FOCUS 14
SECURITY CONFERENCE

Deep Dive: Endpoint Security—Tips and Tricks for Getting the Most from Your Endpoint Suite

Sean Slattery | Caribbean Solutions Lab
Dennis London | London Security Solutions

Speakers

FOCUS 14
SECURITY CONFERENCE

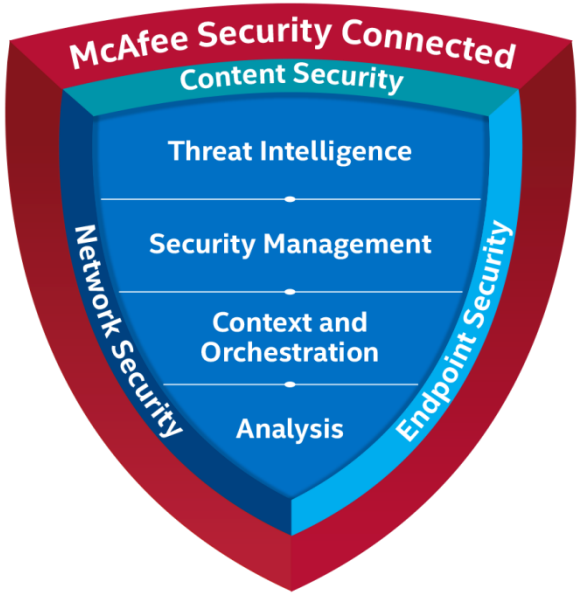
Sean Slattery
Technical Director
Caribbean Solutions Lab

Dennis London
Founder and Vice President
London Security Solutions

Agenda

FOCUS 14
SECURITY CONFERENCE

- Building a Strong Foundation
- Dealing with Emerging Threats
- Developing Organizational Intelligence
- Leveraging Third-Party Threat Intelligence
- Security and IT, Friends at Last—Application Management and More



Objectives

FOCUS 14
SECURITY CONFERENCE

- Correctly deploy and use McAfee® endpoint technologies with best practice tips.
- Use ePolicy Orchestrator® (McAfee ePO™) to improve your endpoint security while reducing management overhead.
- Discover new ways to optimize your processes to get the most of your McAfee investment.

Disclaimer: These techniques come from actual customer environments. Please use only for your own benefit.

Best Practices

Is there such a thing?

A process or practice that:

- The leaders in the field are doing today.
- Generally leads to useful results with cost effectiveness.

“Perhaps this should be termed ‘useful practices.’”

—Anton Chuvakin, Research Vice President, Gartner Security and Risk Management Group

Best Practices

Sharing is caring

You are not alone. There is safety in numbers:

- No single entity will see every threat.
- Cultivate a security community.

Defense-in-depth—multiple layers of complementary and reinforcing tools:

- Successive layers of web security at the endpoint, network, gateway.
- Our favorite is to layer private and community-based threat intelligence.

The Holy Grail: Correlation, Integration, and Automation Across ALL Technology

Photo: By Bare Dreamer (Flickr) [CC-BY-2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons

Source: *Lloyds Risk Index 2013*

Microsoft Threat Data

Security bulletins

2013:

- 106 published.
- 40% critical.
- 60% important.
- 100% IE threats mitigated by the removal of administrative rights.
- 76% Microsoft Office threats mitigated by the removal of administrative rights.
- 37% of all threats mitigated by the removal of administrative rights.

2014:

- 55 published to date (September).
- 33% critical.
- 67% important.
- 100% IE threats mitigated by the removal of administrative rights.
- 100% Microsoft Office threats mitigated by the removal of administrative rights.
- 35% of all threats mitigated by the removal of administrative rights.

Source: Microsoft

Building a Strong Foundation

Not All Tools Are Created Equal

Source: Cuthroat Kitchen, Food Network

ePolicy Orchestrator (McAfee ePO)

FOCUS 14 SECURITY CONFERENCE

Effective Management Requires Manageability:

- Agents are king—happy agents, happy life.
- Nothing happens unless you instruct/configure it.
- Backup your security keys, policies, dashboards, reports, database, and more.
- Keep up with McAfee versions, patches, and hot fixes.

