Securing The Virtual Data Center

Peter A. Starceski and James A. Kelly

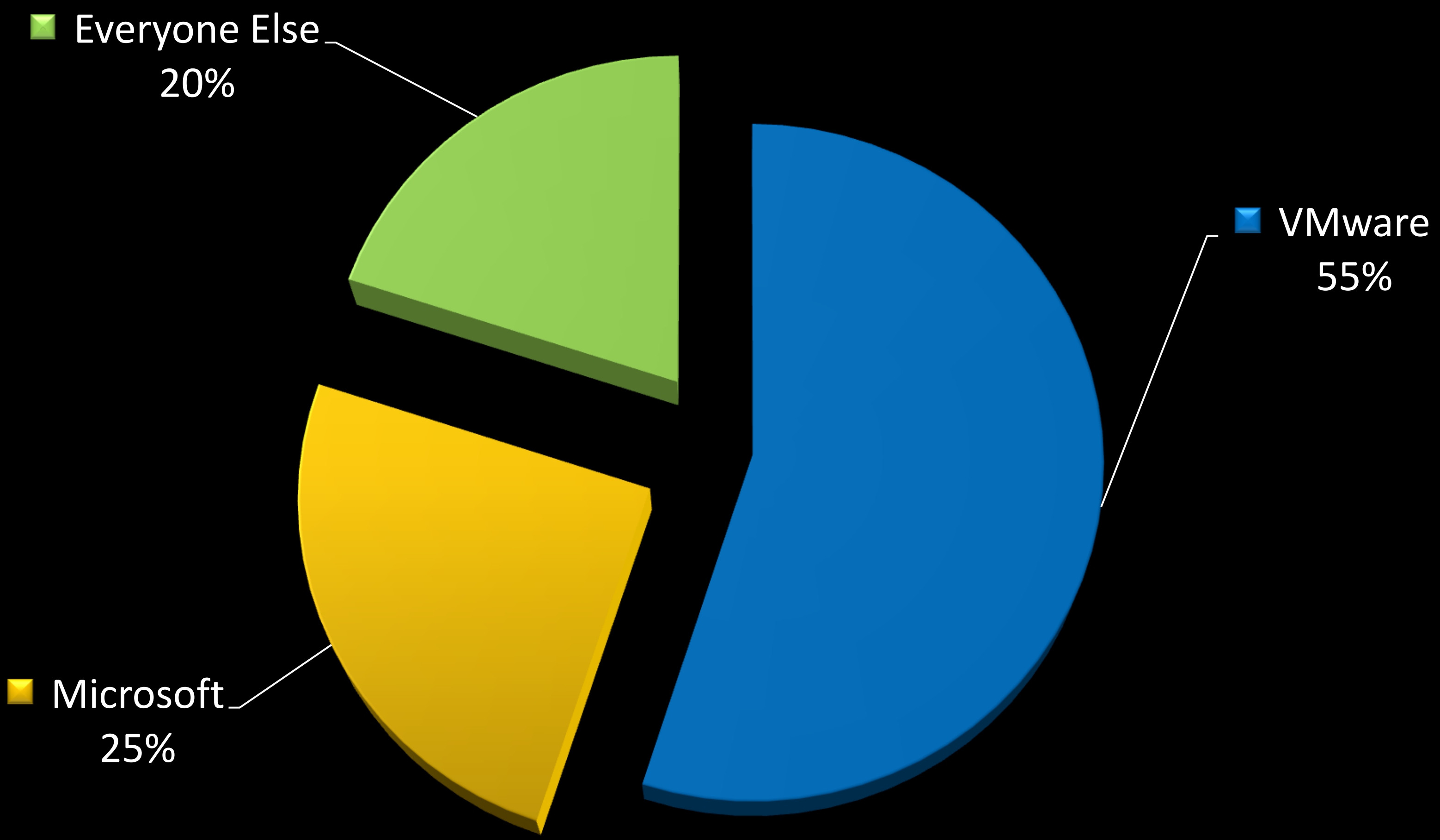
Principal Security Engineers

Challenges With Virtualization

Guest Virtual Machine Pain Points

- Heavy resource usage from Security Applications
  - #1 - Disk IO
  - Memory and CPU also important
  - Amount of time it take to scan is important
  - Network IO not as important
    - Customers willing to tradeoff between Disk I/O & Network I/O

Enterprise Hypervisor Market Share



Virtualization Use Cases

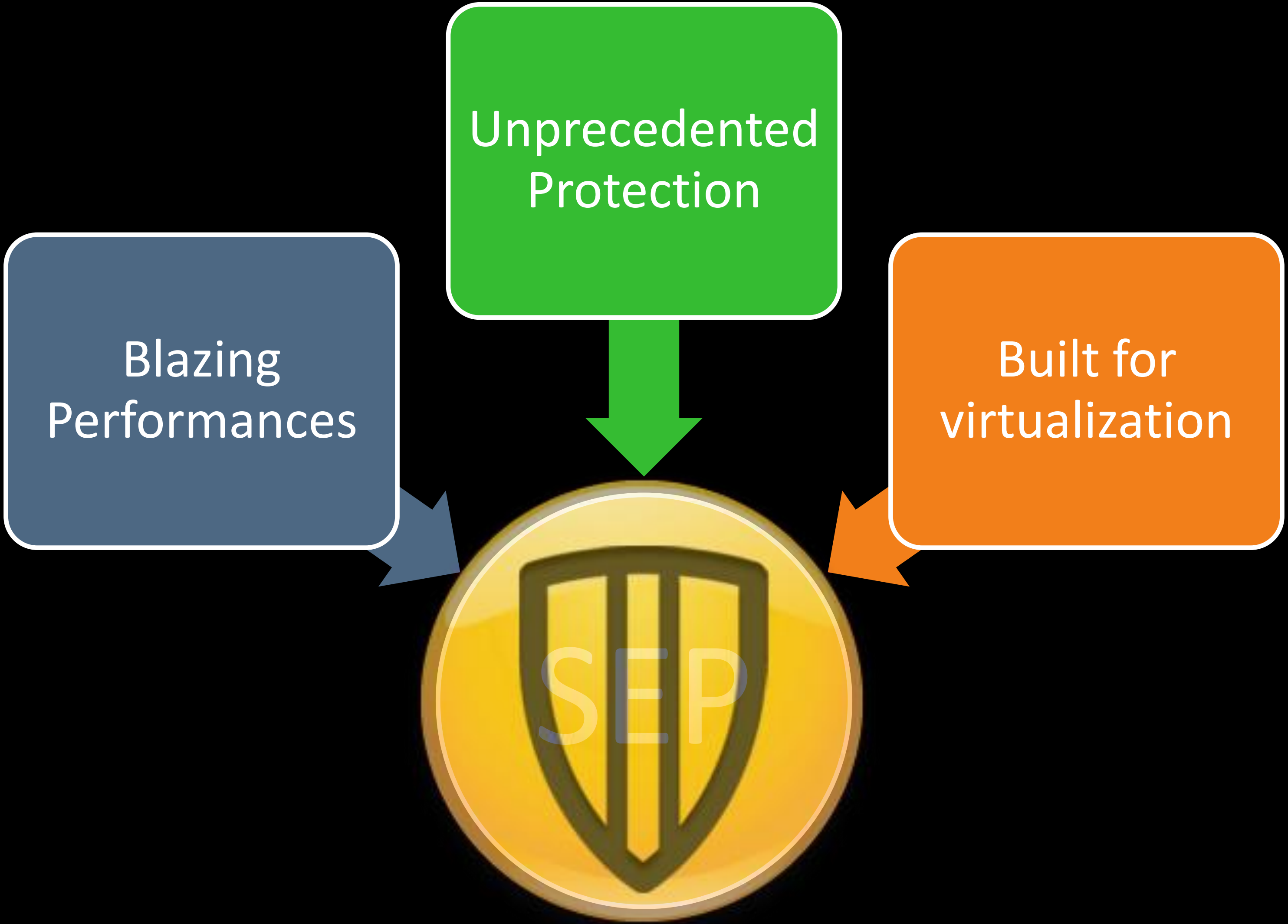
- Persistent Desktops
- Non-Persistent Desktops (VDI)
  - This is the fastest growing use case

Limitations of Endpoint Security Solutions

- Most solutions are designed for physical machines
- Heavy resource usage from security operations
  - AV and definition update "storms"
  - Disk IO due to shared storage
    - Activity on one VM can affect all the VMs in the cluster
  - Memory and CPU usage is a concern
    - Baseline memory usage
    - Peak usage during scanning
  - Network IO is less of a concern
- VMs come and go quickly
  - Hard to keep track of them
  - Need to be able to secure all VMs

SEP 12.1.2 (Jaguar):
Protection and Performance

SEP 12.1x

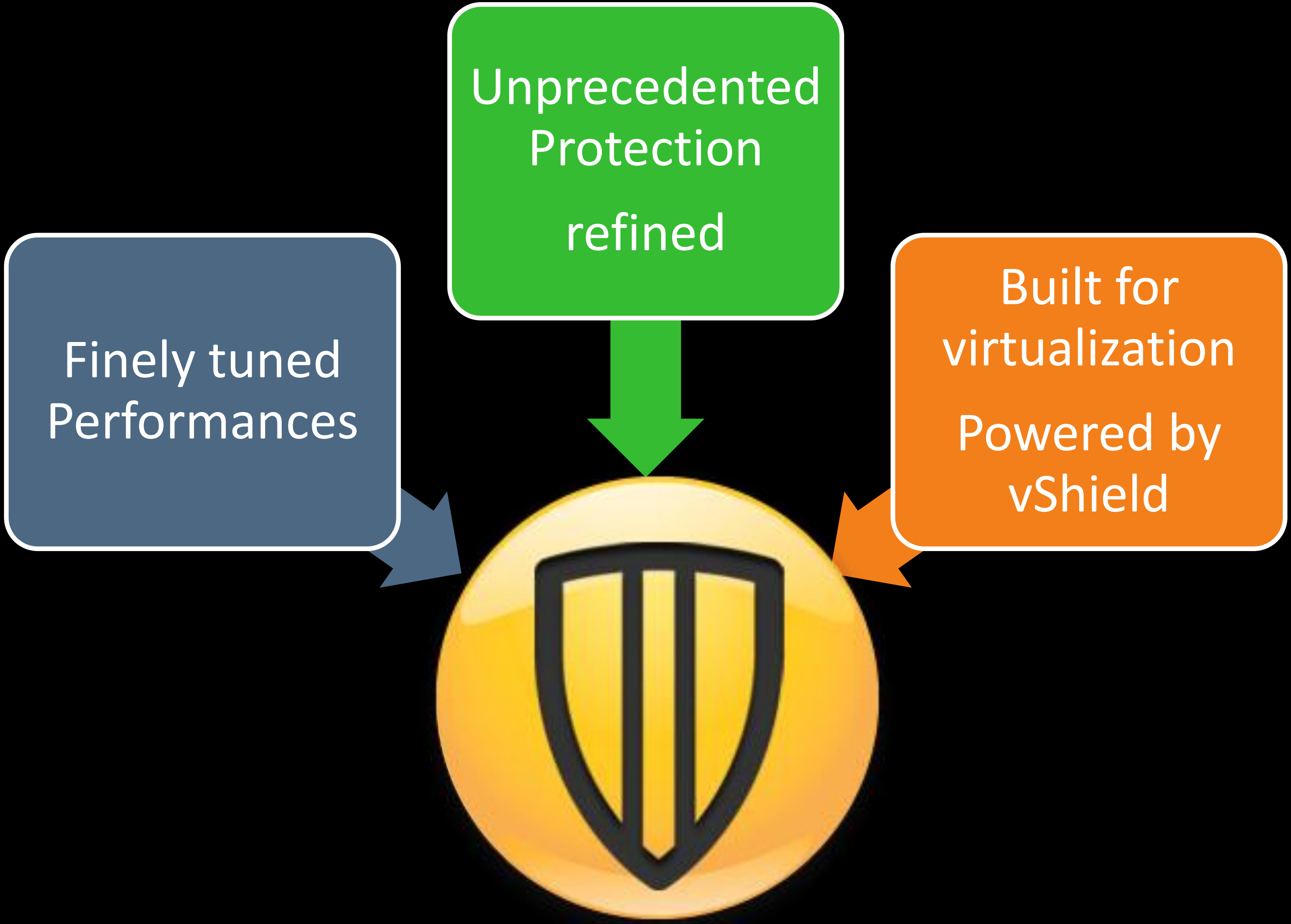


Unprecedented Protection

Blazing Performances

Built for virtualization

SEP 12.1.2 (Jaguar)



