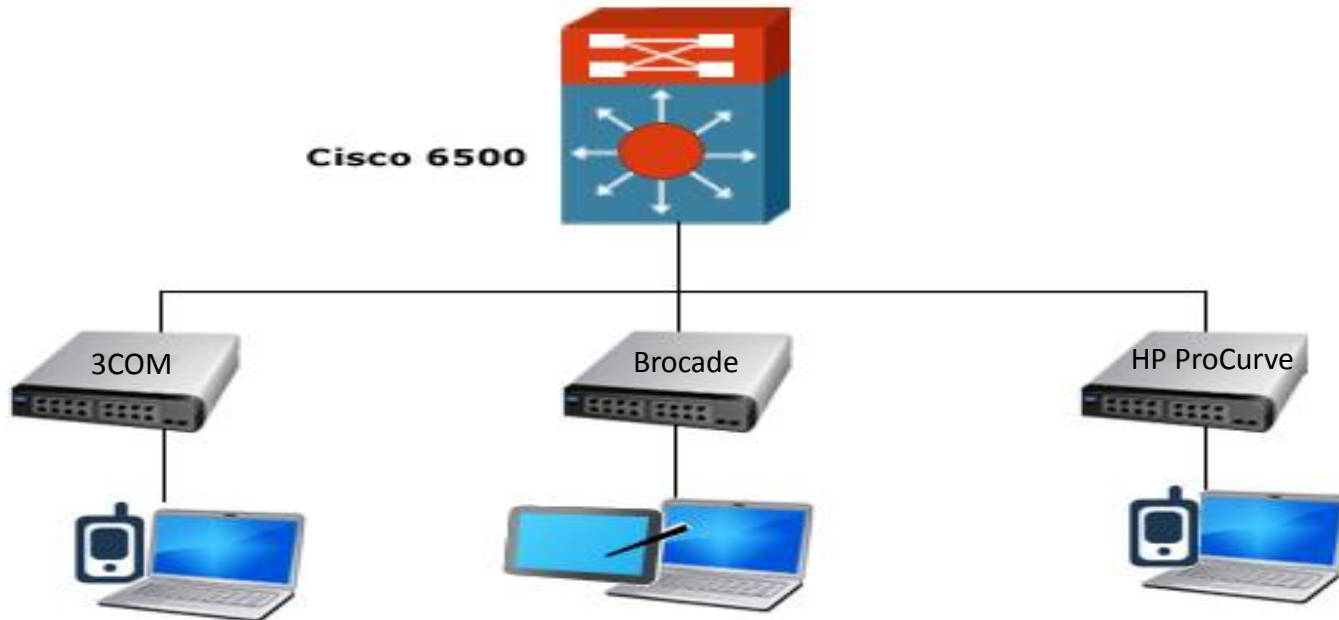


# **Why NetFlow for BYOD Networks**



## In-Depth Tracking

- NetFlow provides real-time information about network traffic
- BYOD monitoring begins at the access layer - Closer to traffic source



