FOCUS 12
SECURITY CONFERENCE

SECURITY MANAGEMENT: THE GPS OF SECURITY

Deep Dive - Operationalizing Security

Sean Slattery
Caribbean
Solutions Lab

Dennis London
London Security
Solutions

Chris Laasch
Cal Poly Pomona

January 23, 2013

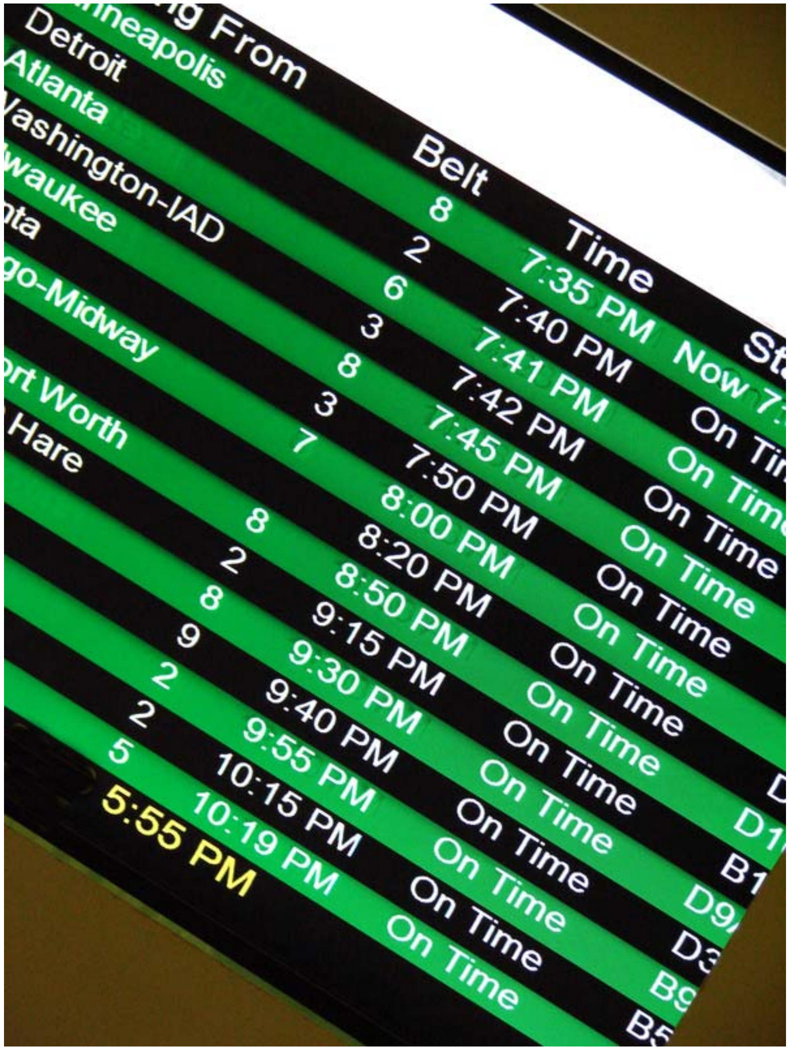
McAfee
An Intel Company

Objectives

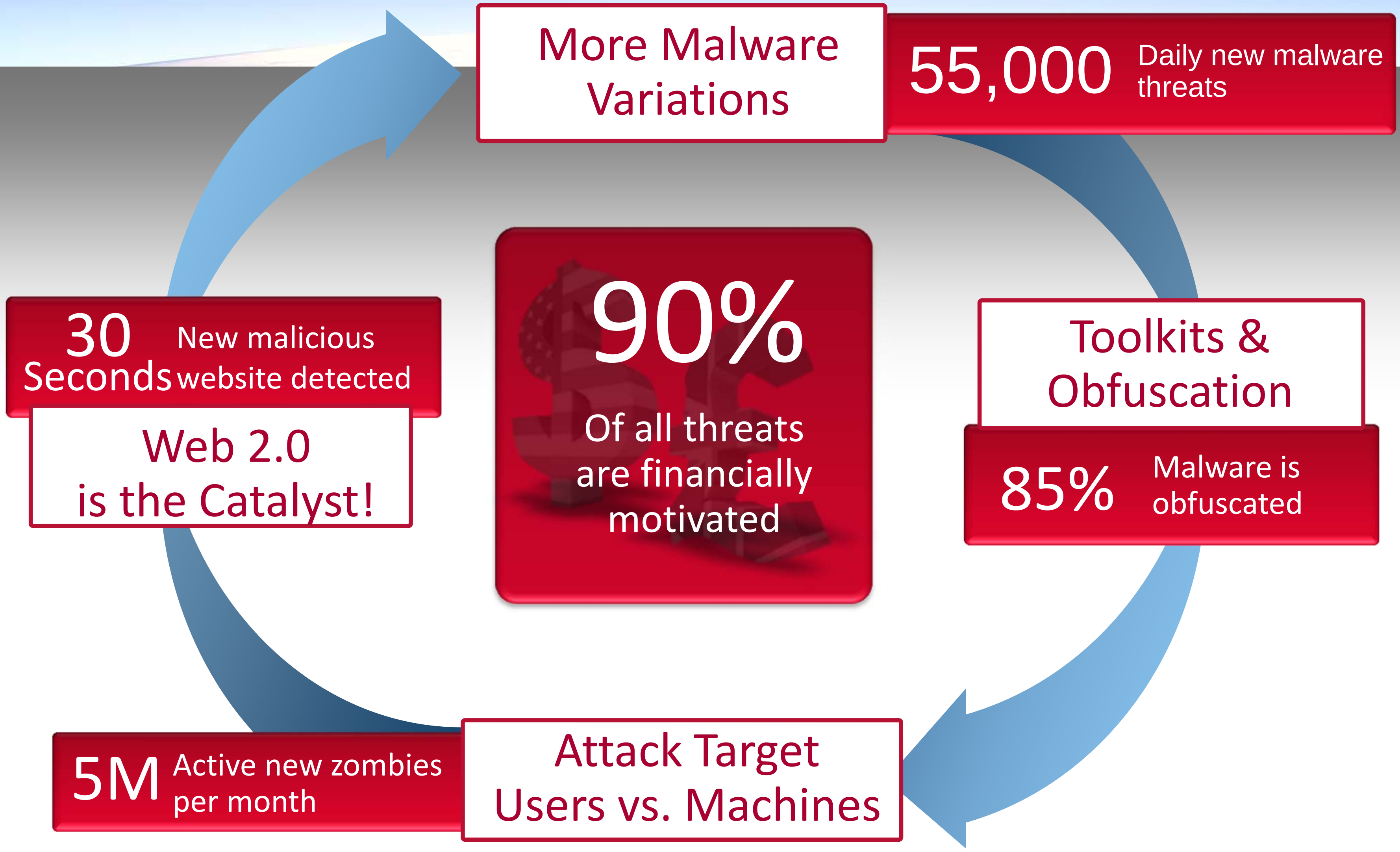
- To give you practical guidance to be more effective and efficient
- Provide you with insight into what is happening in your environment
- Hopefully teach you a new technique or function which you can immediately use upon returning

Need to Know

- Where am I?
- Where am I going?
- How am I going to get there?



Today’s Security Landscape



More Malware Variations

55,000 Daily new malware threats

Toolkits & Obfuscation

85% Malware is obfuscated

Attack Target Users vs. Machines

5M Active new zombies per month

30 Seconds New malicious website detected

Web 2.0 is the Catalyst!

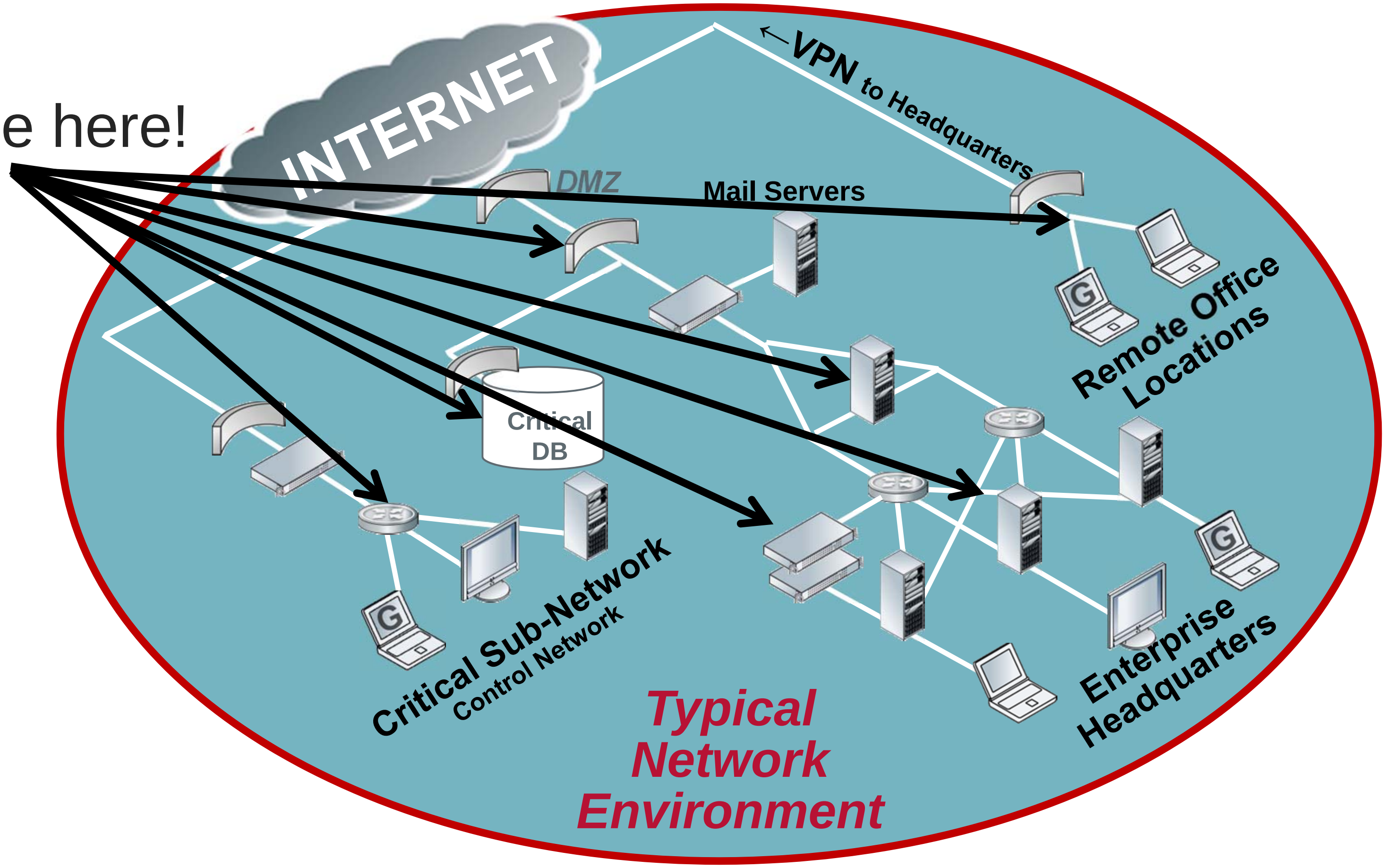
90% Of all threats are financially motivated

Security = Management

What do we need to manage?

Where am I?

You are here!



Change Happens

The threats are evolving and so must our approach.

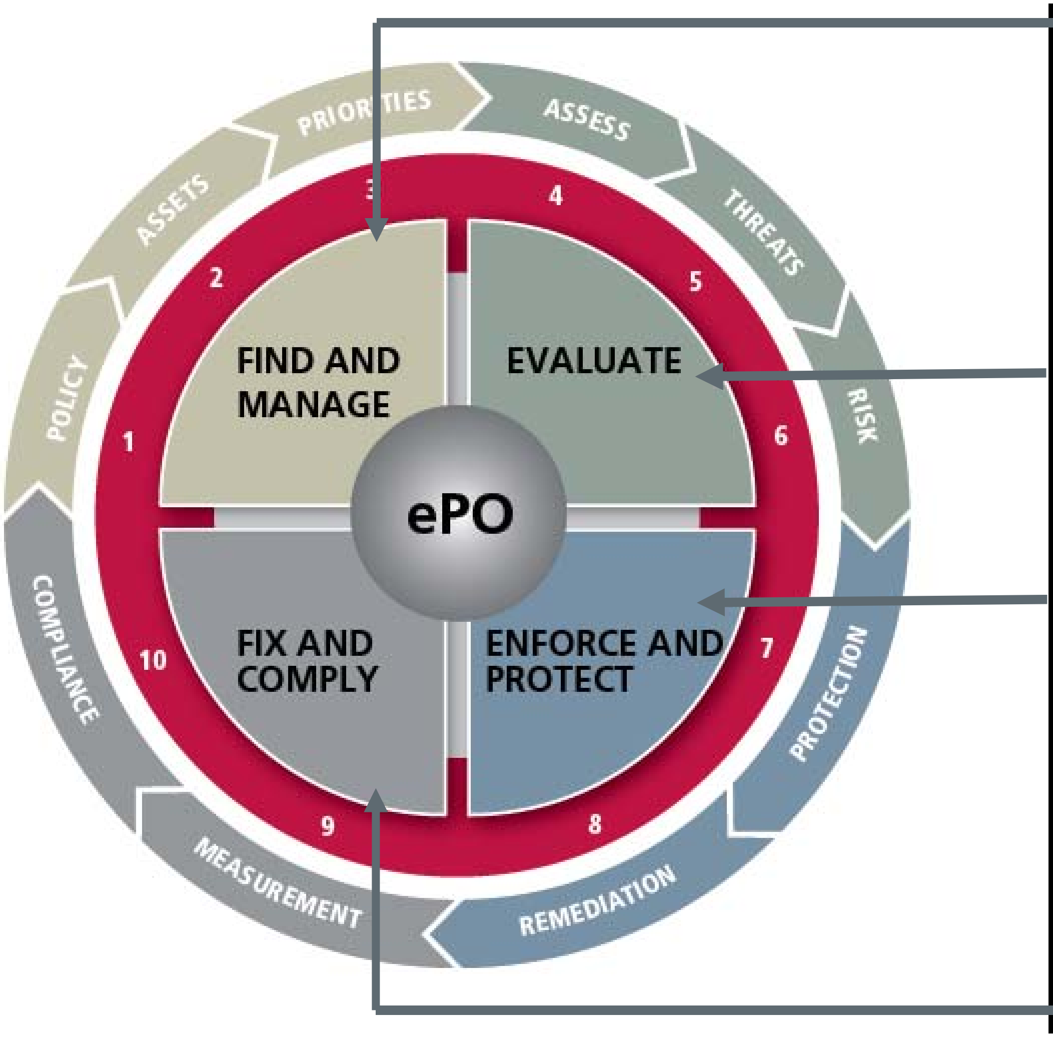
Where am I going?

Give the **hardest job** to the **laziest person** and they'll find the easiest way to do it!

How am I getting there?

Security is a continual process

FOCUS12 SECURITY CONFERENCE



Identify & group assets	• Machine import • Machine discovery • Rogue detection
Determine risk	• Infection reporting • Measure vulnerability • Notification
Protect and block	• Configuration • Enforcement • Maintenance
Measure compliance	• Coverage reporting • Compliance reporting • System compliance • McAfee NAC

How am I getting there?

Consider CIA

FOCUS 12 SECURITY CONFERENCE

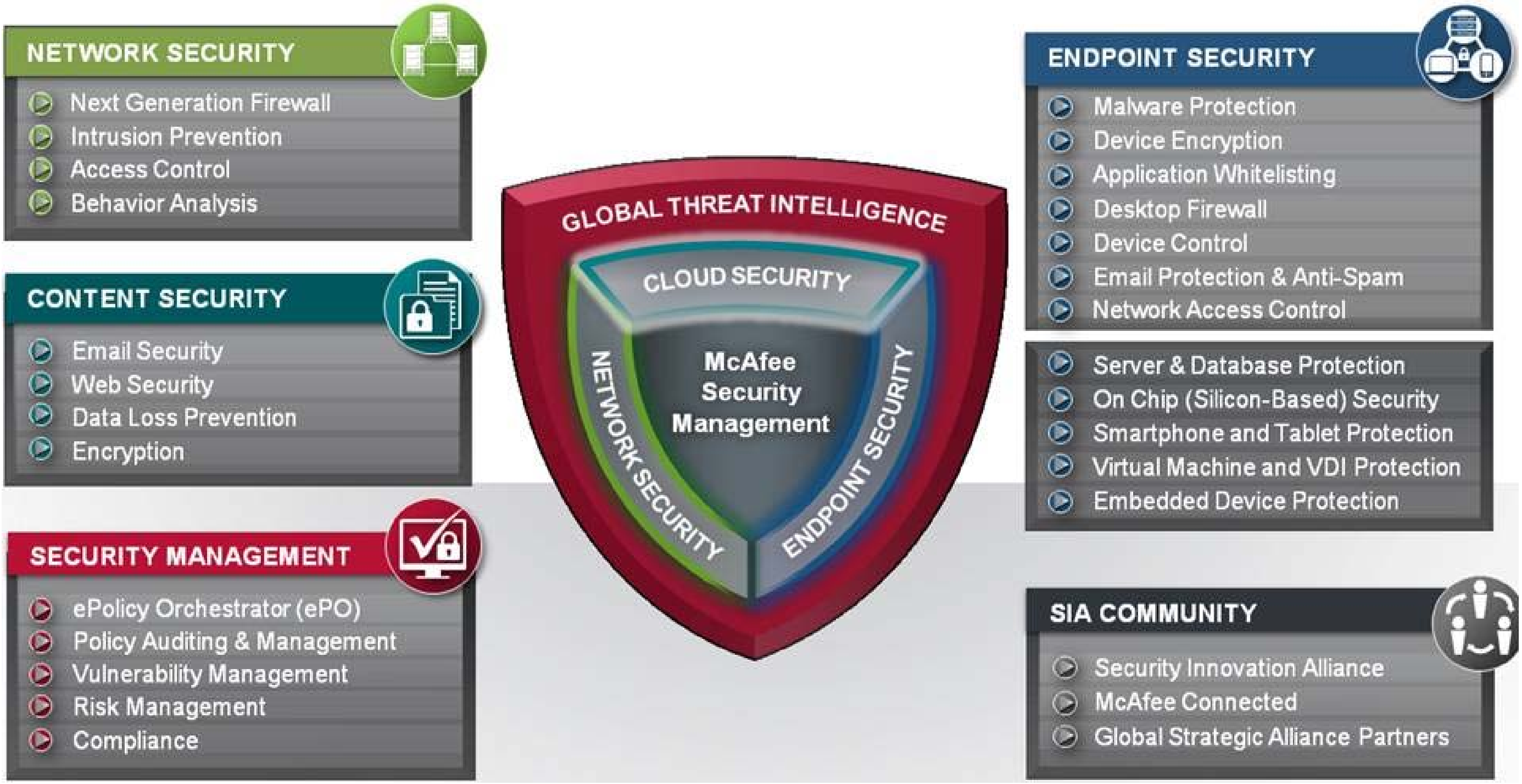
- C – Correlation
- I – Integration
- A – Automation

Let’s take a leaf out of Apple’s book in terms of integration.

Our people, processes and technology to work together

FOCUS12 SECURITY CONFERENCE

McAfee Security Connected



NETWORK SECURITY

- Next Generation Firewall
- Intrusion Prevention
- Access Control
- Behavior Analysis

CONTENT SECURITY

- Email Security
- Web Security
- Data Loss Prevention
- Encryption

SECURITY MANAGEMENT

- ePolicy Orchestrator (ePO)
- Policy Auditing & Management
- Vulnerability Management
- Risk Management
- Compliance

ENDPOINT SECURITY

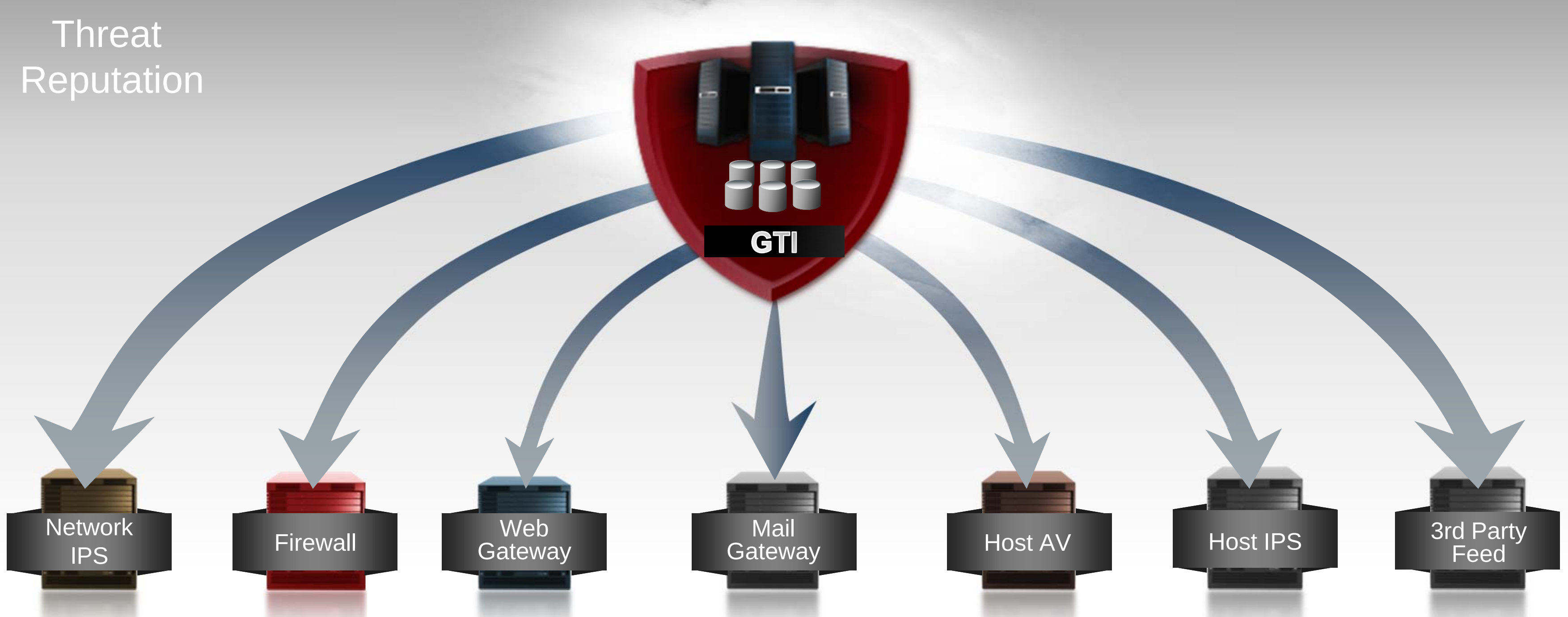
- Malware Protection
- Device Encryption
- Application Whitelisting
- Desktop Firewall
- Device Control
- Email Protection & Anti-Spam
- Network Access Control

- Server & Database Protection
- On Chip (Silicon-Based) Security
- Smartphone and Tablet Protection
- Virtual Machine and VDI Protection
- Embedded Device Protection

SIA COMMUNITY

- Security Innovation Alliance
- McAfee Connected
- Global Strategic Alliance Partners

Global Threat Intelligence



300M IPS Attacks/Mo.

300M IPS Attacks/Mo.

2B Botnet C&C IP Reputation Queries/Mo.

20B Message Reputation Queries/Mo.