Unprecedented Protection

refined

Finely tuned Performances

Built for virtualization

Powered by vShield

Virtualization

Powered by vShield Endpoint

VMware vShield is:

vShield Edge

- VPN
- Load Balancer
- Firewall

vShield App

- Protects against Network Based Threats
- Improved Compliance (PCI, HIPPA)

vShield Endpoint

- **Enable antivirus offload**

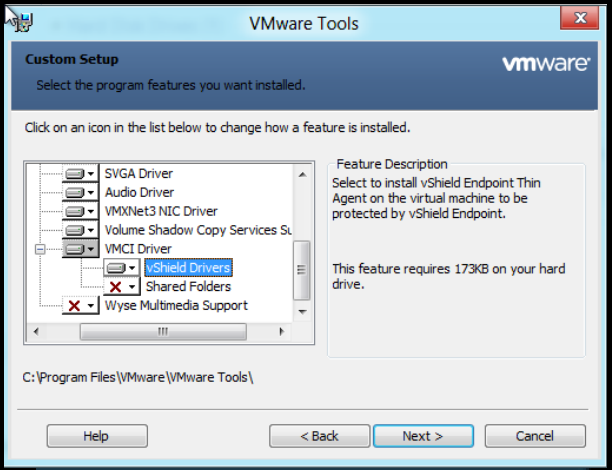
What is vShield Endpoint? (VMware definition)

- Goal - Optimize endpoint security in VMware virtual environments
  - Offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance
  - Streamline antivirus and anti-malware deployment and monitoring in VMware environments

vShield endpoint components

vShield Endpoint plugs directly into vCenter and consists of three components:

- Hardened security virtual appliances, delivered by VMware partners
- Thin agent for virtual machines to offload security events (included in VMware Tools)
- VMware Endpoint ESX® hypervisor module to enable communication between the thin agent and the security virtual appliance at the hyper-visor layer



VMware Tools

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

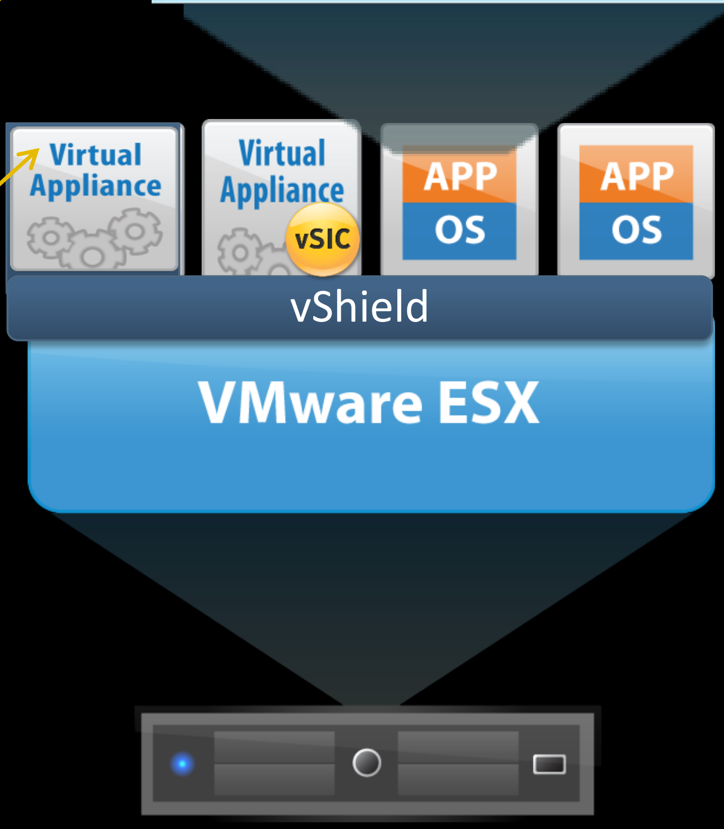
- SVGA Driver
- Audio Driver
- VMXNet3 NIC Driver
- Volume Shadow Copy Services Su
- VMCI Driver
  - vShield Drivers
  - ☒ Shared Folders
- ☒ Wyse Multimedia Support

Feature Description

Select to install vShield Endpoint Thin Agent on the virtual machine to be protected by vShield Endpoint.

This feature requires 173KB on your hard drive.

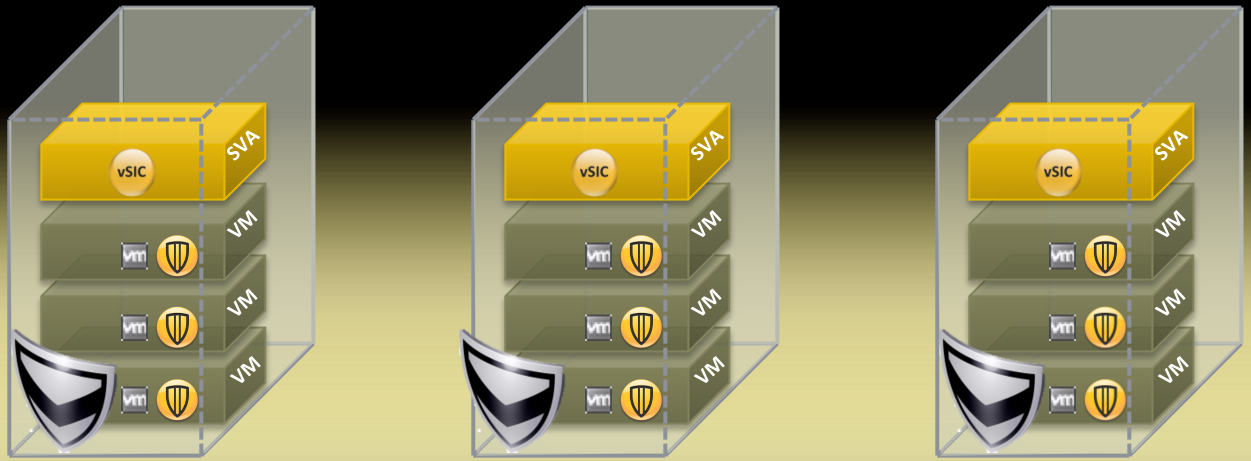
C:\Program Files\VMware\VMware Tools\



Solving Performance Issues on the Endpoint

vShield Endpoint Integration

Symantec Endpoint Protection



Virtual Client Tagging

Offline Image Scanning

Resource Leveling

Virtual Image Exception

Shared Insight Cache

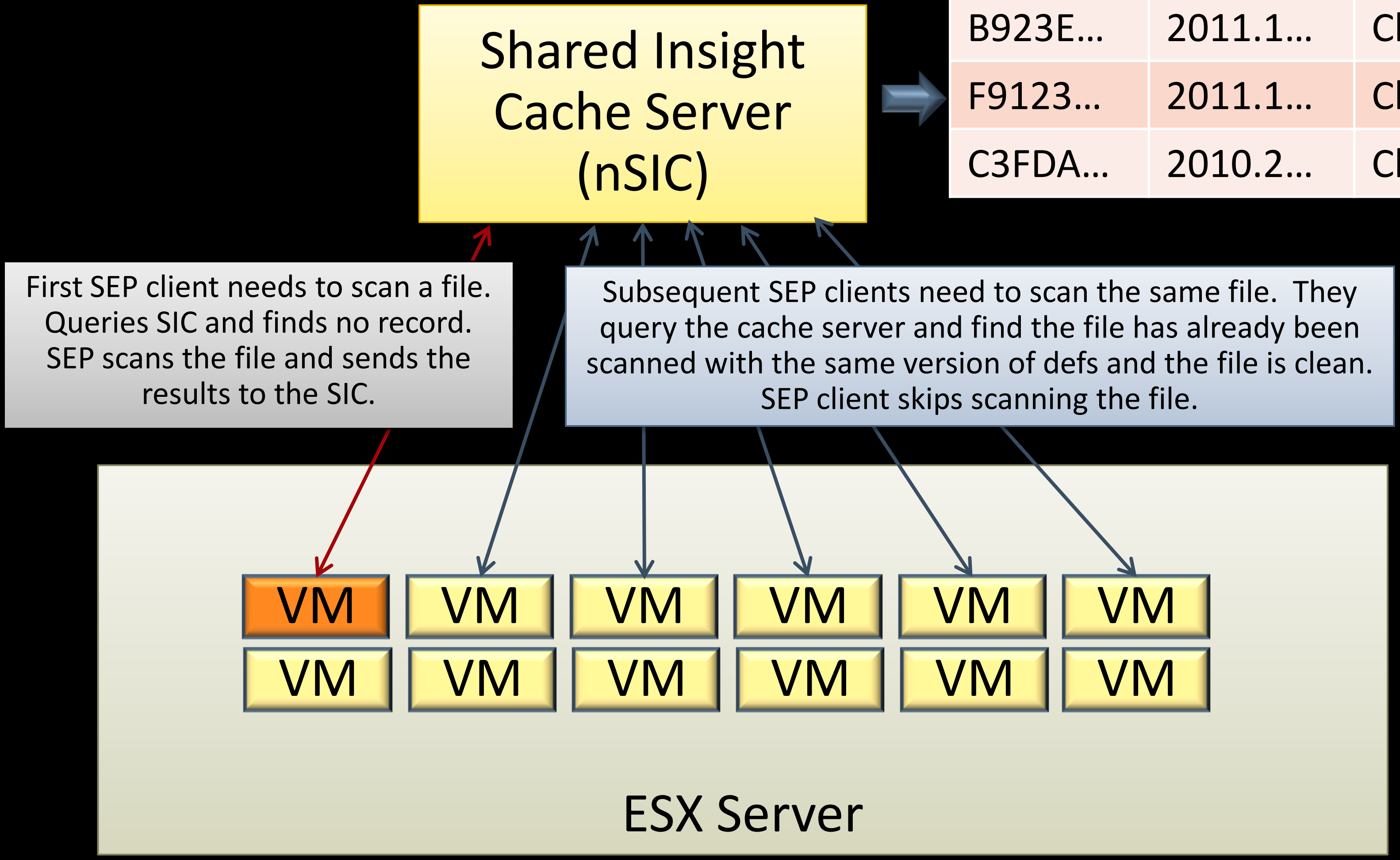
vShield-enabled Shared Insight Cache

Introducing SIC

- Goal - Optimize endpoint security in VMware virtual environments
  - De-duplicate On-demand and Scheduled scan resource usage.
  - Prevent AV-STORM

Shared Insight Cache - High Level

File Hash	Def Ver	Result
AE32D…	2011.1…	Clean
B923E…	2011.1…	Clean
F9123…	2011.1…	Clean
C3FDA…	2010.2…	Clean



First SEP client needs to scan a file. Queries SIC and finds no record. SEP scans the file and sends the results to the SIC.

Subsequent SEP clients need to scan the same file. They query the cache server and find the file has already been scanned with the same version of defs and the file is clean. SEP client skips scanning the file.