McAfee Agent

FOCUS 14 SECURITY CONFERENCE

- Manual deployment—create the FramPkg.exe file and copy to network share.
- URL deployment—new in McAfee ePO software 5.x, hosted on the McAfee ePO server.
- Rogue system detection—detect systems as they broadcast and automatically deploy
- Group policy deployment—extract msi and supporting files from agent installation package.
- Microsoft Active Directory (AD) synchronization—ensure that AD is clean and contains few stale objects.
- Peer-to-peer updating—new in MA 5.
- Certain point products, such as SiteAdvisor® Enterprise, McAfee Device Control, McAfee DLP, and McAfee Encryption, enable user-based policies and management and are not just device-centric.

Manage Remote Systems

Remote agent handler

- A DMZ remote agent handler enables a secure agent to the McAfee ePO software server communication over the Internet.
- Agent handler components require fast, reliable access to the SQL database.
- Inbound firewall ports are the same as agent to server and agent to server secure.
- Requires configuration of published (public) DNS name and IP address.

Reporting

Go beyond basic queries

- Queries are normally built using all filters in place, for example, generation time, tags, user, threat name.
- Multiple queries can be combined in a report, but creating “n” reports requires “n” times the number of queries. This can quickly get out of hand and be difficult to maintain.
- Reports and runtime criteria to the rescue to be leveraged with “generic” unfiltered queries.
- Schedule or manually run reports as often as you need, specifying new criteria at each run.

Creating a report is easy. Select multiple queries, and choose “New Report” from “Selection. Customize Runtime Criteria.”

Maintenance

Care and feeding of your database

- Regularly run a server task to purge the database of old events, such as threat and client events older than 90 days.
- Refer to KB67184 for a recommended SQL maintenance plan.
- New in DEC/DLP 9.3 is incident task runner for extended DLP automation.
  - Automate the process using the DLP incident tasks runner server task.

Incident List | **Incident Tasks**

State	Name ▲	Description	Criteria	Type
Enabled	Purge Events Older than 45 Days		Occurred (UTC) Is not within the last 45 Days	Purge

- Check out “McAfee ePO Maintenance Utility” in Community DOC-4021.

Real Time for McAfee ePO

Are my endpoints healthy now?

Check on your endpoints over your morning coffee:

- Health of the McAfee agent, VirusScan® Enterprise, McAfee Host Intrusion Prevention System.
- Check for errors.
- Check on status of versions, content, service state.

Take immediate action to remediate:

- Start services.
- Initiate communication.

Other uses:

- Query registry keys, software, and hardware inventory, even USB devices.

Dealing with Emerging Threats

MS14-021

VirusScan access protection rules

User-defined access protection rules are very powerful and can assist with mitigating threats by preventing file access from a certain process:

- Include: iexplore.exe
- Exclude: *none*
- File or folder name to block: **\vgx.dll
- File actions to prevent: read access and files being accessed

Remember to use a descriptive name and monitor the threat event log for matching events –threat name starts with *user-defined rules: rule name.*

VSE88 Patch 4 extends the maximum limit of include and exclude processes to 5199 characters. Consider using full paths for exclusions e.g. C:\Windows\system32\svchost.exe rather than svchost.exe.

Cryptolocker

VirusScan access protection

Rule Name: Cryptolocker – Block EXE in AppData

- Include: *.*
- Exclude: C:\PROGRA~1\Box\BOXSYN~1\BoxSync.exe, C:\Users\sslattery\AppData\Local\Apps\Evernote\Evernote\Evernote.exe
- File or folder to block: **\Users**\AppData***.exe
- File actions to prevent: file write access, new file creation

Repeat rule creation to protect registry keys, and to allow only authorized processes to key file types, such as doc, docx, pdf, crt, jpb, mdb, edb, and others.

KB54812—Using wildcards with VirusScan exclusions.

Cryptolocker

Host intrusion prevention custom signatures

Rule: Cryptolocker – Block EXE in AppData

Rule Type: Files

Operations: Create, Execute, Write

Parameters:

- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

Note differences in wildcard behavior between VirusScan and host intrusion prevention (HIPS).

Developing Organizational Intelligence

Build a Whitelist Using HIPS

This is one approach. Many are possible.