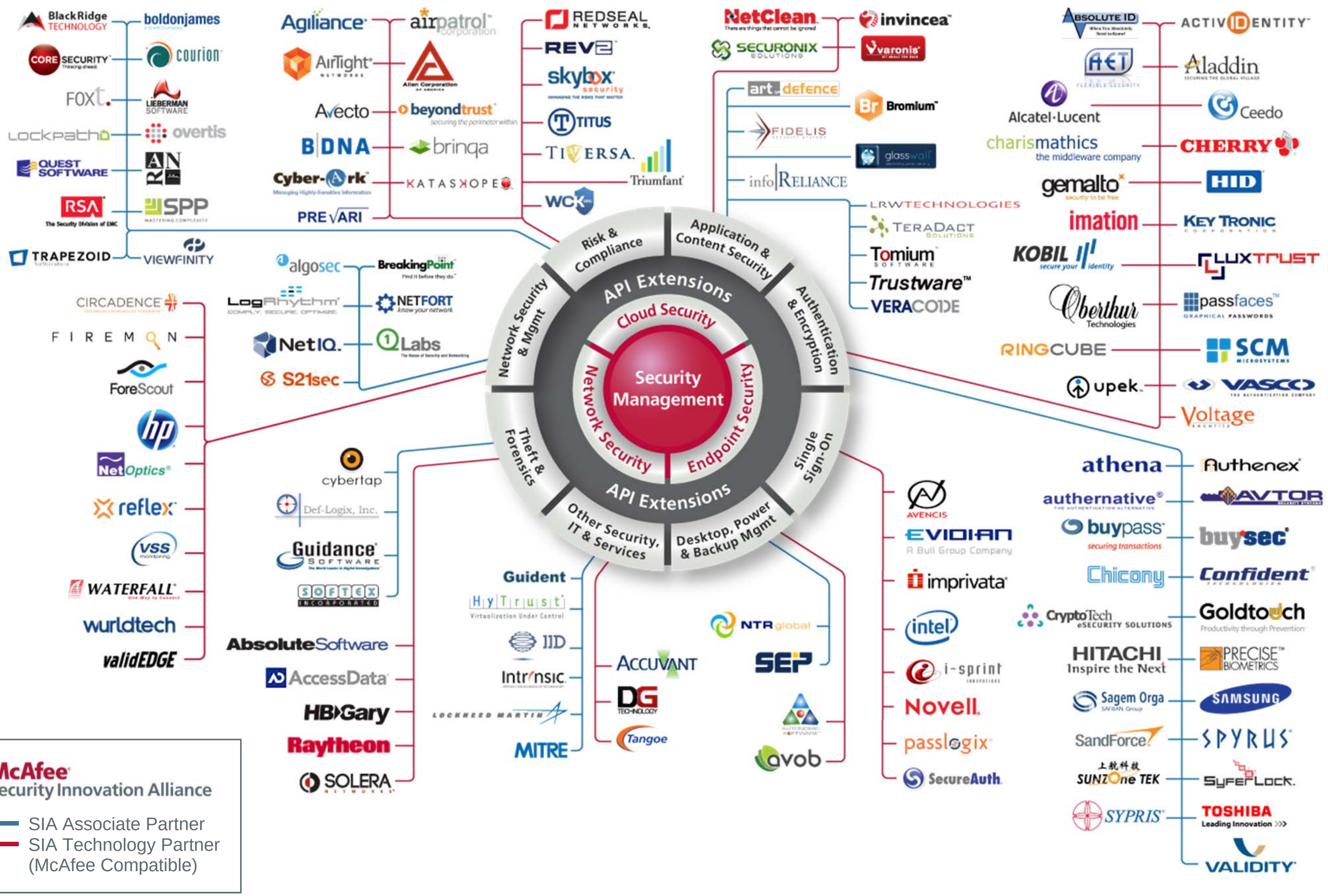
2.5B Malware Reputation Queries/Mo.

300M IPS Attacks/Mo.

Geo Location Feeds

McAfee's Extensible Platform for Security Risk Management

FOCUS12 SECURITY CONFERENCE



McAfee Security Innovation Alliance

SIA Associate Partner

SIA Technology Partner (McAfee Compatible)

Waypoints

- ePolicy Orchestrator
- VirusScan Enterprise 8.8
- Host IPS 8
- Web Security (Endpoint and Gateway)
- Device Control
- Trust Control Suite (Cloud)

Use Case #1
Actionable Intelligence

FOCUS 12 SECURITY CONFERENCE

- Challenge: Customer happily showed me a clean ePO console i.e. not a single event and was quite pleased. Yet they allowed uncontrolled removable media and Internet access and had never audited their environment.

- Solution:
  - Install VSE on ePO server, along with VSE patch and reboot
  - Discover that environment was full of malware. ePO had lost connectivity with database over three months earlier
  - Deploy Web Filtering for Endpoints, Device Control and Host IPS 8

Sometimes a lack of data can be actionable too!

Develop a plan to periodically audit and test your environment. Use www.csm-testcenter.org which has structured tests for web, antivirus, network and data.

McAfee ePolicy Orchestrator

Tags

- System Tags are virtual labels useful in management and reporting
- Manually assigned vs Criteria based
- Some Available Properties are:

Agent Handler
Custom 1, 2, 3, 4
Free system drive space
IP Address
Is Laptop

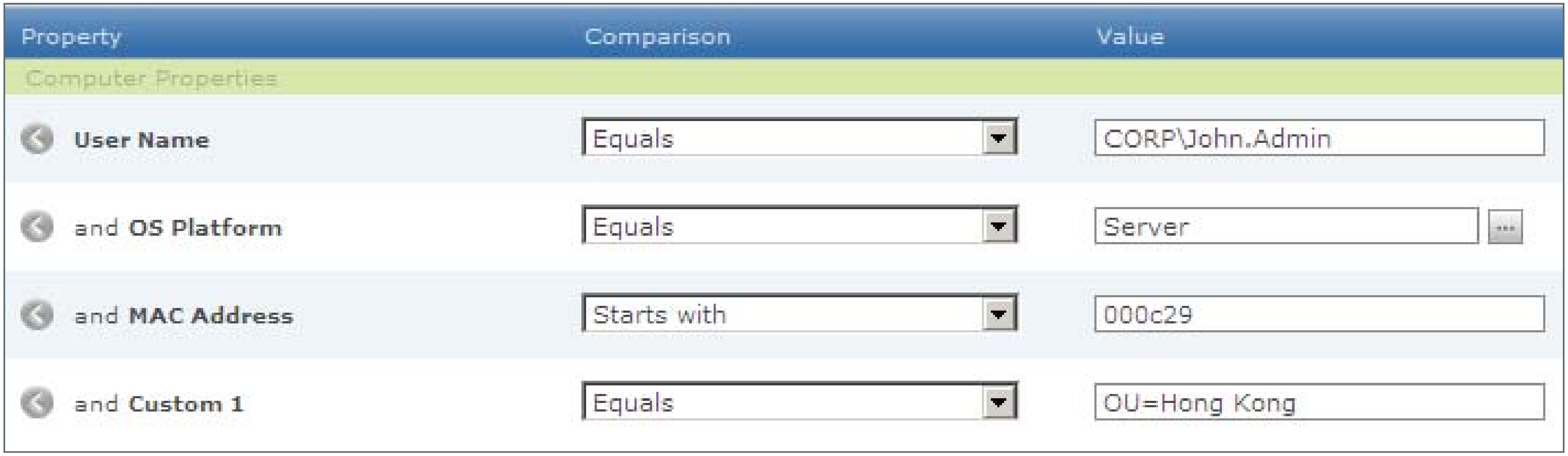
MAC Address
OS Platform
Service Pack
Total Physical Memory
User

Policy Assignment Rules can apply a policy to all systems with a certain tag e.g. Pilot, regardless of System Tree location

McAfee ePolicy Orchestrator

Tags

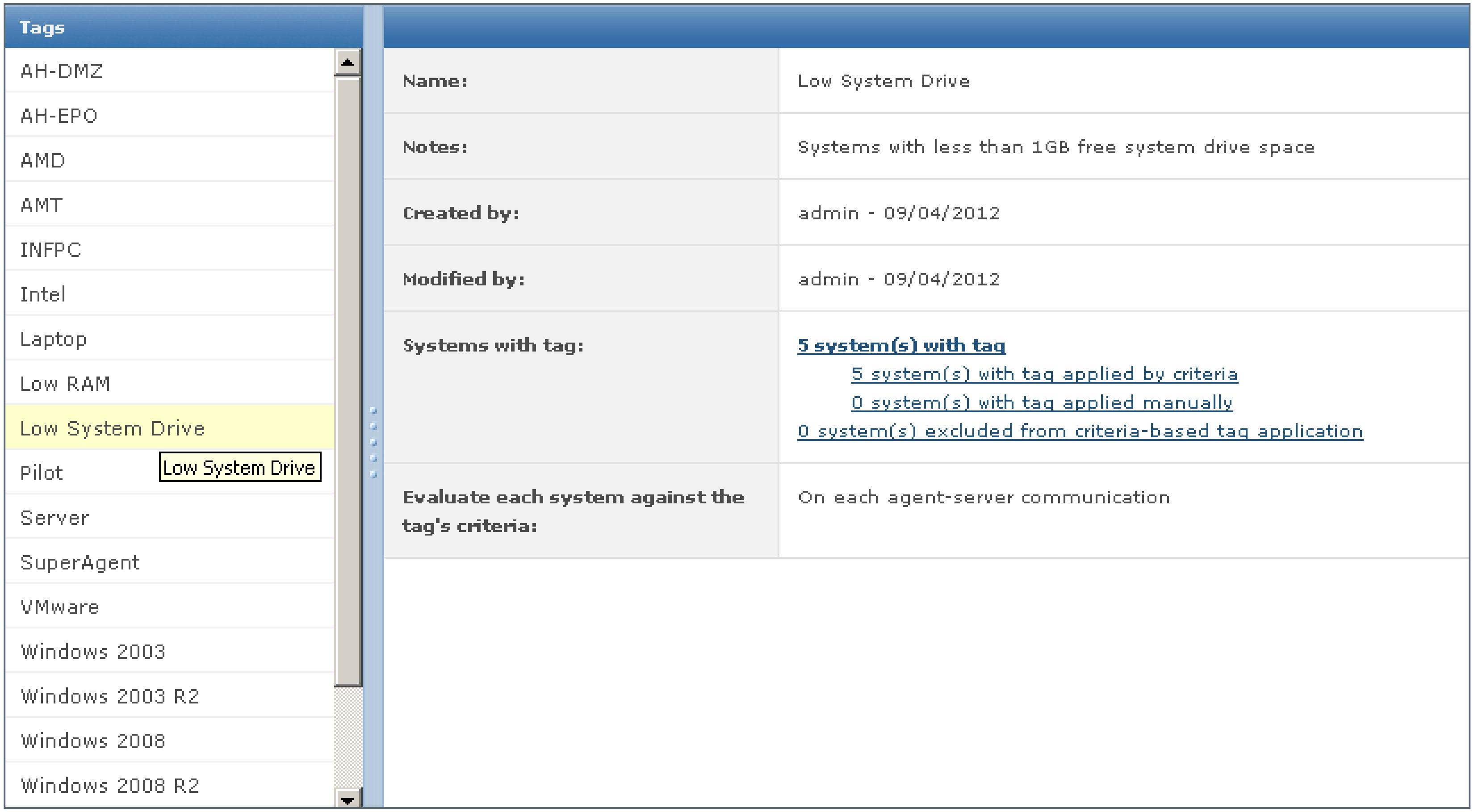
Building a criteria based tag:



Property	Comparison	Value
Computer Properties		
User Name	Equals	CORP\John.Admin
and OS Platform	Equals	Server
and MAC Address	Starts with	000c29
and Custom 1	Equals	OU=Hong Kong

Automatically tag high-risk or suspicious systems for additional monitoring or stricter policies

McAfee ePolicy Orchestrator
Tags



Tags

- AH-DMZ
- AH-EPO
- AMD
- AMT
- INFPC
- Intel
- Laptop
- Low RAM
- Low System Drive
- Pilot
- Server
- SuperAgent
- VMware
- Windows 2003
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2

Name:	Low System Drive
Notes:	Systems with less than 1GB free system drive space
Created by:	admin - 09/04/2012
Modified by:	admin - 09/04/2012
Systems with tag:	**5 system(s) with tag** 5 system(s) with tag applied by criteria 0 system(s) with tag applied manually 0 system(s) excluded from criteria-based tag application
Evaluate each system against the tag's criteria:	On each agent-server communication

Use Case #2
Tagging for PCI Compliance

- Challenges – meet PCI compliance standards:
  - Use a firewall between the public network and the payment card data. Keep the firewall updated.
  - Use AV software on all machines and ensure that the software is updated.
  - Monitor all access to the network and cardholder data environment.
  - Regularly test your security systems and your network environment.

- Solution: Key is Auditable, Viewable and Actionable
  - Tagged PCI devices are automatically moved based on IP address
  - HIPS = second layer firewall with addition of GTI protection. Monitors access and alerts when the primary firewall is not behaving
  - Daily email status summary executive summary. Detection of rogue systems, GTI/HIPS alerts, AV alerts.
  - Weekly Vulnerability Scan summary of clients and servers.
  - Custom PCI dashboards including HIPS, AV, Site Advisor, and the McAfee Vulnerability manager.

Use Case #3

Mobility

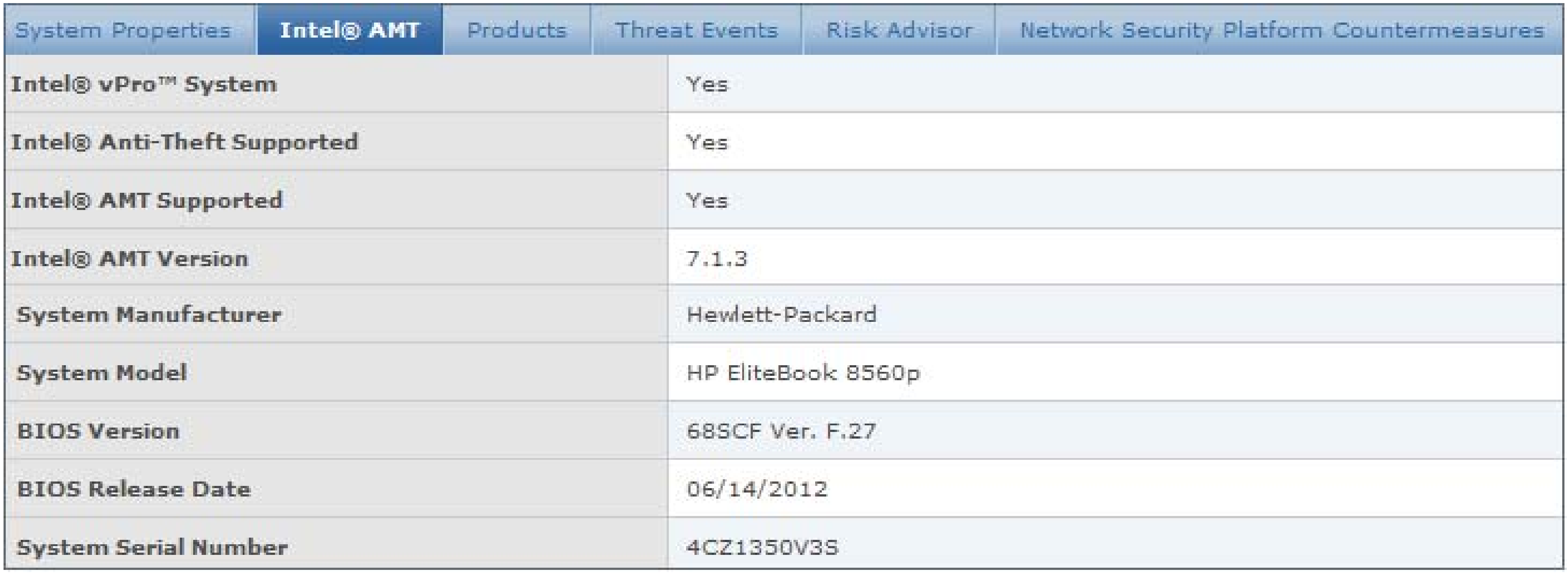
FOCUS 12 SECURITY CONFERENCE

- Challenge: Customer has a highly mobile workforce and needs to adapt policies as to when users leave the protected LAN. The requirement is to strengthen security settings when no longer behind firewalls, IPS and other gateways.

- Solution:
  - Create criteria based system tags based upon Agent Handler.
  - The DMZ Agent handler has an assignment rule only allowing access from laptops
  - The firewall rules only allow access from the Internet
  - System Tree sorting moves laptops into a Roaming group with appropriate VirusScan Enterprise, Host IPS, SiteAdvisor Enterprise, and Device Control policies applied

McAfee ePolicy Orchestrator
Deep Command Discovery Plugin

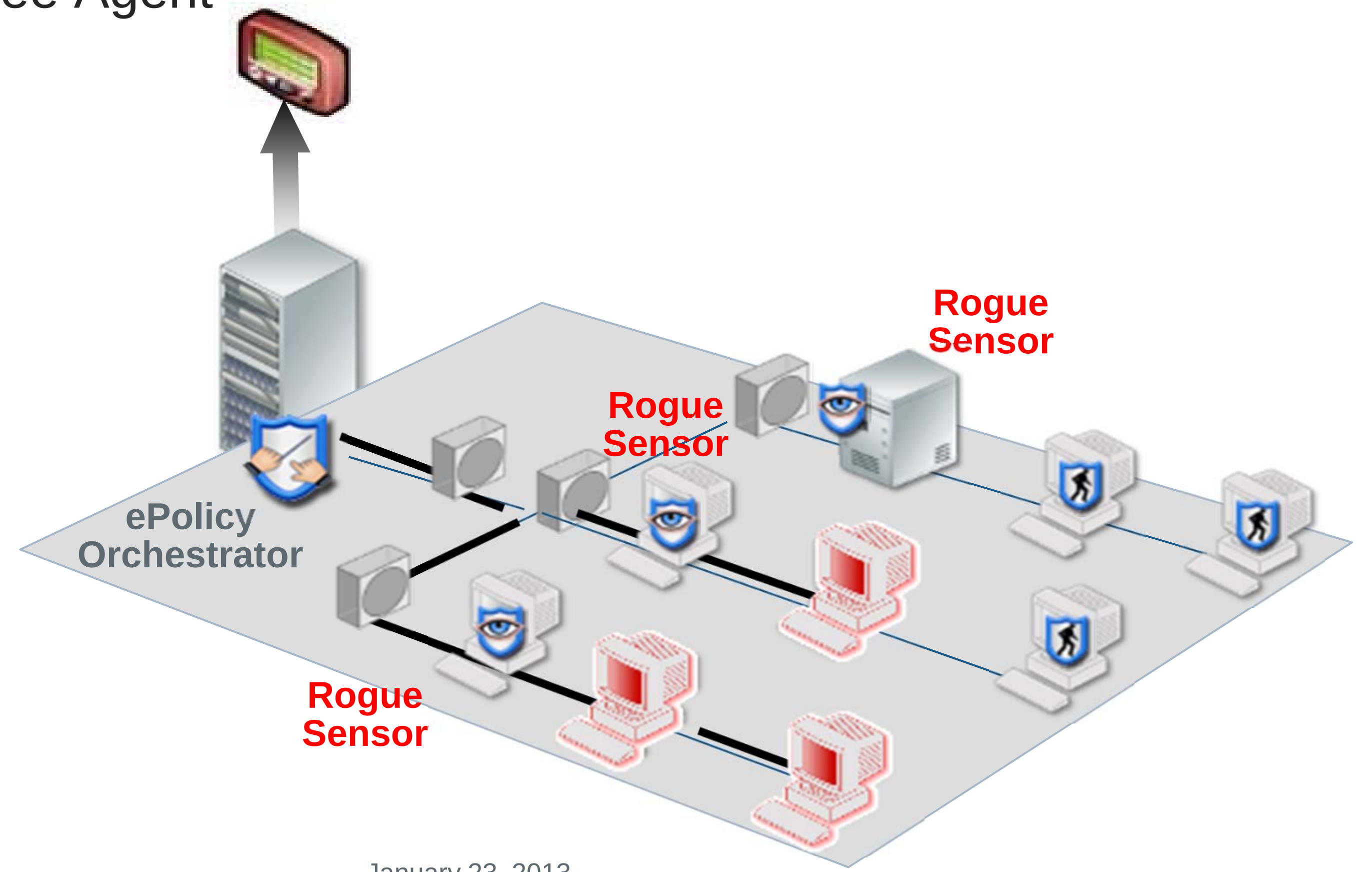
- Free Plug-In for McAfee Agent
- Reports useful hardware information including manufactoruer, model, BIOS version, and serial number



Intel® vPro™ System	Yes
Intel® Anti-Theft Supported	Yes
Intel® AMT Supported	Yes
Intel® AMT Version	7.1.3
System Manufacturer	Hewlett-Packard
System Model	HP EliteBook 8560p
BIOS Version	68SCF Ver. F.27
BIOS Release Date	06/14/2012
System Serial Number	4CZ1350V3S

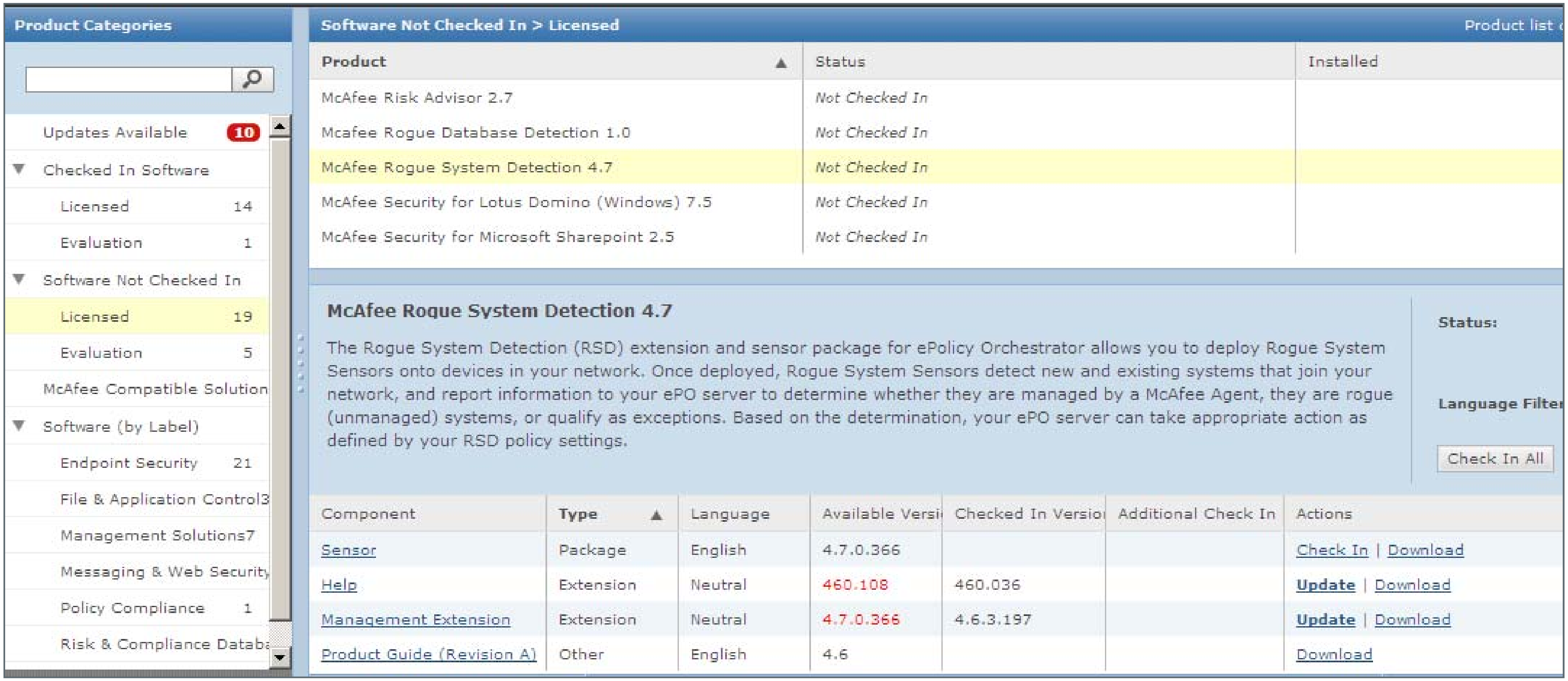
McAfee ePolicy Orchestrator
Rogue System Detection 4.7

- Rogue System Sensors are software agents that listen to network traffic relay the information to ePO for action
- Actions included Automated Responses for email notification and pushing McAfee Agent



McAfee ePolicy Orchestrator
RSD 4.7 via Software Manager

- Version 4.7 released and accessible via ePO 4.6.3 Software Manager



Product	Status	Installed
McAfee Risk Advisor 2.7	*Not Checked In*	
Mcafee Rogue Database Detection 1.0	*Not Checked In*	
McAfee Rogue System Detection 4.7	*Not Checked In*	
McAfee Security for Lotus Domino (Windows) 7.5	*Not Checked In*	
McAfee Security for Microsoft Sharepoint 2.5	*Not Checked In*	

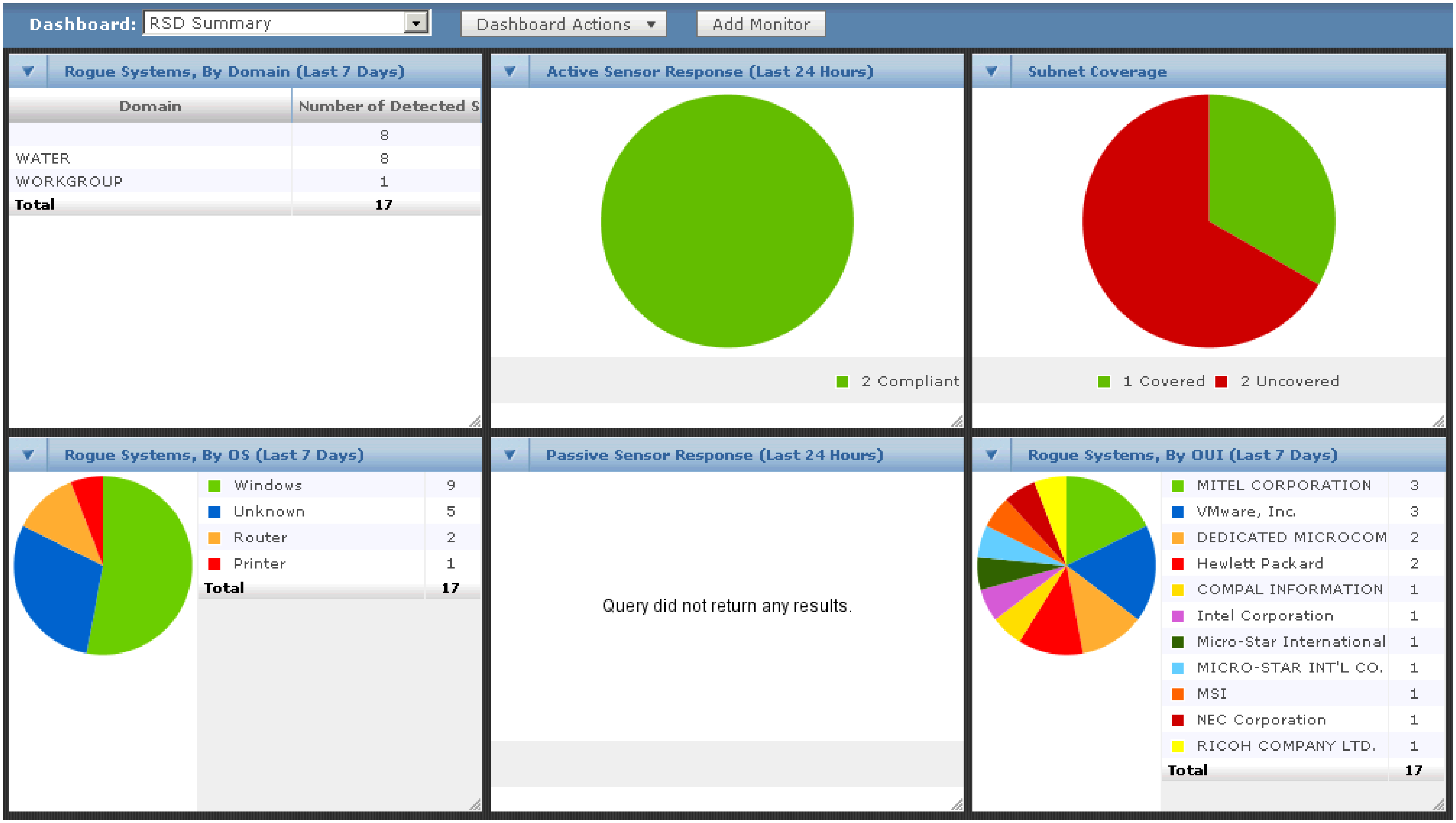
McAfee Rogue System Detection 4.7

The Rogue System Detection (RSD) extension and sensor package for ePolicy Orchestrator allows you to deploy Rogue System Sensors onto devices in your network. Once deployed, Rogue System Sensors detect new and existing systems that join your network, and report information to your ePO server to determine whether they are managed by a McAfee Agent, they are rogue (unmanaged) systems, or qualify as exceptions. Based on the determination, your ePO server can take appropriate action as defined by your RSD policy settings.