Shared Insight Cache

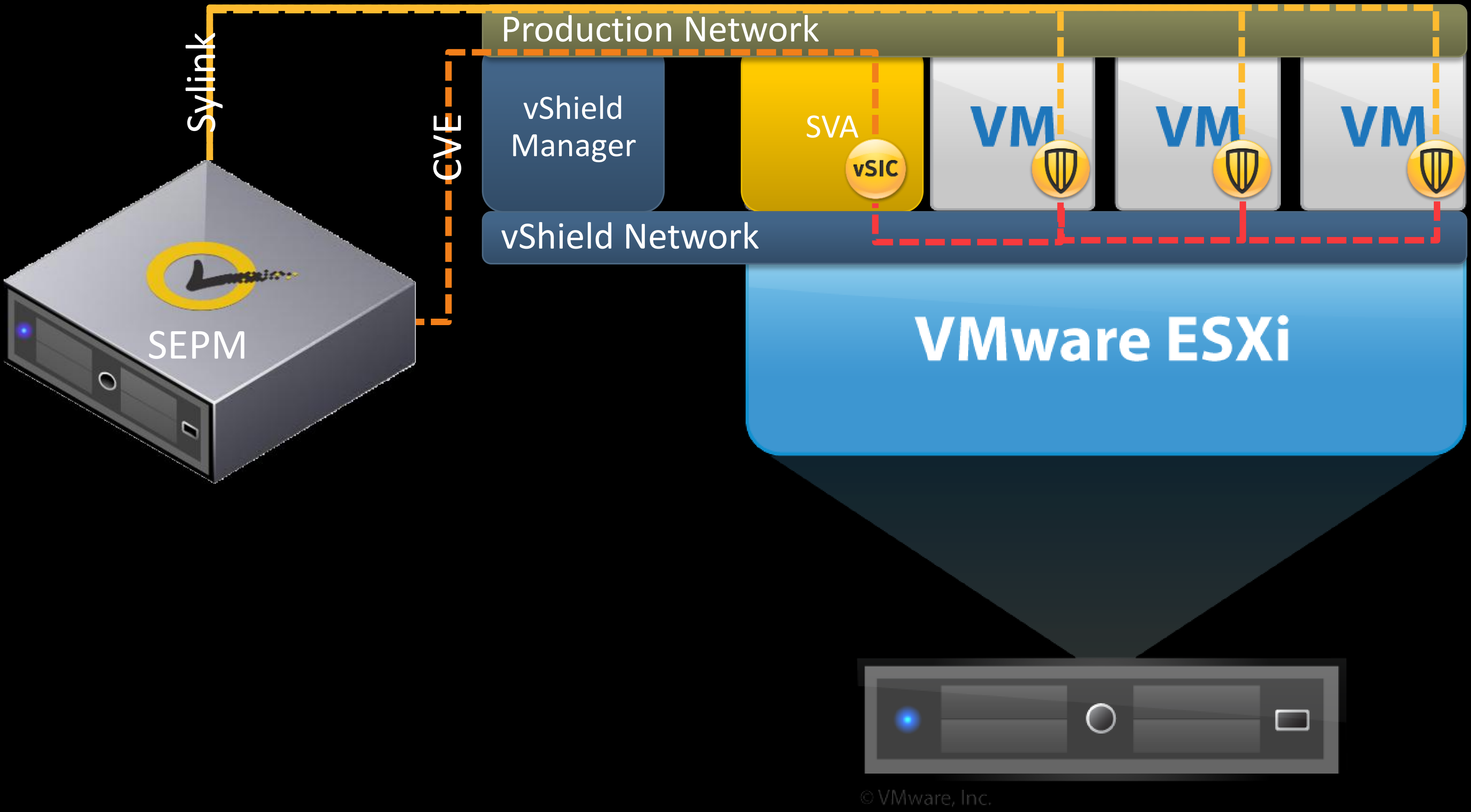
The Shared Insight Cache provides a shared cache across multiple virtual machines to reduce I/O by preventing different VMs from scanning similar files

- Applies to all On-Demand Scans (User Initiated, Scheduled, Admin Defined). Does not apply to auto-protect
- Scalable to thousands of clients per server
- Applies to all files (Not just Binary Executables)
- Data is keyed off of file hash and definition version. Latest definition version wins
  - Definitions can be updated in the middle of a scan
- Cache Server runs with all data completely in memory. Disk is only used for logging
- Not available on SBE version.

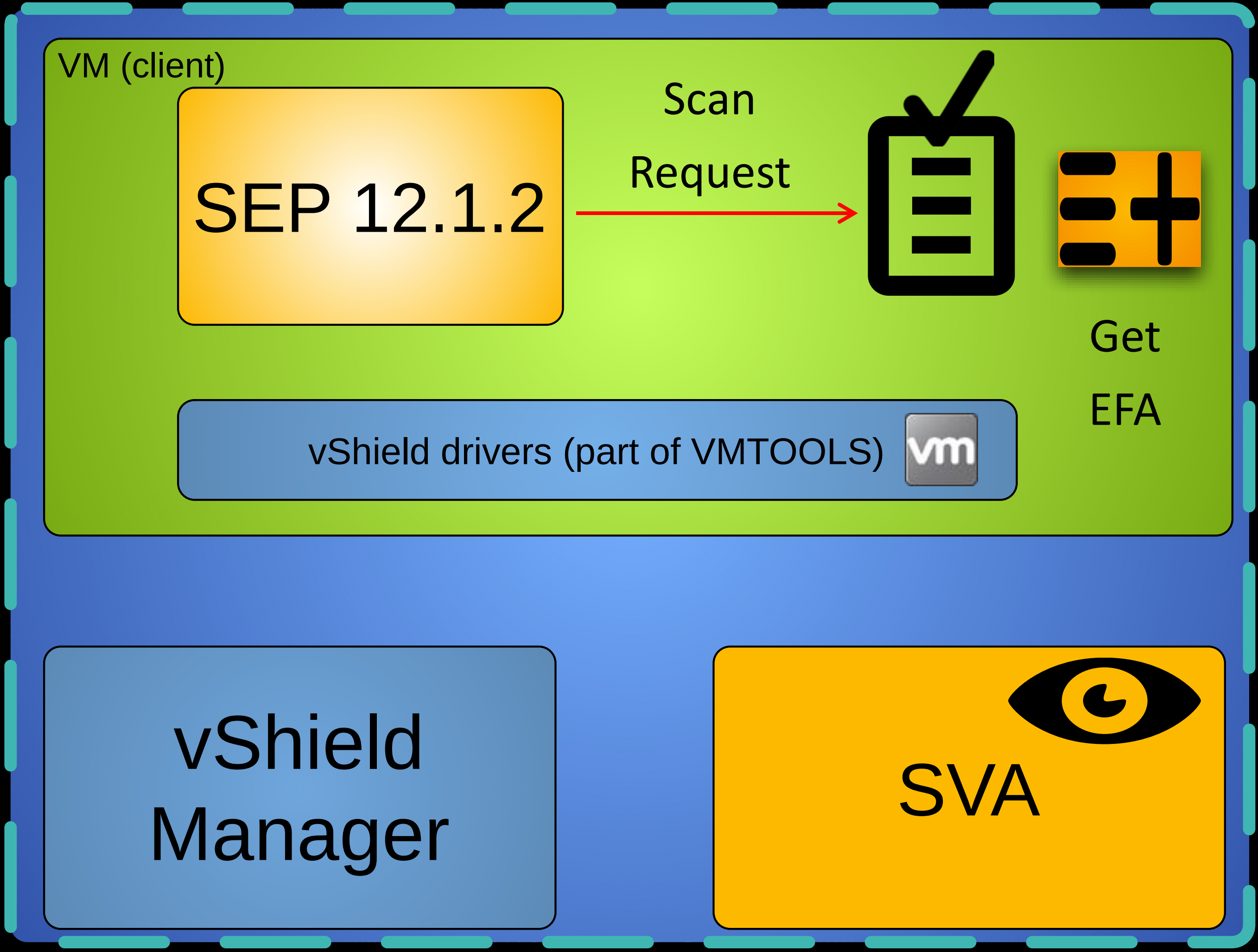
Introducing vSIC: vShield enabled Shared Insight Cache

- Automated vSIC association : simpler administration
- Reduces the scanning of identical files by VM's on the same hypervisor
- Reduces I/0 and CPU usage over non shared insight cache enabled endpoints
- Lighter virtual network usage than the concurrence (hash Vs File)
- Allows higher VM density
- Does not apply to auto-protect

vSIC components overview



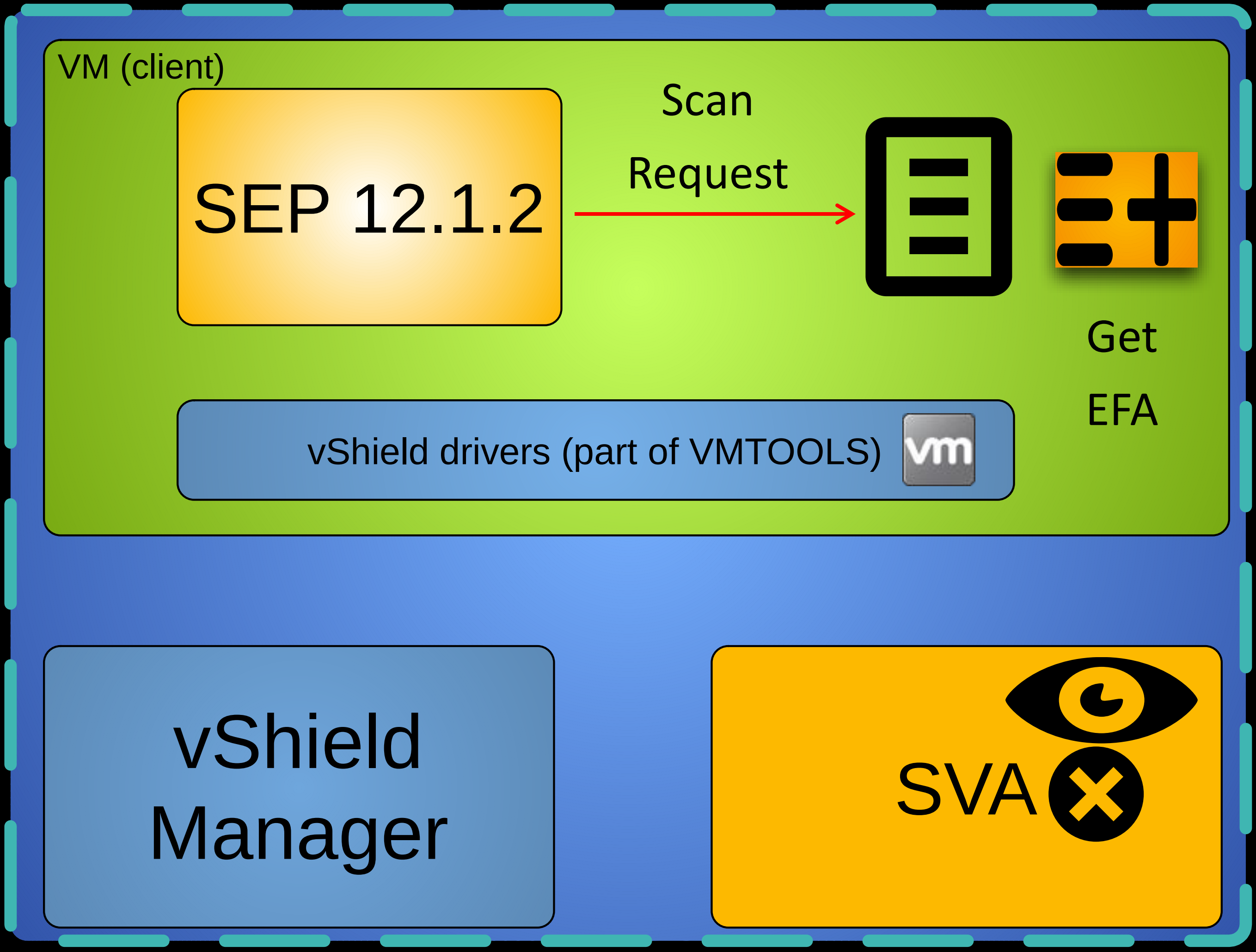
vSIC communication flow: Unknown file



Scan the file:

Proceed with the AV scan

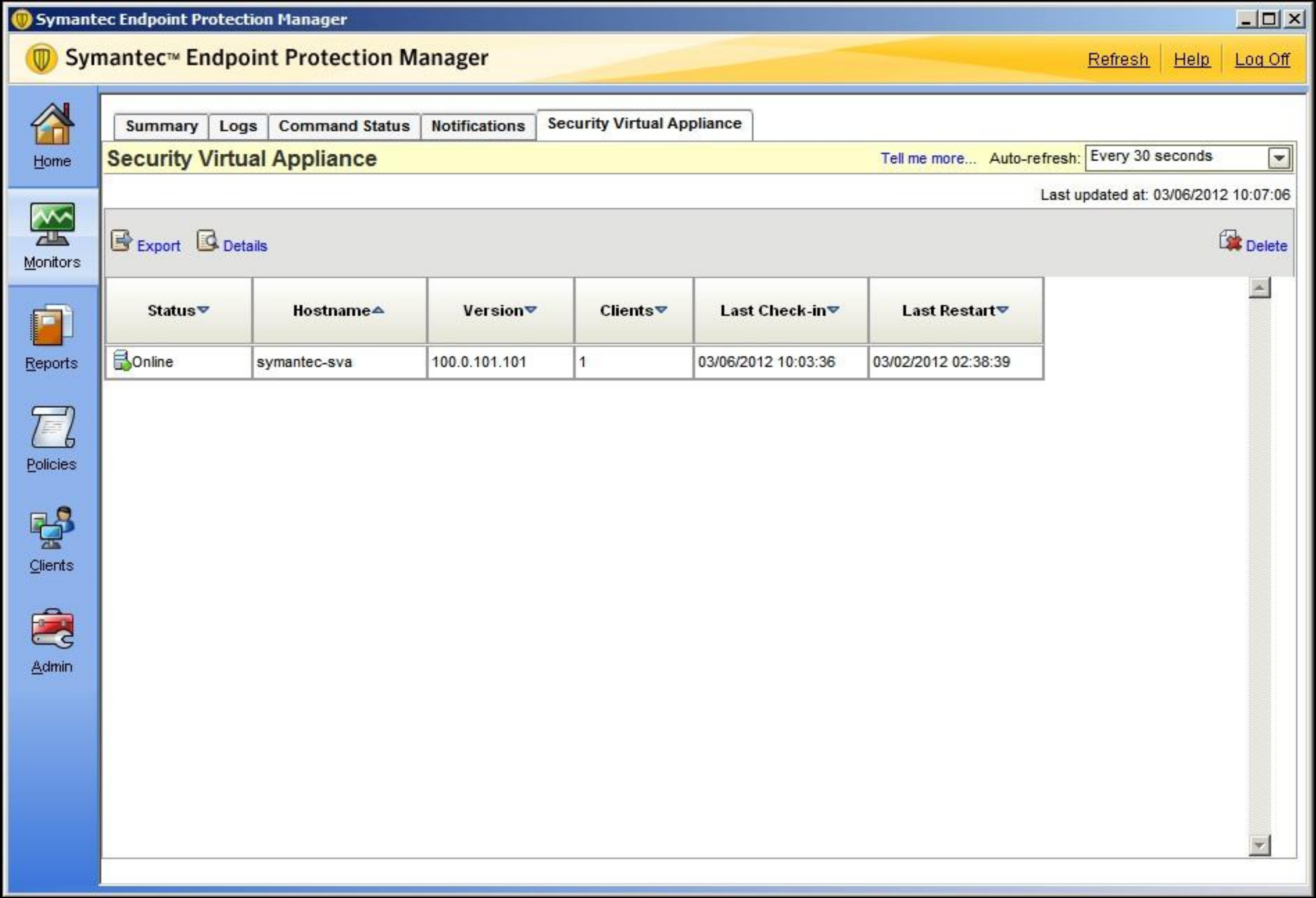
vSIC communication flow: known file



Skip the file:

AV kills the scan request and moves to the next file.

SEPM – Security Virtual Appliance Monitor



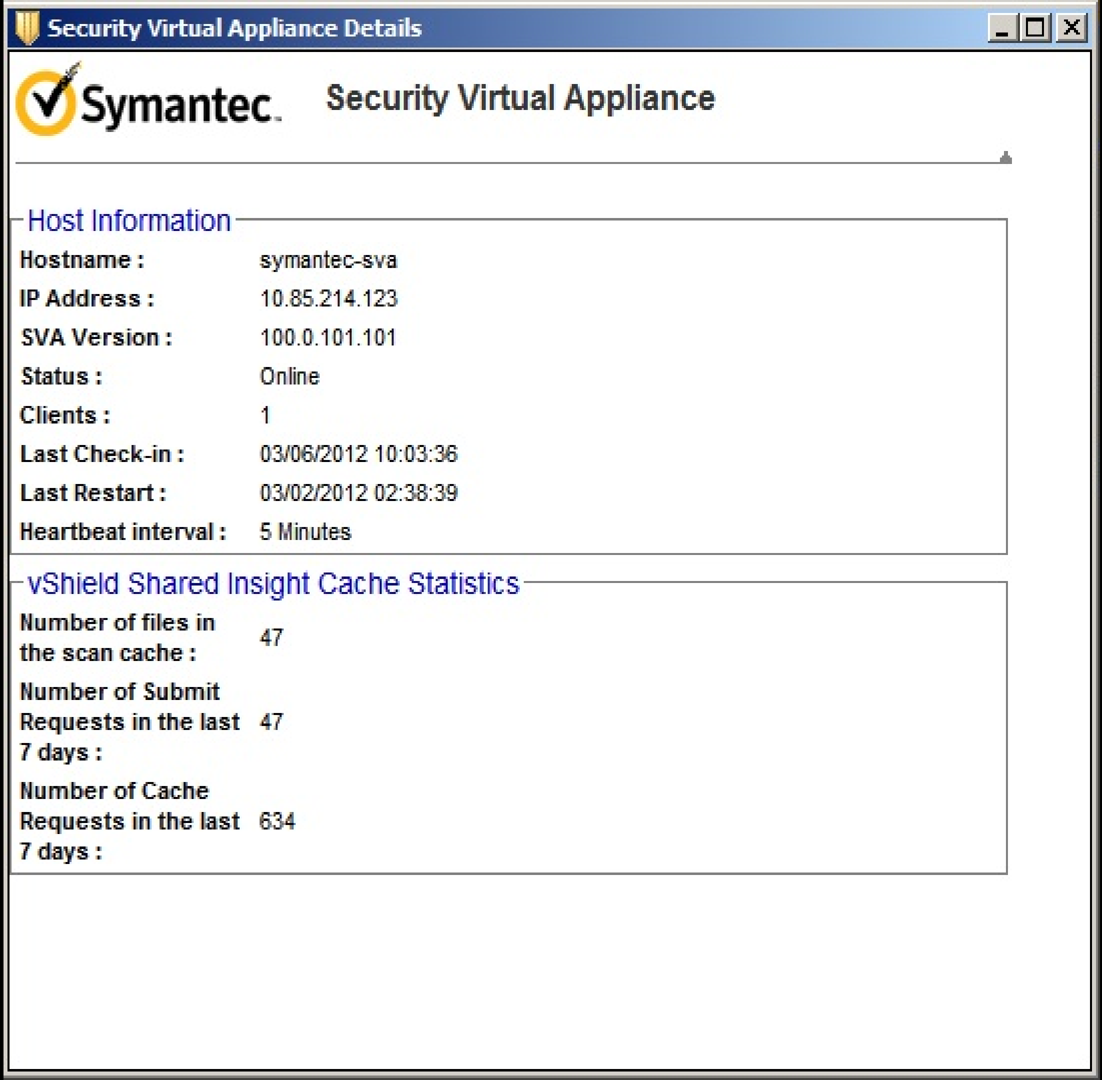
Security Virtual Appliance

Auto-refresh: Every 30 seconds

Last updated at: 03/06/2012 10:07:06

Status	Hostname	Version	Clients	Last Check-in	Last Restart
Online	symantec-sva	100.0.101.101	1	03/06/2012 10:03:36	03/02/2012 02:38:39

SEPM – Security Virtual Appliance Details



Security Virtual Appliance

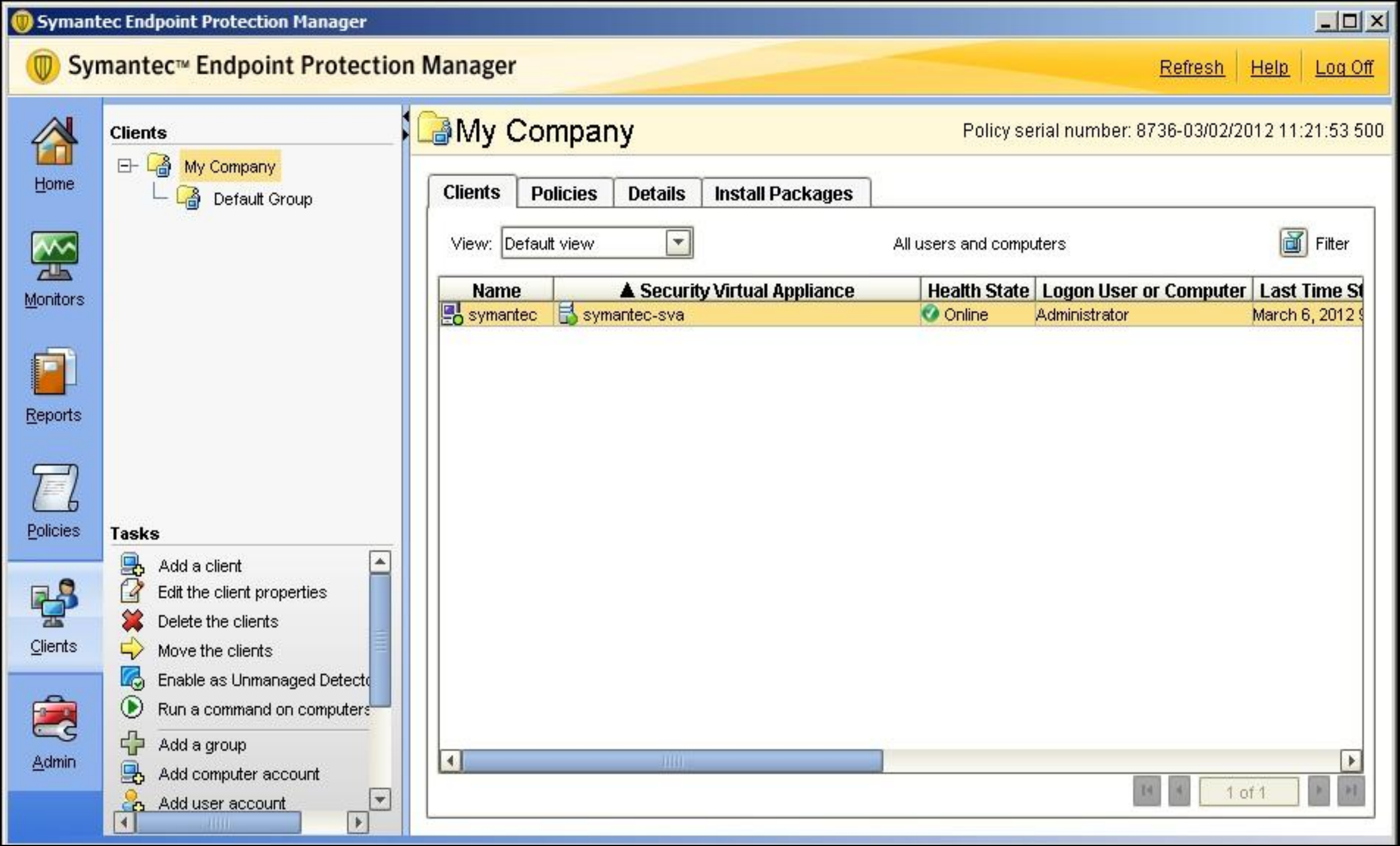
Host Information

Hostname :	symantec-sva
IP Address :	10.85.214.123
SVA Version :	100.0.101.101
Status :	Online
Clients :	1
Last Check-in :	03/06/2012 10:03:36
Last Restart :	03/02/2012 02:38:39
Heartbeat interval :	5 Minutes

vShield Shared Insight Cache Statistics

Number of files in the scan cache :	47
Number of Submit Requests in the last 7 days :	47
Number of Cache Requests in the last 7 days :	634

