

Securing Your Digital World™

FOCUS¹¹

SECURITY CONFERENCE

DATE HERE

Caribbean Solutions Lab, London Security Solutions, The Walt Disney Company, and McAfee: Deep Dive – Endpoint Protection Tips and Tricks

Sean Slattery

Technical Director & McAfee Instructor, Caribbean Solutions Lab

Dennis London

Partner & Principal Consultant, London Security Solutions



Objectives



- Product awareness tour of a popular suite: Endpoint Protection Advanced (EPA)
- Highlight key features within point products that will improve security and compliance
- Use cases and real life examples of the point products combined



Midsize Businesses Should Invest in Information Security

ID Number: G00136396, 9 December 2005

- Focus on ease of installation and deployment
 - Look for ease of manageability
 - Exploit integrated solutions
 - Limit technology providers
 - Look for extensibility of functionality
-
- Automation
 - Consistency of policy creation and behavior

Endpoint Protection Advanced

A photograph of three business professionals (two men and one woman) looking at a laptop screen in a meeting. The image is tilted and has a semi-transparent white overlay.

ePolicy Orchestrator 4.6

VirusScan Enterprise 8.8

Host IPS 8

SiteAdvisor Enterprise 3.5

Web Reporter 5.2

Device Control 9.2

Policy Auditor 5.3

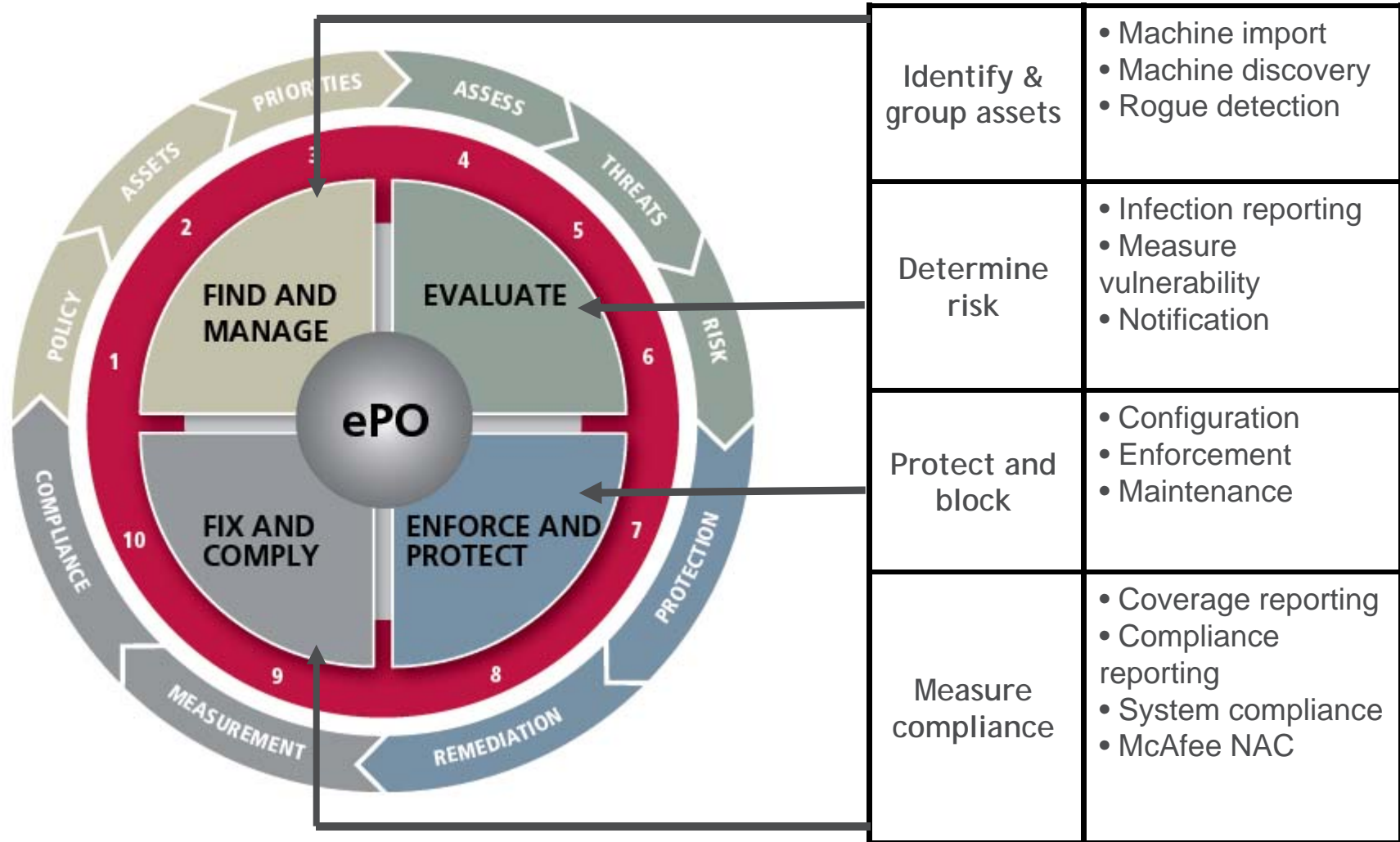
Perspective



- Very diverse customers base ranging from 7-nodes offshore financial services, 27,000-node government to 65,000 nodes commercial
- Full range of the security purchasing lifecycle: presales, services, instruction



Security is continual process



Audience Poll



- How many are IT generalists who must divide their time between security and other responsibilities?
- Who wants to manage fewer security consoles, fewer policies?
- Who is relatively new to McAfee solutions?
- What is the average size of your installations? Under 50? 500? 5000? Anyone greater than 10,000?

Building and Maintaining a Strong Foundation

- To have good management you need a manageable infrastructure
- Agent is king
- Nothing happens unless you tell it to
- Backup your server, security keys, policies, etc
- Periodically purge the logs via server task
- Keep up with McAfee versions, patches and hotfixes

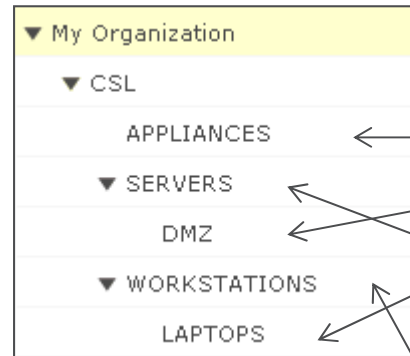
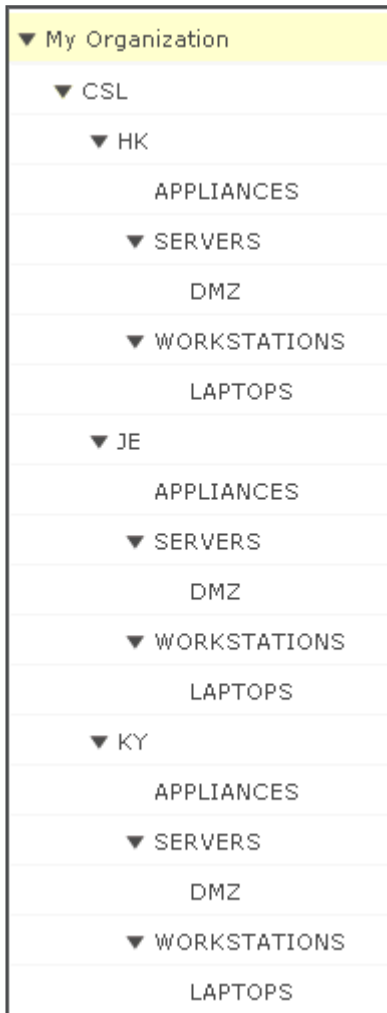


Periodically audit your system by generating some events and verify logs and notifications e.g. test files at www.eicar.org or www.spycar.org for endpoints or www.csm-testcenter.org for web.