1. Enable Signature 6010: Generic Application Hooking and Signature 6011: Generic Application Invocation Protection with Severity Level of Informational.
2. Use HIPS reporting tool and aggregate events based on signature.
3. Create trusted applications from recorded events.
4. Apply different and even multiple trusted application policies to different parts of the organization.

Define trusted applications based on signing authority, for example, Microsoft of one definition for every Microsoft process and file hash.

Name	File name	Fingerprint	File description	Signer
C:\PROGRAM FILES\INTERNET EXPLORER\IEXPLORE.EXE				CN=MICROSOFT CORPORATION, OU=MOPR, O=MICROSOFT ...

Bonus Slide

HIPS expert rule

This approach provides fast Cryptolocker protection using your trusted applications database.

Monitoring File System

VirusScan access protection and HIPS custom rules

Custom rules enable monitoring of the entire file systems for suspicious behavior.

Monitor specific locations:

- C:\Program Files & C:\Program Files (x86)
- %Temp%, %AppData%, %ProgramData%, %SystemRoot%
- C:\Windows
- C:\Windows\System & System32
- & C:\Windows\System32\Drivers

Monitor exploitable processes:

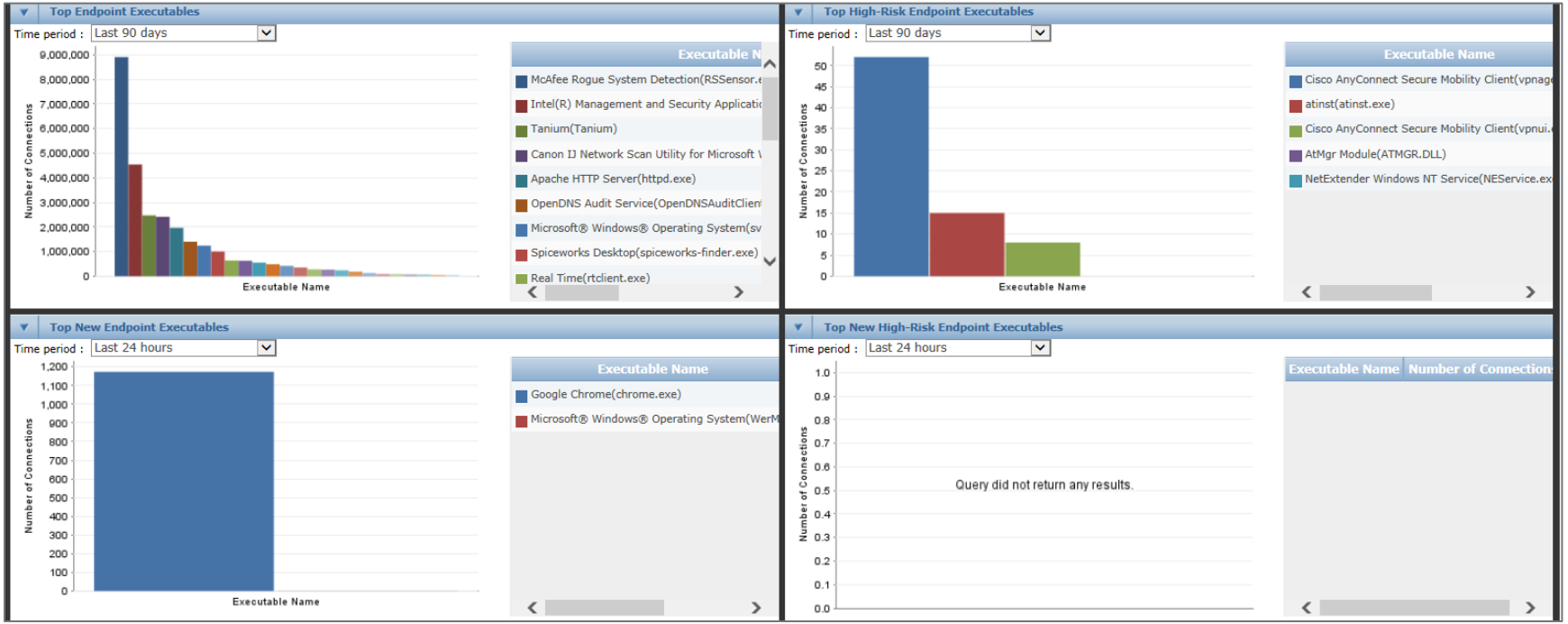
Java - C:\Program Files (x86)\Java\jre7\bin\java.exe