SEPM – Clients View



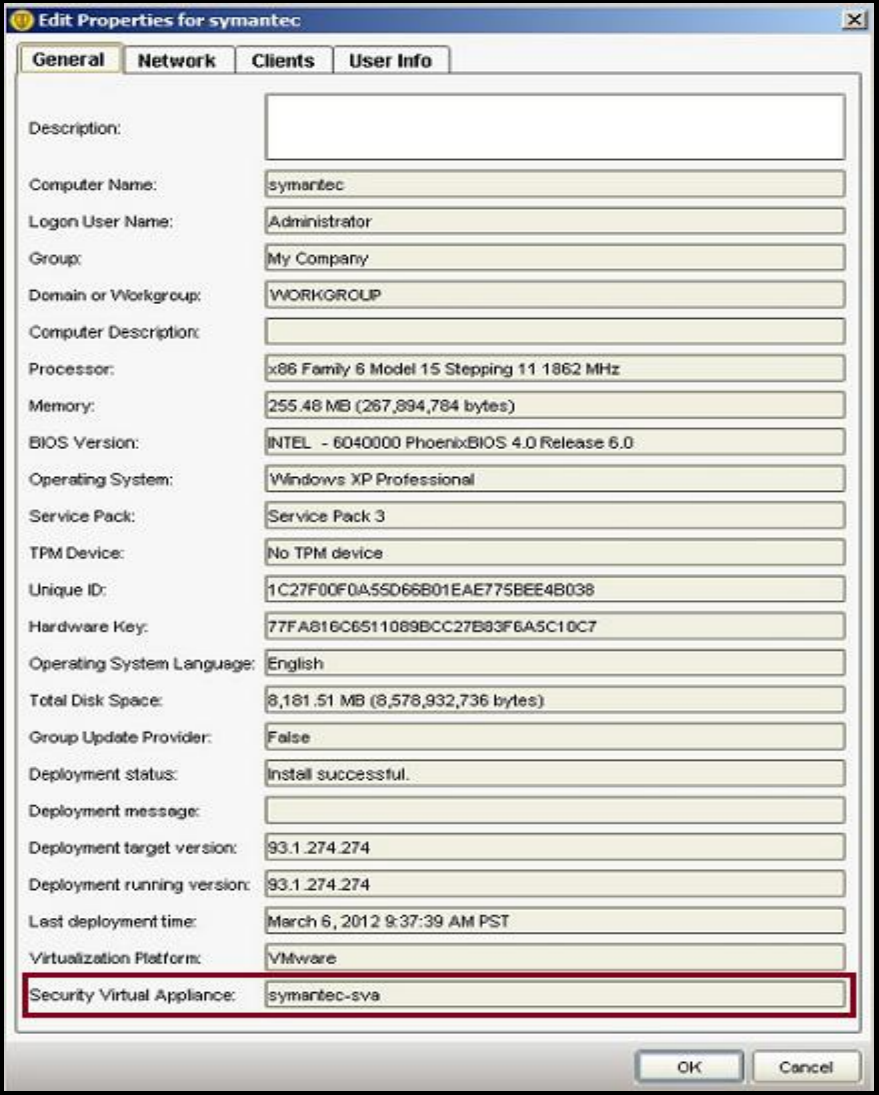
Policy serial number: 8736-03/02/2012 11:21:53 500

View: Default view

All users and computers

Name	▲ Security Virtual Appliance	Health State	Logon User or Computer	Last Time St
symantec	symantec-sva	Online	Administrator	March 6, 2012

SEPM – Clients Details



Edit Properties for symantec

Description:	
Computer Name:	symantec
Logon User Name:	Administrator
Group:	My Company
Domain or Workgroup:	WORKGROUP
Computer Description:	
Processor:	x86 Family 6 Model 15 Stepping 11 1862 MHz
Memory:	255.48 MB (267,894,784 bytes)
BIOS Version:	INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0
Operating System:	Windows XP Professional
Service Pack:	Service Pack 3
TPM Device:	No TPM device
Unique ID:	1C27F00F0A55D66B01EAE775BEE4B038
Hardware Key:	77FA816C6511089BCC27B83F6A5C10C7
Operating System Language:	English
Total Disk Space:	8,181.51 MB (8,578,932,736 bytes)
Group Update Provider:	False
Deployment status:	Install successful.
Deployment message:	
Deployment target version:	93.1.274.274
Deployment running version:	93.1.274.274
Last deployment time:	March 6, 2012 9:37:39 AM PST
Virtualization Platform:	VMware
Security Virtual Appliance:	symantec-sva

SVA – Security Profile

- PEN Tests
  - CCS Vulnerability Scan
  - Nessus Scan
- Login Settings
  - Root account login disabled
    - 'sudo' subsystem to elevate privileges is required
  - SSH disabled by default
- Cent OS minimal install
  - Packages updated prior to Release
  - Customers should not be updating packages

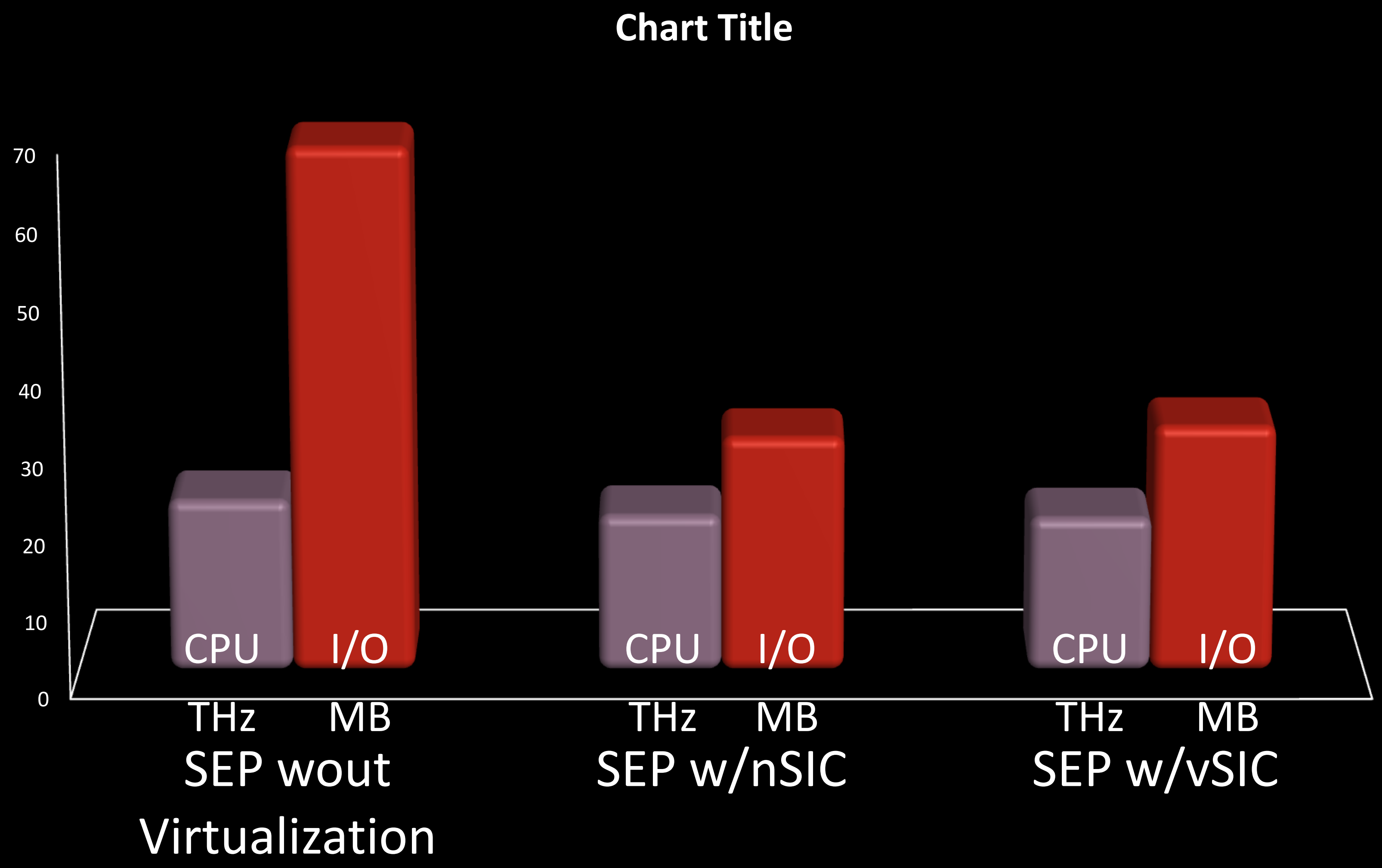
SVA – Virtual Machine Settings

- Settings based upon VMware Hardening Guidelines
  - Prevent virtual disk shrinking
    - isolation.tools.diskWiper.disable=TRUE
    - isolation.tools.diskShrink.disable=TRUE
  - Prevent other users from spying on administrator remote consoles
    - RemoteDisplay.maxConnections=1
  - Prevent unauthorized removal, connection and modification of devices
    - isolation.device.connectable.disable=TRUE
    - isolation.device.edit.disable=TRUE
  - Disable VM-to-VM communication through VMCI
    - vmci0.unrestricted=FALSE
  - Limit VM log file size and number
    - logging=FALSE
    - log.rotateSize=1000000
    - log.keepOld=10

SVA – Virtual Machine Settings

- Settings based upon VMware Hardening Guidelines, Continued…
  - Limit informational messages from the VM to the VMX file
    - tools.setInfo.sizeLimit=1048576
  - Disable certain unexposed features
    - isolation.tools.unity.push.update.disable=TRUE
    - isolation.tools.ghi.launchmenu.change=TRUE
    - isolation.tools.memSchedFakeSampleStats.disable=TRUE
    - isolation.tools.getCreds.disable=TRUE
    - isolation.tools.hgfsServerSet.disable = TRUE
  - Disable remote operations within the guest
    - guest.command.enabled=FALSE
  - Do not send host performance information to guests
    - tools.guestlib.enableHostInfo=FALSE

Performance Comparison – Internal Tests*



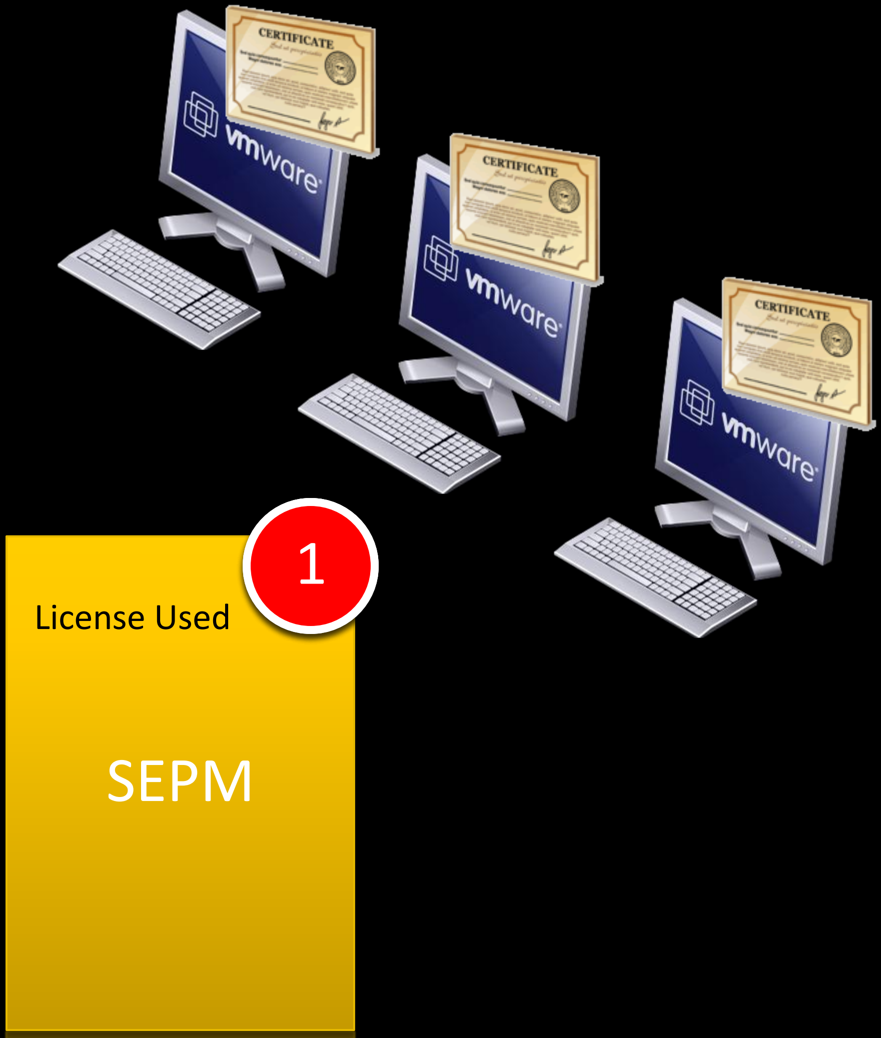
vSIC VS nSIC

Use case	vSIC	nSIC
Few ESX, large amount of VM	Flexible, easy to manage and install.	Require a large dedicated server with lots of RAM
Large amount of ESX	Need to deploy the SVA on each ESX node.	Can use one SIC server, higher maintenance cost as additional grouping on the console is required.
Use Motion/DRS	Automatic vSIC detection	Static mapping