KISS – Keep it Stupid & Simple



- System Tree – Complex vs Simple – Tags – System Tree Sorting

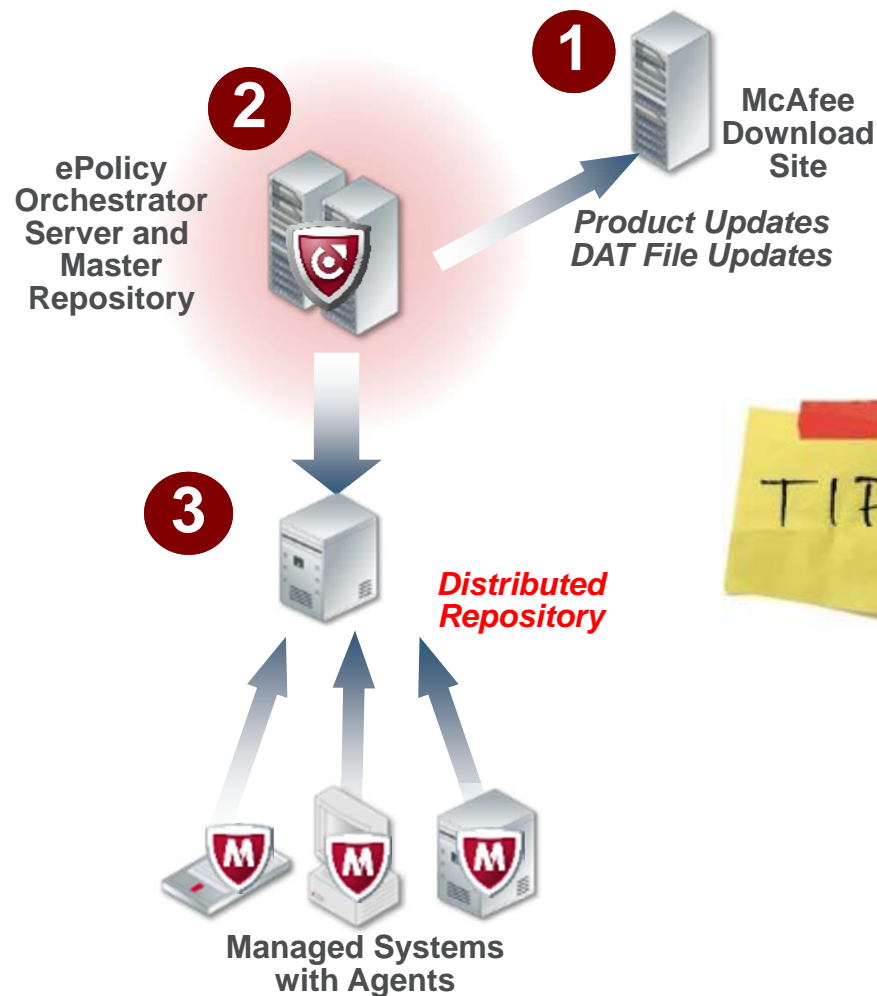


Tags
Appliance
DMZ
Laptops
Server
VMware
Windows 2003
Windows 2008 R2
Windows 7
Windows XP
Workstation



For pilot deployments, associate a manual tag e.g. pilot with a targeted deployment task

Distributing Applications & Content



Place Distributed Repositories on remote ends of slower network links. Branch office domain controllers are good candidates.

Super Agent Repositories



- Configure via Agent Policy

Convert agents to SuperAgents (Windows only)

Use systems running SuperAgents as distributed repositories

Repository path:

- Create server task to replicate or use Global Updating

1. Actions:

Replication type: Replicate to:

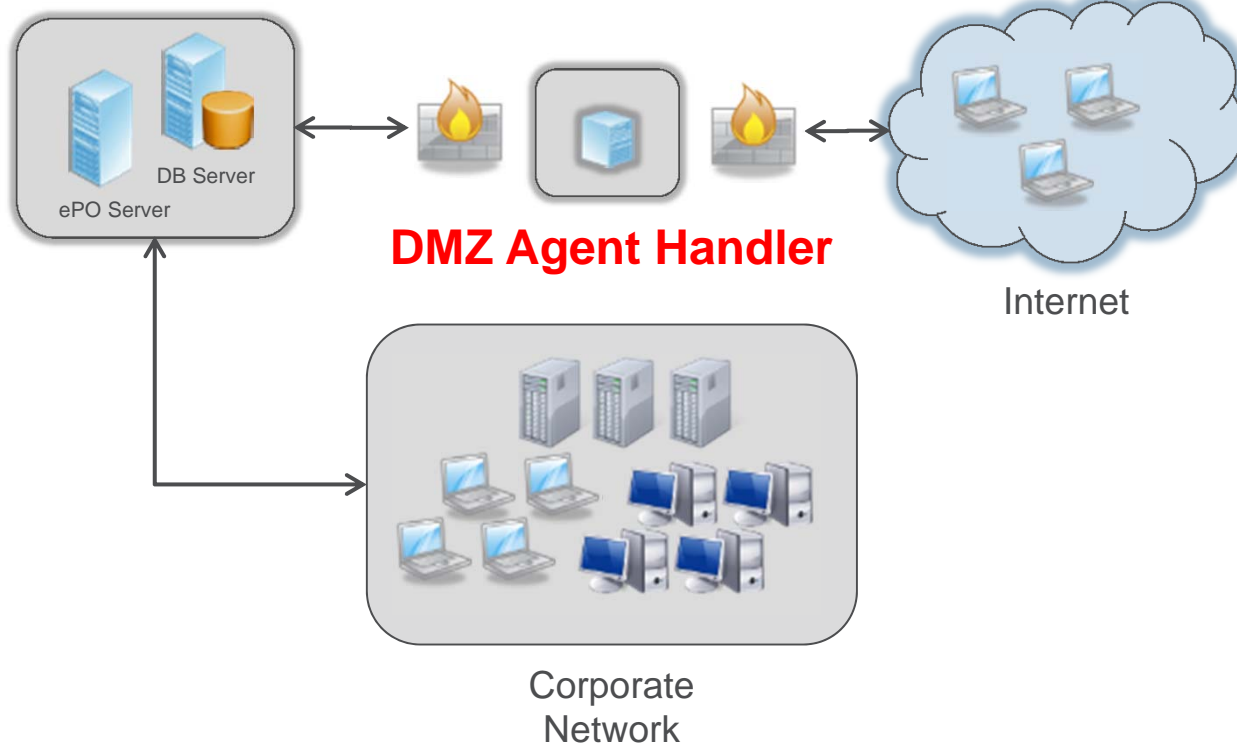
All repositories

Selected repositories: 0

Securely Handling Remote Systems



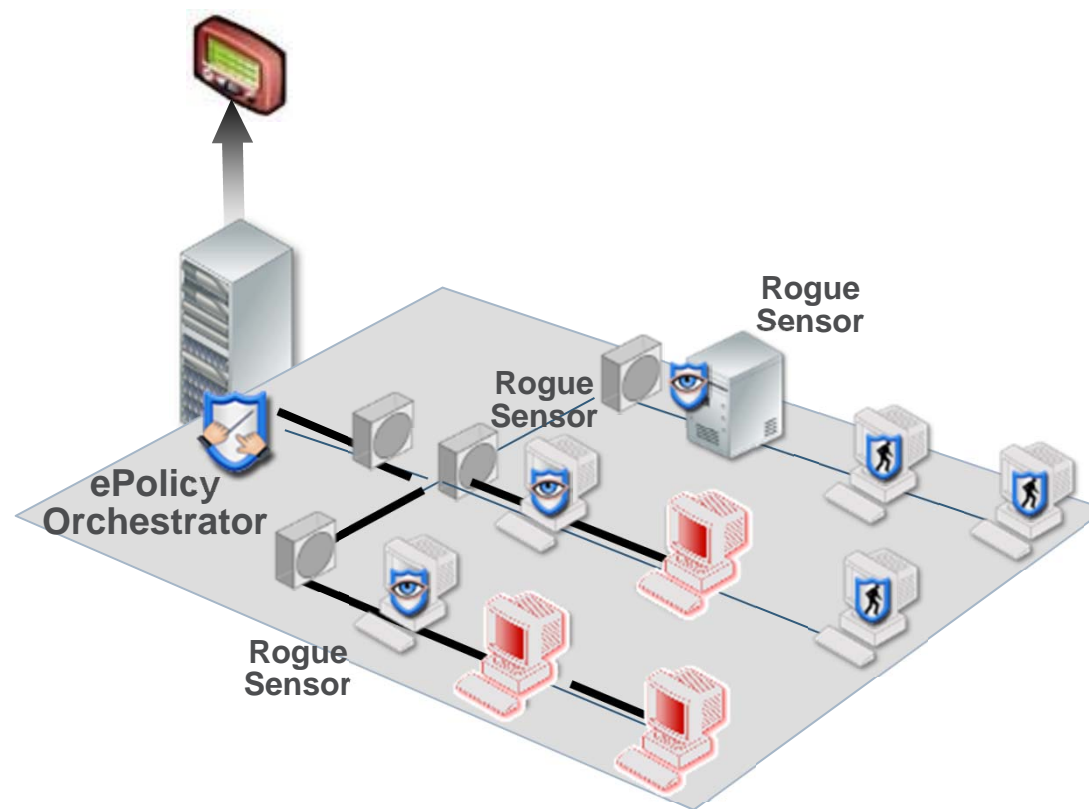
Handler List				
Handler DNS Name	Handler IP Address	Published DNS Name	Published IP Address	Last Co
web01.local	192.168.197.21	citri-ky	209.27.	8/3/11
epo01.local	192.168.197.32			8/5/11