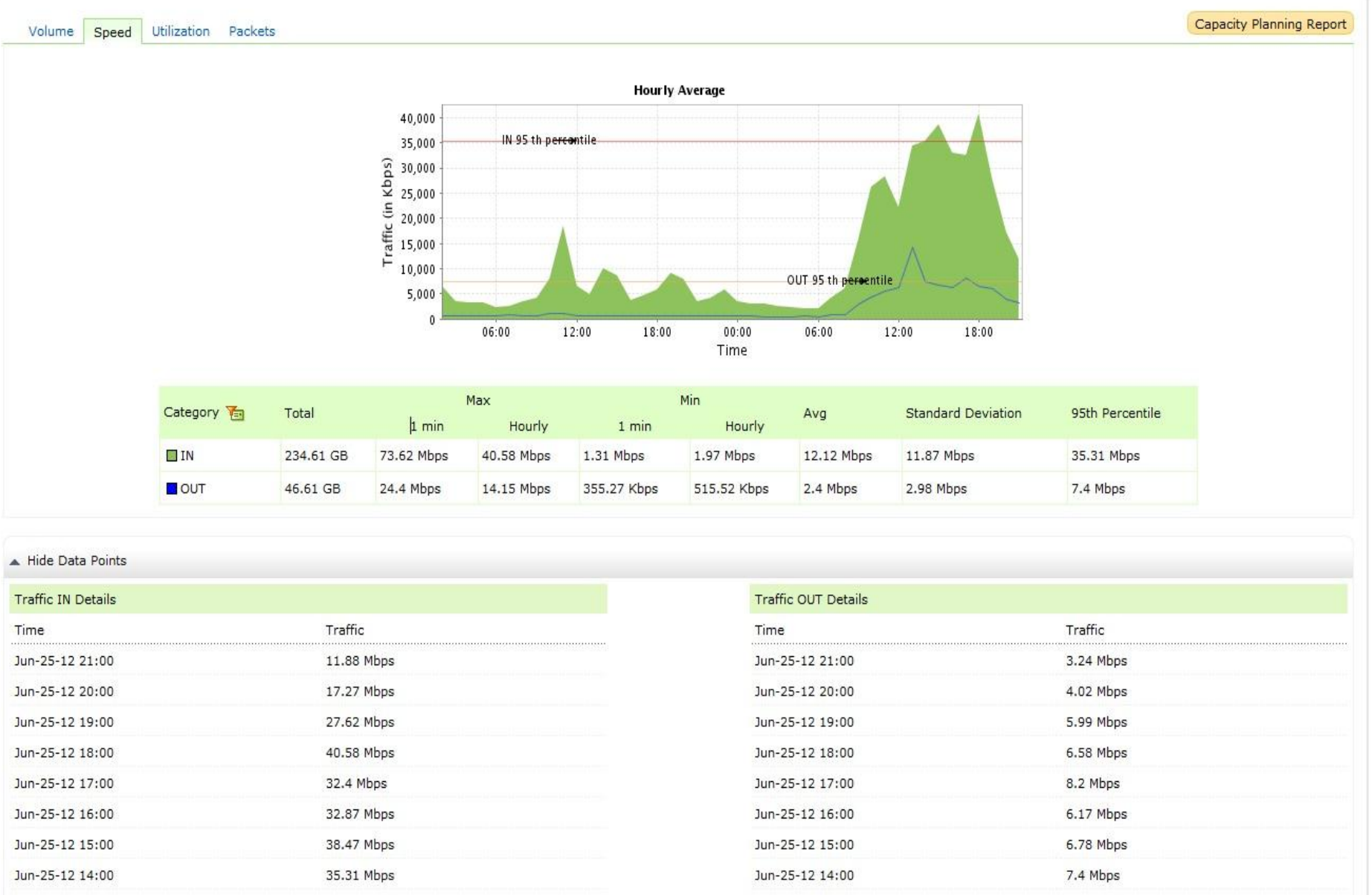
## In-Depth Tracking

- NetFlow provides real-time information about network traffic
- BYOD monitoring begins at the access layer - Closer to traffic source
- Flow export supported on most enterprise devices including core and access layer switches
- No impact on the network and devices due to flow export

## In-Depth Tracking

- NetFlow provides real-time information about network traffic
- BYOD monitoring begins at the access layer - Closer to traffic source
- Flow export supported on most enterprise devices including core and access layer switches
- No impact on the network and devices due to flow export
- Track impact of BYOD on bandwidth, who are the top talkers for each interface and IP Subnet
- What are the devices doing on your network, what application is being used and what is the destination of traffic

# In-Depth Tracking



# In-Depth Tracking

TrafficApplicationSourceDestinationQoSConversationMulticastMedianetNBARCBQoSSecurity Events