Component	Type	Language	Available Versi	Checked In Versio	Additional Check In	Actions
Sensor	Package	English	4.7.0.366			Check In | Download
Help	Extension	Neutral	460.108	460.036		**Update** | Download
Management Extension	Extension	Neutral	4.7.0.366	4.6.3.197		**Update** | Download
Product Guide (Revision A)	Other	English	4.6			Download

McAfee ePolicy Orchestrator

Rogue System Detection



Rogue Systems, By Domain (Last 7 Days)

Domain	Number of Detected S
	8
WATER	8
WORKGROUP	1
Total	**17**

Active Sensor Response (Last 24 Hours)

🟩 2 Compliant

Subnet Coverage

🟩 1 Covered 🟥 2 Uncovered

Rogue Systems, By OS (Last 7 Days)

🟩 Windows	9
🟦 Unknown	5
🟧 Router	2
🟥 Printer	1
Total	**17**

Passive Sensor Response (Last 24 Hours)

Query did not return any results.

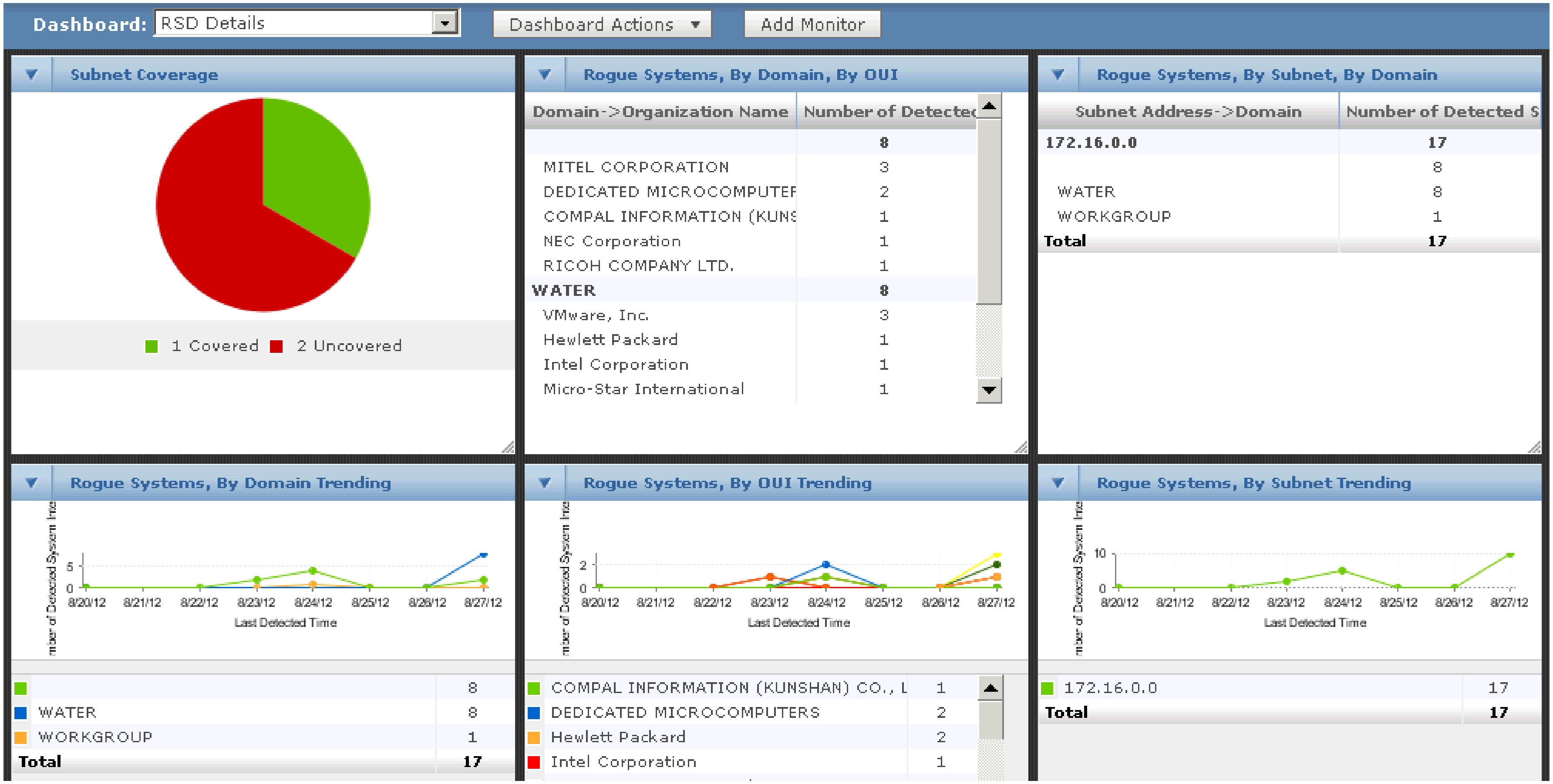
Rogue Systems, By OUI (Last 7 Days)

🟩 MITEL CORPORATION	3
🟦 VMware, Inc.	3
🟧 DEDICATED MICROCOM	2
🟥 Hewlett Packard	2
🟨 COMPAL INFORMATION	1
🟪 Intel Corporation	1
🟩 Micro-Star International	1
🟦 MICRO-STAR INT'L CO.	1
🟧 MSI	1
🟥 NEC Corporation	1
🟨 RICOH COMPANY LTD.	1
Total	**17**

McAfee ePolicy Orchestrator
Rogue System Detection

FOCUS 12 SECURITY CONFERENCE

Key variables: Subnet, Domain, Organization



Subnet Coverage

🟩 1 Covered 🟥 2 Uncovered

Rogue Systems, By Domain, By OUI

Domain->Organization Name	Number of Detectec
	8
MITEL CORPORATION	3
DEDICATED MICROCOMPUTEF	2
COMPAL INFORMATION (KUNS	1
NEC Corporation	1
RICOH COMPANY LTD.	1
WATER	**8**
VMware, Inc.	3
Hewlett Packard	1
Intel Corporation	1
Micro-Star International	1

Rogue Systems, By Subnet, By Domain

Subnet Address->Domain	Number of Detected S
172.16.0.0	**17**
	8
WATER	8
WORKGROUP	1
Total	**17**

Rogue Systems, By Domain Trending

🟩		8
🟦	WATER	8
🟧	WORKGROUP	1
	Total	**17**

Rogue Systems, By OUI Trending

🟩	COMPAL INFORMATION (KUNSHAN) CO., L	1
🟦	DEDICATED MICROCOMPUTERS	2
🟧	Hewlett Packard	2
🟥	Intel Corporation	1

Rogue Systems, By Subnet Trending

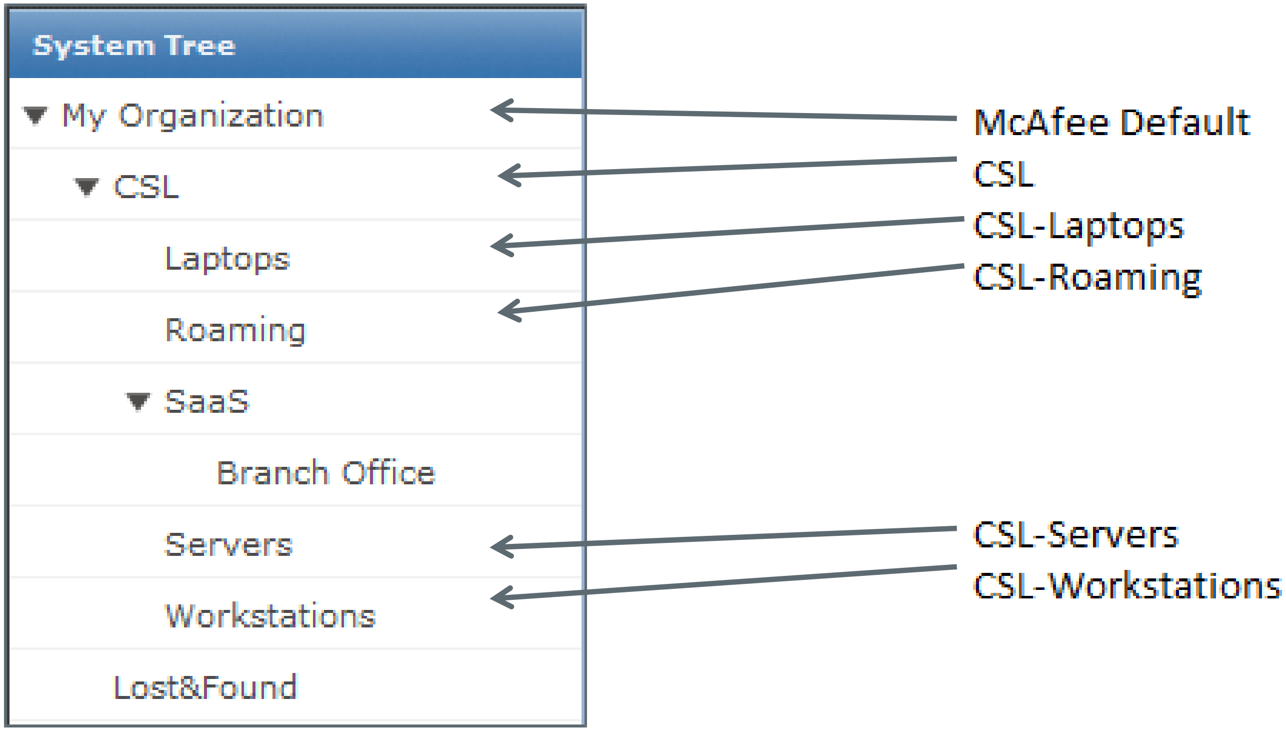
🟩	172.16.0.0	17
	Total	**17**

Update your OUIs via Server Task. Pre-filter responses for known unmanageable devices such as telephones, and printers

McAfee ePolicy Orchestrator

Policy Management

- Staff changes, server changes and rebuilds create policy sprawl.
- How can you tell all of those My Default policies apart?
- KISS – Keep it Stupid Simple



System Tree

- My Organization
  - CSL
    - Laptops
    - Roaming
    - SaaS
      - Branch Office
    - Servers
    - Workstations
  - Lost&Found

McAfee Default

CSL

CSL-Laptops

CSL-Roaming

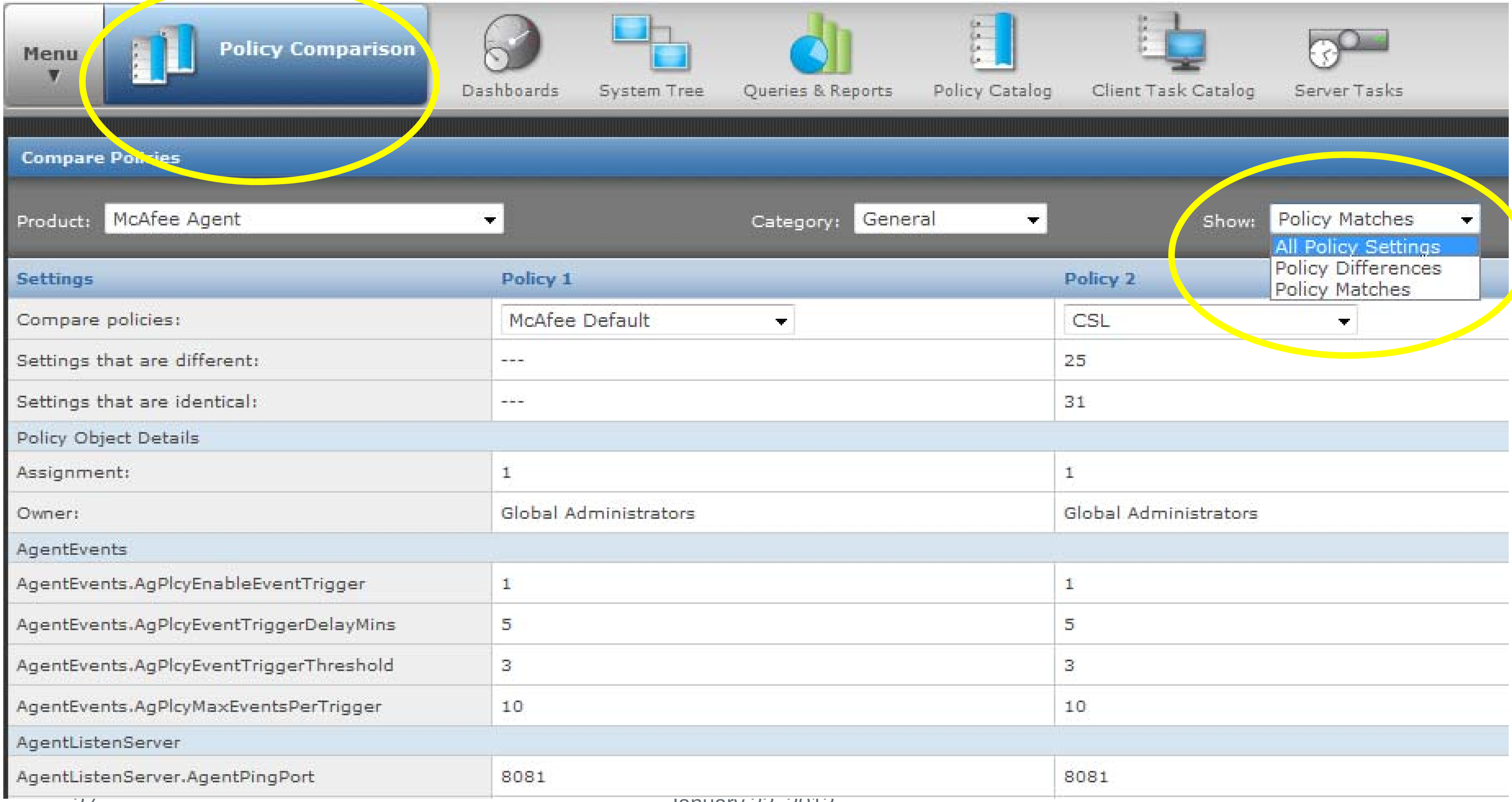
CSL-Servers

CSL-Workstations

Query for broken policy inheritance to document your tree and assignments

McAfee ePolicy Orchestrator
Policy Management

- What if there was a tool to compare and help document your policies? There is!



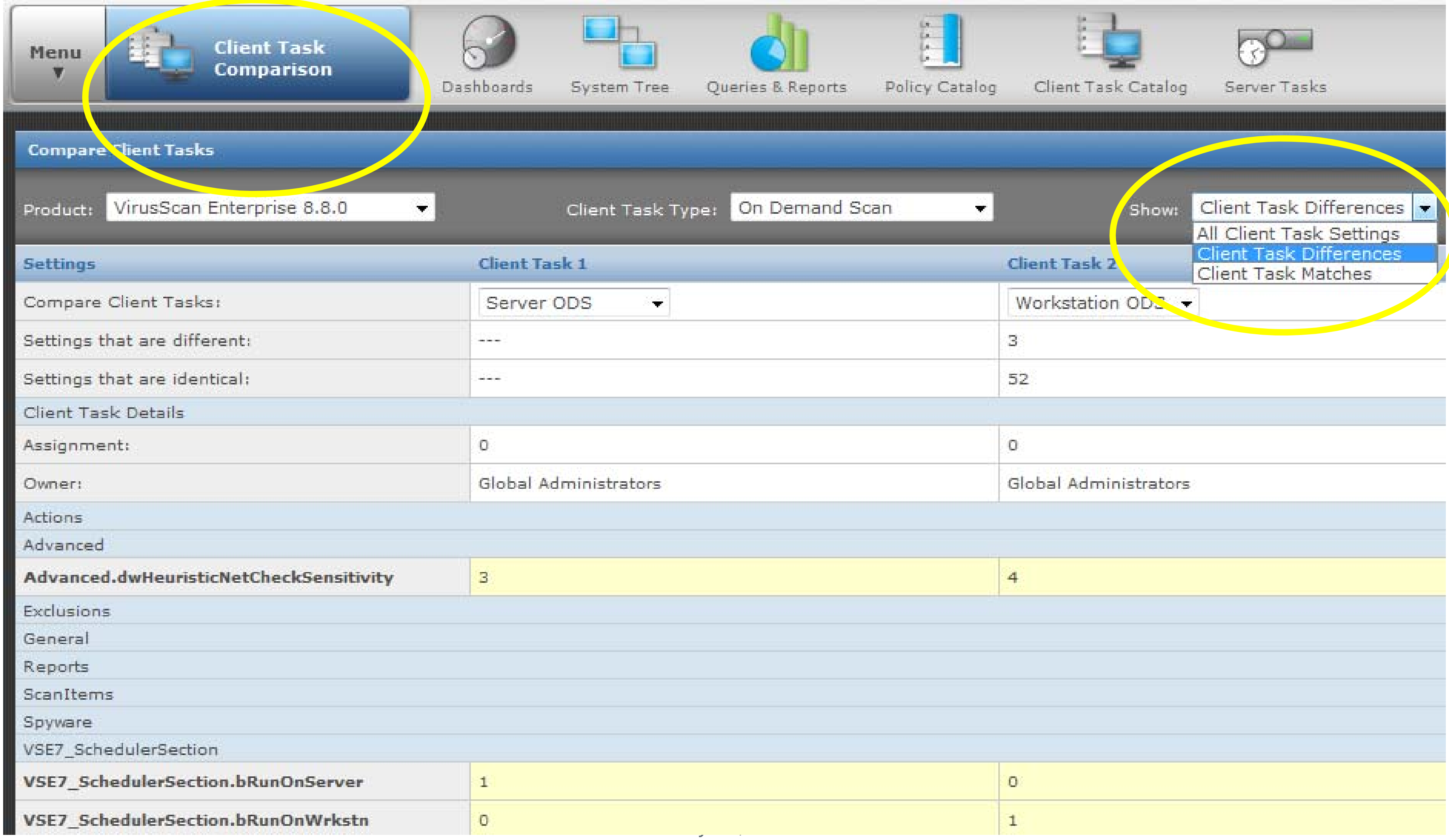
Compare Policies

Product: McAfee Agent Category: General Show: Policy Matches

Settings	Policy 1	Policy 2
Compare policies:	McAfee Default	CSL
Settings that are different:	---	25
Settings that are identical:	---	31
Policy Object Details		
Assignment:	1	1
Owner:	Global Administrators	Global Administrators
AgentEvents		
AgentEvents.AgPlcyEnableEventTrigger	1	1
AgentEvents.AgPlcyEventTriggerDelayMins	5	5
AgentEvents.AgPlcyEventTriggerThreshold	3	3
AgentEvents.AgPlcyMaxEventsPerTrigger	10	10
AgentListenServer		
AgentListenServer.AgentPingPort	8081	8081

McAfee ePolicy Orchestrator
Client Task Management

- What about comparing and documenting your client tasks? Yes!



Compare Client Tasks

Product: VirusScan Enterprise 8.8.0

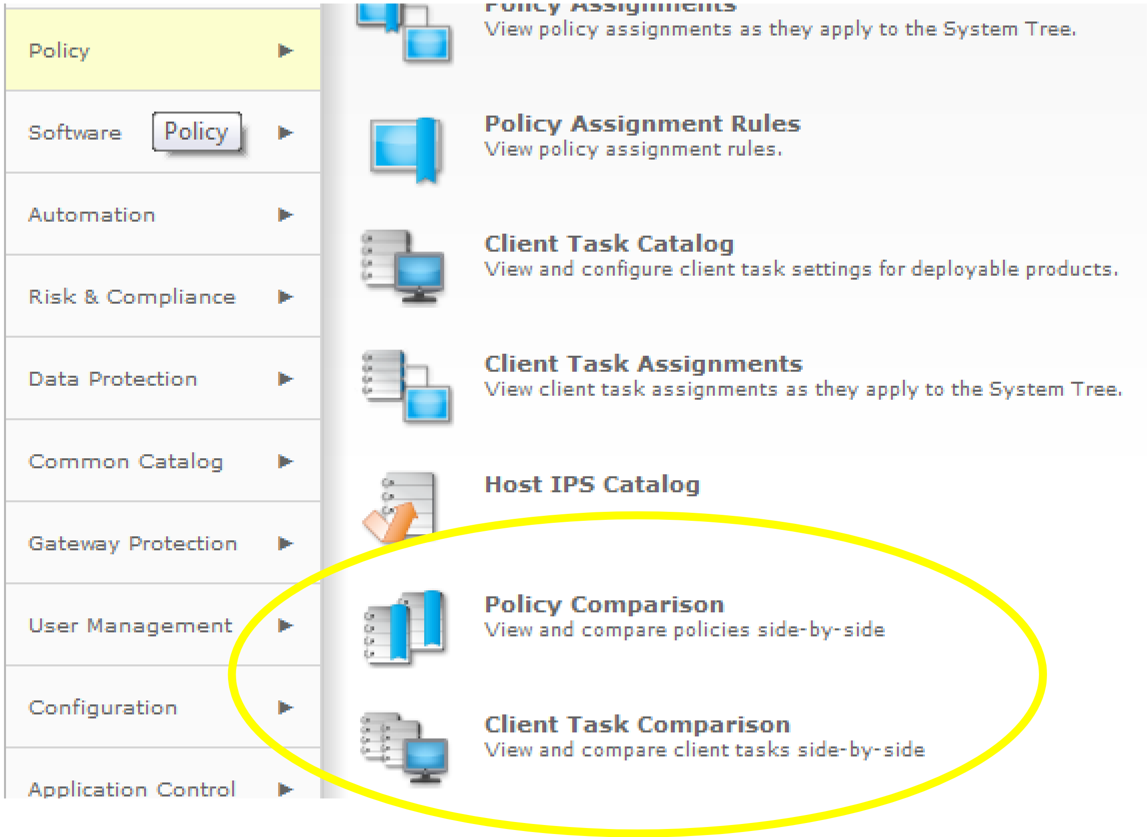
Client Task Type: On Demand Scan

Show: Client Task Differences

Settings	Client Task 1	Client Task 2
Compare Client Tasks:	Server ODS	Workstation ODS
Settings that are different:	---	3
Settings that are identical:	---	52
Client Task Details		
Assignment:	0	0
Owner:	Global Administrators	Global Administrators
Actions		
Advanced		
Advanced.dwHeuristicNetCheckSensitivity	3	4
Exclusions		
General		
Reports		
ScanItems		
Spyware		
VSE7_SchedulerSection		
VSE7_SchedulerSection.bRunOnServer	1	0
VSE7_SchedulerSection.bRunOnWrkstn	0	1

McAfee ePolicy Orchestrator
Policy & Client Task Comparison Tool

- When authenticated to ePO enter the following urls:
  - https://hostname:port/PolicyMgmt/comparePolicies.do
  - https://hostname:port/PolicyMgmt/compareClientTasks.do



Policy Assignments
View policy assignments as they apply to the System Tree.