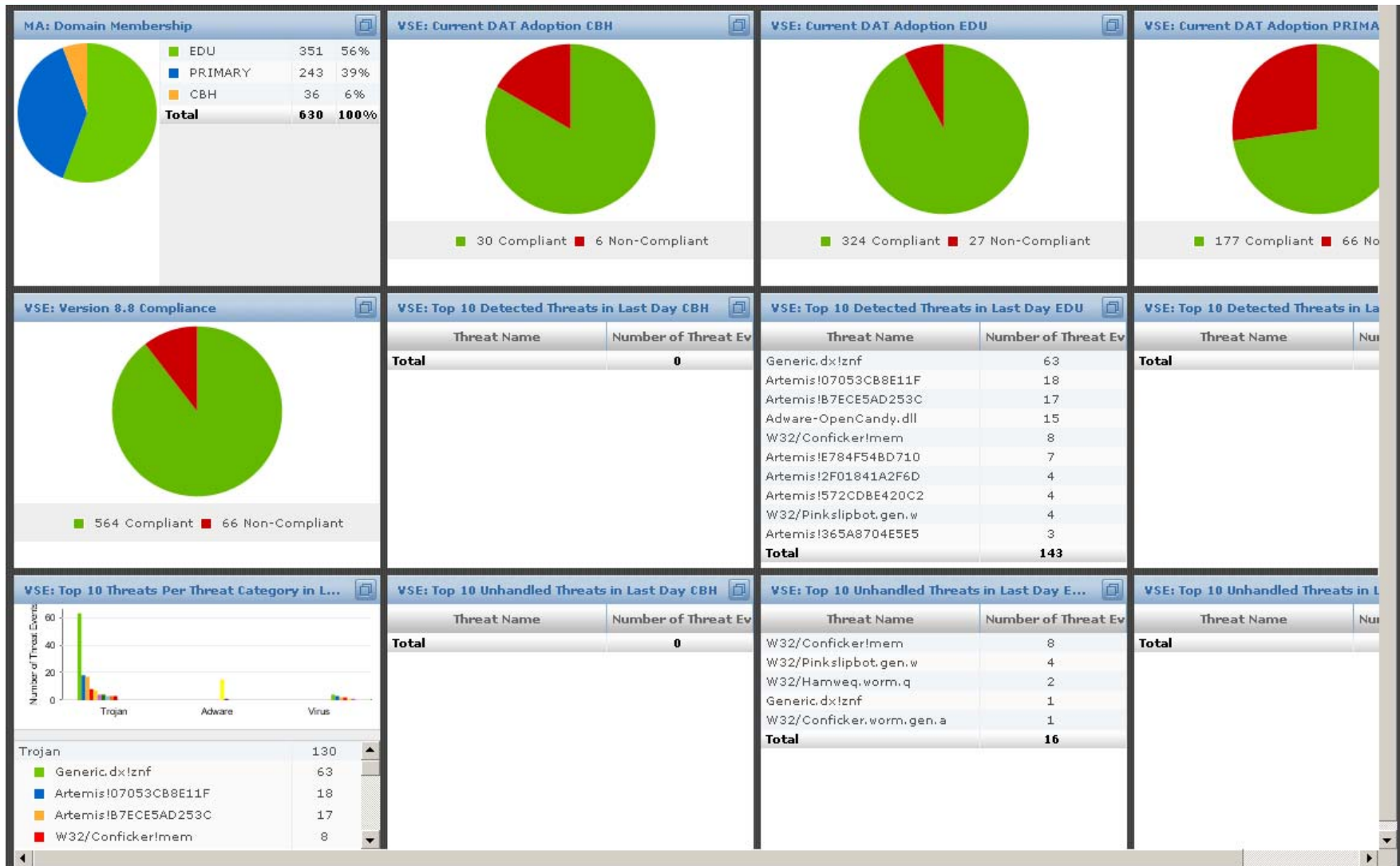
Detecting and Managing Rogue Systems

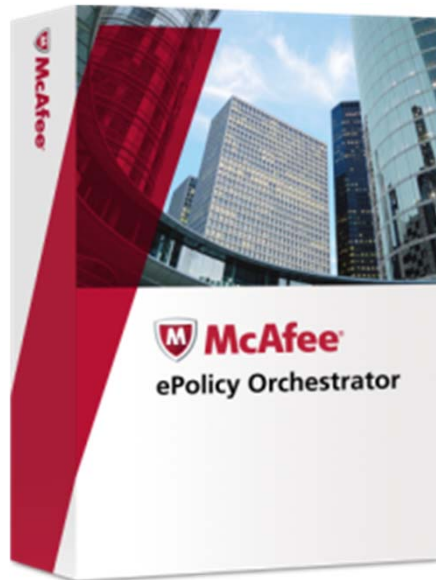


- Rogue System Sensors – one per broadcast domain or on DHCP server
- Automatic Response – Add Deploy Agent and Alert Administrator actions



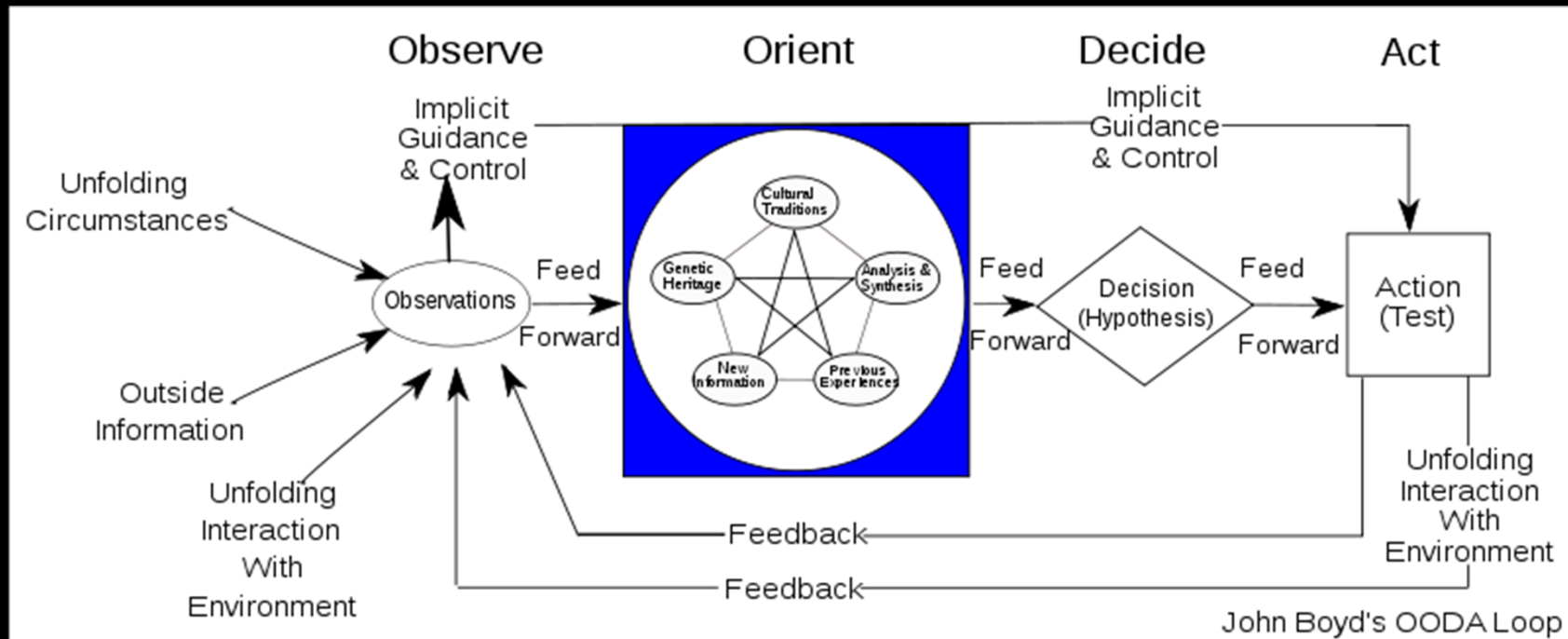
Monitoring and Reporting





Question about ePO?

What is O.O.D.A.



Using the O.O.D.A. Loop with VirusScan



- Observe
 - What are the problems in your environment?
 - Is your only solution VSE – “what can an AV scanner do?”
- Orient
 - Unlock the true potential of VSE 8.8
- Decide
 - What is more important?
 - Your user’s access or your security
- Act
 - Review your logs, decide your actions, test configurations, and deploy

NOTE – this can be done with just about every McAfee technology

True Potential of VirusScan Enterprise



Regain desktop control from users

Enforce change controls

Provide real Zero-Day protection

You can Prevent FakeAV

Learn to Exclude – Not disable

VSE – Users with Admin Privileges



Users were granted Admin privileges years ago

- Regain control regardless of permissions

Consumerization of IT

- Users can purchase better equipment

Easier for user to do updates

- May be easier but not necessarily safer

Best Practices



Removing local administrative rights from users mitigates against:

- 75% of the Critical Windows 7 vulnerabilities reported by Microsoft to date
- 100% of Microsoft Office vulnerabilities reported in 2010
- 100% of Internet Explorer and IE 8 vulnerabilities reported in 2010
- 64% of **ALL** Microsoft vulnerabilities reported in 2010