IN

OUT

Last Hour

From: 2012-06-26 00:13

To: 2012-06-26 01:13

Show IP | Show Geo Locations | Show Network

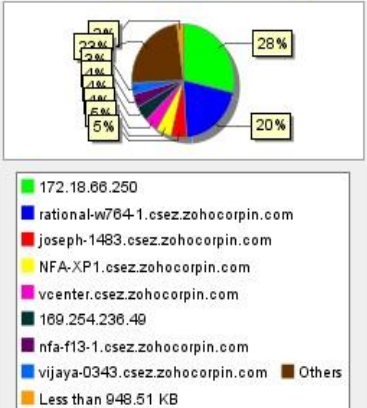
Showing 1 to 10View per page 10

Source	Traffic(Total: 47.42 MB)	% of total traffic
172.18.66.250	13.49 MB	28%
rational-w764-1.csez.zohocorpin.com	9.71 MB	20%
joseph-1483.csez.zohocorpin.com	2.29 MB	5%
NFA-XP1.csez.zohocorpin.com	2.29 MB	5%
vcenter.csez.zohocorpin.com	2.03 MB	4%
169.254.236.49	2.02 MB	4%
nfa-f13-1.csez.zohocorpin.com	1.82 MB	4%
vijaya-0343.csez.zohocorpin.com	1.63 MB	3%
binoy-1362.csez.zohocorpin.com	532.38 KB	1%
172.18.2.206	432.52 KB	1%

Showing 1 to 10

Top Traffic - SourceIN

172.18.2.101 [ IfIndex2 ]