Javaw - C:\Program Files (x86)\Java\jre7\bin\javaw.exe

Internet Explorer - C:\Program Files (x86)\iexplore.exe

Endpoint Intelligence Agent

Monitor trust of active processes



Endpoint Intelligence Agent

Answers what, when, and where

Risk	Executable Name	Version	Hash	Number of Connections
Very High	Cisco AnyConnect Secure Mobility Client(vpnagent.exe)	3	78836108cf5ac6a0b365ac50a72f16d6	22
Moderate	Skype(Skype.exe)	6.18.59.106	d0d52b4c5b5482920f8ee5d654b4f146	176,623
Moderate	DNSCRYPT-PROXY.EXE		2185b3a7661db08b7f14e664ab529bf7	18,393
Moderate	VLC media player(vlc.exe)	2.1.3	550005223c0eebfa602c37dcb5497abd	9
Moderate	Evernote®(Evernote.exe)	5	ab59b6a995d93de02438ad248ded363a	90
Moderate	SoftPerfect Network Scanner(NETSCAN.EXE)	5.4.11.0	4c1653c708c3e253ed27d13c09ba063c	1

Executable Information | Top Reported Endpoints

Name:	Cisco AnyConnect Secure Mobility Client(vpnagent.exe)
Risk:	Very High
Hash:	78836108cf5ac6a0b365ac50a72f16d6
Version:	3
First seen on:	29 Jul, 2014 08:54:22 PM COT
Last seen on:	14 Sep, 2014 12:35:13 AM COT

Executable Information | **Top Reported Endpoints**

System Name	Domain Name	Operating System	IP Address	Number of Connections
P3X-787	CSL	Windows 7 Workstation	192.168.1.54	53

Custom Process Blocking

- Good—VirusScan 8.x supports custom file detections based on file name.
- Better—Stinger 12 supports custom file hashes for immediate deletion.
- Best—HIPS custom rule for more sustained operations:
  - Custom rule.
  - Rule type: program.
- Operations: open for access, run target executable.
- Target executable:
  - Use fingerprint (hash).
  - How about signer certificate?

Leveraging Third-Party Intelligence

Tor Exit Nodes

HIPS

Challenge: Configure HIPS firewall blocking based on large and changing lists:

Answer: HIPS catalog to the rescue!

1. Build an empty network list using the HIPS catalog.
2. Build block rule in the HIPS catalog.
3. Add rule from catalog to policies.
4. Periodically import (after cleaning up format) lists of IPs and domains into the HIPS catalog.

My production policies currently have more than 50,000 entries.

More Options

Why not develop and cultivate your own?

Host IPS Catalog — **Options ▼**

Item type: Network | Show Filter Options — **Catalog items:** Import | Export

Name ▼	Actions
► Autorun.worm (pdf.exe)	Edit | Duplicate | Delete | Export
► Country Threat Intelligence	Edit | Duplicate | Delete | Export
► Cryptolocker_RU	Edit | Duplicate | Delete | Export
► localhost	Edit | Duplicate | Delete | Export
► Malware Domain List	Edit | Duplicate | Delete | Export
► Malware Domains	Edit | Duplicate | Delete | Export
► Palevo Tracker	Edit | Duplicate | Delete | Export
► TOR Exit Nodes	Edit | Duplicate | Delete | Export
► Trusted Network	Edit | Duplicate | Delete | Export
► Zeus Tracker	Edit | Duplicate | Delete | Export