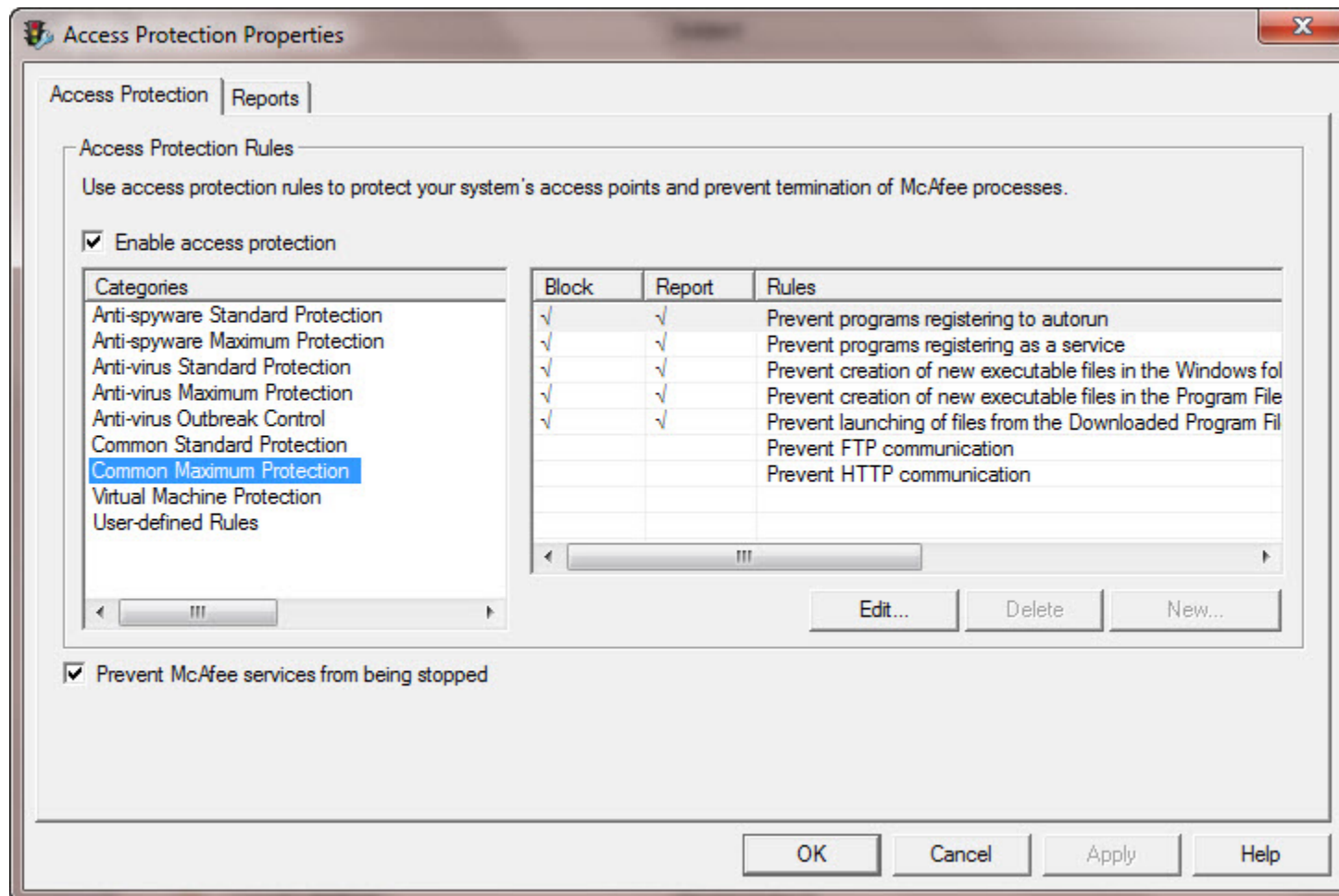
Source: BeyondTrust 2010 Microsoft Vulnerability Report

February 5, 2013

Enforcing Change Control with VSE 8.8



Change Control Management, Zero-Day Protection



McAfee has released the following documents with detailed information about FakeAlert characteristics, symptoms, prevention, and mitigation.

PD23178 - Threat Advisory: Combating FakeAlerts

<https://kc.mcafee.com/corporate/index?page=content&id=PD23178>

PD23177 - Threat Advisory: FakeAlert System Defender

<https://kc.mcafee.com/corporate/index?page=content&id=PD23177>

By using the Access Protection rules explained in the McAfee Labs report, you will have a few additional benefits besides preventing FakeAV:

- No more unauthorized applications
- Regain control of the Change Control process
- End the “multi-clicker” issues
- And many more advantages

- Reports and Queries
 - Top 10's
 - Schedule reports for reoccurring dates/times
 - Trend Analysis
- Dashboards
 - Are combined views of queries and reports
 - Defaults are good but don't always meet your specific needs
 - Customize per individual (CIO, CISO, VP-IT, DIR, MGR, you)
- Automatic Responses
 - Are you using any or do you run in a knee-jerk reactionary state?

KB66909

Master KB Article for Exclusions

You need to study it, know it, and bookmark it.
“Learn to exclude – not disable” – Dennis London



Question about VirusScan?

To Patch or Not to Patch?



Host IPS Buffer Overflow Protection mitigates:

- 100% of current Critical Adobe and Apple Vulnerabilities
- 100% of current Critical Severity and 81% of current High Severity Microsoft Vulnerabilities
- 80% of current Critical Google Chrome Vulnerabilities
- 85% of Mozilla High Severity Vulnerabilities

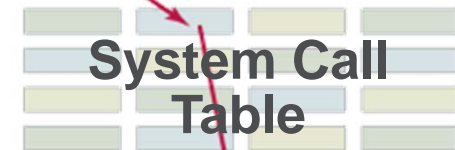
Source: McAfee Labs, valid as of publishing date: 1 August 2011

How Does HIPS Work?



- McAfee Host IPS validates system calls made into the different layers of the OS and kernel
- Calls are matched to a constantly updated database of both specific and generic attack behaviors
- If an attack is found, pre-emptive action is automatically taken ranging from 'Log Event' to 'Prevent'
- All activity on the host is seen and analyzed, and is not impaired by encryption, switched data or reliance on system log information

User Mode



OS
Kernel

Kernel Mode



Accessing HIPS Events and Rules



The screenshot displays the McAfee ePolicy Orchestrator 4.6.0 (Build 1029) interface. The main window is titled "Host IPS" and shows a list of events and rules. The interface includes a navigation menu on the left, a top navigation bar with icons for Dashboards, Systems Tree, Queries & Reports, Policy Catalog, and Software Manager, and a main content area with a table of events and rules.

Host IPS

Reporting

Systems

Policy

Software

Automation

Risk & Compliance

User Management

Configuration

Dashboards
Access your favorite queries and charts in a quick overview format.

Queries & Reports
View existing queries and reports, create new charts, tables, and graphs with the Query Builder, or design new reports using the Report Editor.

Threat Event Log
View threat and security events from your managed systems.

McAfee Labs
View the currently tracked security threats from McAfee Labs.

Risk Metrics
Displays enterprise risk information from Risk Advisor.

Host IPS
View and manage Host IPS event and client learned rules.

Host IPS 8.0

Blocking Client Rules

Severity: All Severities

Hidden/Unhidden: Unhidden

Aggregate Clear

Name	Event Category	Signature Name (No...	Threat Target IPv4 A...	Action Taken		
APVIS-270	Network IPS	TCP Port Scan	10.100.1.14	Blocked		
KV2KB-604	Buffer Overflow	Suspicious Function In...	172.40.2.92	Blocked		
KV2KB-120	Buffer Overflow	Suspicious Function In...	172.40.0.120	Blocked		
KV2KB-383	File system	Outlook Envelope - Da...	172.40.2.73	Permitted		
APXP-377	File system	Outlook Envelope - Co...	10.90.1.121	Permitted		
KV2KB-39	Buffer Overflow	Suspicious Function In...	172.40.0.39	Blocked		
APXP-44	File system	Outlook Envelope - Co...	10.90.0.44	Permitted		
APXP-394	Network IPS	MSSQL Resolution Ser...	10.90.1.138	Blocked		
APVIS-32	Buffer Overflow	Suspicious Function In...	10.100.0.32	Blocked		
APXP-997	Network IPS	MSSQL Resolution Ser...	10.90.3.229	Blocked		
4/24/11 4:40:21 PM	Warning	DEMO-SRV2KB-30	Program	IE Envelope - Executio...	172.40.0.30	Permitted
4/24/11 4:10:07 PM	Critical	DEMO-LAPXP-399	Network IPS	MSSQL Resolution Ser...	10.90.1.139	Blocked
4/24/11 1:33:12 PM	Critical	DEMO-LAPXP-631	Network IPS	MSSQL Resolution Ser...	10.90.2.139	Blocked
4/24/11 12:54:39 PM	Critical	DEMO-LAPXP-1030	Network IPS	Vulnerabilities in DRS...	10.90.4.6	Blocked
4/24/11 7:29:33 AM	Warning	DEMO-LAPVIS-1532	Program	IE Envelope - Abnorm...	10.100.3.232	Permitted
4/24/11 4:30:30 AM	Critical	DEMO-LAPVIS-1172	Buffer Overflow	Suspicious Function In...	10.100.4.148	Blocked
4/24/11 4:07:39 AM	Critical	DEMO-LAPXP-260	Buffer Overflow	Suspicious Function In...	10.90.1.4	Blocked
4/24/11 1:41:28 AM	Critical	DEMO-LAPXP-1124	Buffer Overflow	Suspicious Function In...	10.90.4.100	Blocked
4/23/11 10:27:24 PM	Warning	DEMO-LAPVIS-321	File system	Outlook Envelope - Co...	10.100.1.63	Permitted
4/23/11 7:34:20 PM	Critical	DEMO-LAPXP-346	Network IPS	Vulnerabilities in DRS...	10.90.1.90	Blocked
4/23/11 6:13:11 AM	Critical	DEMO-LAPVIS-1083	Buffer Overflow	Suspicious Function In...	10.100.4.39	Blocked
4/23/11 5:33:35 AM	Warning	DEMO-LAPXP-1093	Program	IE Envelope - Abnorm...	10.90.4.29	Permitted

Select all in this page Select all in all pages 1132 items in 143 pages. Go to page: 1