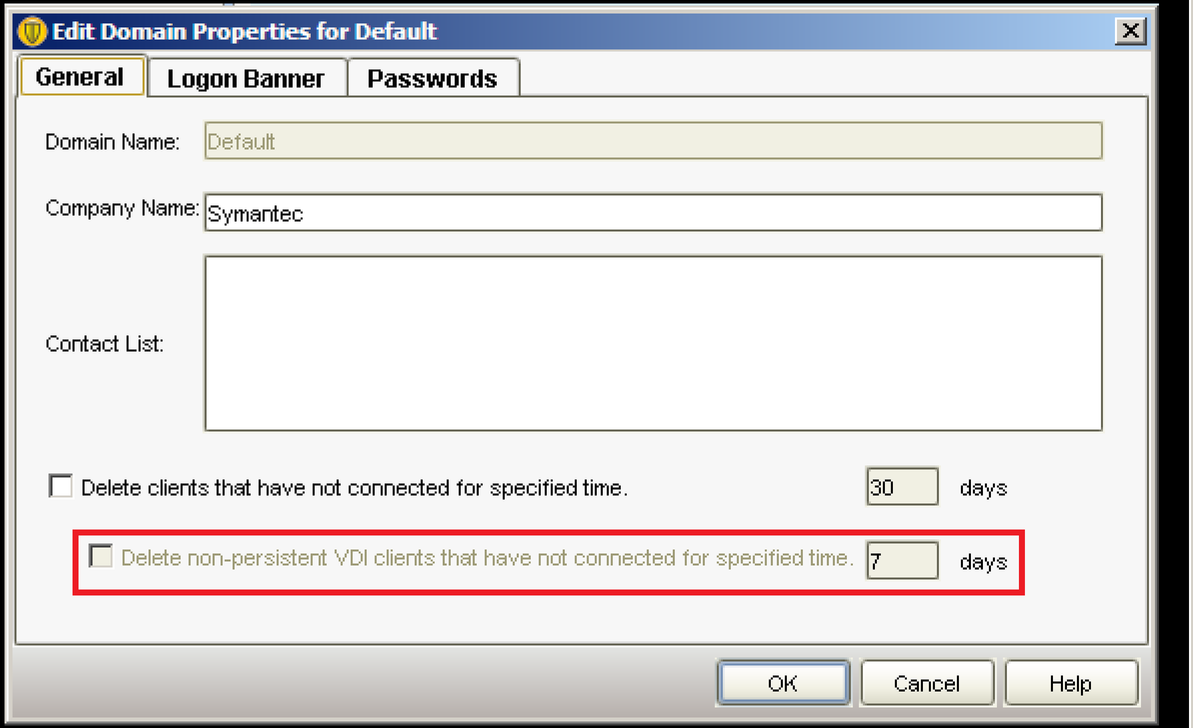
Non-Persistent VDI refinements

Solving licensing issues

- Registry setting to identify a VM as a Non-persistent VDI
- Customer should set this in the base image
- Non-Persistent VDI Aging policy in SEPM
- Licensing Change: Only Online Non-Persistent VDI clients are counted
- Client view filter



SEPM – Non-persistent VDI aging setting & Filtering



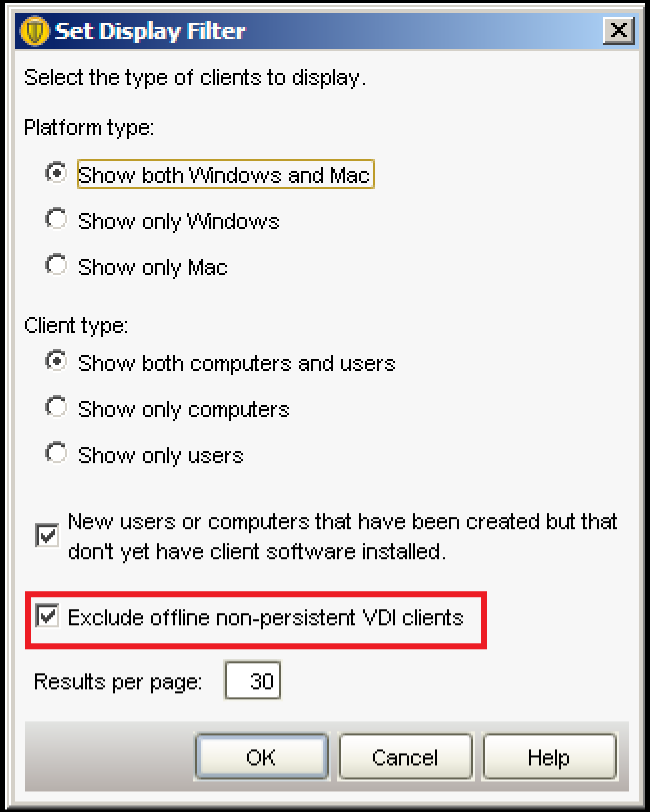
Domain Name: Default

Company Name: Symantec

Contact List:

☐ Delete clients that have not connected for specified time. 30 days

☐ Delete non-persistent VDI clients that have not connected for specified time. 7 days



Select the type of clients to display.

Platform type:

● Show both Windows and Mac

○ Show only Windows

○ Show only Mac

Client type:

● Show both computers and users

○ Show only computers

○ Show only users

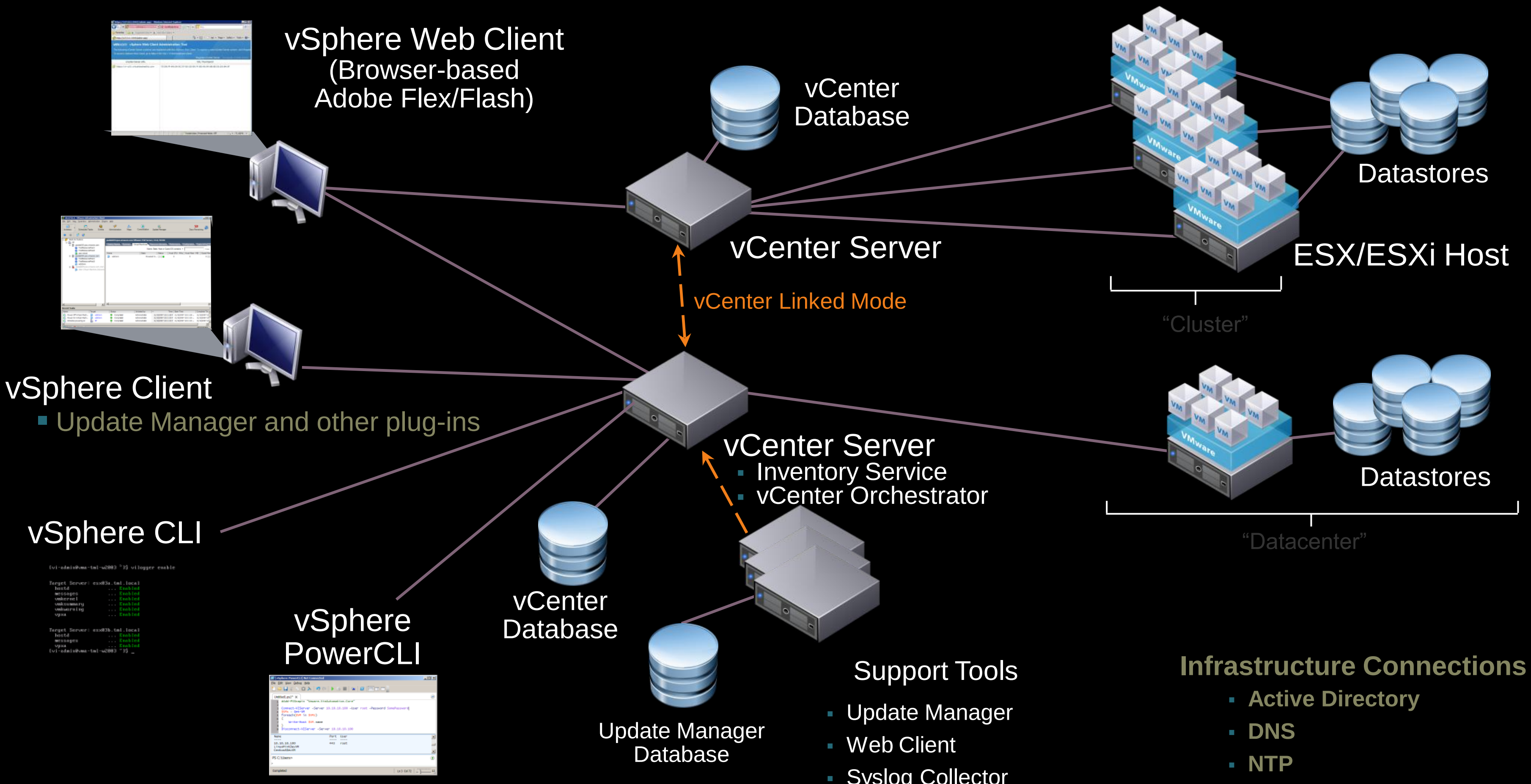
☑ New users or computers that have been created but that don't yet have client software installed.

☑ Exclude offline non-persistent VDI clients

Results per page: 30

Critical System Protection (CSP): Securing and Monitoring the Virtual Data Center

The Virtual Infrastructure



vSphere Web Client
(Browser-based
Adobe Flex/Flash)

vCenter
Database

vCenter Server

vCenter Linked Mode

ESX/ESXi Host

Datastores

"Cluster"

vSphere Client
- Update Manager and other plug-ins

vCenter Server
- Inventory Service
- vCenter Orchestrator

Datastores

"Datacenter"

vSphere CLI

```
[vi-admin@vma-tml-w2003 ~]$ vilogger enable

Target Server: esx03a.tml.local
  hostd                 ... Enabled
  messages              ... Enabled
  vmkernel              ... Enabled
  vmksummary            ... Enabled
  vmkwarning            ... Enabled
  vpxa                  ... Enabled

Target Server: esx03b.tml.local
  hostd                 ... Enabled
  messages              ... Enabled
  vpxa                  ... Enabled
[vi-admin@vma-tml-w2003 ~]$ _
```

vSphere
PowerCLI

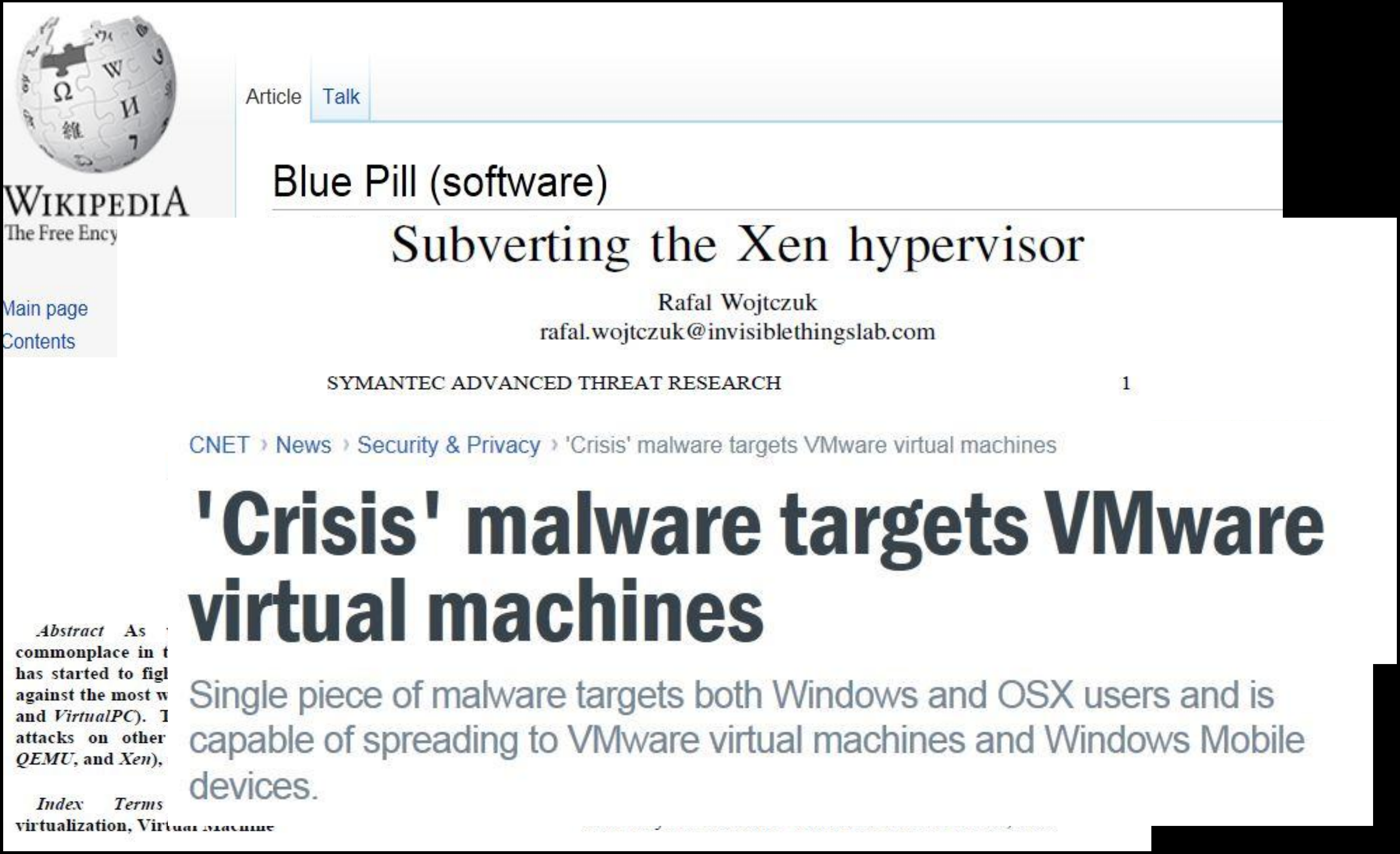
vCenter
Database

Update Manager
Database

Support Tools
- Update Manager
- Web Client
- Syslog Collector
- ESXi Dump Collector
- Auto Deploy
- Authentication Proxy