Policy Assignment Rules
View policy assignment rules.

Client Task Catalog
View and configure client task settings for deployable products.

Client Task Assignments
View client task assignments as they apply to the System Tree.

Host IPS Catalog

Policy Comparison
View and compare policies side-by-side

Client Task Comparison
View and compare client tasks side-by-side

What dashboards are useful?

Layered security needs layered analysis

- Layer 1 – Snapshot with basic correlation of users, hosts, IP, etc.
- Layer 2 - Trending
- Layer 3 – Multi level correlation which assists with policy tuning e.g. exclusions

Filter dashboards and queries on tag e.g. Server, Workstation, Laptop, DMZ, SQL, Exchange, Sales, Marketing, Country, etc.

Waypoints

FOCUS 12 SECURITY CONFERENCE

- ePolicy Orchestrator
- VirusScan Enterprise 8.8
- Host IPS 8
- Web Security (Endpoint and Gateway)
- Device Control
- Trust Control Suite (Cloud)

VirusScan® Enterprise

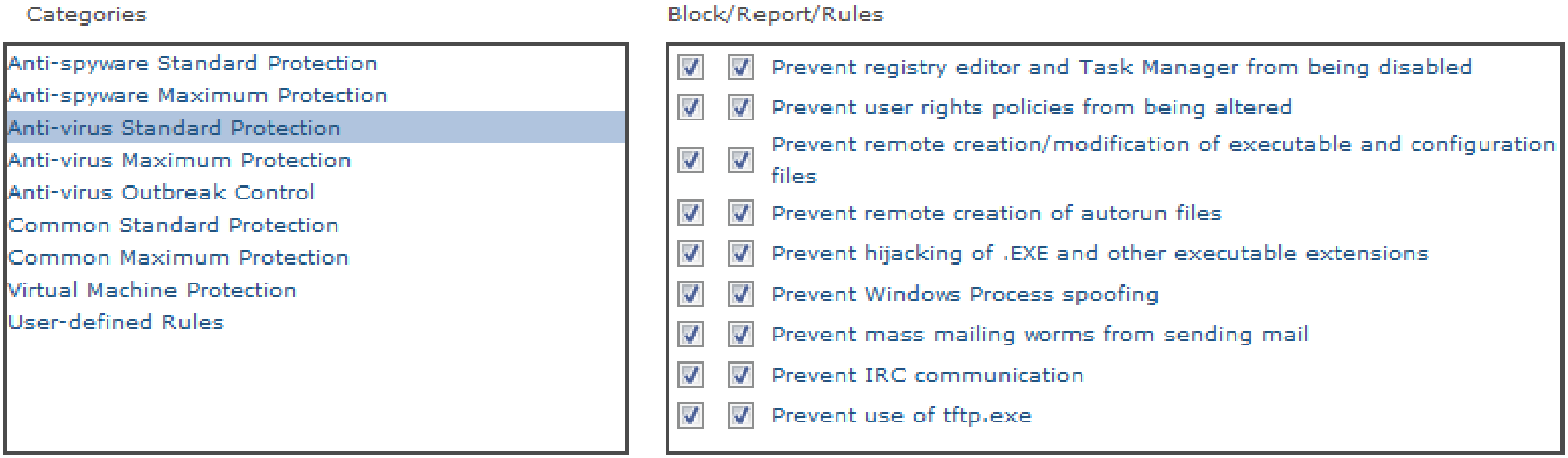
FOCUS 12 SECURITY CONFERENCE

Key things to monitor:

- Access Protection Rules
  - What is the behavior of our environment?
- Artemis – GTI File Reputation
  - What new fangled threats are in our environment?
- Analyzer method – On Access Scan vs On Demand Scan
  - How are threats being addressed?

VirusScan® Enterprise
Access Protection Rules

- Consider using:
  - Prevent HTTP communication
  - Protect network settings
  - Block read and write access to all shares (for Workstations)



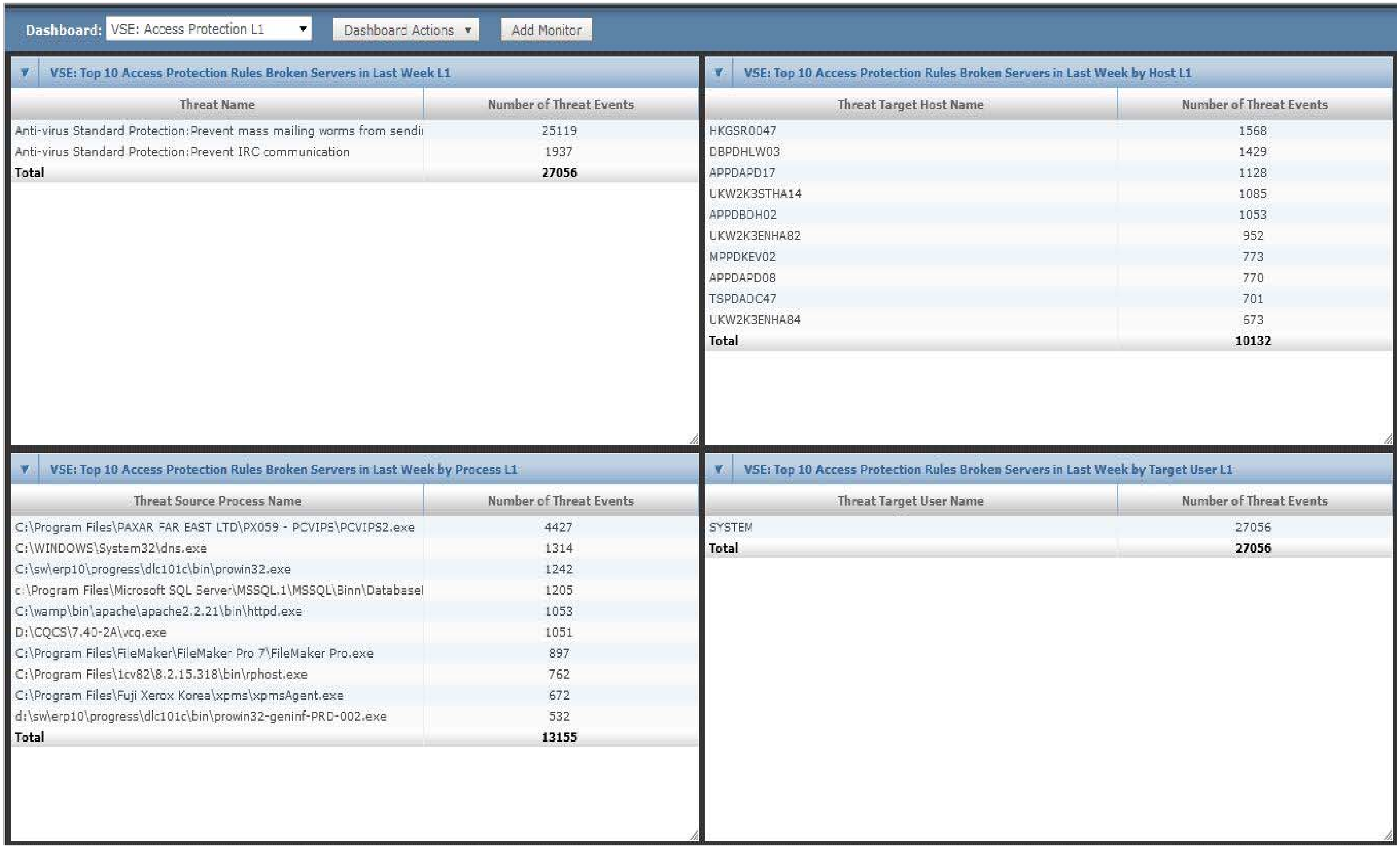
Categories

Anti-spyware Standard Protection
Anti-spyware Maximum Protection
Anti-virus Standard Protection
Anti-virus Maximum Protection
Anti-virus Outbreak Control
Common Standard Protection
Common Maximum Protection
Virtual Machine Protection
User-defined Rules

Block/Report/Rules

☑ ☑ Prevent registry editor and Task Manager from being disabled
☑ ☑ Prevent user rights policies from being altered
☑ ☑ Prevent remote creation/modification of executable and configuration files
☑ ☑ Prevent remote creation of autorun files
☑ ☑ Prevent hijacking of .EXE and other executable extensions
☑ ☑ Prevent Windows Process spoofing
☑ ☑ Prevent mass mailing worms from sending mail
☑ ☑ Prevent IRC communication
☑ ☑ Prevent use of tftp.exe

VirusScan® Enterprise
Access Protection Rules: Level 1 Snapshot



Dashboard: VSE: Access Protection L1

VSE: Top 10 Access Protection Rules Broken Servers in Last Week L1

Threat Name	Number of Threat Events
Anti-virus Standard Protection:Prevent mass mailing worms from sendi	25119
Anti-virus Standard Protection:Prevent IRC communication	1937
Total	**27056**

VSE: Top 10 Access Protection Rules Broken Servers in Last Week by Host L1

Threat Target Host Name	Number of Threat Events
HKGSR0047	1568
DBPDHLW03	1429
APPDAPD17	1128
UKW2K3STHA14	1085
APPDBDH02	1053
UKW2K3ENHA82	952
MPPDKEV02	773
APPDAPD08	770
TSPDADC47	701
UKW2K3ENHA84	673
Total	**10132**

VSE: Top 10 Access Protection Rules Broken Servers in Last Week by Process L1

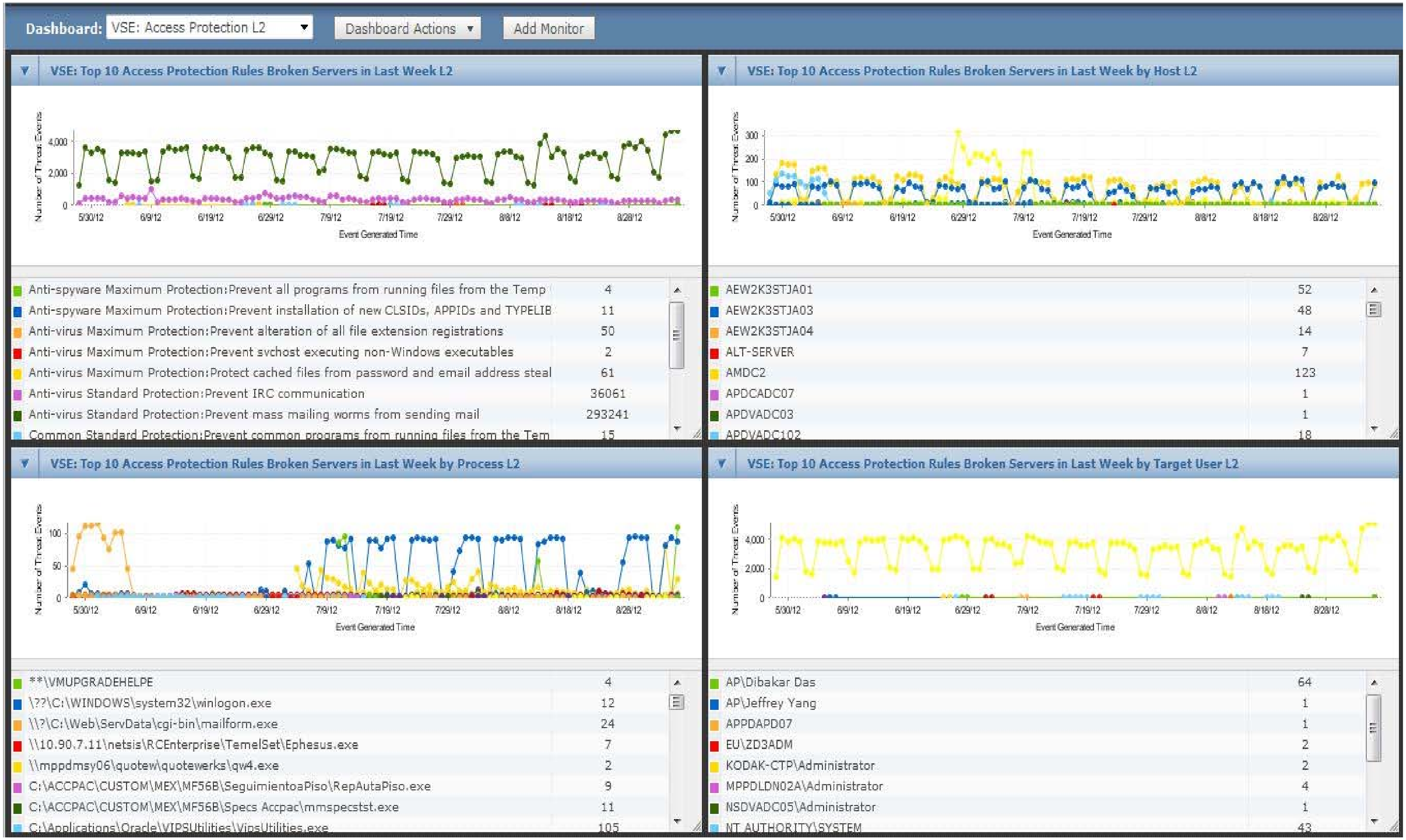
Threat Source Process Name	Number of Threat Events
C:\Program Files\PAXAR FAR EAST LTD\PX059 - PCVIPS\PCVIPS2.exe	4427
C:\WINDOWS\System32\dns.exe	1314
C:\sw\erp10\progress\dlc101c\bin\prowin32.exe	1242
c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\Databasel	1205
C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe	1053
D:\CQCS\7.40-2A\vcq.exe	1051
C:\Program Files\FileMaker\FileMaker Pro 7\FileMaker Pro.exe	897
C:\Program Files\1cv82\8.2.15.318\bin\rphost.exe	762
C:\Program Files\Fuji Xerox Korea\xpms\xpmsAgent.exe	672
d:\sw\erp10\progress\dlc101c\bin\prowin32-geninf-PRD-002.exe	532
Total	**13155**

VSE: Top 10 Access Protection Rules Broken Servers in Last Week by Target User L1

Threat Target User Name	Number of Threat Events
SYSTEM	27056
Total	**27056**

VirusScan® Enterprise
Access Protection Rules: Level 2 Trending

FOCUS 12 SECURITY CONFERENCE



VSE: Top 10 Access Protection Rules Broken Servers in Last Week L2

🟩	Anti-spyware Maximum Protection:Prevent all programs from running files from the Temp	4
🟦	Anti-spyware Maximum Protection:Prevent installation of new CLSIDs, APPIDs and TYPELIB	11
🟧	Anti-virus Maximum Protection:Prevent alteration of all file extension registrations	50
🟥	Anti-virus Maximum Protection:Prevent svchost executing non-Windows executables	2
🟨	Anti-virus Maximum Protection:Protect cached files from password and email address steal	61
🟪	Anti-virus Standard Protection:Prevent IRC communication	36061
🟩	Anti-virus Standard Protection:Prevent mass mailing worms from sending mail	293241
🟦	Common Standard Protection:Prevent common programs from running files from the Tem	15

VSE: Top 10 Access Protection Rules Broken Servers in Last Week by Host L2

🟩	AEW2K3STJA01	52
🟦	AEW2K3STJA03	48
🟧	AEW2K3STJA04	14
🟥	ALT-SERVER	7
🟨	AMDC2	123
🟪	APDCADC07	1
🟩	APDVADC03	1
🟦	APDVADC102	18

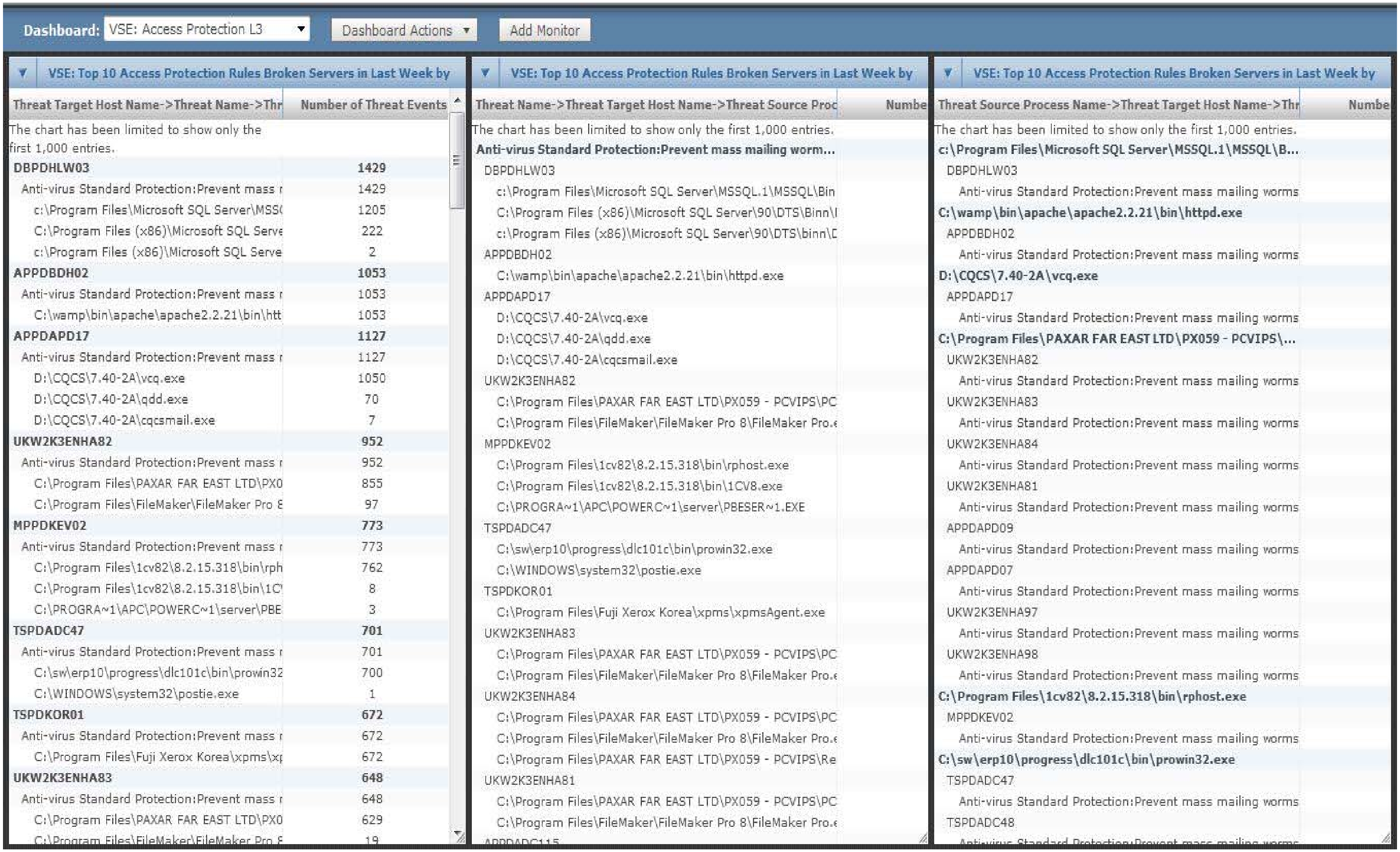
VSE: Top 10 Access Protection Rules Broken Servers in Last Week by Process L2

🟩	**\VMUPGRADEHELPE	4
🟦	\??\C:\WINDOWS\system32\winlogon.exe	12
🟧	\\?\C:\Web\ServData\cgi-bin\mailform.exe	24
🟥	\\10.90.7.11\netsis\RCEnterprise\TemelSet\Ephesus.exe	7
🟨	\\mppdmsy06\quotew\quotewerks\qw4.exe	2
🟪	C:\ACCPAC\CUSTOM\MEX\MF56B\SeguimientoaPiso\RepAutaPiso.exe	9
🟩	C:\ACCPAC\CUSTOM\MEX\MF56B\Specs Accpac\mmspecstst.exe	11
🟦	C:\Applications\Oracle\VIPSUtilities\VipsUtilities.exe	105

VSE: Top 10 Access Protection Rules Broken Servers in Last Week by Target User L2

🟩	AP\Dibakar Das	64
🟦	AP\Jeffrey Yang	1
🟧	APPDAPD07	1
🟥	EU\ZD3ADM	2
🟨	KODAK-CTP\Administrator	2
🟪	MPPDLDN02A\Administrator	4
🟩	NSDVADC05\Administrator	1
🟦	NT AUTHORITY\SYSTEM	43

VirusScan® Enterprise
Access Protection Rules: Level 3 Policy Tuning



VSE: Top 10 Access Protection Rules Broken Servers in Last Week by

Threat Target Host Name->Threat Name->Thr	Number of Threat Events
The chart has been limited to show only the first 1,000 entries.	
DBPDHLW03	**1429**
Anti-virus Standard Protection:Prevent mass r	1429
c:\Program Files\Microsoft SQL Server\MSS	1205
C:\Program Files (x86)\Microsoft SQL Serve	222
c:\Program Files (x86)\Microsoft SQL Serve	2
APPDBDH02	**1053**
Anti-virus Standard Protection:Prevent mass r	1053
C:\wamp\bin\apache\apache2.2.21\bin\htt	1053
APPDAPD17	**1127**
Anti-virus Standard Protection:Prevent mass r	1127
D:\CQCS\7.40-2A\vcq.exe	1050
D:\CQCS\7.40-2A\qdd.exe	70
D:\CQCS\7.40-2A\cqcsmail.exe	7
UKW2K3ENHA82	**952**
Anti-virus Standard Protection:Prevent mass r	952
C:\Program Files\PAXAR FAR EAST LTD\PX0	855
C:\Program Files\FileMaker\FileMaker Pro 8	97
MPPDKEV02	**773**
Anti-virus Standard Protection:Prevent mass r	773
C:\Program Files\1cv82\8.2.15.318\bin\rph	762
C:\Program Files\1cv82\8.2.15.318\bin\1C	8
C:\PROGRA~1\APC\POWERC~1\server\PBE	3
TSPDADC47	**701**
Anti-virus Standard Protection:Prevent mass r	701
C:\sw\erp10\progress\dlc101c\bin\prowin32	700
C:\WINDOWS\system32\postie.exe	1
TSPDKOR01	**672**
Anti-virus Standard Protection:Prevent mass r	672
C:\Program Files\Fuji Xerox Korea\xpms\xp	672
UKW2K3ENHA83	**648**
Anti-virus Standard Protection:Prevent mass r	648
C:\Program Files\PAXAR FAR EAST LTD\PX0	629
C:\Program Files\FileMaker\FileMaker Pro 8	19

VSE: Top 10 Access Protection Rules Broken Servers in Last Week by

Threat Name->Threat Target Host Name->Threat Source Proc	Numbe
The chart has been limited to show only the first 1,000 entries.	
Anti-virus Standard Protection:Prevent mass mailing worm...	
DBPDHLW03	
c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Bin	
C:\Program Files (x86)\Microsoft SQL Server\90\DTS\Binn\	
c:\Program Files (x86)\Microsoft SQL Server\90\DTS\binn\	
APPDBDH02	
C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe	
APPDAPD17	
D:\CQCS\7.40-2A\vcq.exe	
D:\CQCS\7.40-2A\qdd.exe	
D:\CQCS\7.40-2A\cqcsmail.exe	
UKW2K3ENHA82	
C:\Program Files\PAXAR FAR EAST LTD\PX059 - PCVIPS\PC	
C:\Program Files\FileMaker\FileMaker Pro 8\FileMaker Pro.	
MPPDKEV02	
C:\Program Files\1cv82\8.2.15.318\bin\rphost.exe	
C:\Program Files\1cv82\8.2.15.318\bin\1CV8.exe	
C:\PROGRA~1\APC\POWERC~1\server\PBESER~1.EXE	
TSPDADC47	
C:\sw\erp10\progress\dlc101c\bin\prowin32.exe	
C:\WINDOWS\system32\postie.exe	
TSPDKOR01	
C:\Program Files\Fuji Xerox Korea\xpms\xpmsAgent.exe	
UKW2K3ENHA83	
C:\Program Files\PAXAR FAR EAST LTD\PX059 - PCVIPS\PC	
C:\Program Files\FileMaker\FileMaker Pro 8\FileMaker Pro.	
UKW2K3ENHA84	
C:\Program Files\PAXAR FAR EAST LTD\PX059 - PCVIPS\PC	
C:\Program Files\FileMaker\FileMaker Pro 8\FileMaker Pro.	
C:\Program Files\PAXAR FAR EAST LTD\PX059 - PCVIPS\Re	
UKW2K3ENHA81	
C:\Program Files\PAXAR FAR EAST LTD\PX059 - PCVIPS\PC	
C:\Program Files\FileMaker\FileMaker Pro 8\FileMaker Pro.	
APPDADC115	