Actions Show Source Systems Show Target Systems

HIPS Client Events



The screenshot shows the McAfee Host IPS console interface. The top navigation bar includes 'Menu', 'Host IPS', 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', and 'Software Manager'. The main content area is divided into a 'System Tree' on the left and a central panel. The central panel has tabs for 'Events', 'IPS Client Rules', 'Firewall Client Rules', and 'Application Blocking Client Rules'. Under the 'Events' tab, there are filters for 'Event type' (set to 'All Events'), 'Severity', 'Read/Unread' (set to 'Unread'), and 'Hidden/Unhidden'. Below the filters is a table titled 'My Organization' with the following data:

	Event Generate...	Threat Severity	System Name	Event Category
<input type="checkbox"/>	4/26/11 3:43:04 PM	Critical	DEMO-LAPVIS-270	Network IPS
<input type="checkbox"/>	4/26/11 4:01:15 AM	Critical	DEMO-SRV2K8-604	Buffer Overflow
<input type="checkbox"/>	4/26/11 2:13:13 AM	Critical	DEMO-SRV2K8-120	Buffer Overflow

HIPS Client Rules



The screenshot shows the McAfee management console interface. At the top, there is a navigation bar with a 'Menu' dropdown and a 'Host IPS' button. To the right of these are icons for 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', and 'Software Mana'. Below the navigation bar, the 'System Tree' on the left shows 'My Organization' selected. The main content area has tabs for 'Events', 'IPS Client Rules', 'Firewall Client Rules', and 'Application Blocking Client Rules'. The 'IPS Client Rules' tab is active, displaying a 'Creation time' filter set to 'No Filter' and a search input field. Below this, a table header is visible with columns for 'My Organization', 'Enabled', 'Creation Date', 'Last Modified Date', and 'System N'.

My Organization	Enabled	Creation Date	Last Modified Date	System N
-----------------	---------	---------------	--------------------	----------

HIPS Firewall Client Rules



The screenshot displays the McAfee Host IPS management console. The top navigation bar includes a 'Menu' dropdown and several icons for 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', and 'Software Manager'. The main interface is divided into a left-hand 'System Tree' and a right-hand main content area. The 'System Tree' shows a hierarchy starting with 'My Organization', which is expanded to show 'DEMO', and further sub-categories: 'DEMO-Laptops', 'DEMO-Servers', 'DEMO-Workstations', and 'Lost&Found'. The main content area has tabs for 'Events', 'IPS Client Rules', 'Firewall Client Rules' (which is selected), and 'Application Blocking Client Rules'. Below the tabs, there is a 'Creation time' filter set to 'No Filter' and a search input field. At the bottom, a table header is visible with columns: 'My Organization', 'Enabled', 'Effective Reaction', 'Direction', and 'IP Protocol'.

HIPS Application Blocking Rules



The screenshot shows the McAfee Host IPS management console. The top navigation bar includes a 'Menu' dropdown, a 'Host IPS' button, and icons for 'Dashboards', 'System Tree', 'Queries & Reports', 'Policy Catalog', and 'Software Manager'. The left sidebar shows a 'System Tree' with 'My Organization' expanded to show 'DEMO', 'DEMO-Laptops', 'DEMO-Servers', 'DEMO-Workstations', and 'Lost&Found'. The main content area has tabs for 'Events', 'IPS Client Rules', 'Firewall Client Rules', and 'Application Blocking Client Rules'. The 'Application Blocking Client Rules' tab is active, showing a 'Creation time' filter set to 'No Filter' and a search box. Below this is a table with the following columns: 'Enabled', 'Creation Date', 'Modified Date', and 'System Name'. The table is currently empty.

Enabled	Creation Date	Modified Date	System Name
---------	---------------	---------------	-------------

HIPS Policy Categories

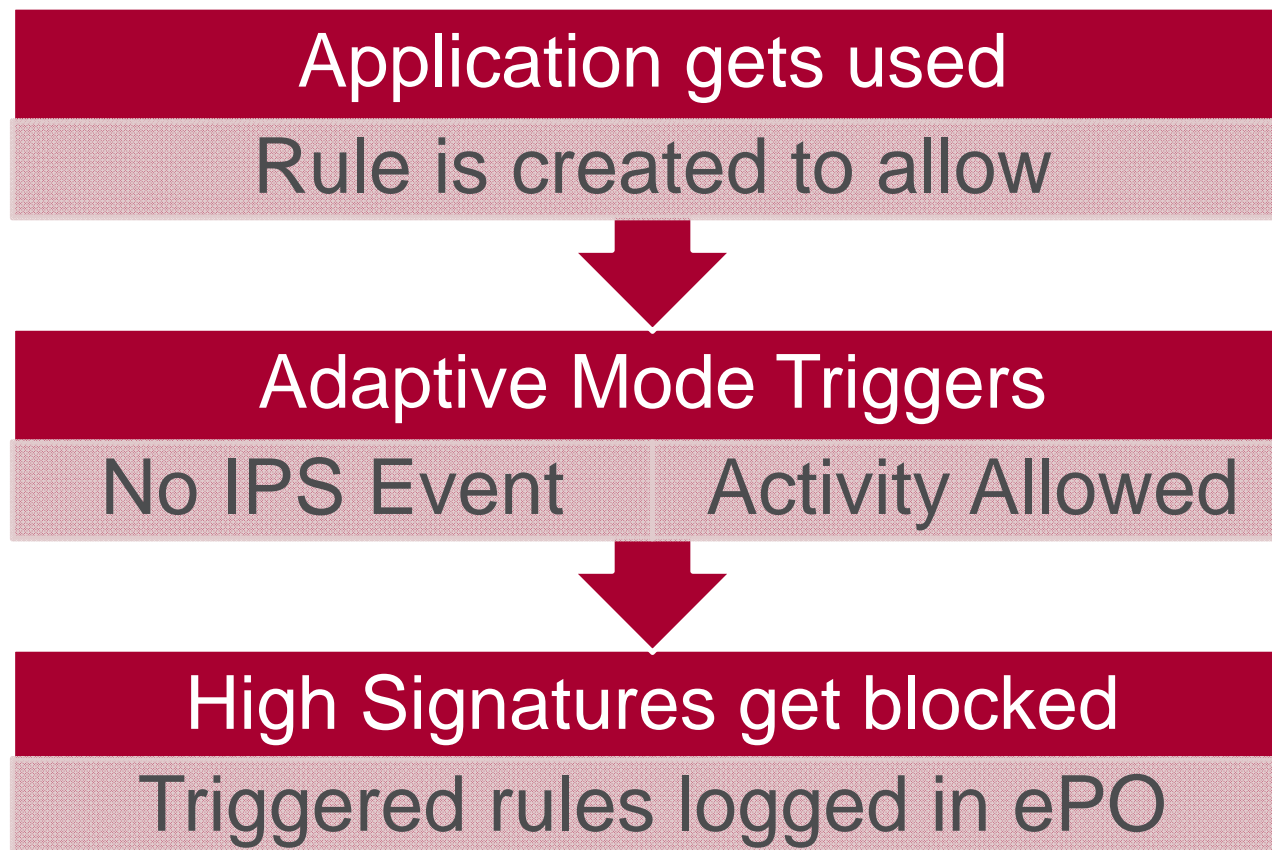


Select this policy...	For these options...
Basic Protection (McAfee Default)	<ul style="list-style-type: none">• Prevent high severity level signatures and ignore the rest
Enhanced Protection	<ul style="list-style-type: none">• Prevent high and medium severity level signatures and ignore the rest
Maximum Protection	<ul style="list-style-type: none">• Prevent high, medium, and low severity level signatures and log the rest
Prepare for Enhanced Protection	<ul style="list-style-type: none">• Prevent high and log medium severity level signatures and ignore the rest
Prepare for Maximum Protection	<ul style="list-style-type: none">• Prevent high and medium severity level signatures, log low severity level signatures, and ignore the rest
Warning	<ul style="list-style-type: none">• Log high severity level signatures and ignore the rest

HIPS Adaptive Mode



Adaptive Mode is an extremely powerful tool for creating HIPS rules based on the host's activity...without admin interaction.



HIPS Adaptive Mode



Dashboards System Tree Queries & Reports Policy Catalog Sol

Host Intrusion Prevention 8.0:IPS > IPS Options (All Platforms) > LSS Adaptive Mode

IPS status:	<input checked="" type="checkbox"/> Host IPS enabled <input checked="" type="checkbox"/> Adaptive mode enabled (rules are learned automatically)
IPS client rules:	<input checked="" type="checkbox"/> Retain existing client rules when this policy is enforced
Windows only:	<input type="checkbox"/> Network IPS enabled <input checked="" type="checkbox"/> Automatically block network intruders: For (minutes): <input type="text" value="10"/> <input checked="" type="checkbox"/> Retain blocked hosts <input type="checkbox"/> Automatically include network-facing and service-based applications in the a <input type="checkbox"/> Startup IPS protection enabled



Question about Host IPS?

Field Notes



- Artemis, AntiSpyware, Access Protection, Not Best Practices, Rogue System Detection and Host IPS



- What happened to my perimeter? Life happened.
- Why endpoint protection? Mobile users!
- Site Advisor – Browser based Security Filtering for IE, Firefox, Chrome
- Web Filtering for Endpoints – Content Filtering at the Browser
- Web Reporter (Separate Server Install)

Explicitly permit trusted sites e.g.