Security and IT—Friends at Last

Application Management

Real Time for McAfee ePO

FOCUS 14 SECURITY CONFERENCE

Installed Applications

Name	Version	Silent Uninstall String	Uninstallable
7-Zip 9.20 (x64 edition)	9.20.00.0	MsiExec.exe /X{23170F69-40C1-2702-0920-000001000000} /qn /noreboot	Is Uninstallable
Adblock Plus for IE	1.1	"C:\ProgramData\Package Cache\{fd97d1e2-368a-4cd9-af63-8eeff938044a}\adblockplusie	Not Uninstallable
Adblock Plus for IE (32-bit and 64-bit)	99.9	MsiExec.exe /X{1CAFFEC6-23B4-484B-B17B-3200BE5C5636} /qn /noreboot	Is Uninstallable
Adobe Acrobat XI Pro	11.0.08	MsiExec.exe /X{AC76BA86-1033-FFFF-7760-000000000006} /qn /noreboot	Is Uninstallable
Adobe Flash Player 14 ActiveX	14.0.0.125	C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_14_0_0_125_ActiveX.exe -maintain a	Not Uninstallable
Adobe Flash Player 14 Plugin	14.0.0.125	C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_14_0_0_125_Plugin.exe -maintain pl	Not Uninstallable
Adobe Flash Player 15 ActiveX	15.0.0.152	C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_15_0_0_152_ActiveX.exe -maintain a	Not Uninstallable
Adobe Flash Player 15 Plugin	15.0.0.152	C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32_15_0_0_152_Plugin.exe -maintain pl	Not Uninstallable
Alcor Micro Smart Card Reader Driver	1.7.16.0	C:\Program Files (x86)\InstallShield Installation Information\{F24F876B-7D71-4BD6-88E9-	Not Uninstallable
Apache HTTP Server 2.2.14	2.2.14	MsiExec.exe /X{85262A06-2D8C-4BC1-B6ED-5A705D09CFFC} /qn /noreboot	Is Uninstallable
Apple Application Support	3.0.6	MsiExec.exe /X{78002155-F025-4070-85B3-7C0453561701} /qn /noreboot	Is Uninstallable
Apple Mobile Device Support	7.1.2.6	MsiExec.exe /X{6AF2AC2A-3532-43FD-9F4D-BDC9C0D724C7} /qn /noreboot	Is Uninstallable

Gathering inventory is easy. From here it is a trivial process to remotely uninstall.

Application Management

McAfee ePO Endpoint Deployment Kit (EEDK)

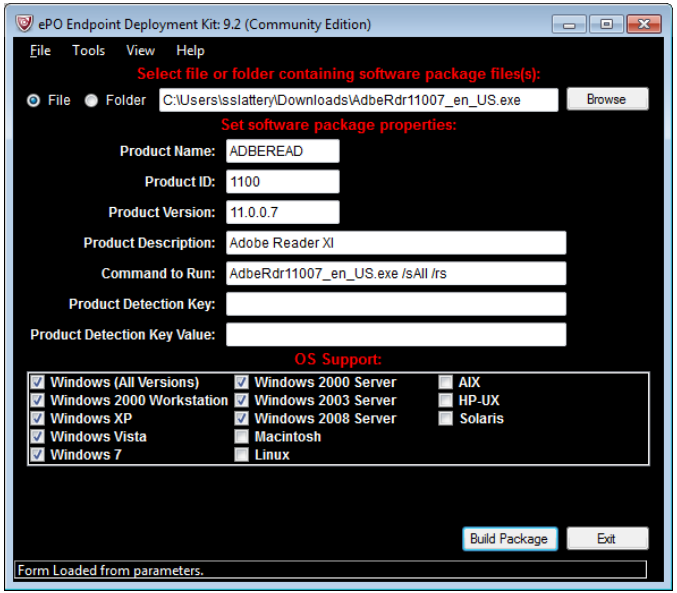
FOCUS 14 SECURITY CONFERENCE

Commonly deployed: Adobe Reader, Adobe Flash, Java, Mozilla Firefox, hot fixes

Products and components:

Adobe Reader XI 11.0.0.7 | Action: Install | Language: Language Neutral | Branch: Current

Command line:



Can McAfee ePO Software Do That?

Server Tasks

- Launching local executables from McAfee ePO software?
  - MSI installer—msiexec.exe.
  - Registry editor—reg.exe or regedit.exe.
  - Kill a task—taskkill.exe.
  - Update group policy—gpupdate.exe.
  - And many more …

Using McAfee for non-McAfee functions?

Configuration

Registered Executables

New Registered Executable

Registered Executables

For security purposes, registered executables cannot be added or edited unless you are viewing this console from the server system.