172.18.66.250

rational-w764-1.csez.zohocorpin.com

joseph-1483.csez.zohocorpin.com

NFA-XP1.csez.zohocorpin.com

vcenter.csez.zohocorpin.com

169.254.236.49

nfa-f13-1.csez.zohocorpin.com

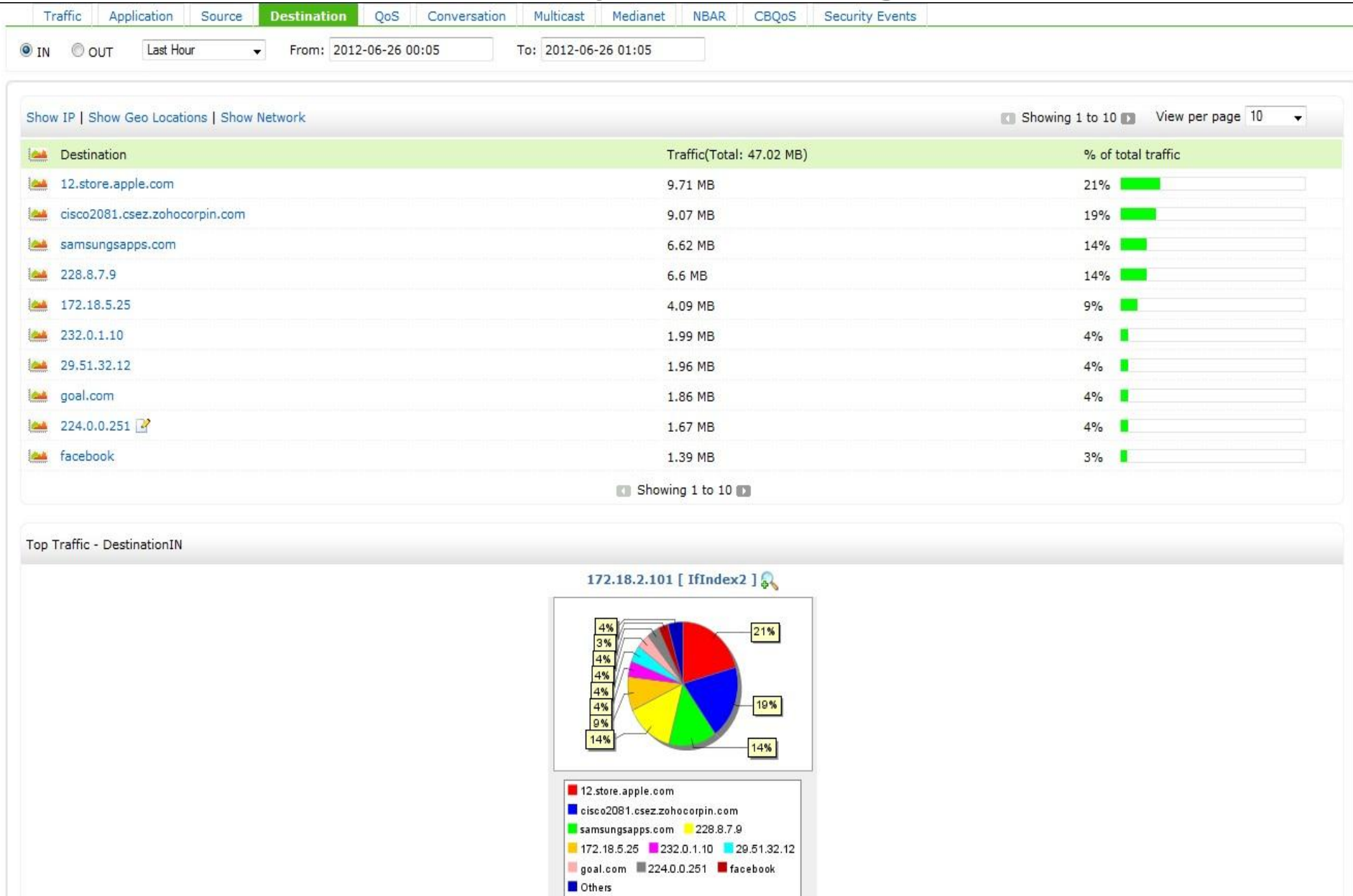
vijaya-0343.csez.zohocorpin.com

binoy-1362.csez.zohocorpin.com

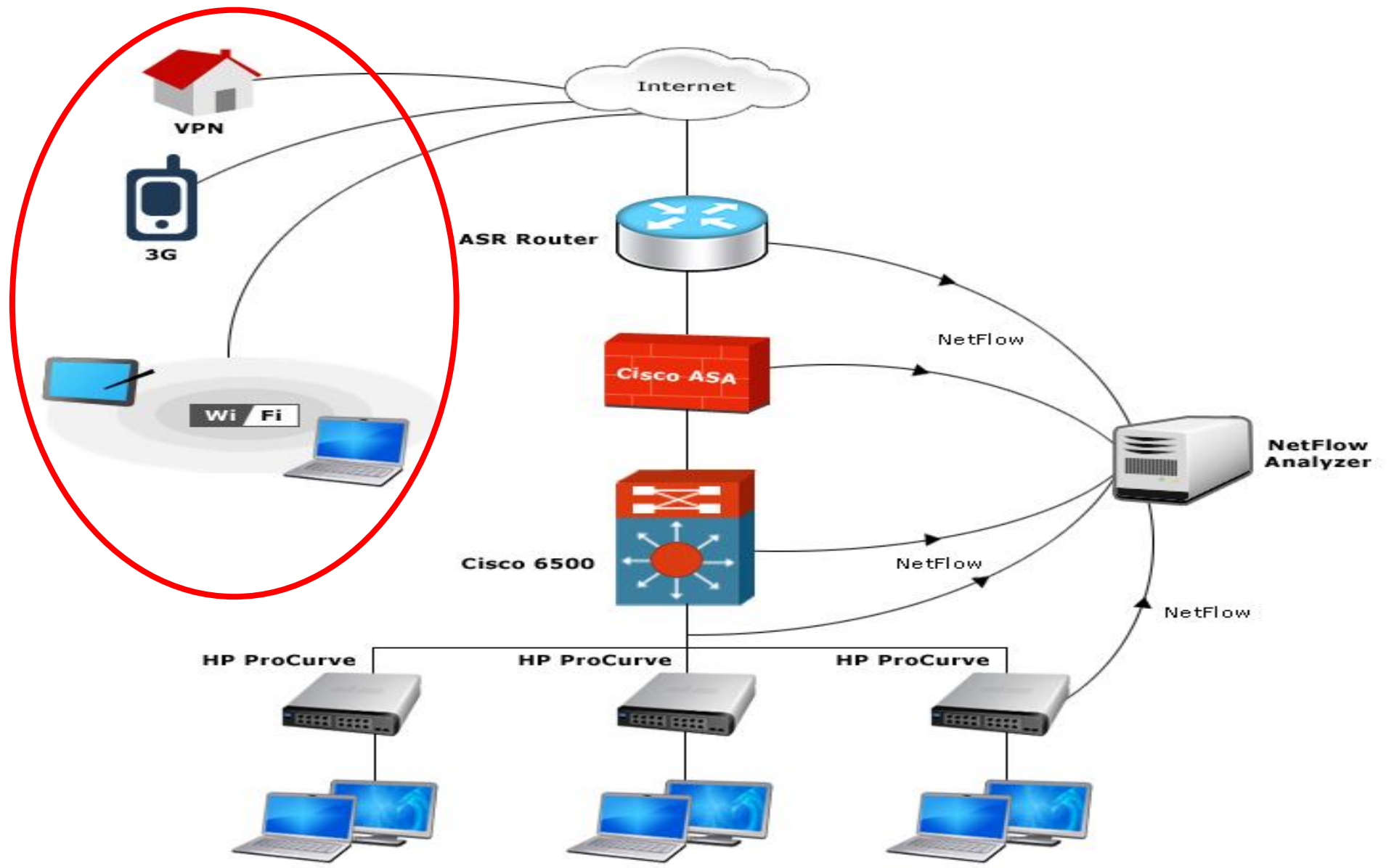
172.18.2.206

Less than 948.51 KB

# In-Depth Tracking



# Where is the Network Perimeter





## Where is the Network Perimeter

- Vanishing network perimeter – Increase in telecommuting and hence more remote connections with BYOD
- Stolen mobile devices or malware infected devices can be used to connect to the enterprise network over VPN
- Flow export supported by all major firewalls and routers
- Use NetFlow data to see which device is connecting over tunnels and where the traffic is headed



# Where is the Network Perimeter

Application | Application Groups | Top Sites

Protocol Distribution | Showing 1 to 41 | View per page 50

Application	Traffic(Total: 154.54 MB)	% of total traffic
Unknown_App [ Show Ports ]	70.97 MB	46% <div></div>
ESP Traffic	25.11 MB	16% <div></div>
GRE	16.3 MB	11% <div></div>
icmp	7.97 MB	5% <div></div>
ssdp	6.87 MB	4% <div></div>
mdns	6.36 MB	4% <div></div>
bootps	4.79 MB	3% <div></div>
netbios-dgm	4.7 MB	3% <div></div>
llmnr	3.07 MB	2% <div></div>
cslistener	1.84 MB	1% <div></div>

## New-Age Malwares

- BYOD growth = Increase in malwares targeting mobile devices
- Most new malwares are zero day based - No signature for IDS or IPS to identify and stop the malwares
- Infected devices are sometimes physically carried into the network after being infected from elsewhere
- IDS and IPS in the internal network is not feasible due to costs
- Network traffic behavior analysis can help with anomaly detection