.mcafee.com
.nai.com
.trustedsource.org



Installation notes: ePO extension and deployment package

- Explicitly Prohibit – Custom messaging



Syntax does not require * wildcard prefix.
Include link to corporate logo

Web Filtering for Endpoints



- Content Actions
- Recommended for Blocking - Risk/Fraud/Crime Functional Group

SiteAdvisor Enterprise Plus 3.0.0 > Content Actions > CSL

Manage Category Actions

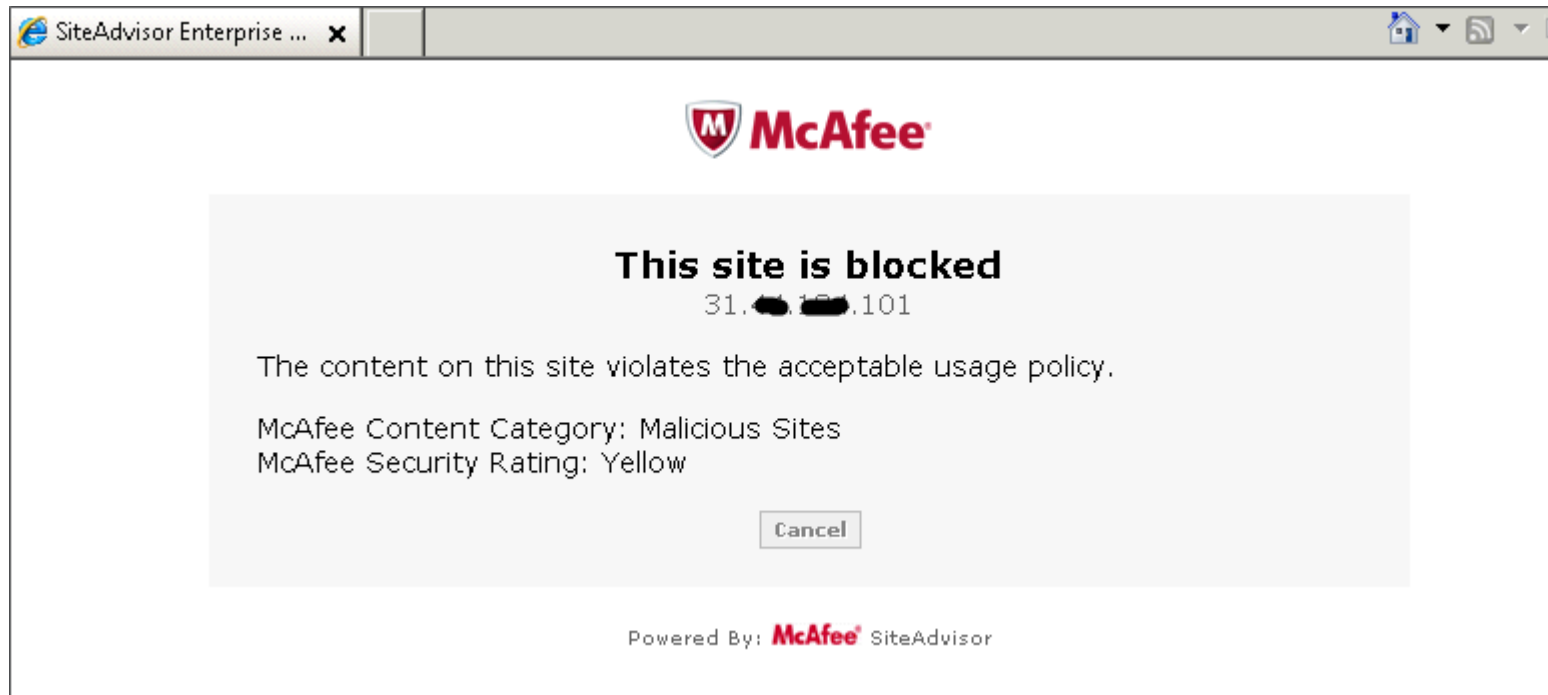
SiteAdvisor Enterprise Plus 3.0.0 > Content Actions > CSL

Functional Group: Risk/Fraud/Crime Risk Group: All Risk Groups Action: All Actions Filter: Clear

Content Categories

<input type="checkbox"/>	Content Category ▲	Functional Group	Risk Group	Action
<input type="checkbox"/>	Malicious Sites	Risk/Fraud/Crime	Security	Block
<input type="checkbox"/>	Phishing	Risk/Fraud/Crime	Security	Block
<input type="checkbox"/>	Spam URLs	Risk/Fraud/Crime	Security	Block
<input type="checkbox"/>	Spyware/Adware	Risk/Fraud/Crime	Security	Block

Content Filtering



Content and Security filtering leverages the best of GTI

SiteAdvisor Enterprise in ePO



- ePO Dashboards are focused on security rating events

Dashboard: SAE+: Warned/Blocked Dashboard Actions Add Monitor

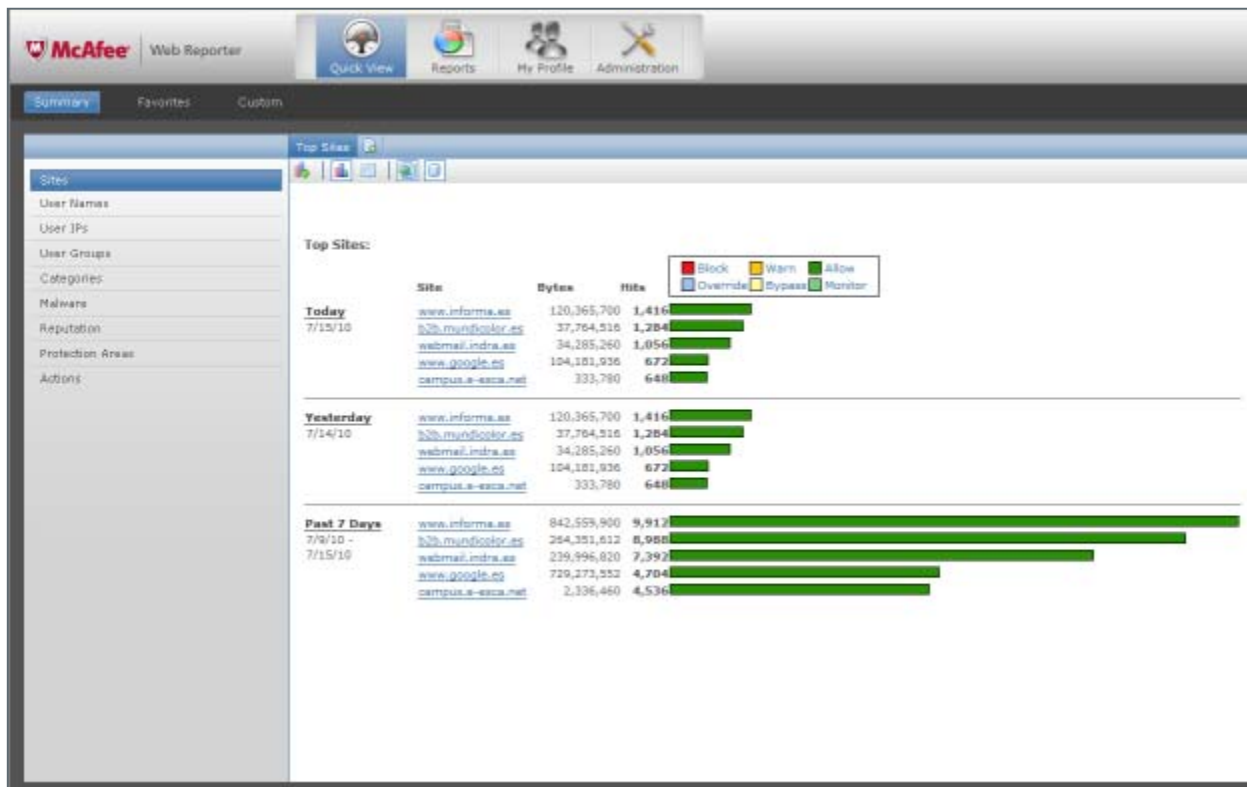
SAE+: Top 100 Blocked Sites		SAE+: Top 100 Blocked Red Sites	
Domain	Sum of Count	Domain	Sum of Count
173.212.247.108	4	184.105.178.85	4
184.105.178.85	4	208.43.239.180	2
208.43.239.180	2	208.73.210.29	2
208.73.210.29	2	221.8.69.25	2
221.8.69.25	2	74.208.164.166	2
74.208.164.166	2	87.106.24.200	2
87.106.24.200	2	9down.com	2
9down.com	2	143.215.130.33	1
143.215.129.26	1	149.20.56.33	1
143.215.130.33	1	vantech.com	1
143.215.143.11	1	Total	19

SAE+: Top 100 Warned-Cancelled Sites		SAE+: Top 100 Warned-Continued Sites	
Domain	Sum of Count	Domain	Sum of Count
75.101.167.212	2	75.101.167.212	2
173.212.247.108	1	Total	2
31.44.184.101	1		
bbqforums.net	1		
Total	5		

Web Reporter



- Web Reporter focus on Content Filtering Events
- Configure ePO client task to “Send Web Reporter Logs” when Idle 5m
- Automatic Email Reports to Heads of Department - Top 10 Users, Top 10 Sites, Top 10 Sites Accessed By Top 10 Users, Top 10 Blocked





Question about SiteAdvisor?