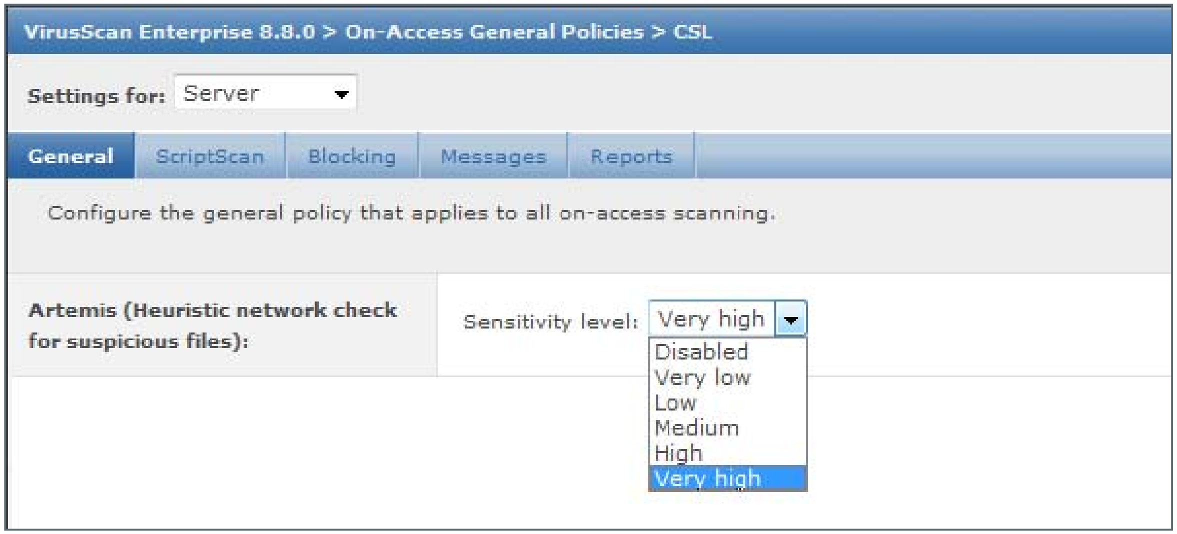
VSE: Top 10 Access Protection Rules Broken Servers in Last Week by

Threat Source Process Name->Threat Target Host Name->Thr	Numbe
The chart has been limited to show only the first 1,000 entries.	
c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\B...	
DBPDHLW03	
Anti-virus Standard Protection:Prevent mass mailing worms	
C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe	
APPDBDH02	
Anti-virus Standard Protection:Prevent mass mailing worms	
D:\CQCS\7.40-2A\vcq.exe	
APPDAPD17	
Anti-virus Standard Protection:Prevent mass mailing worms	
C:\Program Files\PAXAR FAR EAST LTD\PX059 - PCVIPS\...	
UKW2K3ENHA82	
Anti-virus Standard Protection:Prevent mass mailing worms	
UKW2K3ENHA83	
Anti-virus Standard Protection:Prevent mass mailing worms	
UKW2K3ENHA84	
Anti-virus Standard Protection:Prevent mass mailing worms	
UKW2K3ENHA81	
Anti-virus Standard Protection:Prevent mass mailing worms	
APPDAPD09	
Anti-virus Standard Protection:Prevent mass mailing worms	
APPDAPD07	
Anti-virus Standard Protection:Prevent mass mailing worms	
UKW2K3ENHA97	
Anti-virus Standard Protection:Prevent mass mailing worms	
UKW2K3ENHA98	
Anti-virus Standard Protection:Prevent mass mailing worms	
C:\Program Files\1cv82\8.2.15.318\bin\rphost.exe	
MPPDKEV02	
Anti-virus Standard Protection:Prevent mass mailing worms	
C:\sw\erp10\progress\dlc101c\bin\prowin32.exe	
TSPDADC47	
Anti-virus Standard Protection:Prevent mass mailing worms	
TSPDADC48	
Anti-virus Standard Protection:Prevent mass mailing worms	

VirusScan® Enterprise

Artemis GTI File Reputation

- On Access General Policy



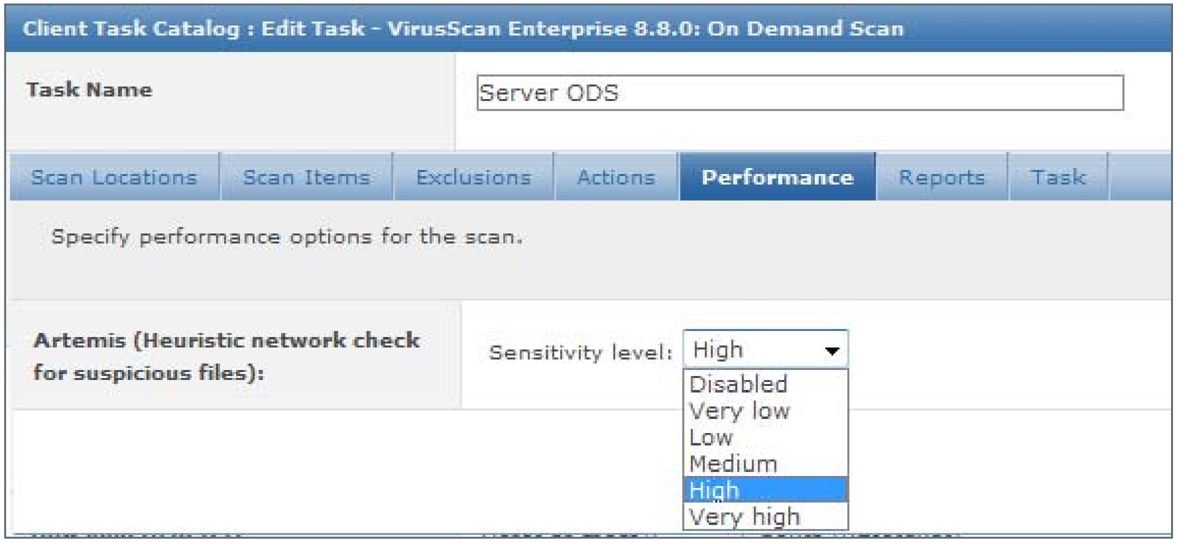
VirusScan Enterprise 8.8.0 > On-Access General Policies > CSL

Settings for: Server

Configure the general policy that applies to all on-access scanning.

Artemis (Heuristic network check for suspicious files): Sensitivity level: Very high

- On-Demand Scan Client Task



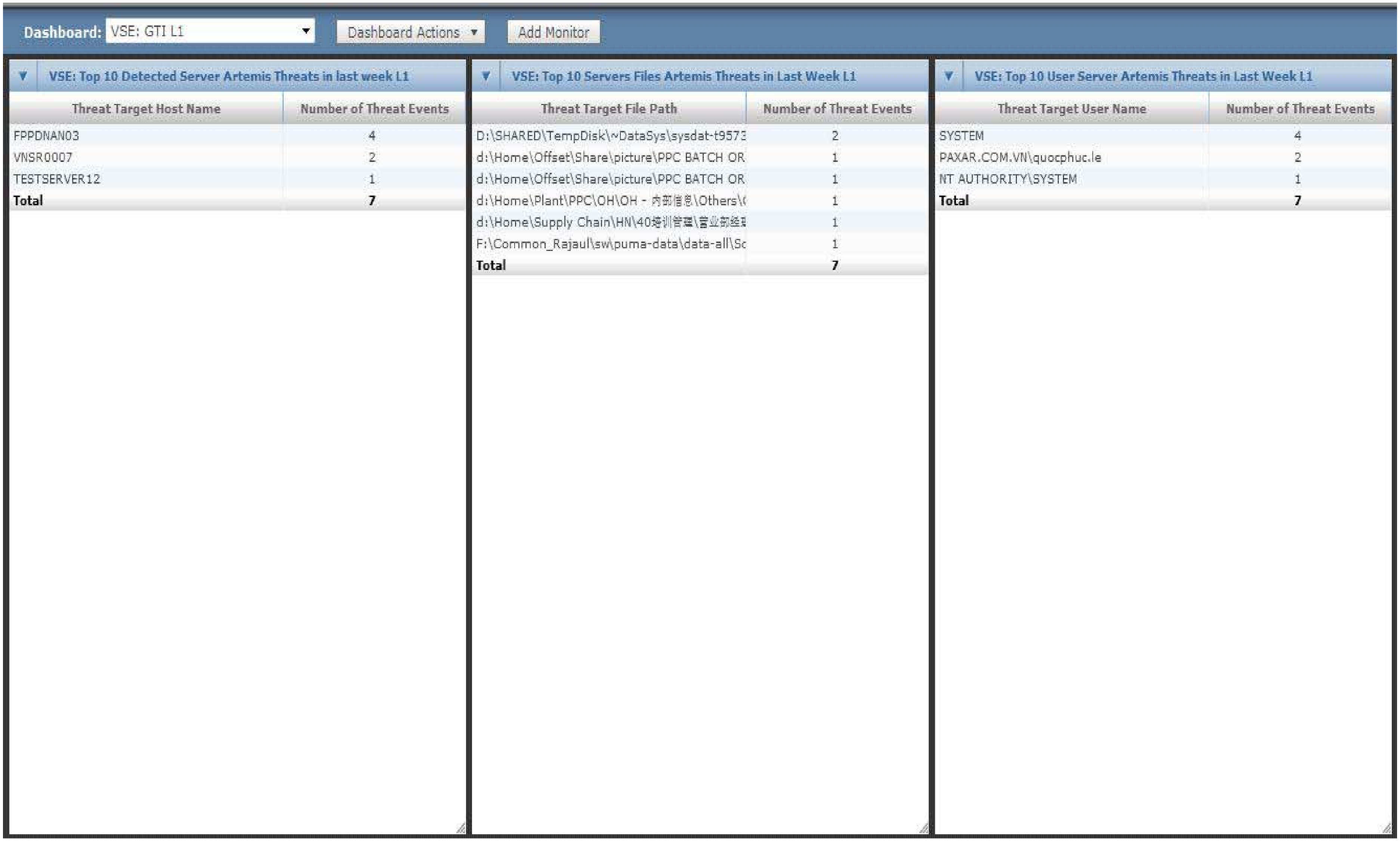
Client Task Catalog : Edit Task - VirusScan Enterprise 8.8.0: On Demand Scan

Task Name: Server ODS

Specify performance options for the scan.

Artemis (Heuristic network check for suspicious files): Sensitivity level: High

VirusScan® Enterprise
Artemis Level 1 Snapshot



VSE: Top 10 Detected Server Artemis Threats in last week L1

Threat Target Host Name	Number of Threat Events
FPPDNAN03	4
VNSR0007	2
TESTSERVER12	1
Total	**7**

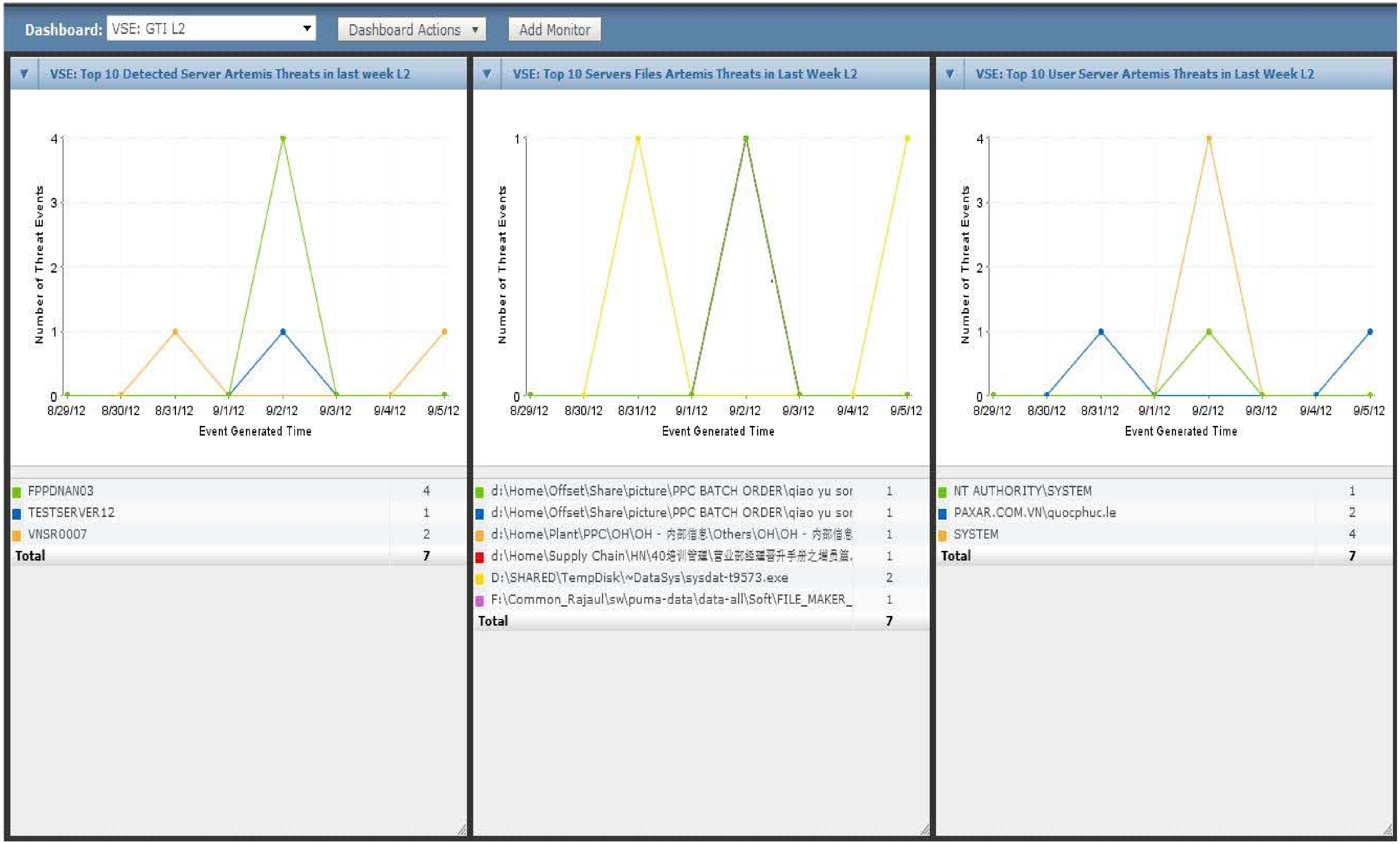
VSE: Top 10 Servers Files Artemis Threats in Last Week L1

Threat Target File Path	Number of Threat Events
D:\SHARED\TempDisk\~DataSys\sysdat-t9573	2
d:\Home\Offset\Share\picture\PPC BATCH OR	1
d:\Home\Offset\Share\picture\PPC BATCH OR	1
d:\Home\Plant\PPC\OH\OH - 内部信息\Others\	1
d:\Home\Supply Chain\HN\40培训管理\营业部经	1
F:\Common_Rajaul\sw\puma-data\data-all\Sc	1
Total	**7**

VSE: Top 10 User Server Artemis Threats in Last Week L1

Threat Target User Name	Number of Threat Events
SYSTEM	4
PAXAR.COM.VN\quocphuc.le	2
NT AUTHORITY\SYSTEM	1
Total	**7**

VirusScan® Enterprise
Artemis Level 2 Trending


Dashboard: VSE: GTI L2
Dashboard Actions
Add Monitor
VSE: Top 10 Detected Server Artemis Threats in last week L2
VSE: Top 10 Servers Files Artemis Threats in Last Week L2
VSE: Top 10 User Server Artemis Threats in Last Week L2
Number of Threat Events
Event Generated Time
0
1
2
3
4
8/29/12
8/30/12
8/31/12
9/1/12
9/2/12
9/3/12
9/4/12
9/5/12

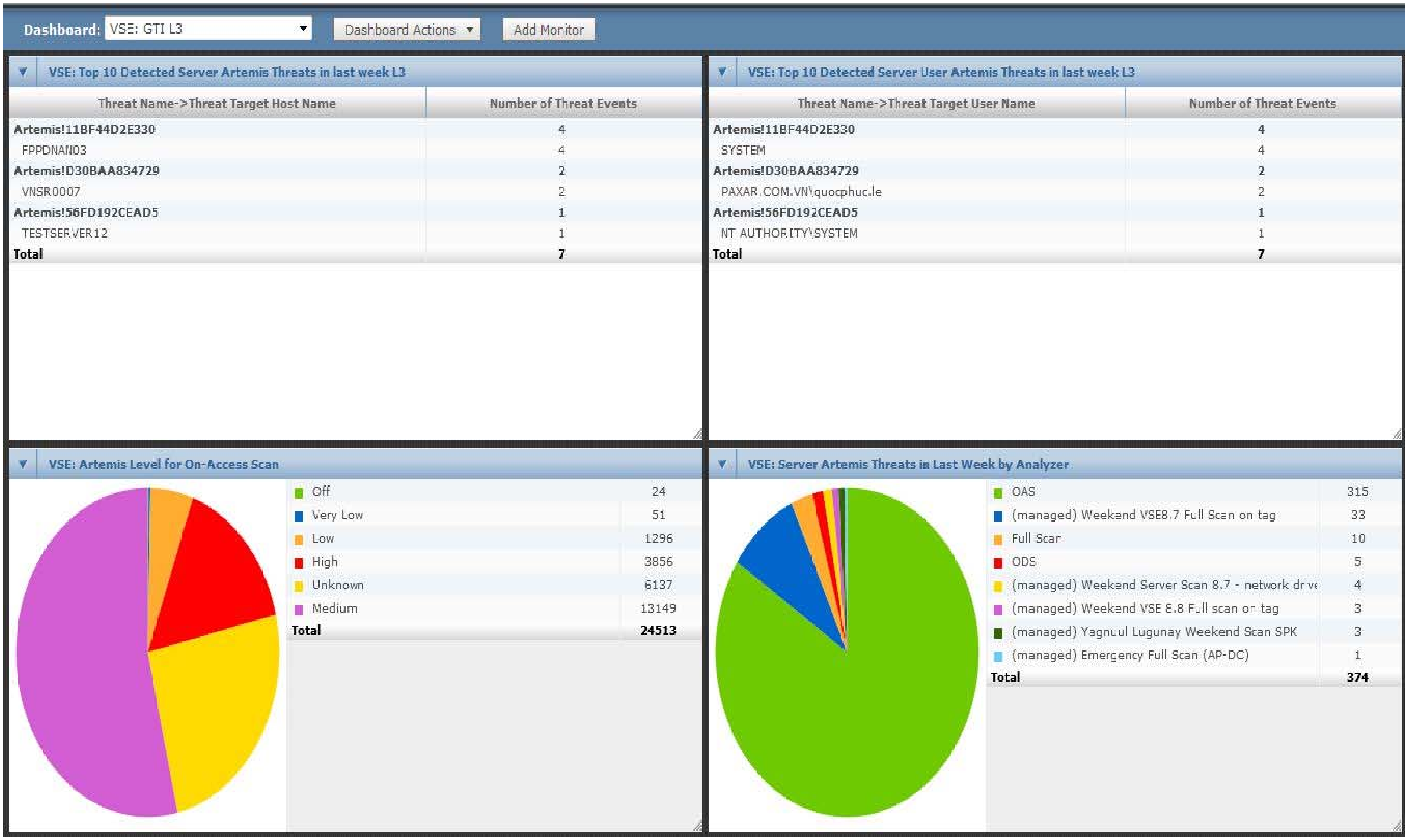
🟩 FPPDNAN03	4
🟦 TESTSERVER12	1
🟧 VNSR0007	2
Total	**7**

🟩 d:\Home\Offset\Share\picture\PPC BATCH ORDER\qiao yu sor	1
🟦 d:\Home\Offset\Share\picture\PPC BATCH ORDER\qiao yu sor	1
🟧 d:\Home\Plant\PPC\OH\OH - 内部信息\Others\OH\OH - 内部信息	1
🟥 d:\Home\Supply Chain\HN\40培训管理\营业部经理晋升手册之操质篇.	1
🟨 D:\SHARED\TempDisk\~DataSys\sysdat-t9573.exe	2
🟪 F:\Common_Rajaul\sw\puma-data\data-all\Soft\FILE_MAKER_	1
Total	**7**

🟩 NT AUTHORITY\SYSTEM	1
🟦 PAXAR.COM.VN\quocphuc.le	2
🟧 SYSTEM	4
Total	**7**

VirusScan® Enterprise
Artemis Level 3 Policy Tuning

FOCUS12 SECURITY CONFERENCE



Dashboard: VSE: GTI L3

VSE: Top 10 Detected Server Artemis Threats in last week L3

Threat Name->Threat Target Host Name	Number of Threat Events
Artemis!11BF44D2E330	4
FPPDNAN03	4
Artemis!D30BAA834729	2
VNSR0007	2
Artemis!56FD192CEAD5	1
TESTSERVER12	1
Total	**7**

VSE: Top 10 Detected Server User Artemis Threats in last week L3

Threat Name->Threat Target User Name	Number of Threat Events
Artemis!11BF44D2E330	4
SYSTEM	4
Artemis!D30BAA834729	2
PAXAR.COM.VN\quocphuc.le	2
Artemis!56FD192CEAD5	1
NT AUTHORITY\SYSTEM	1
Total	**7**

VSE: Artemis Level for On-Access Scan

🟩 Off	24
🟦 Very Low	51
🟧 Low	1296
🟥 High	3856
🟨 Unknown	6137
🟪 Medium	13149
Total	**24513**

VSE: Server Artemis Threats in Last Week by Analyzer

🟩 OAS	315
🟦 (managed) Weekend VSE8.7 Full Scan on tag	33
🟧 Full Scan	10
🟥 ODS	5
🟨 (managed) Weekend Server Scan 8.7 - network drive	4
🟪 (managed) Weekend VSE 8.8 Full scan on tag	3
🟩 (managed) Yagnuul Lugunay Weekend Scan SPK	3
🟦 (managed) Emergency Full Scan (AP-DC)	1
Total	**374**

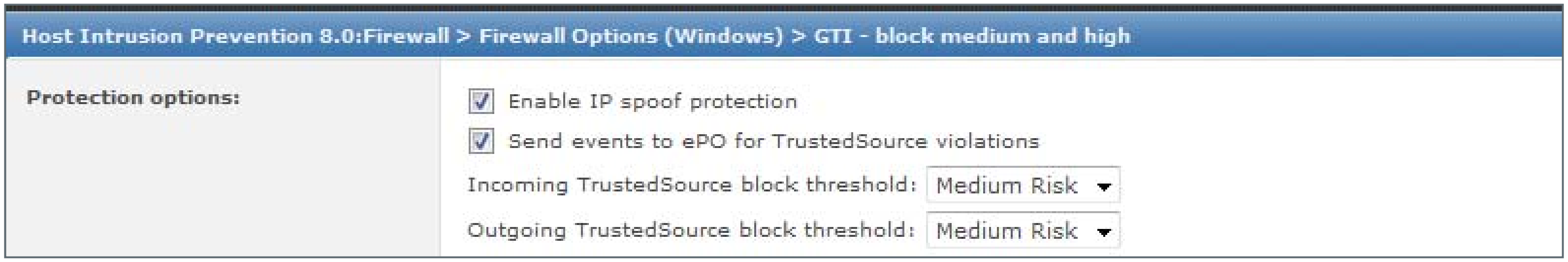
Waypoints

FOCUS 12 SECURITY CONFERENCE

- ePolicy Orchestrator
- VirusScan Enterprise 8.8
- Host IPS 8
- Web Security (Endpoint and Gateway)
- Device Control
- Trust Control Suite (Cloud)

Host IPS 8
GTI IP Reputation

Firewall Options



Host Intrusion Prevention 8.0:Firewall > Firewall Options (Windows) > GTI - block medium and high

Protection options:

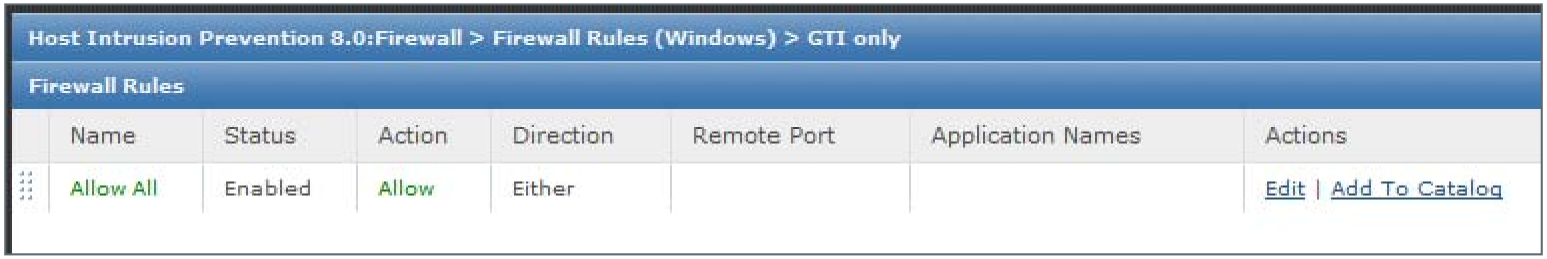
☑ Enable IP spoof protection

☑ Send events to ePO for TrustedSource violations

Incoming TrustedSource block threshold: Medium Risk

Outgoing TrustedSource block threshold: Medium Risk

Firewall Rules



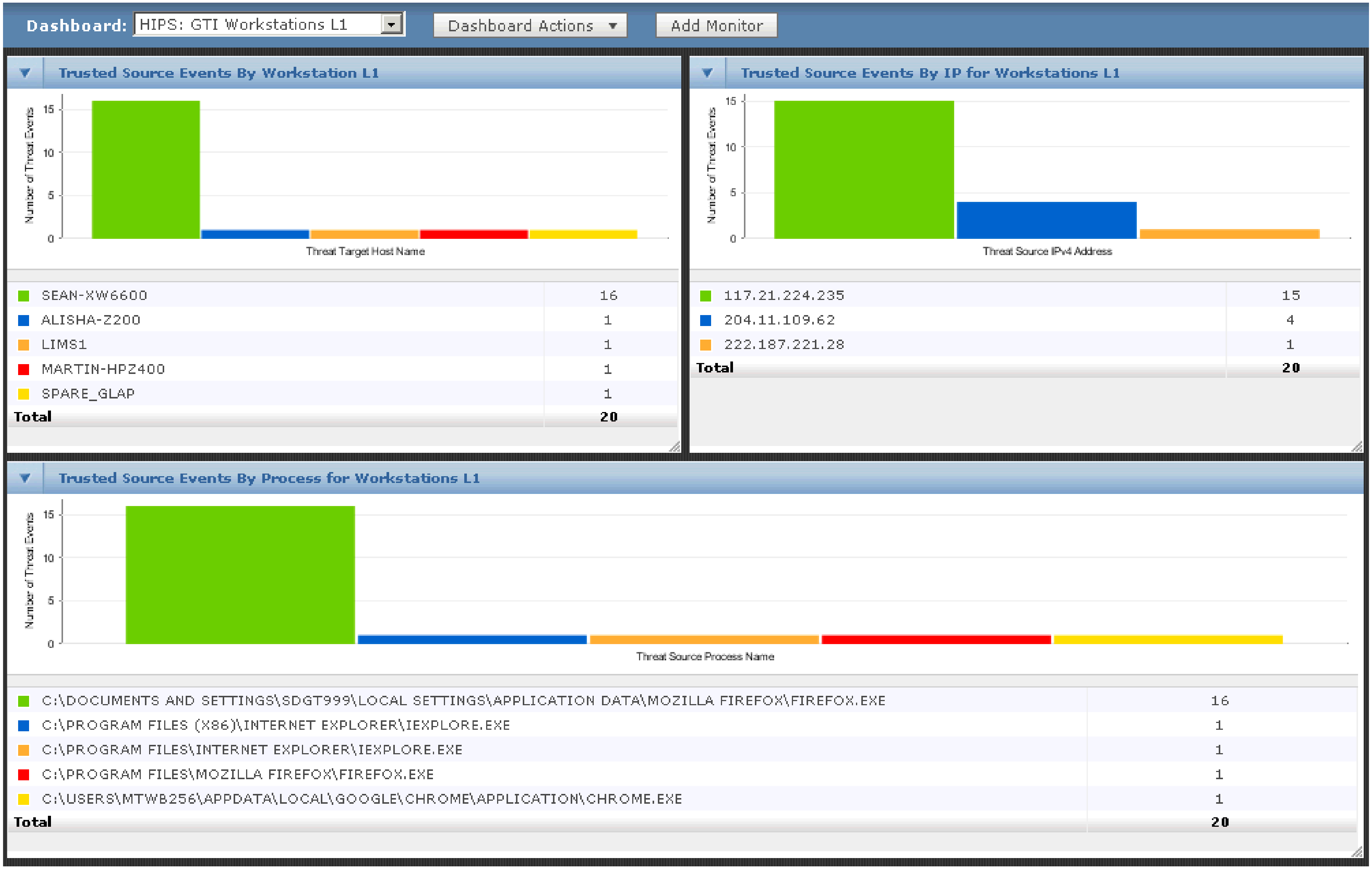
Host Intrusion Prevention 8.0:Firewall > Firewall Rules (Windows) > GTI only

Firewall Rules

Name	Status	Action	Direction	Remote Port	Application Names	Actions
Allow All	Enabled	Allow	Either			Edit | Add To Catalog

Host IPS 8
GTI Trusted Source Level 1 Snapshot

FOCUS 12 SECURITY CONFERENCE



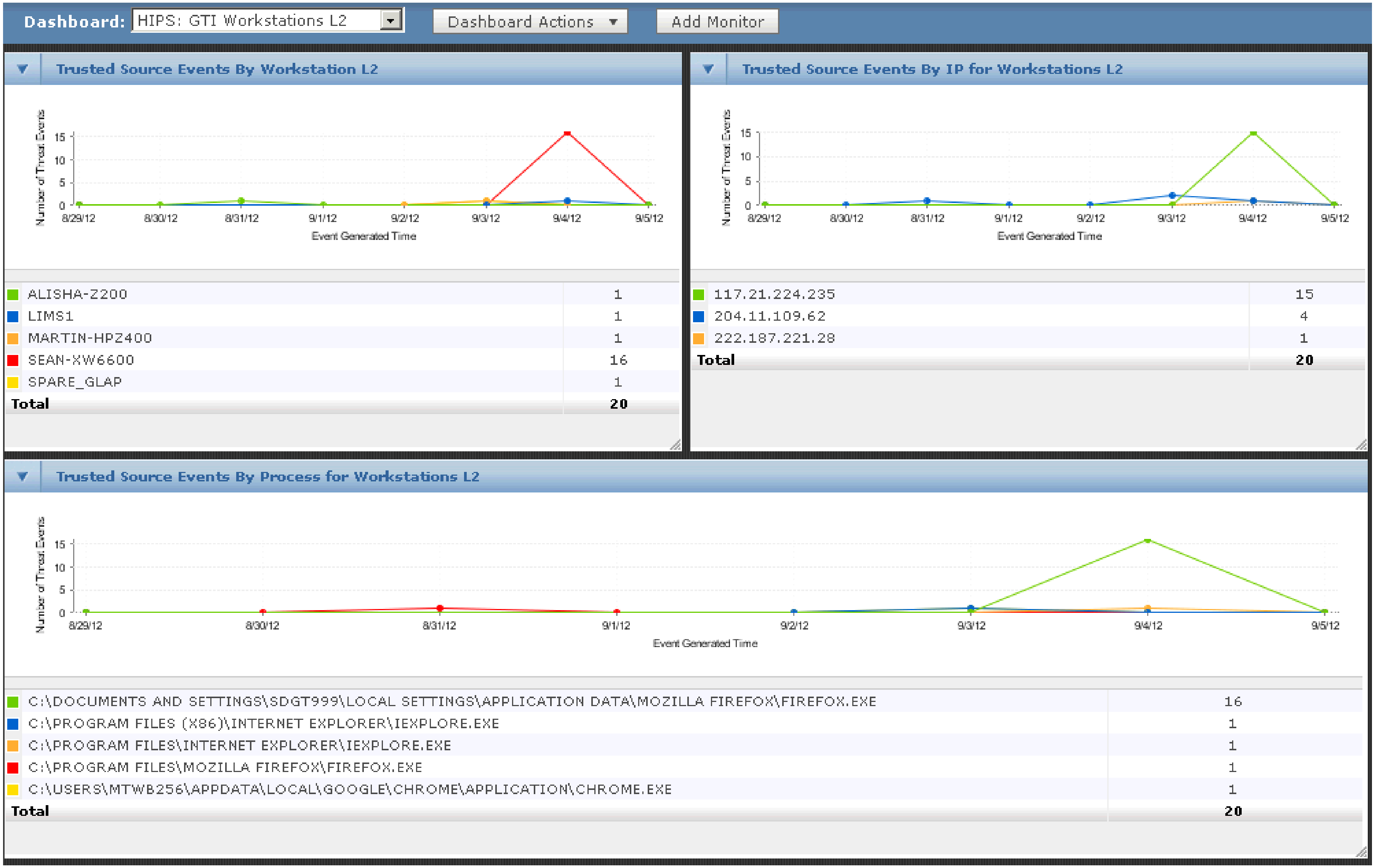
Dashboard: HIPS: GTI Workstations L1
Dashboard Actions ▼
Add Monitor
Trusted Source Events By Workstation L1
Number of Threat Events
15
10
5
0
Threat Target Host Name
Trusted Source Events By IP for Workstations L1
Number of Threat Events
15
10
5
0
Threat Source IPv4 Address
Trusted Source Events By Process for Workstations L1
Number of Threat Events
15
10
5
0
Threat Source Process Name

🟩 SEAN-XW6600	16
🟦 ALISHA-Z200	1
🟧 LIMS1	1
🟥 MARTIN-HPZ400	1
🟨 SPARE_GLAP	1
Total	**20**

🟩 117.21.224.235	15
🟦 204.11.109.62	4
🟧 222.187.221.28	1
Total	**20**

🟩 C:\DOCUMENTS AND SETTINGS\SDGT999\LOCAL SETTINGS\APPLICATION DATA\MOZILLA FIREFOX\FIREFOX.EXE	16
🟦 C:\PROGRAM FILES (X86)\INTERNET EXPLORER\IEXPLORE.EXE	1
🟧 C:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE	1
🟥 C:\PROGRAM FILES\MOZILLA FIREFOX\FIREFOX.EXE	1
🟨 C:\USERS\MTWB256\APPDATA\LOCAL\GOOGLE\CHROME\APPLICATION\CHROME.EXE	1
Total	**20**

Host IPS 8
GTI Trusted Source Level 2 Trending



Trusted Source Events By Workstation L2

🟩	ALISHA-Z200	1
🟦	LIMS1	1
🟧	MARTIN-HPZ400	1
🟥	SEAN-XW6600	16
🟨	SPARE_GLAP	1
	Total	**20**

Trusted Source Events By IP for Workstations L2

🟩	117.21.224.235	15
🟦	204.11.109.62	4
🟧	222.187.221.28	1
	Total	**20**

Trusted Source Events By Process for Workstations L2

🟩	C:\DOCUMENTS AND SETTINGS\SDGT999\LOCAL SETTINGS\APPLICATION DATA\MOZILLA FIREFOX\FIREFOX.EXE	16
🟦	C:\PROGRAM FILES (X86)\INTERNET EXPLORER\IEXPLORE.EXE	1
🟧	C:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE	1
🟥	C:\PROGRAM FILES\MOZILLA FIREFOX\FIREFOX.EXE	1
🟨	C:\USERS\MTWB256\APPDATA\LOCAL\GOOGLE\CHROME\APPLICATION\CHROME.EXE	1
	Total	**20**

FOCUS12 SECURITY CONFERENCE

Host IPS 8

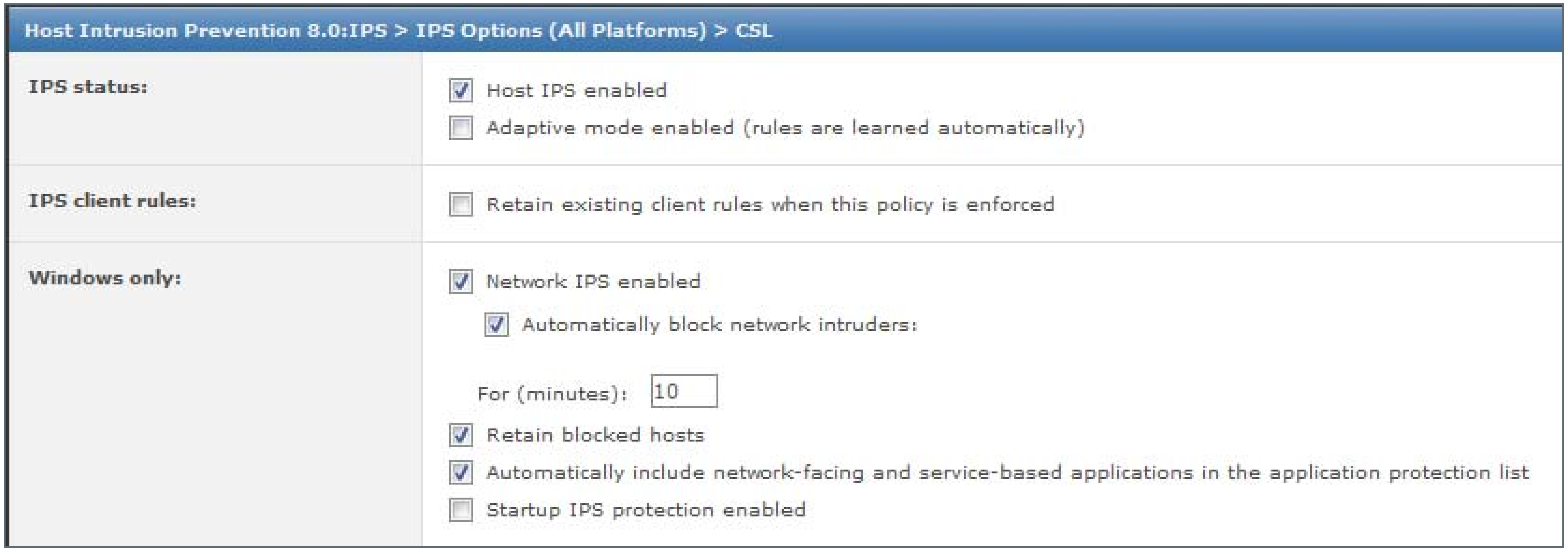
- Adobe Vulnerabilities for 2012
  - 89% were classified as Critical
  - 95% of those mitigated by Host IPS BOP

- Microsoft Vulnerabilities for 2012
  - 38% were classified as Critical
  - 57% of those mitigated by removing admin rights
  - All Office and IE vulnerabilities mitigated by removal of admin rights or Host IPS or Network IPS

- Source: Microsoft, Adobe, McAfee
- Data valid 1 January 2012 – 31 August 2012

Host IPS 8
IPS Module

- IPS Options



Host Intrusion Prevention 8.0:IPS > IPS Options (All Platforms) > CSL

IPS status:

☑ Host IPS enabled

□ Adaptive mode enabled (rules are learned automatically)

IPS client rules:

□ Retain existing client rules when this policy is enforced

Windows only:

☑ Network IPS enabled

☑ Automatically block network intruders:

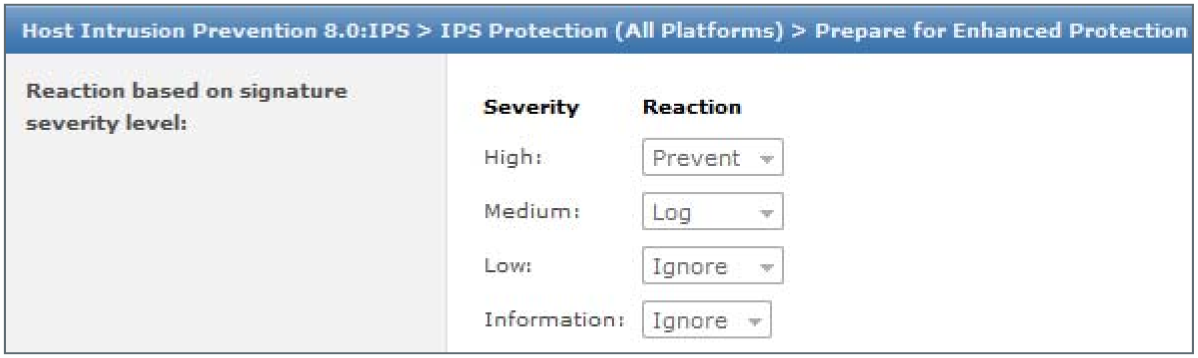
For (minutes): 10

☑ Retain blocked hosts

☑ Automatically include network-facing and service-based applications in the application protection list

□ Startup IPS protection enabled

- IPS Protection

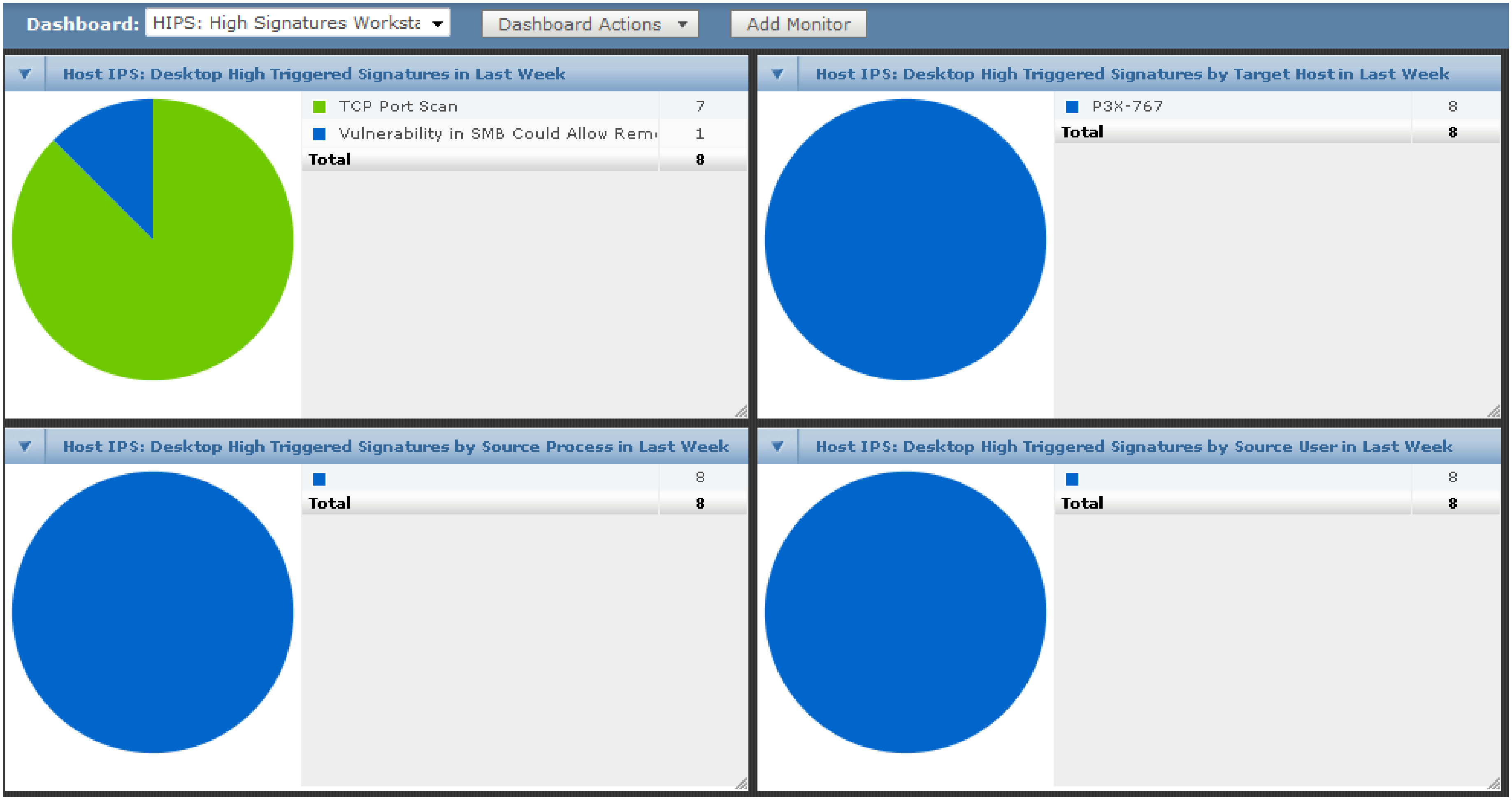


Host Intrusion Prevention 8.0:IPS > IPS Protection (All Platforms) > Prepare for Enhanced Protection

Reaction based on signature severity level:

Severity	Reaction
High:	Prevent
Medium:	Log
Low:	Ignore
Information:	Ignore

Host IPS 8
IPS High Signatures Level 1 Snapshot



Dashboard: HIPS: High Signatures Workst

Host IPS: Desktop High Triggered Signatures in Last Week

🟩	TCP Port Scan	7
🟦	Vulnerability in SMB Could Allow Rem	1
Total		**8**

Host IPS: Desktop High Triggered Signatures by Target Host in Last Week

🟦	P3X-767	8
Total		**8**

Host IPS: Desktop High Triggered Signatures by Source Process in Last Week

🟦	8
Total	**8**

Host IPS: Desktop High Triggered Signatures by Source User in Last Week

🟦	8
Total	**8**

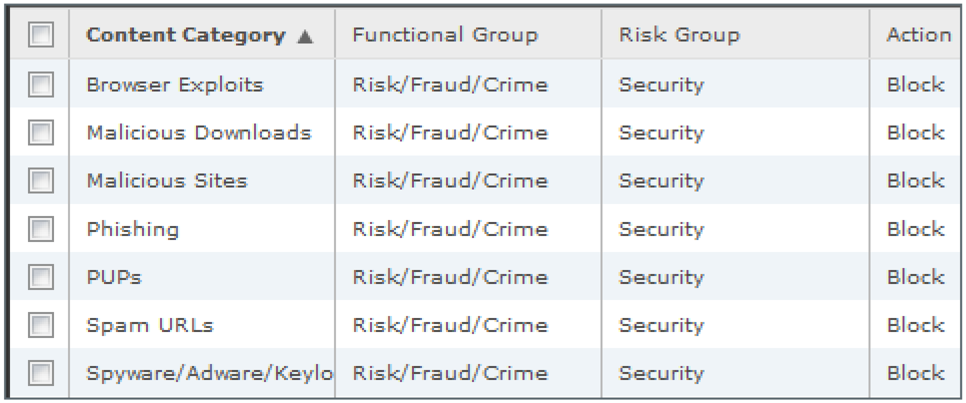
Waypoints

- ePolicy Orchestrator
- VirusScan Enterprise 8.8
- Host IPS 8
- Web Security (Endpoint and Gateway)
- Device Control
- Trust Control Suite (Cloud)

Web Security

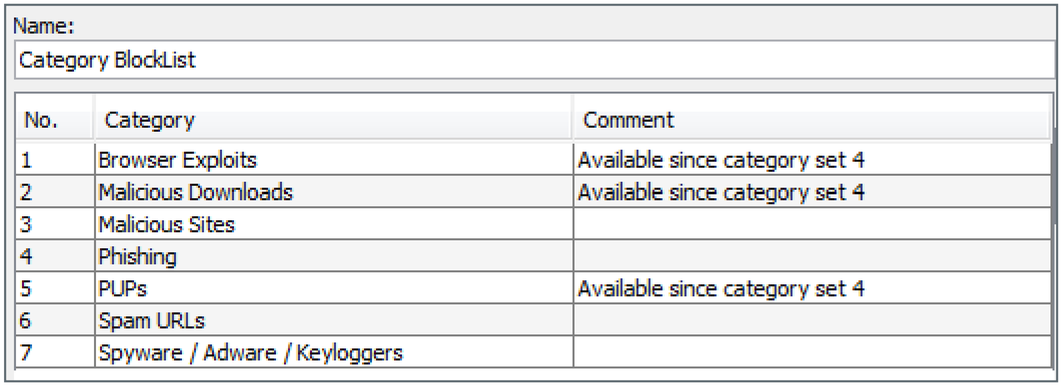
Typical Security Policy

- Web Filtering for Endpoints (leverages SiteAdvisor Enterprise)



□	Content Category ▲	Functional Group	Risk Group	Action
□	Browser Exploits	Risk/Fraud/Crime	Security	Block
□	Malicious Downloads	Risk/Fraud/Crime	Security	Block
□	Malicious Sites	Risk/Fraud/Crime	Security	Block
□	Phishing	Risk/Fraud/Crime	Security	Block
□	PUPs	Risk/Fraud/Crime	Security	Block
□	Spam URLs	Risk/Fraud/Crime	Security	Block
□	Spyware/Adware/Keylo	Risk/Fraud/Crime	Security	Block

- McAfee Web Gateway



Name:

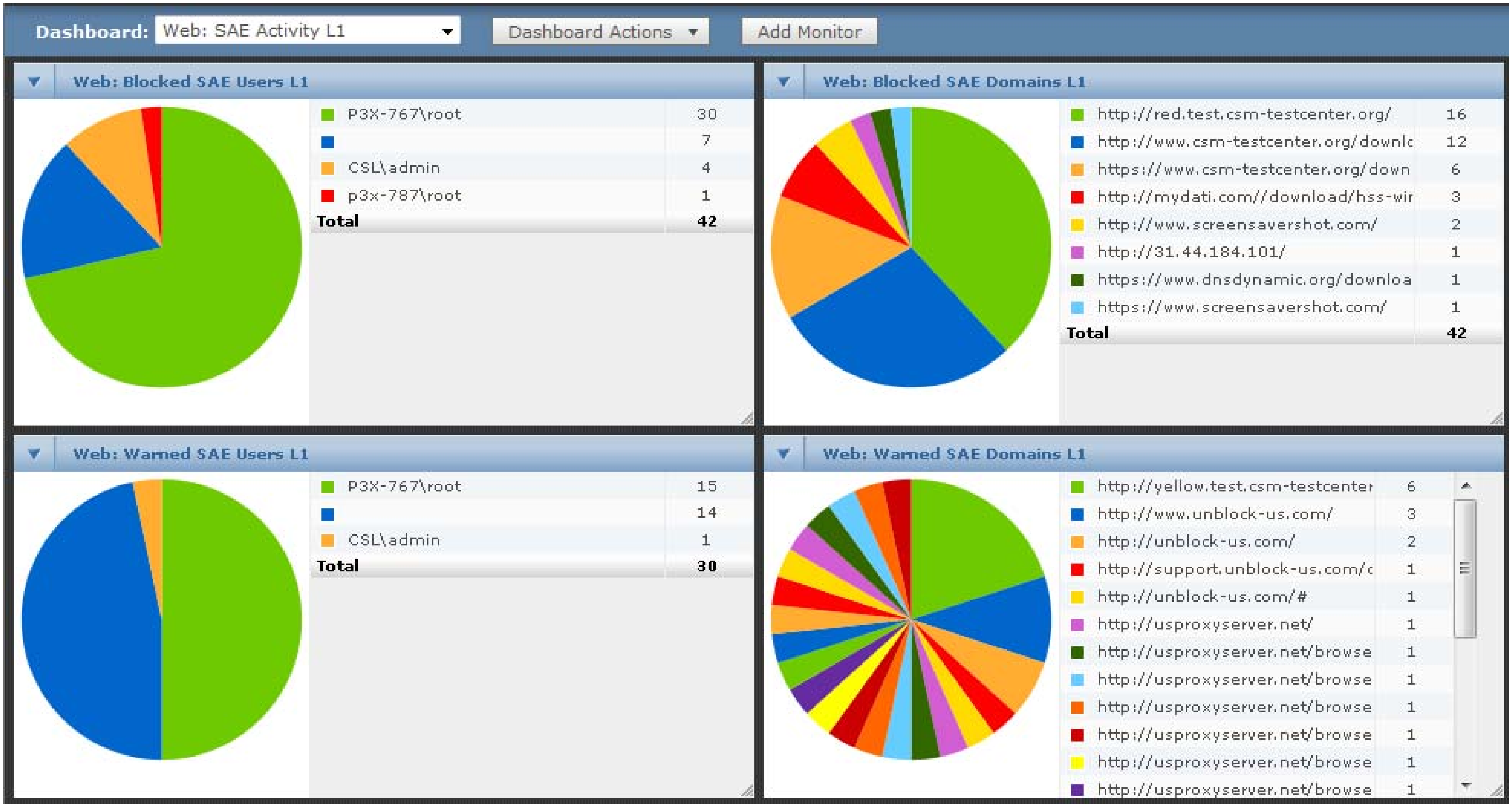
Category BlockList

No.	Category	Comment
1	Browser Exploits	Available since category set 4
2	Malicious Downloads	Available since category set 4
3	Malicious Sites	
4	Phishing	
5	PUPs	Available since category set 4
6	Spam URLs	
7	Spyware / Adware / Keyloggers	

Web Security

Web Filtering for Endpionts

FOCUS 12 SECURITY CONFERENCE



Web: Blocked SAE Users L1

🟩	P3X-767\root	30
🟦		7
🟧	CSL\admin	4
🟥	p3x-787\root	1
Total		**42**

Web: Blocked SAE Domains L1

🟩	http://red.test.csm-testcenter.org/	16
🟦	http://www.csm-testcenter.org/downlc	12
🟧	https://www.csm-testcenter.org/down	6
🟥	http://mydati.com//download/hss-wir	3
🟨	http://www.screensavershot.com/	2
🟪	http://31.44.184.101/	1
🟩	https://www.dnsdynamic.org/downloa	1
🟦	https://www.screensavershot.com/	1
Total		**42**

Web: Warned SAE Users L1

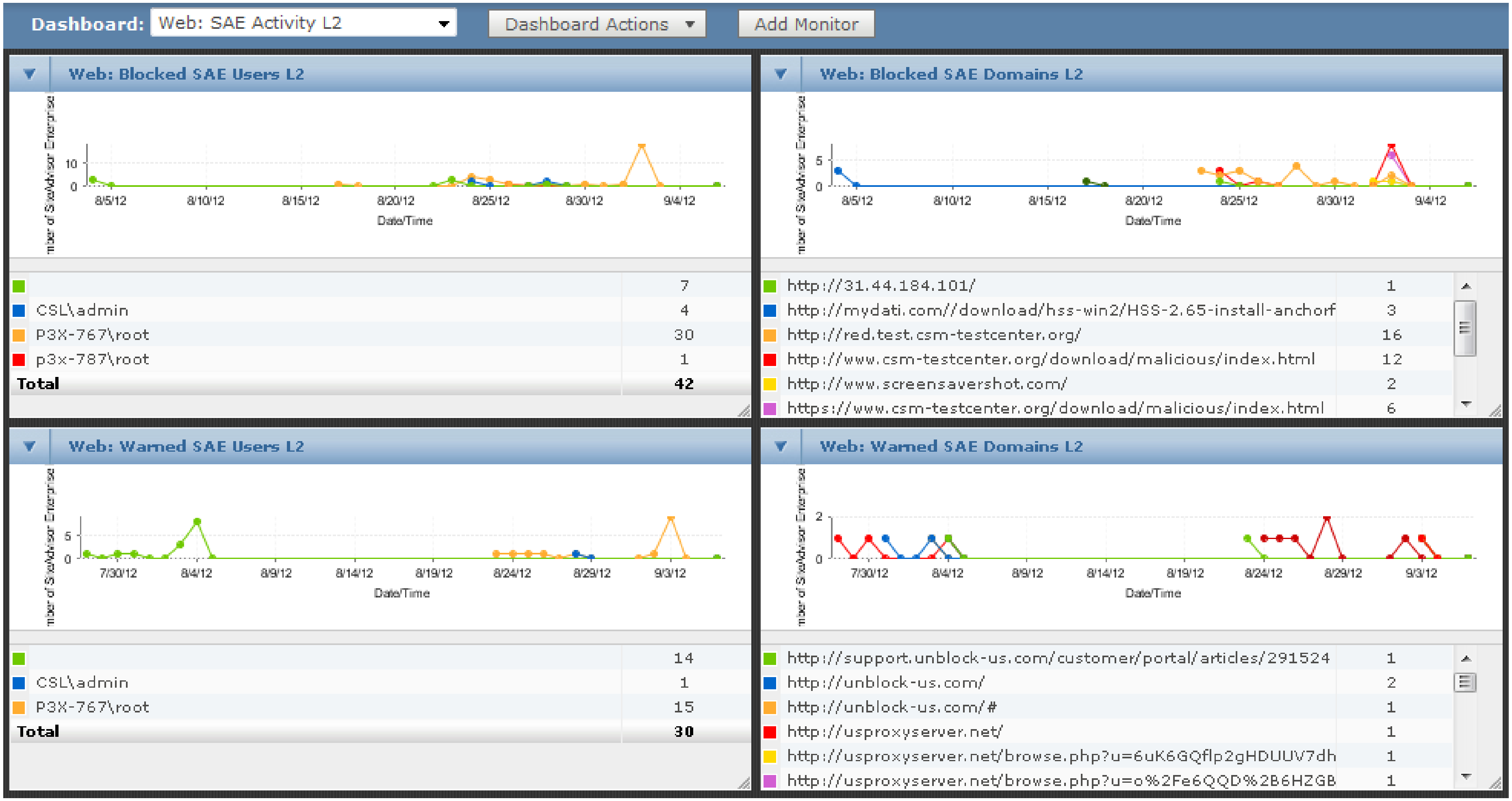
🟩	P3X-767\root	15
🟦		14
🟧	CSL\admin	1
Total		**30**

Web: Warned SAE Domains L1

🟩	http://yellow.test.csm-testcenter	6
🟦	http://www.unblock-us.com/	3
🟧	http://unblock-us.com/	2
🟥	http://support.unblock-us.com/c	1
🟨	http://unblock-us.com/#	1
🟪	http://usproxyserver.net/	1
🟩	http://usproxyserver.net/browse	1
🟦	http://usproxyserver.net/browse	1
🟧	http://usproxyserver.net/browse	1
🟥	http://usproxyserver.net/browse	1
🟨	http://usproxyserver.net/browse	1
🟪	http://usproxyserver.net/browse	1

Web Security

Web Filtering for Endpoints



Web: Blocked SAE Users L2

🟩		7
🟦	CSL\admin	4
🟧	P3X-767\root	30
🟥	p3x-787\root	1
Total		**42**

Web: Blocked SAE Domains L2

🟩	http://31.44.184.101/	1
🟦	http://mydati.com//download/hss-win2/HSS-2.65-install-anchorf	3
🟧	http://red.test.csm-testcenter.org/	16
🟥	http://www.csm-testcenter.org/download/malicious/index.html	12
🟨	http://www.screensavershot.com/	2
🟪	https://www.csm-testcenter.org/download/malicious/index.html	6

Web: Warned SAE Users L2

🟩		14
🟦	CSL\admin	1
🟧	P3X-767\root	15
Total		**30**

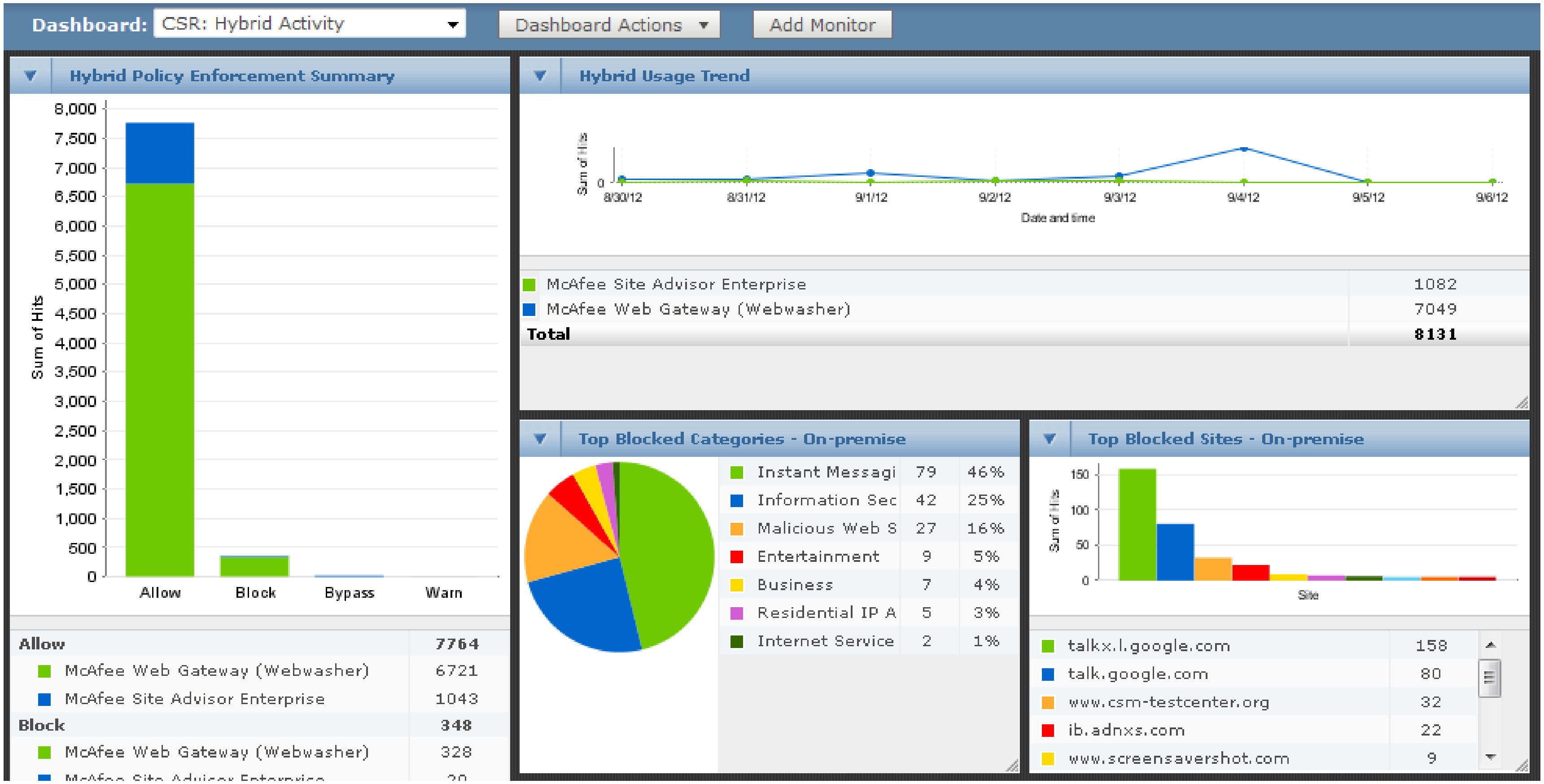
Web: Warned SAE Domains L2

🟩	http://support.unblock-us.com/customer/portal/articles/291524	1
🟦	http://unblock-us.com/	2
🟧	http://unblock-us.com/#	1
🟥	http://usproxyserver.net/	1
🟨	http://usproxyserver.net/browse.php?u=6uK6GQflp2gHDUUV7dh	1
🟪	http://usproxyserver.net/browse.php?u=o%2Fe6QQD%2B6HZGB	1

Web Security
Content Security Reporter

Key Variable: Log Source (typically SAE, MWG, or SaaS)

- Why not user group, location or department?



Hybrid Policy Enforcement Summary

Allow	**7764**
🟩 McAfee Web Gateway (Webwasher)	6721
🟦 McAfee Site Advisor Enterprise	1043
Block	**348**
🟩 McAfee Web Gateway (Webwasher)	328
🟦 McAfee Site Advisor Enterprise	20

Hybrid Usage Trend

🟩 McAfee Site Advisor Enterprise	1082
🟦 McAfee Web Gateway (Webwasher)	7049
Total	**8131**

Top Blocked Categories - On-premise

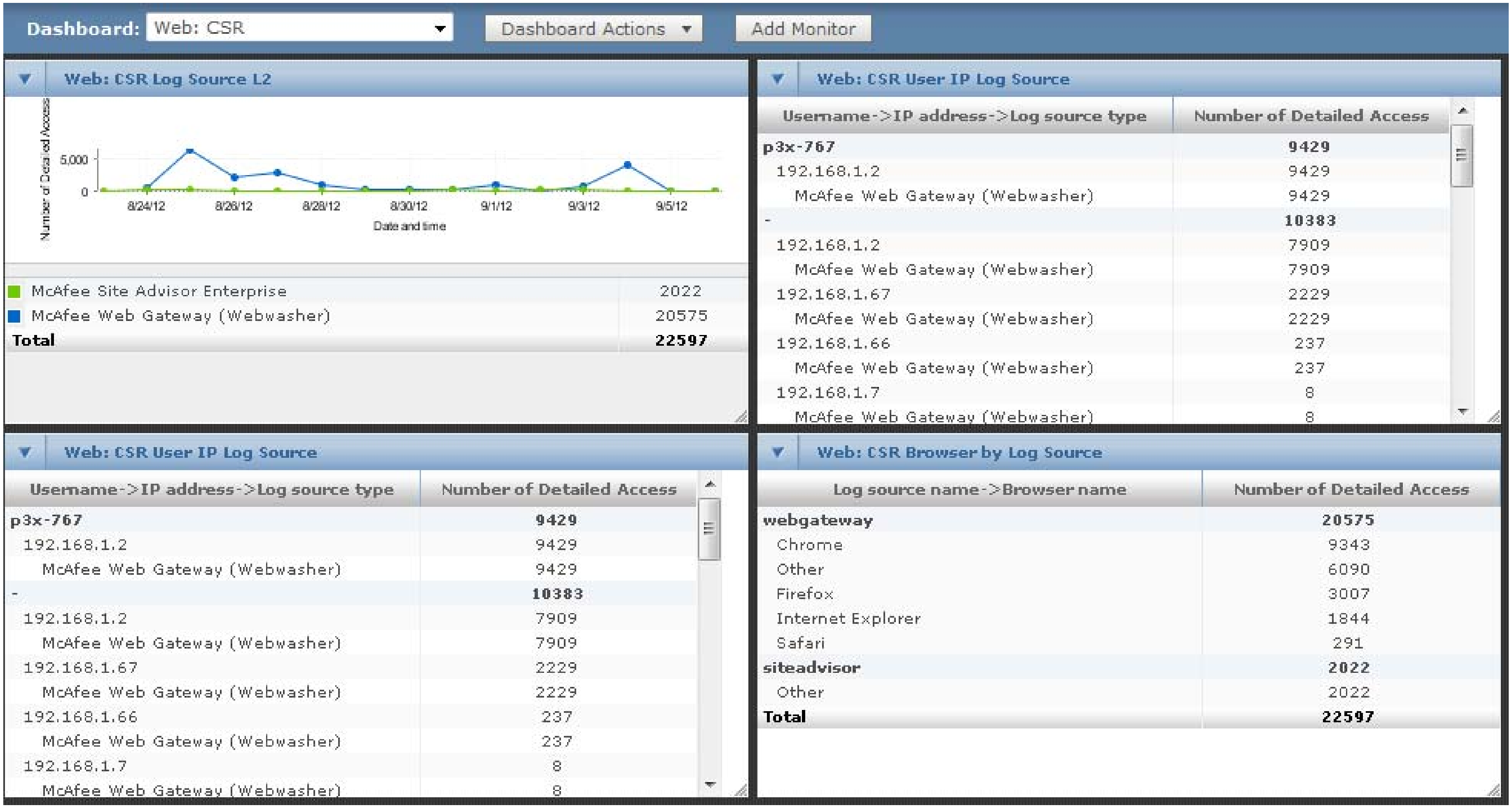
🟩 Instant Messagi	79	46%
🟦 Information Sec	42	25%
🟧 Malicious Web S	27	16%
🟥 Entertainment	9	5%
🟨 Business	7	4%
🟪 Residential IP A	5	3%
🟩 Internet Service	2	1%

Top Blocked Sites - On-premise

🟩 talkx.l.google.com	158
🟦 talk.google.com	80
🟧 www.csm-testcenter.org	32
🟥 ib.adnxs.com	22
🟨 www.screensavershot.com	9

Web Security

Content Security Reporter



Web: CSR Log Source L2

🟩 McAfee Site Advisor Enterprise	2022
🟦 McAfee Web Gateway (Webwasher)	20575
Total	**22597**

Web: CSR User IP Log Source

Username->IP address->Log source type	Number of Detailed Access
p3x-767	**9429**
192.168.1.2	9429
McAfee Web Gateway (Webwasher)	9429
-	**10383**
192.168.1.2	7909
McAfee Web Gateway (Webwasher)	7909
192.168.1.67	2229
McAfee Web Gateway (Webwasher)	2229
192.168.1.66	237
McAfee Web Gateway (Webwasher)	237
192.168.1.7	8
McAfee Web Gateway (Webwasher)	8

Web: CSR User IP Log Source

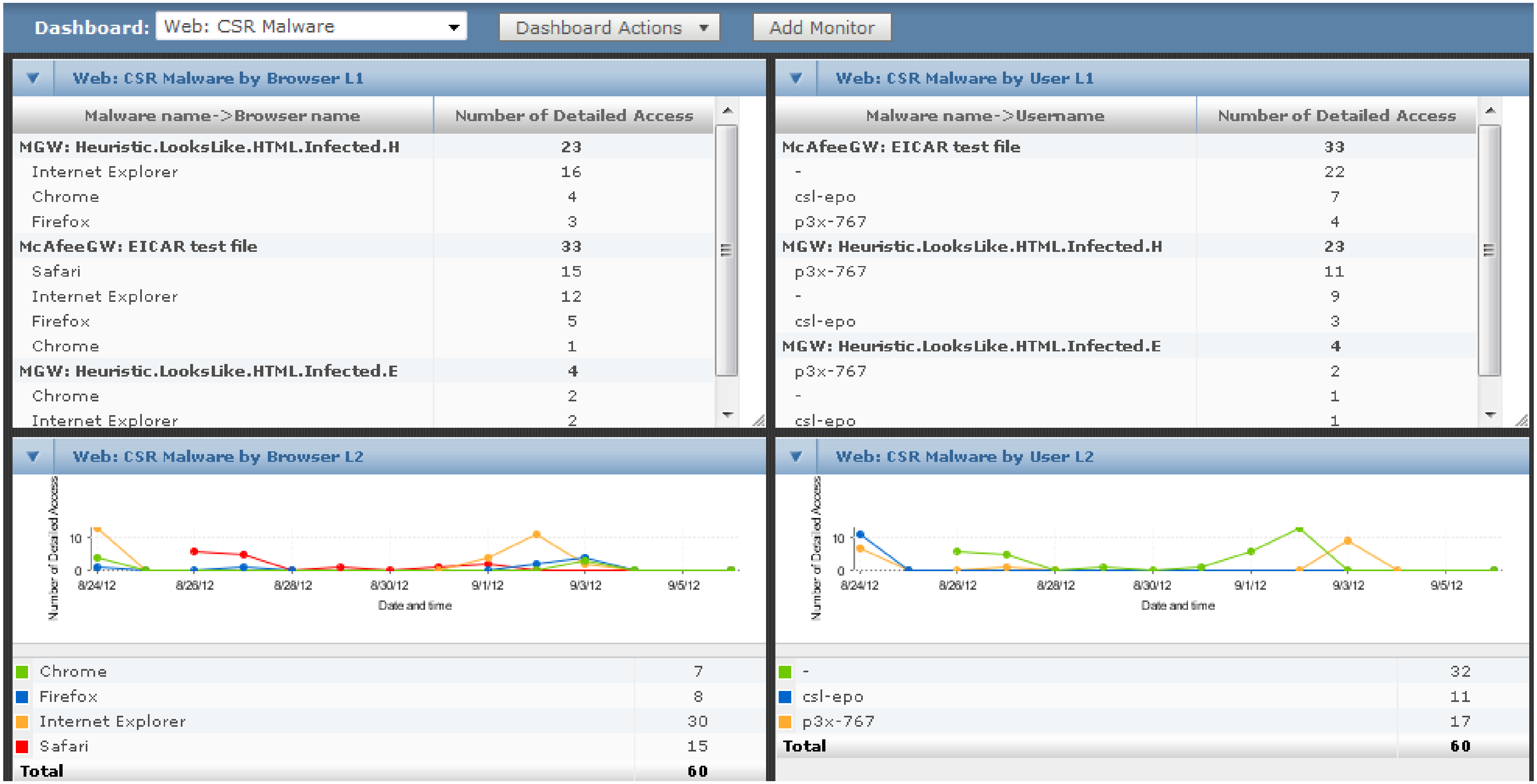
Username->IP address->Log source type	Number of Detailed Access
p3x-767	**9429**
192.168.1.2	9429
McAfee Web Gateway (Webwasher)	9429
-	**10383**
192.168.1.2	7909
McAfee Web Gateway (Webwasher)	7909
192.168.1.67	2229
McAfee Web Gateway (Webwasher)	2229
192.168.1.66	237
McAfee Web Gateway (Webwasher)	237
192.168.1.7	8
McAfee Web Gateway (Webwasher)	8

Web: CSR Browser by Log Source

Log source name->Browser name	Number of Detailed Access
webgateway	**20575**
Chrome	9343
Other	6090
Firefox	3007
Internet Explorer	1844
Safari	291
siteadvisor	**2022**
Other	2022
Total	**22597**

Web Security

Content Security Reporter



Dashboard: Web: CSR Malware ▾

▼ Web: CSR Malware by Browser L1

Malware name->Browser name	Number of Detailed Access
MGW: Heuristic.LooksLike.HTML.Infected.H	**23**
Internet Explorer	16
Chrome	4
Firefox	3
McAfeeGW: EICAR test file	**33**
Safari	15
Internet Explorer	12
Firefox	5
Chrome	1
MGW: Heuristic.LooksLike.HTML.Infected.E	**4**
Chrome	2
Internet Explorer	2

▼ Web: CSR Malware by User L1

Malware name->Username	Number of Detailed Access
McAfeeGW: EICAR test file	**33**
-	22
csl-epo	7
p3x-767	4
MGW: Heuristic.LooksLike.HTML.Infected.H	**23**
p3x-767	11
-	9
csl-epo	3
MGW: Heuristic.LooksLike.HTML.Infected.E	**4**
p3x-767	2
-	1
csl-epo	1

▼ Web: CSR Malware by Browser L2

🟩 Chrome	7
🟦 Firefox	8
🟧 Internet Explorer	30
🟥 Safari	15
Total	**60**

▼ Web: CSR Malware by User L2

🟩 -	32
🟦 csl-epo	11
🟧 p3x-767	17
Total	**60**

Use Case #4

Bandwidth & Accountability

- Challenge: How is Internet being used in a distributed environment with Web Filtering for Endpoints and McAfee Web Gateway

- Solution: Create different Log Sources in Web Reporter (since replaced with Content Security Reporter). Compare utilization between sites. Track employee behavior between sites.