Name ▲	Path	Run As
FTP Retrieve	c:\Windows\System32\ftp.exe	local.admin
GP Update	C:\Windows\System32\gpupdate.exe	local.admin
Launch msiexec	c:\Windows\System32\msiexec.exe	local.admin
Launch Registry Editor	C:\Windows\System32\reg.exe	local.admin
Net Command	C:\Windows\System32\net.exe	local.admin
Services Command	C:\Windows\System32\sc.exe	local.admin
SLUI.exe for Microsoft Genuine Authorization	C:\Windows\System32\slui.exe	local.admin
Taskkill	C:\Windows\System32\taskkill.exe	local.admin

Example 1: VirusScan failed to remove Kaspersky

FOCUS 14 SECURITY CONFERENCE

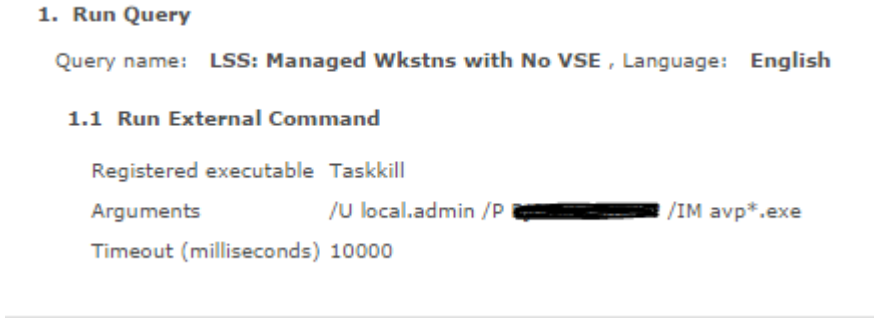
Step 1

VirusScan installer failed to remove Kaspersky …

if it was password protected.

Note: Kaspersky agents were not communicating with Kaspersky management server, and the local password was incorrect.

- Used server tasks to:
  - Stop service using taskkill.exe



Example 1: VirusScan couldn't remove Kaspersky

FOCUS 14 SECURITY CONFERENCE

Step 2

Now that the service was stopped, we could change the password.

- Used server task to:
  - Launch registry editor and remove password protection.

1. Run Query

Query name: **LSS: Managed Wkstns with No VSE** , Language: **English**

1.1 Apply Tag

Tag: Kaspersky

1.2 Run External Command

Registered executable	Launch Registry Editor
Arguments	ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\protected\AVP80\settings" /v EnablePswrdProtect /d 0 /t REG_DWORD /f
Timeout (milliseconds)	25000

Example 1: VirusScan couldn't remove Kaspersky

FOCUS 14 SECURITY CONFERENCE

Step 3

With the service stopped and the password removed, we could proceed.

- Used server task to:
  - Launch msiexec.exe to remove Kaspersky.

1. Run Query

Query name: **LSS: Has Kaspersky Anti-virus Installed** , Language: **English**

1.1 Run External Command

Registered executable	Launch msiexec
Arguments	/x {8F023021-A7EB-45D3-9269-D65264C81729} /qn
Timeout (milliseconds)	30000

1.2 Run External Command

Registered executable	Launch msiexec
Arguments	/x {85E0B171-04FA-11D1-B7DA-00A0C90348D6} /qn
Timeout (milliseconds)	30000

Did It Work?

It wasn’t 100%, but we were able to remove a large portion of the installs.

- Quick recap:
  - Stopped the service.
  - Modified the registry.
  - Launched MSI to remove.

- And this was all done from the McAfee ePO console.

For the Most Part—Yes

FOCUS 14
SECURITY CONFERENCE

How Can McAfee ePO Software Work for Me?

Make McAfee ePO Work for You

Let's start with the basics

Create or modify queries to work for you and give you what you need. Use tags and policy assignment rules.

- Queries:
  - Machines running current versions of deployed products (for example, VirusScan, McAfee Host Intrusion Prevention, SiteAdvisor Enterprise, McAfee Policy Auditor).
  - Machines with out-of-date .DAT files (for example, not within X version of the repository).
- Tags:
  - Tags to install products, run specific tasks, or just for identification purposes.
- Tasks:
  - Deployment tasks aligned to tags.
- Policy assignment rules:
  - Specific policies for specific tags.

Automating Deployment Tasks

Server task to tag machines

FOCUS 14 SECURITY CONFERENCE

Use queries to tag machines not running required solutions for your environment.