Rank	Top 5 Global Malware
1	Generic!atr
2	Exploit-CVE2009-3867.b
3	Generic.dx
4	W32/Conficker.worm!inf
5	Exploit-CVE2010-0840

McAfee Threats Report: First Quarter 2011

- 3rd common vector along with web and email
- Do you have removable storage policy?
 - If yes, use for enforcement.
 - If not, use data as evidence to drive policy creation
- Monitor and protect servers. Don't be another Wikileaks/US Army

Installation Note: ePO server installation and deployment packages

- Policy Elements
 - Who to control: User Assignment Groups
 - What to control: Device Definitions
 - How to control:
 - Monitor
 - Block
 - Make Read Only
 - Notify User
 - Store Evidence

Example Device Control Device Rules



- Monitor who is using Apple iPad and iPhone 4
 - PnP Device Definition: VID:05AC, PID 129A, PID 1297
 - Action: Monitor
 - User Assignment Group: Domain Users, Domain Admins

- Block all Devices Except Optical for Guests
 - Device Definition:
 - Include: All Removable Storage
 - Exclude: Optical Devices
 - Action: Block
 - User Assignment Group: Domain Guest

Content Protection Rule





- Monitor any file to removable storage
- Be careful about storing evidence with type of rule
- Monitor based upon file type (Adobe, Word, Excel) or source application Email Client, Explorer, Web Browsers

ID	Event Generated Time (UTC)	Event Type	User Name	Computer...	Agent Action(s)	Destination	Severity	Associated Rules
13342	9/2/2011 4:02:58 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\stanny\		CSL Removable St
13341	9/2/2011 4:02:51 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\stanny\		CSL Removable St
13340	9/2/2011 4:02:48 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\stanny\		CSL Removable St
13339	9/2/2011 4:02:45 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\stanny\		CSL Removable St
13337	8/30/2011 7:00:08 PM	Devices: Device Plug	CSL\Stud...	PC3	Block, Monitor...	HL-DT-ST...		Students Remova
13335	8/31/2011 4:52:24 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\dukoral\		CSL Removable St
13334	8/31/2011 4:52:23 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\dukoral\		CSL Removable St
13333	8/31/2011 4:52:23 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\dukoral\		CSL Removable St
13332	8/31/2011 4:52:10 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\		CSL Removable St
13331	8/31/2011 4:52:10 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\		CSL Removable St
13330	8/31/2011 4:52:05 AM	DLP: Removable Storage P...	CSL\sslat...	P3X-777	Monitor	f:\		CSL Removable St
13329	8/31/2011 4:51:56 AM	Devices: Device Plug	CSL\sslat...	P3X-777	Monitor, Notif...	Kingston ...		CSL Removable St

DLP Monitor



 **Devices: Device Plug**
Severity: Low 

Additional details

Agent Version:	9.2.0.305
Policy Name:	DLP Security Policy
Policy Time (UTC):	8/27/2011 1:27:37 PM
Connection State:	Online

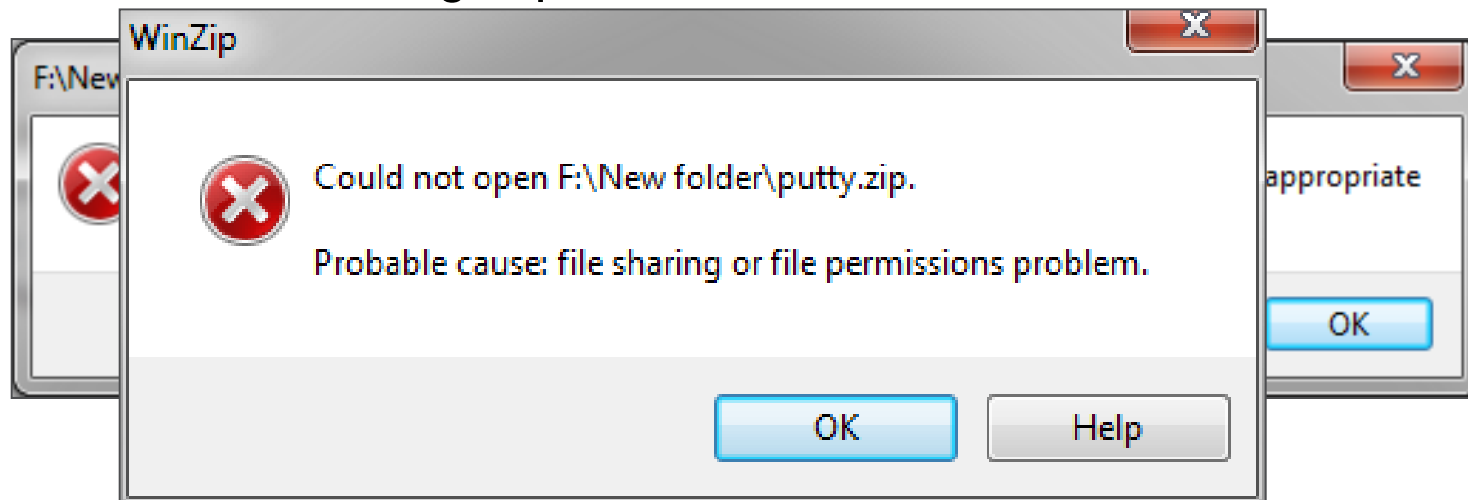
Devices

Device Class GUID:	4D36E967-E325-11CE-BFC1-08002BE10318
Device Class Name:	Disk drives
Device Name:	HP v100w USB Device
Device Compatible ID:	USB\CLASS_08&SUBCLASS_06&PROT_50
Device Instance ID:	USBSTOR\Disk&Ven_HP&Prod_v100w&Rev_1.00\35020213001F&0\{53f56307-b6bf-11d0
Bus Type:	USB
Vendor ID:	03F0
Product ID:	3207
USB Serial Number:	35020213001F 3207
USB Class:	08h - Mass Storage
Device File-System Access:	Read - Write
Volume Label:	HP
Volume Serial Number:	BC7F-25A3
Device File System Type:	FAT16

Device Control File Access Rule



- Prevent access and execution of unknown files from removable storage
- Exe, com, bat, msi, cgi, cmd, jar, dll, scr, vbs and more
- Note that archives e.g. zip will be blocked



Create the rule but leave it disabled. Enable as necessary.



Question about Device Control?

Got Audit(or) Fatigue?



- 51% of large enterprises must meet **over 10 regulations and standards**
 - 15% report more than **75 annually**
- More than 50% spend over \$500K per year on auditing
 - **39% spend over \$1M**
- 57% of large companies have **not** automated 75% of their audit controls
- More than half of organizations **use spreadsheets or no tools at all**
- **In Caribbean, we are often faced with simultaneously meeting compliance regulations from US, Canada, UK and Europe!**

Policy Auditor Can Help



- Automation of:
 - Verification of Microsoft updates. Is Windows Updates working?
 - Verify the application Adobe patches
 - Verify compliance with PCI, SOX, ISO and other security templates.
- Deal with pesky auditors. Don't get stuck by being told you fail an audit but not how/why?

Installation Note: ePO server installation, deployment packages and server tasks to update content from McAfee