Infrastructure Connections
- **Active Directory**
- **DNS**
- **NTP**
- **SMTP**
- **SNMP**

Importance? Virtual Infrastructure Attacks



Wikipedia
The Free Ency

Main page
Contents

Article Talk

Blue Pill (software)

Subverting the Xen hypervisor

Rafal Wojtczuk
rafal.wojtczuk@invisiblethingslab.com

SYMANTEC ADVANCED THREAT RESEARCH 1

Abstract As
commonplace in t
has started to figl
against the most w
and *VirtualPC*). T
attacks on other
QEMU, and *Xen*),

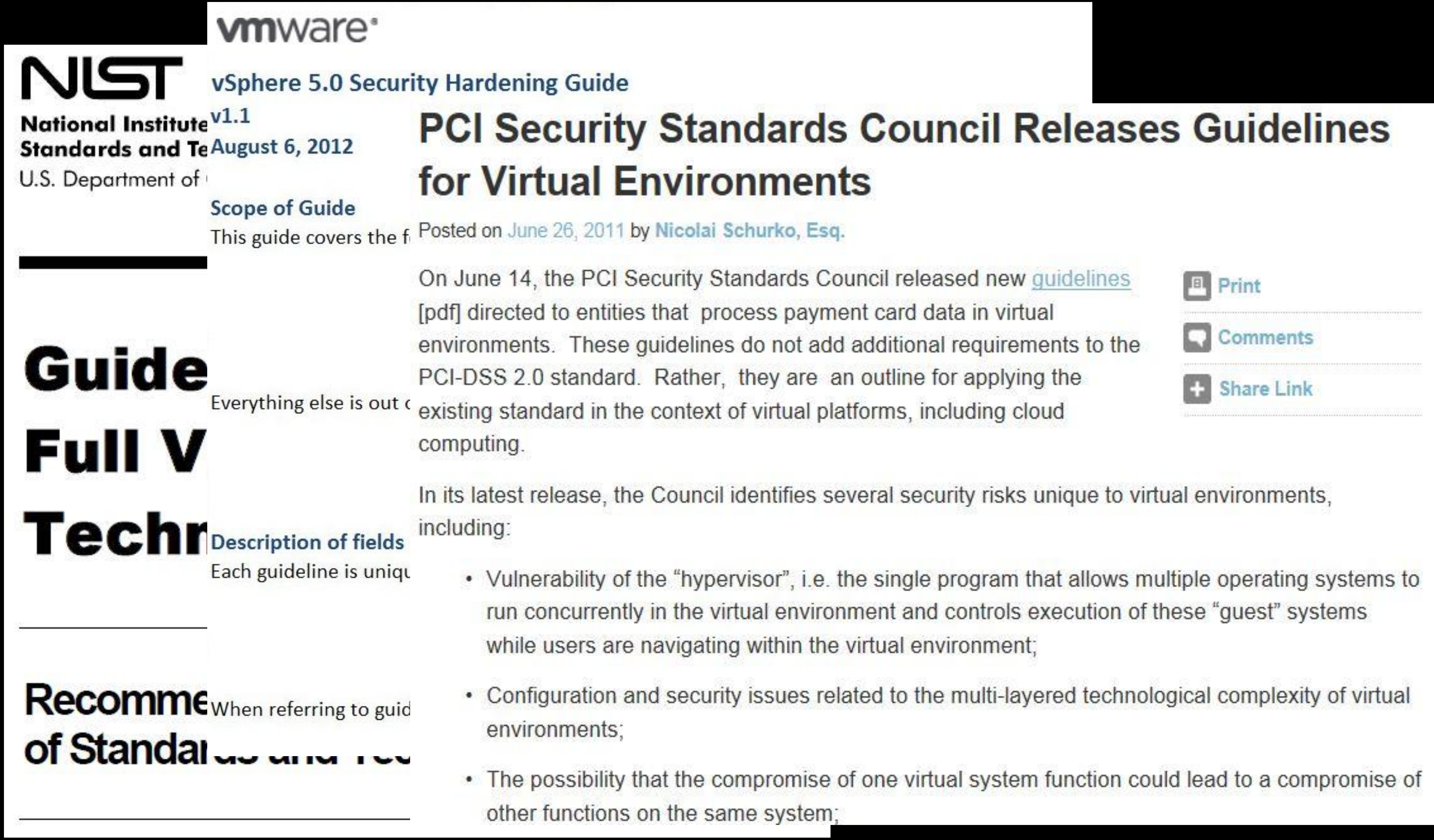
Index Terms
virtualization, Virtual Machine

CNET › News › Security & Privacy › 'Crisis' malware targets VMware virtual machines

'Crisis' malware targets VMware virtual machines

Single piece of malware targets both Windows and OSX users and is capable of spreading to VMware virtual machines and Windows Mobile devices.

Virtual Infrastructure Security Guidelines



NIST

National Institute
Standards and Te
U.S. Department of

Guide
Full V
Techn

Recomme
of Standar

vmware

vSphere 5.0 Security Hardening Guide
v1.1
August 6, 2012

Scope of Guide
This guide covers the f

Everything else is out c

Description of fields
Each guideline is uniqu

When referring to guid

PCI Security Standards Council Releases Guidelines for Virtual Environments

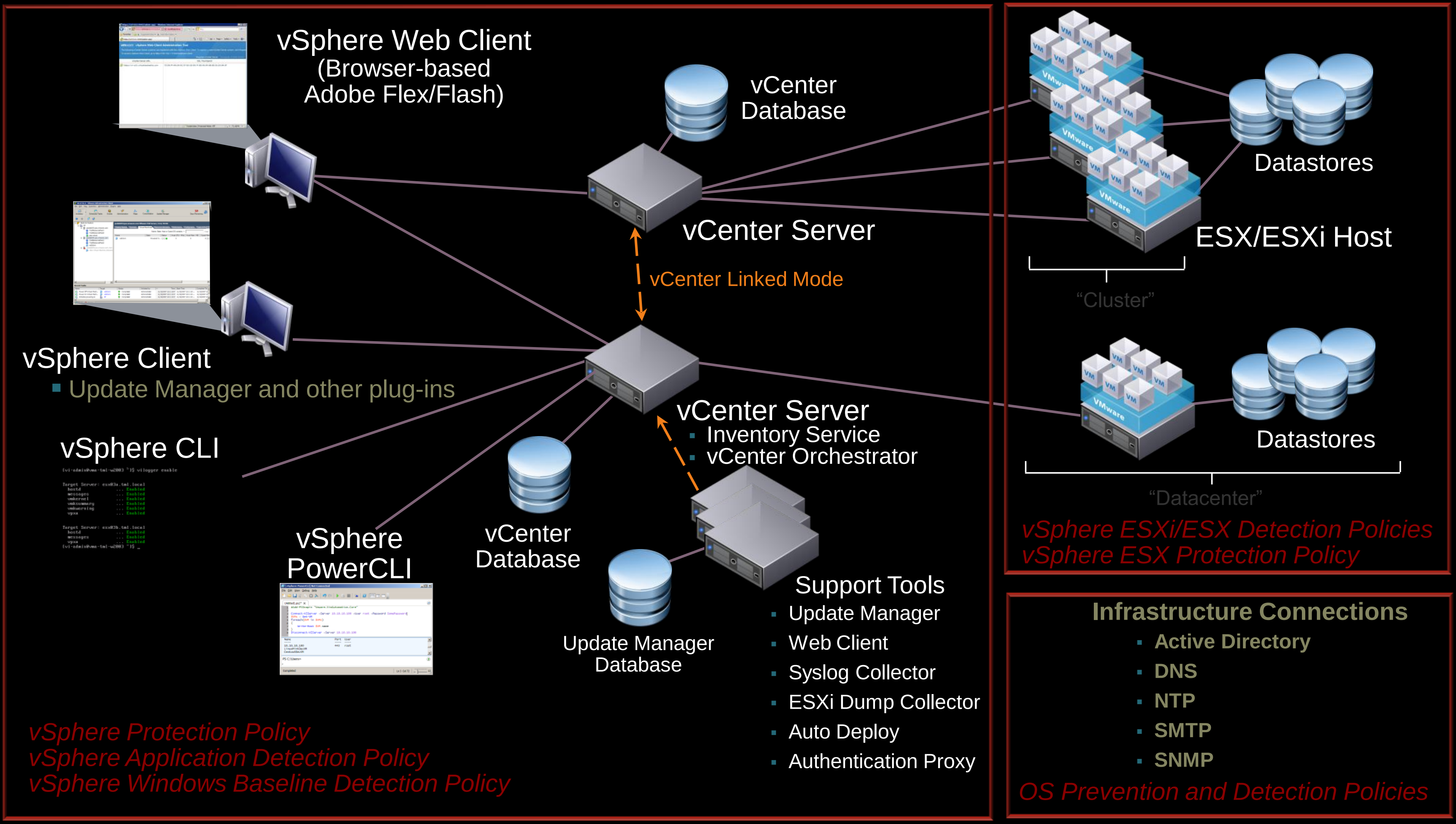
Posted on June 26, 2011 by Nicolai Schurko, Esq.

On June 14, the PCI Security Standards Council released new guidelines [pdf] directed to entities that process payment card data in virtual environments. These guidelines do not add additional requirements to the PCI-DSS 2.0 standard. Rather, they are an outline for applying the existing standard in the context of virtual platforms, including cloud computing.