- Workstations—VirusScan not installed:
  - Apply tag—“Install VirusScan.”
- Workstations—McAfee Host Intrusion Prevention not installed:
  - Apply tag—“Install McAfee Host Intrusion Prevention.”
- Workstations—SiteAdvisor not installed:
  - Apply tag—“Install SiteAdvisor.”
- Workstations—McAfee Deep Defender not installed:
  - Apply tag—“Install McAfee Deep Defender.”
- Rinse and repeat for additional solutions.

Automating Deployment Tasks

Server task to clear tags

Use queries to remove tags from machines running required solutions.

- Workstations—VirusScan Enterprise installed:
  - Clear tag—“Install VirusScan Enterprise”
- Workstations—McAfee Host Intrusion Prevention installed:
  - Clear tag—“Install McAfee Host Intrusion Prevention”
- Workstations—SiteAdvisor Enterprise installed:
  - Clear tag—“Install SiteAdvisor Enterprise”
- Workstations—McAfee Deep Defender installed:
  - Clear tag—“Install McAfee Deep Defender”

Advanced Updating

Server task to force update

Use queries to find machines that are communicating with out-of-date .DAT files.

1. Run Query

Query name: **LSS: Machines With DAT files not within 2 versions in Repository** , Language: **English**

1.1 Run Client Task Now

Run Client Task:	McAfee Agent > Product Update > Daily Update - DAT and Engine
Randomization:	4 minutes
Stop Task on the Client After:	15 minutes
Connect Using:	Wake up Agent using Last Agent Handler
Abort After:	16 minutes
Number of Attempts:	1
Retry Interval:	30 seconds

Policy Configurations

Every solution needs to be customized

Start with best practices and work from there.

- VirusScan Enterprise 8.8:
  - KB66909—Consolidated list of VirusScan Enterprise exclusion articles.
  - KB74059—“Best Practices for On-Demand Scans.”
- McAfee Host Intrusion Prevention 8.0:
  - KB70760—Master list of support articles.

Coming Soon

FOCUS 14 SECURITY CONFERENCE

- McAfee Threat Intelligence Exchange—Improving the threat intelligence exchanges in the McAfee ecosystem.
- ENS 10.x—Convergence of VirusScan, McAfee Host Intrusion Prevention, and SiteAdvisor Enterprise with enhanced logging (for example, file hash).
- .DAT reputation—Pre-update reputation checks: KB55986.
- Anti-malware engine 5700—Live memory scanning and improved archive support.
- Data visualization enhancements for McAfee ePO software—A picture is worth 1,000 events.
- Raptor—Next-generation Stinger tool with heuristics and roll back.
- McAfee Event Reporter 9.5—Mini-SIEM replacement to McAfee Risk Advisor with bi-directional McAfee ePO software integration.

Conclusion and Call-to-Action

FOCUS 14 SECURITY CONFERENCE

- Enhance your security posture using custom rules and organizational threat intelligence.
- Leverage a strong security management platform to benefit other areas of your organization.
- Use the community—learn from other users:
  - http://community.mcafee.com.
  - ePolicy Orchestrator LinkedIn group.
  - Develop your own.
- Remember that security is process, not a product. It's definitely NOT just a checkbox.
- Keep up to date. Subscribe to the McAfee Support Notification Service.

McAfee Acronyms

Just in case

- McAfee ePO: ePolicy Orchestrator
- MA: McAfee agent
- AH: Agent handler
- RSD: Rogue system detection
- RTE: Real Time for McAfee ePO
- VSE: VirusScan Enterprise
- HIPS: McAfee Host Intrusion Prevention System
- DEC: McAfee Device Control
- DLP: McAfee Data Loss Prevention for Endpoint
- EIA: McAfee Endpoint Intelligence Agent
- EEDK: McAfee ePO Endpoint Deployment Kit

Questions & Answers

FOCUS 14 SECURITY CONFERENCE

Rate This Session:

From the FOCUS App select session

#77 “Deep Dive: Endpoint Security Tips and Tricks for Getting the Most from Your Endpoint Suite”

Post-Conference, Access Presentations:

www.mcafee.com/focus14

Password: Empowering14

Learn More:

Sean Slattery – sslattery@caribbeansolutionslab.com

Dennis London – dlondon@londonsecuritysolutions.com