# New-Age Malwares

2011

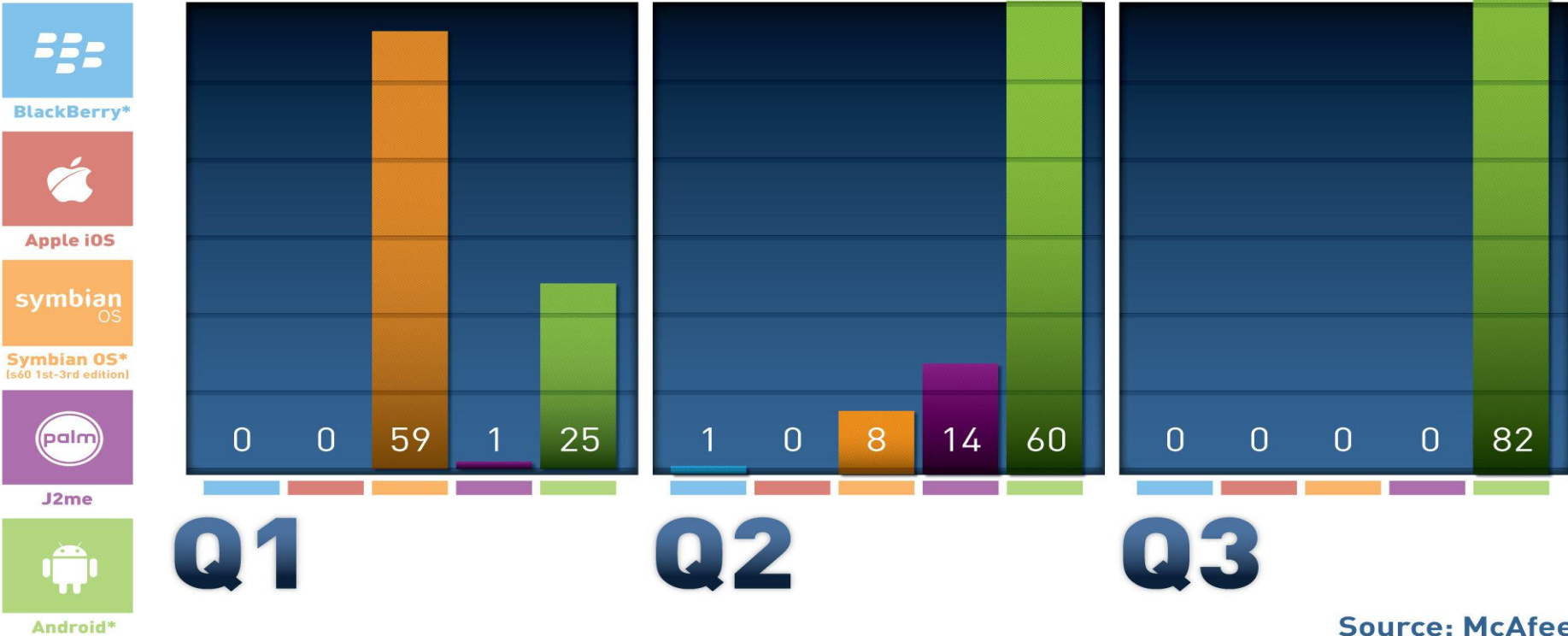
IS SHAPING

up to be

THE YEAR OF MOBILE MALWARE

McAfee's Q3 2011 Threats report shows Android operating system became the exclusive target for all new mobile malware

The amount of malware targeted at Android devices jumped more than **37%** since last quarter to become the most attacked mobile operating system, and puts 2011 on track to be the busiest in mobile and general malware history.