Waypoints

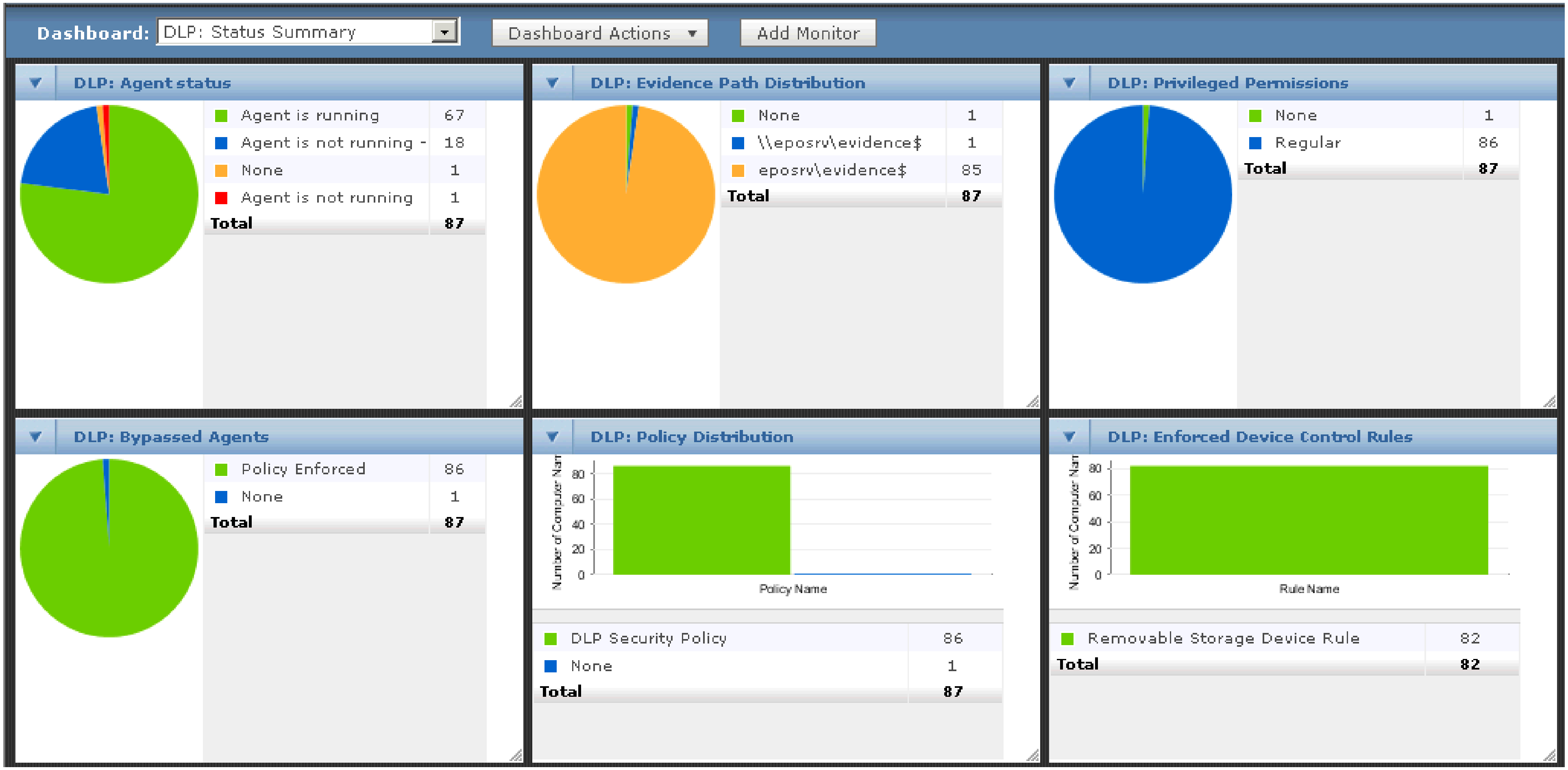
- ePolicy Orchestrator
- VirusScan Enterprise 8.8
- Host IPS 8
- Web Security (Endpoint and Gateway)
- Device Control
- Trust Control Suite (Cloud)

Device Control

- Monitor all removable devices
- Monitor all content based upon application type e.g. word, pdf, database, excel, zip
- Screenshot of policy

Device Control

- Default DLP dash



Dashboard: DLP: Status Summary

DLP: Agent status

🟩	Agent is running	67
🟦	Agent is not running -	18
🟧	None	1
🟥	Agent is not running	1
Total		**87**

DLP: Evidence Path Distribution

🟩	None	1
🟦	\\eposrv\evidence$	1
🟧	eposrv\evidence$	85
Total		**87**

DLP: Privileged Permissions

🟩	None	1
🟦	Regular	86
Total		**87**

DLP: Bypassed Agents

🟩	Policy Enforced	86
🟦	None	1
Total		**87**

DLP: Policy Distribution

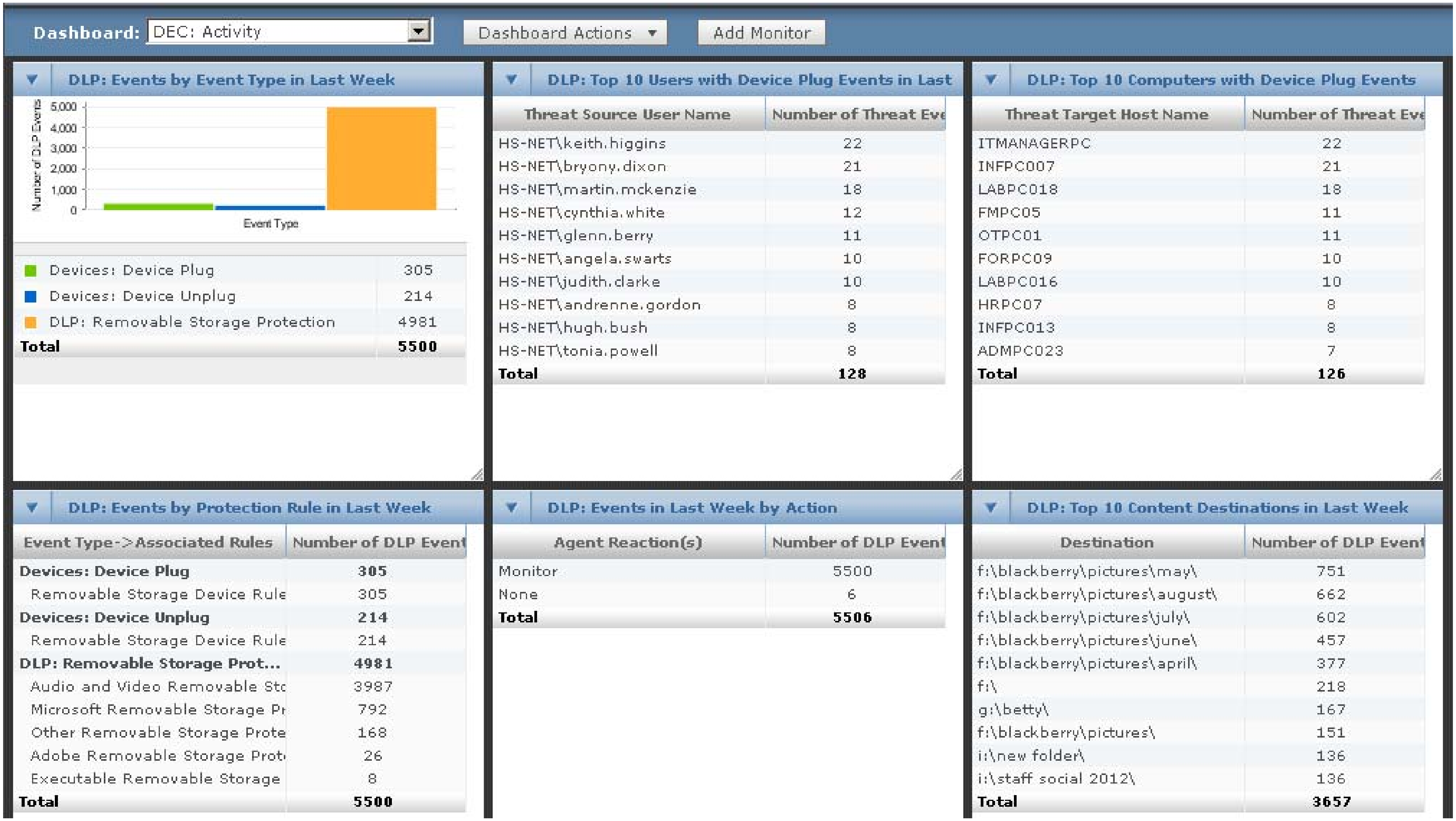
🟩	DLP Security Policy	86
🟦	None	1
Total		**87**

DLP: Enforced Device Control Rules

🟩	Removable Storage Device Rule	82
Total		**82**

Device Control

FOCUS 12 SECURITY CONFERENCE



DLP: Events by Event Type in Last Week

🟩	Devices: Device Plug	305
🟦	Devices: Device Unplug	214
🟧	DLP: Removable Storage Protection	4981
Total		**5500**

DLP: Top 10 Users with Device Plug Events in Last

Threat Source User Name	Number of Threat Eve
HS-NET\keith.higgins	22
HS-NET\bryony.dixon	21
HS-NET\martin.mckenzie	18
HS-NET\cynthia.white	12
HS-NET\glenn.berry	11
HS-NET\angela.swarts	10
HS-NET\judith.clarke	10
HS-NET\andrenne.gordon	8
HS-NET\hugh.bush	8
HS-NET\tonia.powell	8
Total	**128**

DLP: Top 10 Computers with Device Plug Events

Threat Target Host Name	Number of Threat Eve
ITMANAGERPC	22
INFPC007	21
LABPC018	18
FMPC05	11
OTPC01	11
FORPC09	10
LABPC016	10
HRPC07	8
INFPC013	8
ADMPC023	7
Total	**126**

DLP: Events by Protection Rule in Last Week

Event Type->Associated Rules	Number of DLP Event
Devices: Device Plug	**305**
Removable Storage Device Rule	305
Devices: Device Unplug	**214**
Removable Storage Device Rule	214
DLP: Removable Storage Prot...	**4981**
Audio and Video Removable Sto	3987
Microsoft Removable Storage Pr	792
Other Removable Storage Prote	168
Adobe Removable Storage Prot	26
Executable Removable Storage	8
Total	**5500**

DLP: Events in Last Week by Action

Agent Reaction(s)	Number of DLP Event
Monitor	5500
None	6
Total	**5506**

DLP: Top 10 Content Destinations in Last Week

Destination	Number of DLP Event
f:\blackberry\pictures\may\	751
f:\blackberry\pictures\august\	662
f:\blackberry\pictures\july\	602
f:\blackberry\pictures\june\	457
f:\blackberry\pictures\april\	377
f:\	218
g:\betty\	167
f:\blackberry\pictures\	151
i:\new folder\	136
i:\staff social 2012\	136
Total	**3657**

Use Case #5
Managing Updates - problem

- Customer called saying “machines aren’t updating or running the missed tasks like they are supposed to.”

- Upon logging into their ePO server we found:
  - Scheduled task set to run missed tasks after 5 minutes
  - This task had a 2 hour randomized interval

  - Can anyone guess why the updates weren’t happening on a consistent and accurate basis?

Use Case #5
Managing Updates - resolution

FOCUS12 SECURITY CONFERENCE

- The resolution was to setup a task to run “At Logon” with a 5 minute delay.

- We removed the options for:
  - Run missed tasks = 5 minutes
  - Randomization = 2 hours

- The customer now has accurate reports and can show their machines are up to date.

Use Case #6
AD Integration

- Two customers with similar problems:
  - Customer 1 – separate AD and ePO admins, ePO would suddenly show objects (AD sync) for no reason
  - Customer 2 – separate admins for different parts of organization. ePO would suddenly show objects (AD sync) for no reason
  - The problem was incorrect computer placement in AD Organizational Unit
- Solution:
  - Create and apply Group Policy Objects that customizes the McAfee Agent Custom Properties value with the OU location. This is viewable and actionable in the System Tree, Tags, etc
  - Applying a McAfee Agent Custom Property value via GPO applied at the site is a nice way of confirming along with IP address, the location within an organization.

Waypoints

- ePolicy Orchestrator
- VirusScan Enterprise 8.8
- Host IPS 8
- Web Security (Endpoint and Gateway)
- Device Control
- Trust Control Suite (Trust of the Cloud)

Trust the Cloud

FOCUS 12 SECURITY CONFERENCE

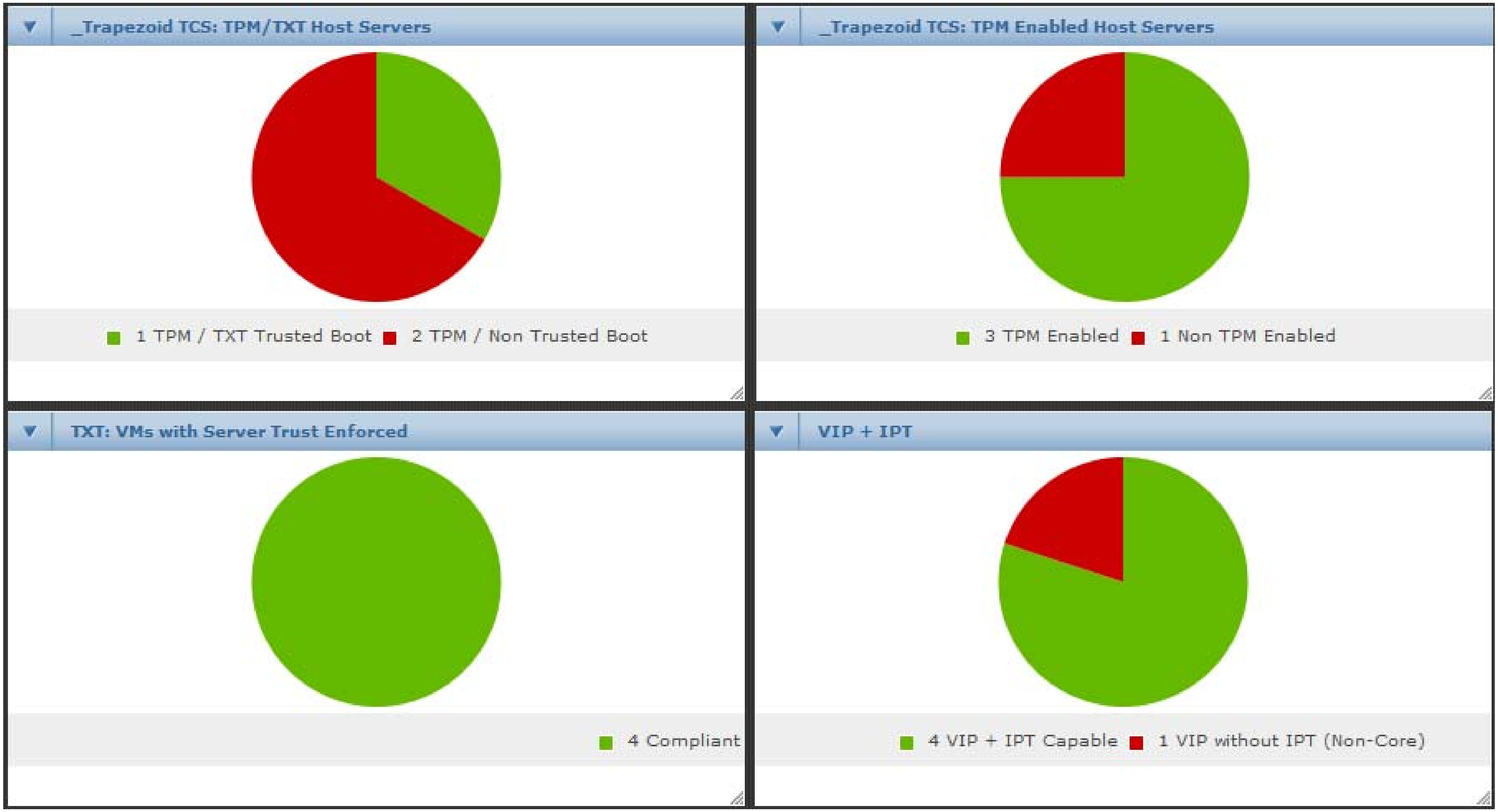
- Intel® Trusted Execution Technology (Intel® TXT)
  - Hardware extensions that enable establishing and verifying the integrity of a platform
  - Is the BIOS a known good version? Is the Operating System/Hypervisor in known good version?

- Trapezoid Trust Control Suite
  - Leverages Intel TXT and McAfee Security Management
  - Trapezoid is a McAfee SIA Partner

- Is my cloud trustworthy? If not, what actions should I take?
  - Deny further client access via MNAC
  - Disable logon in the cloud based application

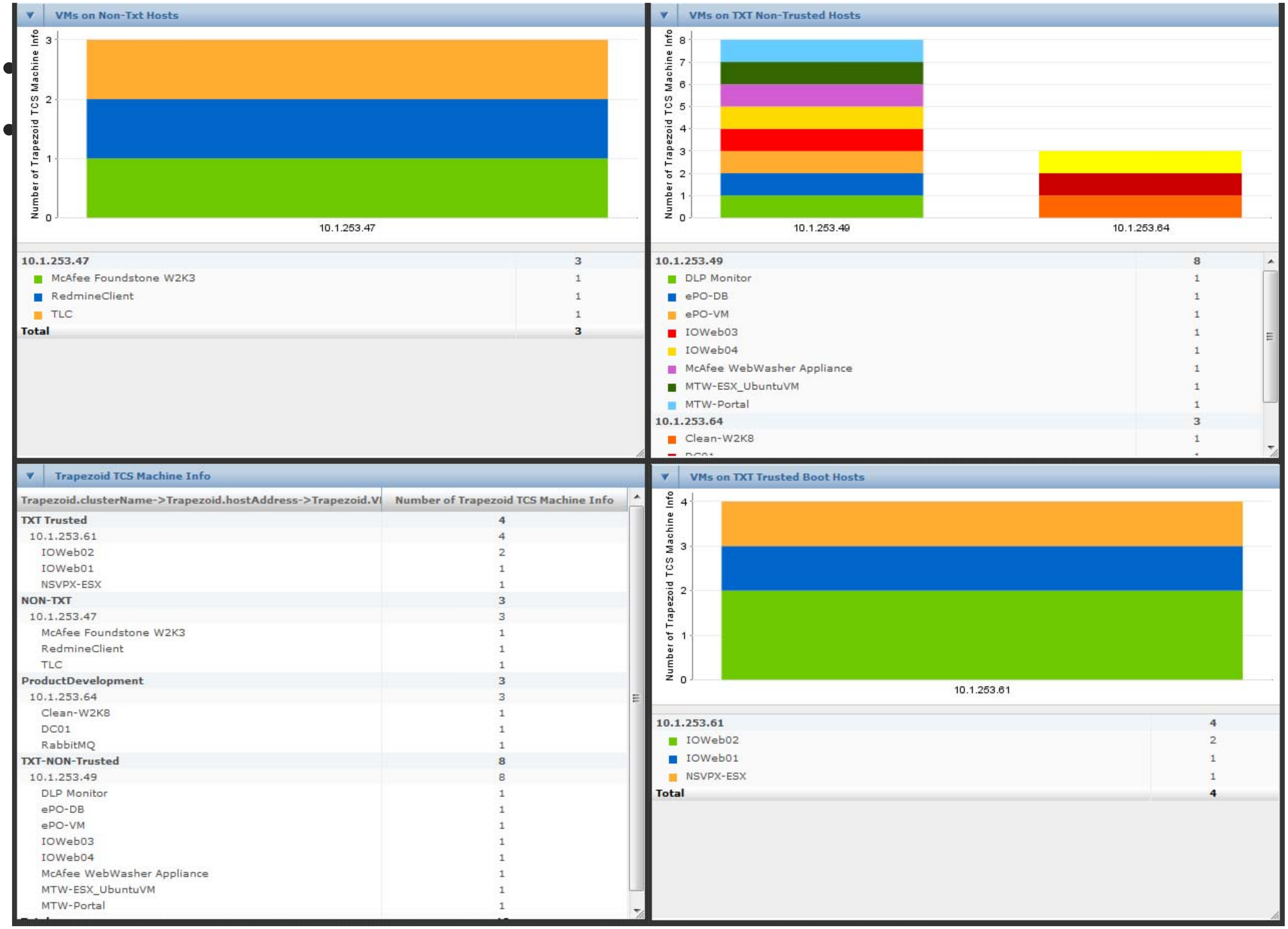
Trusting The Cloud

Trapezoid Trust Control Suite


▼ _Trapezoid TCS: TPM/TXT Host Servers
🟩 1 TPM / TXT Trusted Boot 🟥 2 TPM / Non Trusted Boot
▼ _Trapezoid TCS: TPM Enabled Host Servers
🟩 3 TPM Enabled 🟥 1 Non TPM Enabled
▼ TXT: VMs with Server Trust Enforced
🟩 4 Compliant
▼ VIP + IPT
🟩 4 VIP + IPT Capable 🟥 1 VIP without IPT (Non-Core)

Trusting the Cloud

Trapezoid Trust Control Suite



VMs on Non-Txt Hosts

10.1.253.47	**3**
🟩 McAfee Foundstone W2K3	1
🟦 RedmineClient	1
🟧 TLC	1
Total	**3**

VMs on TXT Non-Trusted Hosts

10.1.253.49	**8**
🟩 DLP Monitor	1
🟦 ePO-DB	1
🟧 ePO-VM	1
🟥 IOWeb03	1
🟨 IOWeb04	1
🟪 McAfee WebWasher Appliance	1
🟩 MTW-ESX_UbuntuVM	1
🟦 MTW-Portal	1
10.1.253.64	**3**
🟧 Clean-W2K8	1
🟥 DC01	1

Trapezoid TCS Machine Info

Trapezoid.clusterName->Trapezoid.hostAddress->Trapezoid.V	Number of Trapezoid TCS Machine Info
TXT Trusted	**4**
10.1.253.61	4
IOWeb02	2
IOWeb01	1
NSVPX-ESX	1
NON-TXT	**3**
10.1.253.47	3
McAfee Foundstone W2K3	1
RedmineClient	1
TLC	1
ProductDevelopment	**3**
10.1.253.64	3
Clean-W2K8	1
DC01	1
RabbitMQ	1
TXT-NON-Trusted	**8**
10.1.253.49	8
DLP Monitor	1
ePO-DB	1
ePO-VM	1
IOWeb03	1
IOWeb04	1
McAfee WebWasher Appliance	1
MTW-ESX_UbuntuVM	1
MTW-Portal	1

VMs on TXT Trusted Boot Hosts

10.1.253.61	**4**
🟩 IOWeb02	2
🟦 IOWeb01	1
🟧 NSVPX-ESX	1
Total	**4**

In Conclusion

- Review your environment
- Enhance your security posture through additional features or options
- Customize your instrumentation
- Use multiple criteria in layers to discover useful data
  - Source IP, process, user, host
  - Target IP, process, user, host
  - Monitor trends in your environment and build of a profile
- Collaborate with your peers

Reminder!

- Security is a process. Monitor, test and audit your environment
- Backup your security keys, policies, dashboards, tasks
- Document your policies, client and server tasks, assignments, ports, db information, credentials, System tree, purge logs
- Keep up to date:
  - – Subscribe to McAfee Support Notification Service
  - – Subscribe to the McAfee Threat Intelligence Service
  - – Use ePO Software Manager server task with an automated email response
  - – Get the free McAfee iOS apps
    - McAfee Global Threat Intelligence
    - McAfee Security Vision

Call to action

- Join the McAfee ePolicy Orchestrator LinkedIn group
- Join McAfee’s The Place
- Download our session handout
- Follow our blog

Get trained. You will be more effective at your job!

Questions?

Frequently Asked Questions

FOCUS12 SECURITY CONFERENCE

- Will you share the dashboards shown?
  - Yes!
- How many repositories do I need?
  - Probably less than you think. But you need to configure appropriate McAfee Agent policies.
- Can you provide a roadmap?
  - Not exactly. Let's call it a guide.
- Can you recommend training?
  - Absolutely, come speak with us!

Presentations

Presentations will be available post-conference at

www.mcafee.com/focus12

Password: 5THFOCUS

McAfee®

An Intel Company