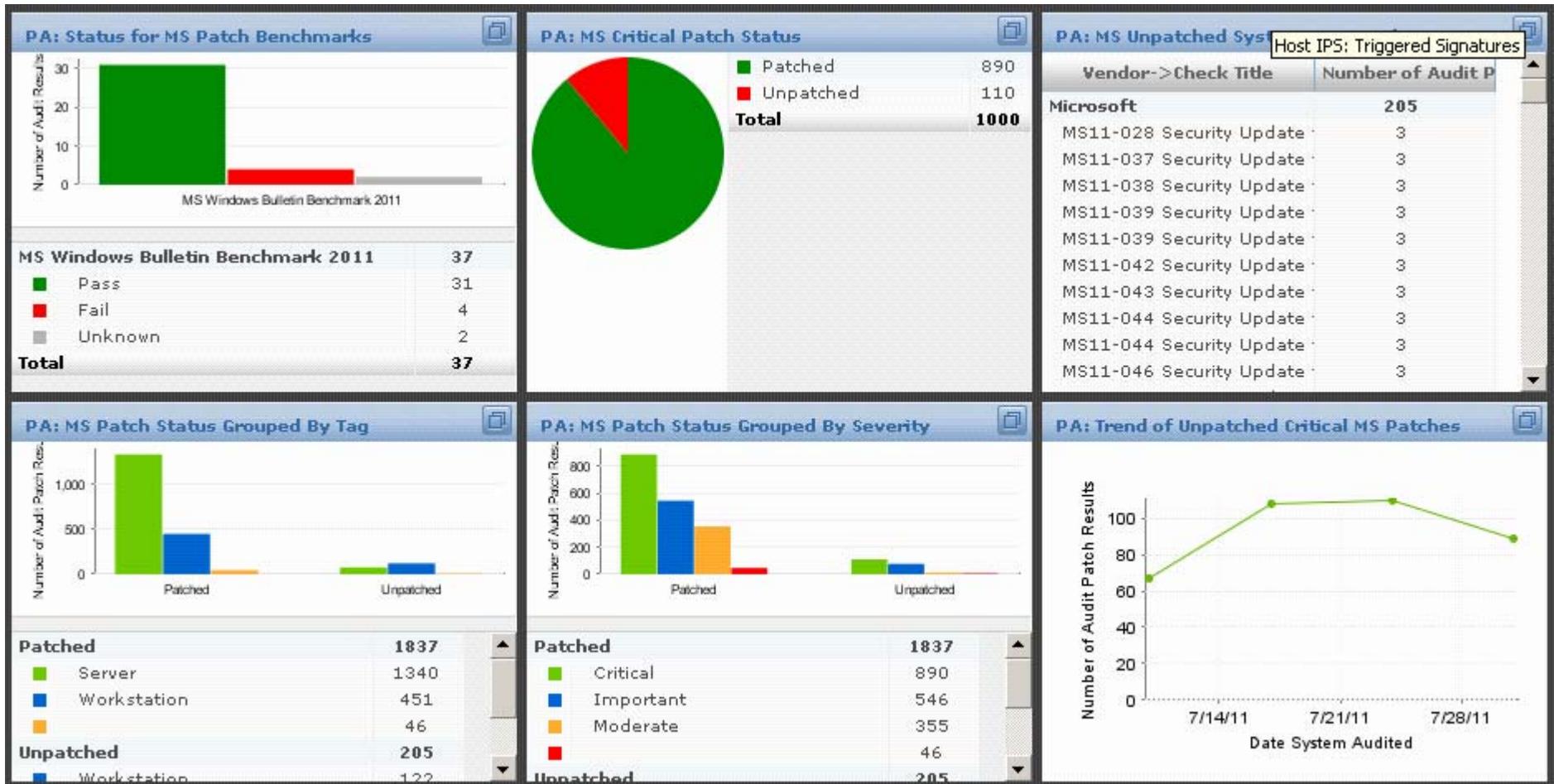
Policy Auditor and MS Patches

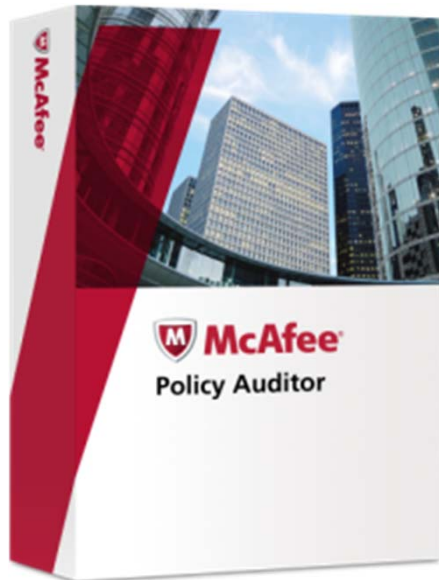


The screenshot shows the McAfee Policy Auditor web interface. At the top, there is a navigation bar with a 'Menu' dropdown and a 'Benchmarks' button. To the right of the navigation bar are icons for 'Dashboards', 'System Tree', 'Queries', and 'Policy Catalog'. The main content area is divided into a left sidebar and a right pane. The sidebar contains a list of menu items: 'Reporting', 'Systems', 'Policy', 'Software', 'Automation', and 'Risk & Compliance'. The 'Risk & Compliance' item is highlighted in yellow. The right pane displays four main sections: 'Audits' (with a magnifying glass icon), 'Waivers' (with a green magnifying glass icon), 'Benchmarks' (with a blue folder icon), and 'Checks' (with a blue folder icon). Each section includes a brief description of its function.

Menu Item	Icon	Section Name	Description
Reporting		Audits	Create, edit, and view Policy Auditor audits.
Systems		Waivers	Request waiver of Policy Auditor results.
Policy		Benchmarks	Create, edit, and view Policy Auditor benchmarks.
Software		Checks	Create, edit, and view Policy Auditor checks.
Automation			
Risk & Compliance			

MS Patch Status Dashboard





Question about Policy Auditor?

What Else is in the EPA Suite?



- EPA is a great foundation for system security
- Security for Email Servers with McAfee Quarantine Manager
- McAfee Encrypted USB Management – centrally enforce device policies and track usage
- McAfee NAC – Software based NAC capable of performing self-enforcement and quarantine



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

What Should You Worry About?



- McAfee Threat Intelligence Service



The screenshot shows a webpage titled "McAfee Labs Threat Advisory". At the top, there is a navigation bar with links for "NEW THREAT OVERVIEW", "PREVIOUS THREATS UPDATES", and "THREAT DETAILS". Below this is the "EXECUTIVE SUMMARY" section, dated August 4, 2011 (MTIS11-141). The summary states that since the last McAfee Labs Security Advisory (August 3), a noteworthy event has occurred: McAfee has released a report covering "Operation Shady RAT".

NEW THREAT OVERVIEW

Operation Shady RAT - Known Attack Components
MTIS11-141-A

IMPORTANCE:	Medium
COVERED PRODUCTS:	DAT Web Gateway Application Control
UNDER ANALYSIS:	BOP Host IPS Network Security Platform Firewall Enterprise

[Back to top](#)

What Should You Worry About?



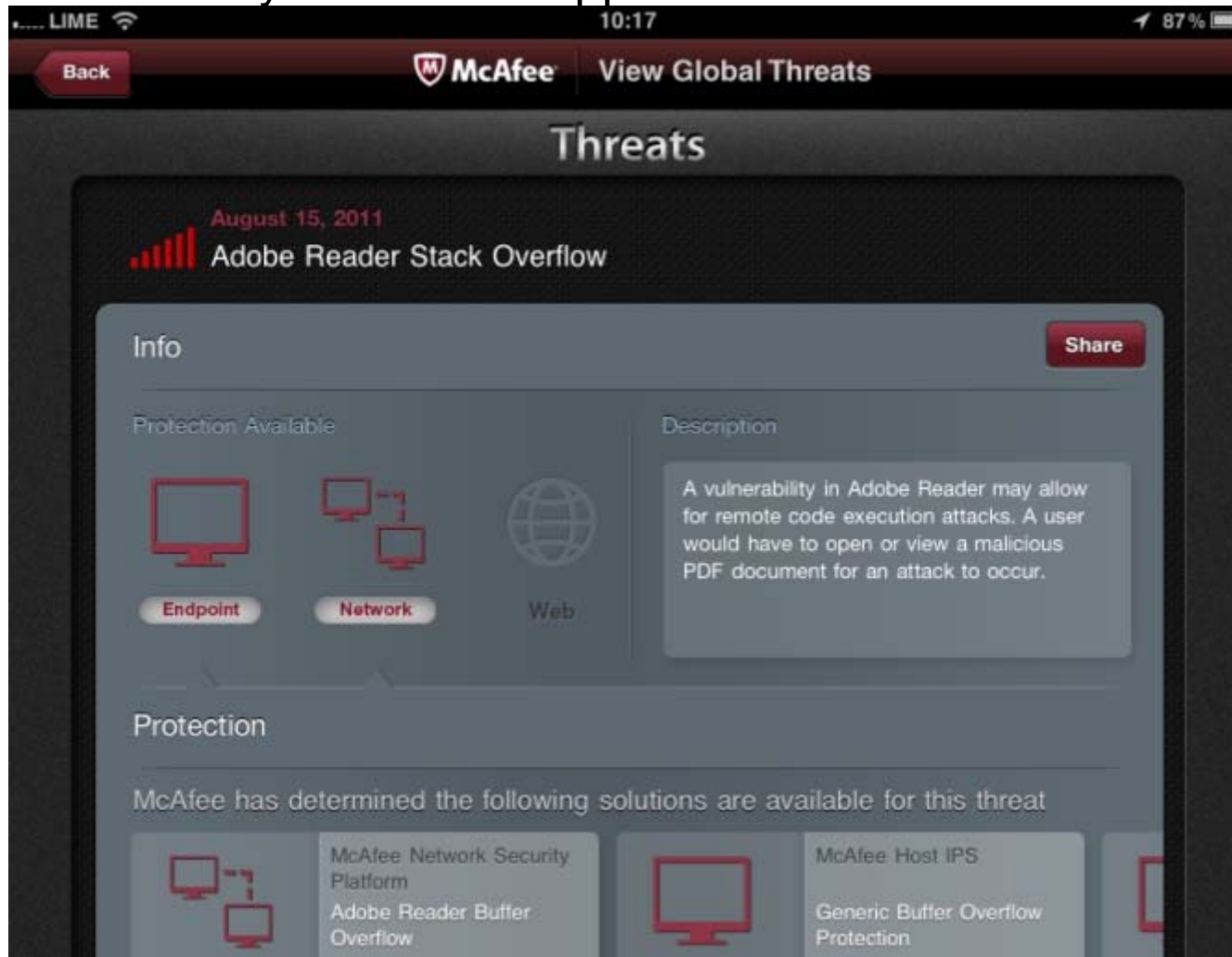
- McAfee Global Threat Intelligence iOS App



What Should You Worry About?



- McAfee Security Vision iOS App



What's in our gear bag?



Questions?



- How many ePO servers do I need?
- How often should I download DAT's from McAfee?
- How often should I perform deploy DAT's i.e. perform Agent Update?
- What are other good access protection rules?
 - Protect Network Settings
 - Block access to read and write access to all shares
 - Make all shares read-only
- What should I do in an outbreak?