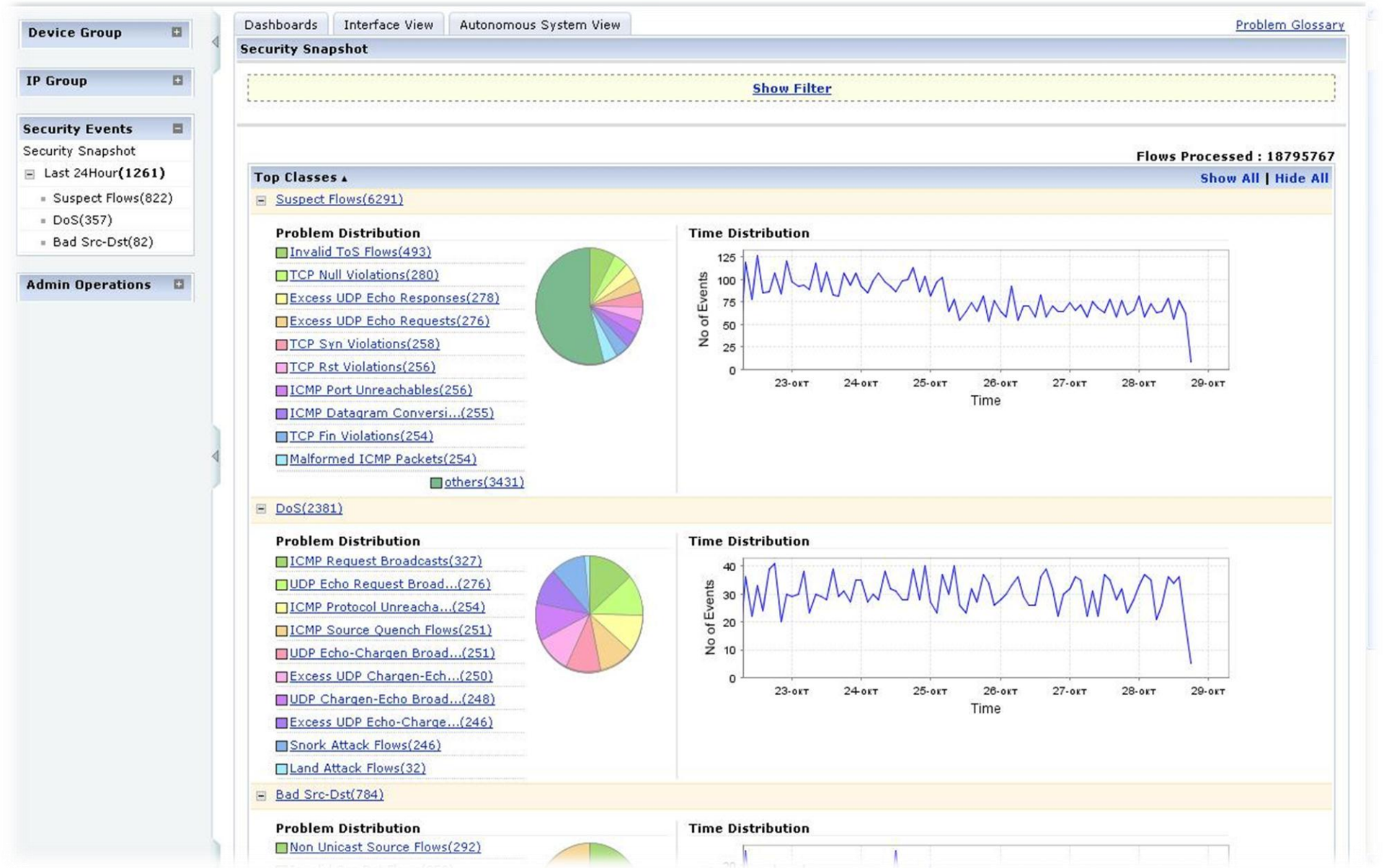
Source: McAfee

\*Includes variants identified after the publishing of McAfee's Q2 Threat Report

## New-Age Malwares

- NetFlow packets holds granular information on IP traffic behavior
- ManageEngine NetFlow Analyzer's has **Advanced Security Analytics Module** (ASAM)
- ASAM leverages on the already exported NetFlow or sFlow data for behavior anomaly detection
- Real time threat detection using **Continuous Stream Mining Engine** technology
- Threats that surpass your IDS and other traditional security systems can be detected
- Anomaly classification based on Offender, Target, Path and Problem

# New-Age Malwares





# New-Age Malwares

White List ▾

Manage ▾

Algorithm Settings ▾

Location ▾

More Actions ▾

Show DNS

Flows Processed : 120459588

Report Details

1 - 25

Per Page : 25

<input type="checkbox"/>	ID	Problem	Offender(s)	Routed via	Target(s)	Time▲	Hits			
<input type="checkbox"/>	136785	Scans / Probes - Empty TCP Diagonal Scan	NA 1: [192.168.1.160]	1: [192.168.1.16 (IfIndex2)]	NA 16: [192.168.5.145, 192.168.5.146, 192.168.5.147, 192.168.5.148, 192.168....	2011-07-29 16:37:45 -- 2011-07-29 16:37:53	16			<a href="#">View</a>
<input type="checkbox"/>	136784	Scans / Probes - Empty TCP Diagonal Scan	NA 1: [192.168.1.132]	1: [192.168.1.16 (IfIndex2)]	NA 16: [192.168.5.144, 192.168.5.145, 192.168.5.146, 192.168.5.152, 192.168....	2011-07-29 16:37:45 -- 2011-07-29 16:37:53	16			<a href="#">View</a>
<input type="checkbox"/>	136783	Scans / Probes - Empty TCP Diagonal Scan	NA 1: [192.168.1.160]	1: [192.168.1.16 (IfIndex2)]	NA 16: [192.168.5.145, 192.168.5.146, 192.168.5.147, 192.168.5.148, 192.168....	2011-07-29 16:30:01 -- 2011-07-29 16:30:08	16			<a href="#">View</a>
<input type="checkbox"/>	136782	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.189]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	90			<a href="#">View</a>
<input type="checkbox"/>	136781	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.188]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	92			<a href="#">View</a>
<input type="checkbox"/>	136779	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.186]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	89			<a href="#">View</a>
<input type="checkbox"/>	136780	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.187]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	94			<a href="#">View</a>
<input type="checkbox"/>	136778	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.185]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	92			<a href="#">View</a>
<input type="checkbox"/>	136777	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.184]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	94			<a href="#">View</a>
<input type="checkbox"/>	136776	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.183]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	92			<a href="#">View</a>
<input type="checkbox"/>	136775	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.182]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	89			<a href="#">View</a>
<input type="checkbox"/>	136773	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.180]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	87			<a href="#">View</a>
<input type="checkbox"/>	136774	Scans / Probes - Short TCP Rst_Ack Port...	NA 10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168....	1: [192.168.1.16 (IfIndex2)]	NA 1: [192.168.6.181]	2011-07-29 16:26:27 -- 2011-07-29 16:27:09	90			<a href="#">View</a>

# New-Age Malwares

Event Id : 305677    Problem : Short TCP Rst_Ack Port Scan		More Info
Field	Value	
Volume	3.57 KB	
Packets	85	
Hits	85	
Unique Source IPs	10: [192.168.4.234, 192.168.4.235, 192.168.4.236, 192.168.4.237, 192.168.4.238, 192.168.4.239, 192.168.4.240, 192.168.4.241, 192.168.4.242, 192.168.4.243]	
Unique Destination IPs	1: [192.168.6.93]	
Unique Source Networks	1: [192.168.4.0/24]	
Unique Destination Networks	1: [192.168.6.0/24]	
Unique Source Ports	85: [11, 12, 13, 14, 15, 16, 18, 19, 20, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 41, 42, 43, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 56, 57, 59, 60, 61, 62, 63, 64, 65, 68, 69, 70, 72, 73, 74, 75, 77, 78, 79, 80, 81, 82, 83, 85...]	
Unique Destination Ports	85: [211, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 239, 240, 241, 243, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 256, 258, 259, 261, 262, 263, 264, 265, 267, 2...]	
Unique Applications	79: [systat, daytime, msp, chargen, ftp-data, ssh, telnet, smtp, nsw-fe, msg-icp, msg-auth, dsp, rap, rip, graphics, name, nickname, mpm, mpm-snd, ni-ftp, auditd, tacacs, re-mail-ck, la-maint, xns-time, domain, xns-ch, xns-auth, ni-mail, acas, whois++,...]	
Unique TCP Flags	1: [_A_R_]	
Unique Protocols	1: [TCP]	
Unique ToS Values	1: [2]	
Unique In Interfaces (Routed Via)	1: [Cisco ASR (IfIndex2)]	
Unique Out Interfaces	1: [Cisco ASR (IfIndex4)]	
Unique Connections	85: [TCP: 192.168.4.234-72--192.168.6.93-217,TCP: 192.168.4.234-73--192.168.6.93-227,TCP: 192.168.4.234-74--192.168.6.93-237,TCP: 192.168.4.234-75--192.168.6.93-247,TCP: 192.168.4.234-77--192.168.6.93-267,TCP: 192.168.4.234-78--192.168.6.93-277,TCP: 192.1 ...Expand	
Unique Router IPs	1 Router(s) • Cisco ASR(127.0.0.1)	

# Conclusion

- **MDM is Evolving – Hold the high-cost investment**
  - Not multi-platform - Apple, Android, Blackberry, Symbian
  - Support for new technologies - IPv6, mobile apps
  - Many solutions are basic - Need to evolve a lot more
- **Security and monitoring most important aspects of BYOD**
- **Leverage on default or low cost technologies like NetFlow**
- **Most Important - Educate users**
  - Why security is more important than the fancy screensaver
  - Why bandwidth is important for the organization



# Questions?

**ManageEngine NetFlow Analyzer is used by over 4000 customers worldwide**

[www.netflowanalyzer.com](http://www.netflowanalyzer.com)

NetFlow Analyzer Blogs:

<https://blogs.netflowanalyzer.com>

User Forums:

<http://forums.netflowanalyzer.com>

LinkedIn:

[http://www.linkedin.com/groups?gid=4208806&trk=hb\\_side\\_g](http://www.linkedin.com/groups?gid=4208806&trk=hb_side_g)

TAC Team:

[netflowanalyzer-support@manageengine.com](mailto:netflowanalyzer-support@manageengine.com)

ManageEngine Sales:

[sales@manageengine.com](mailto:sales@manageengine.com)