In its latest release, the Council identifies several security risks unique to virtual environments, including:

- Vulnerability of the "hypervisor", i.e. the single program that allows multiple operating systems to run concurrently in the virtual environment and controls execution of these "guest" systems while users are navigating within the virtual environment;
- Configuration and security issues related to the multi-layered technological complexity of virtual environments;
- The possibility that the compromise of one virtual system function could lead to a compromise of other functions on the same system;

VMware vSphere Architecture and SCSP Coverage



vSphere Web Client
(Browser-based
Adobe Flex/Flash)

vSphere Client
- Update Manager and other plug-ins

vSphere CLI

```
[vi-admin@vma-tml-w2003 ~]$ vilogger enable

Target Server: esx03a.tml.local
  hostd                 ... Enabled
  messages              ... Enabled
  vmkernel              ... Enabled
  vmksummary            ... Enabled
  vmkwarning            ... Enabled
  vpxa                  ... Enabled

Target Server: esx03b.tml.local
  hostd                 ... Enabled
  messages              ... Enabled
  vpxa                  ... Enabled
[vi-admin@vma-tml-w2003 ~]$ _
```

vSphere
PowerCLI

vCenter
Database

vCenter Server

vCenter Linked Mode

vCenter Server
- Inventory Service
- vCenter Orchestrator

vCenter
Database

Update Manager
Database

Support Tools
- Update Manager
- Web Client
- Syslog Collector
- ESXi Dump Collector
- Auto Deploy
- Authentication Proxy

vSphere Protection Policy
vSphere Application Detection Policy
vSphere Windows Baseline Detection Policy

Datastores

ESX/ESXi Host

“Cluster”

Datastores

“Datacenter”

vSphere ESXi/ESX Detection Policies
vSphere ESX Protection Policy

Infrastructure Connections
- Active Directory
- DNS
- NTP
- SMTP
- SNMP

OS Prevention and Detection Policies

vSphere Policy Focus - Prevention

- Tamper Protection (no unauthorized modification)
  - vSphere binaries (more than traditional executables) tamper protection
  - vSphere configuration file tamper protection
  - vSphere data, log and SSL certificate tamper protection
  - Only vSphere programs (or trusted users/programs) can change contents
- SSL Certificate Protection (no unauthorized access)
  - Globally no access
  - Only trusted users/programs have access
- Network Firewall – Reduce Attack Surface for vSphere Apps
  - Limit inbound/outbound IP addresses vSphere programs can communicate with
- Policy Framework for easy customer modification
  - Complete policy ready to apply to vCenter servers (programs & resources pre-defined)
  - Re-Use Components for off-box utilities and client usage
  - Readily Configurable

vSphere Policy Focus - Detection

- Windows OS RT-FIM, Registry, Audit, Event and Log Monitoring
  - Pre-configured settings suitable for vCenter platform
  - Customer can customize further or choose to use their own Baseline Policy in use on other platforms
- vSphere Real-Time File Integrity Monitoring
  - vSphere binaries (more than traditional executables)
  - vSphere configuration files
- VMware unique hardening Requirements
  - vCenter SSL Certificate Files Usage Monitoring **(VSC02)**
  - vCenter Using Built-in Windows Account **(VSH05)**
- vSphere General Log Monitoring
  - Monitoring of vCenter vpxd log (primary web interaction log)
- Framework for easy customer modification
  - Complete policies (2) ready to apply to vCenter servers (programs & resources pre-defined)
  - Re-Use Components for off-box utilities
  - Readily Configurable

Vmware Hardening Guidelines

VSH01 – Maintain supported operating system, database, and hardware for vCenter

VSH02 – Keep VMware center system properly patched

VSH03 – Provide Windows system protection on VMware vCenter server host

VSH04 – Avoid user login to VMware vCenter server system

VSH06 – Restrict usage of vSphere administrator privilege

VSH10 – Clean up log files after failed installations of VMware vCenter server

VSC03 – Restrict access to SSL certificates

VSC05 – Restrict network access to VMware vCenter server system

VSC06 – Block access to ports not being used by VMware vCenter

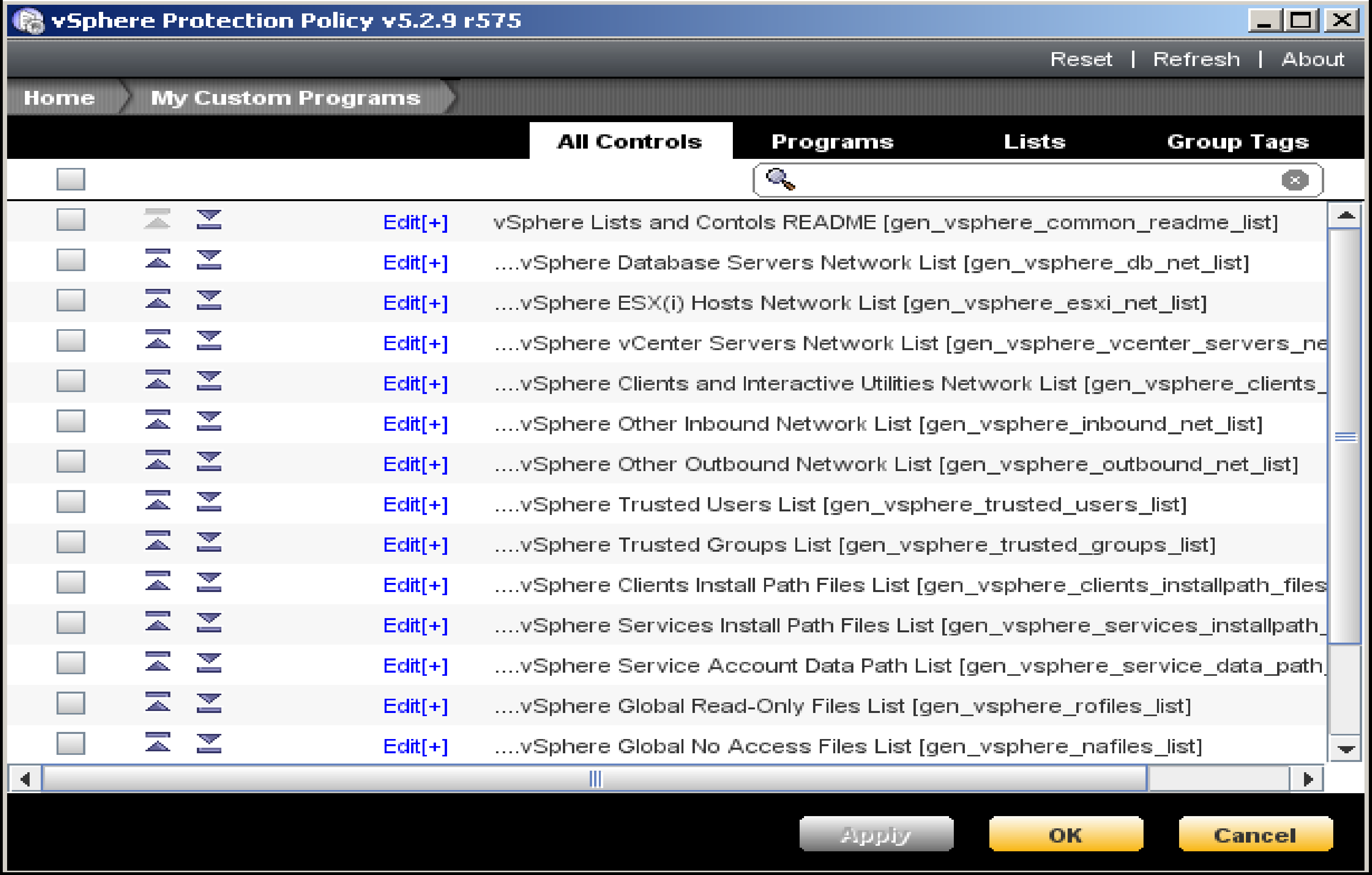
VUM03 – Provide Windows system protection on Update Manager system

VUM04 – Avoid user login to Update Manager system

HMT03 – Establish and maintain ESXi configuration file integrity

HMT15 – the “messages” kernel log file should be monitored for specific errors

vSphere Protection Policy



vSphere Protection Policy v5.2.9 r575

□ Edit[+] vSphere Lists and Contols README [gen_vsphere_common_readme_list]

□ Edit[+] ....vSphere Database Servers Network List [gen_vsphere_db_net_list]

□ Edit[+] ....vSphere ESX(i) Hosts Network List [gen_vsphere_esxi_net_list]

□ Edit[+] ....vSphere vCenter Servers Network List [gen_vsphere_vcenter_servers_ne

□ Edit[+] ....vSphere Clients and Interactive Utilities Network List [gen_vsphere_clients_

□ Edit[+] ....vSphere Other Inbound Network List [gen_vsphere_inbound_net_list]

□ Edit[+] ....vSphere Other Outbound Network List [gen_vsphere_outbound_net_list]

□ Edit[+] ....vSphere Trusted Users List [gen_vsphere_trusted_users_list]

□ Edit[+] ....vSphere Trusted Groups List [gen_vsphere_trusted_groups_list]

□ Edit[+] ....vSphere Clients Install Path Files List [gen_vsphere_clients_installpath_files

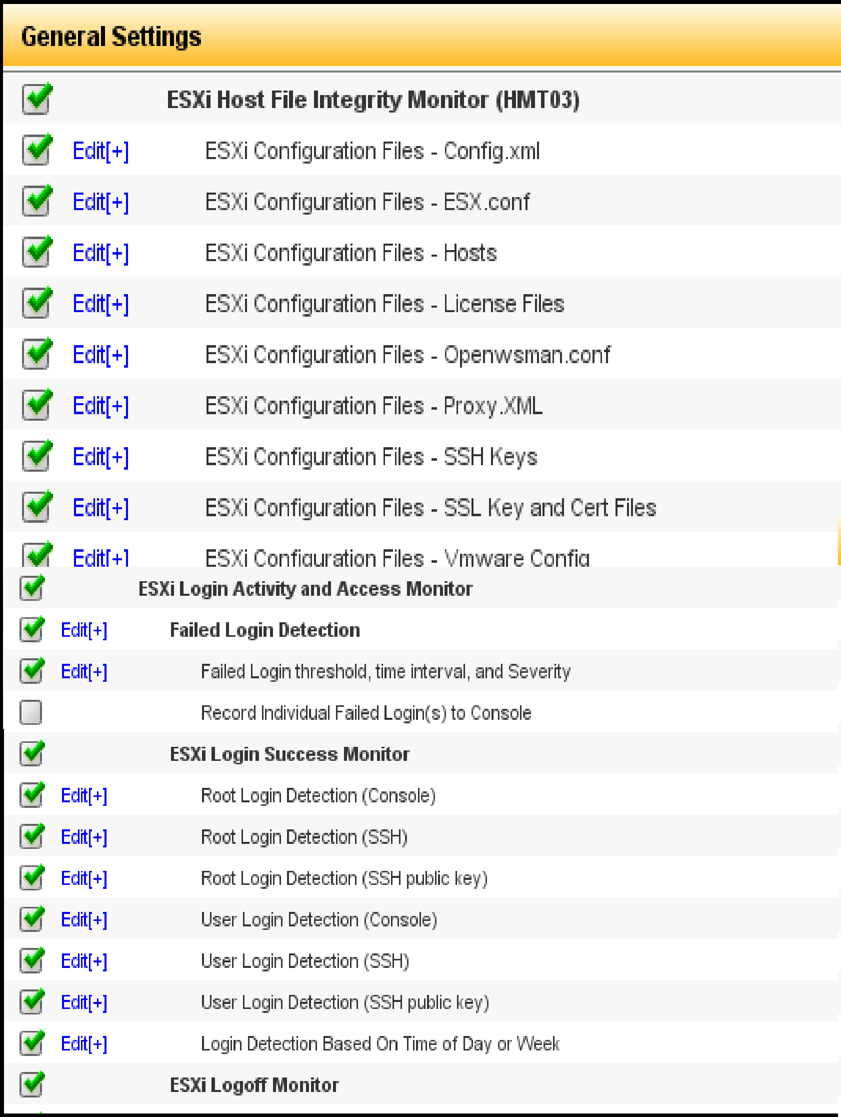
□ Edit[+] ....vSphere Services Install Path Files List [gen_vsphere_services_installpath_

□ Edit[+] ....vSphere Service Account Data Path List [gen_vsphere_service_data_path

□ Edit[+] ....vSphere Global Read-Only Files List [gen_vsphere_rofiles_list]

□ Edit[+] ....vSphere Global No Access Files List [gen_vsphere_nafiles_list]

vSphere ESXi Detection Policy Screenshot – All Rules



General Settings

☑ **ESXi Host File Integrity Monitor (HMT03)**

☑ Edit[+] ESXi Configuration Files - Config.xml

☑ Edit[+] ESXi Configuration Files - ESX.conf

☑ Edit[+] ESXi Configuration Files - Hosts

☑ Edit[+] ESXi Configuration Files - License Files

☑ Edit[+] ESXi Configuration Files - Openwsman.conf

☑ Edit[+] ESXi Configuration Files - Proxy.XML

☑ Edit[+] ESXi Configuration Files - SSH Keys

☑ Edit[+] ESXi Configuration Files - SSL Key and Cert Files

☑ Edit[+] ESXi Configuration Files - Vmware Config

☑ **ESXi Login Activity and Access Monitor**

☑ Edit[+] **Failed Login Detection**

☑ Edit[+] Failed Login threshold, time interval, and Severity

☐ Record Individual Failed Login(s) to Console

☑ **ESXi Login Success Monitor**

☑ Edit[+] Root Login Detection (Console)

☑ Edit[+] Root Login Detection (SSH)

☑ Edit[+] Root Login Detection (SSH public key)

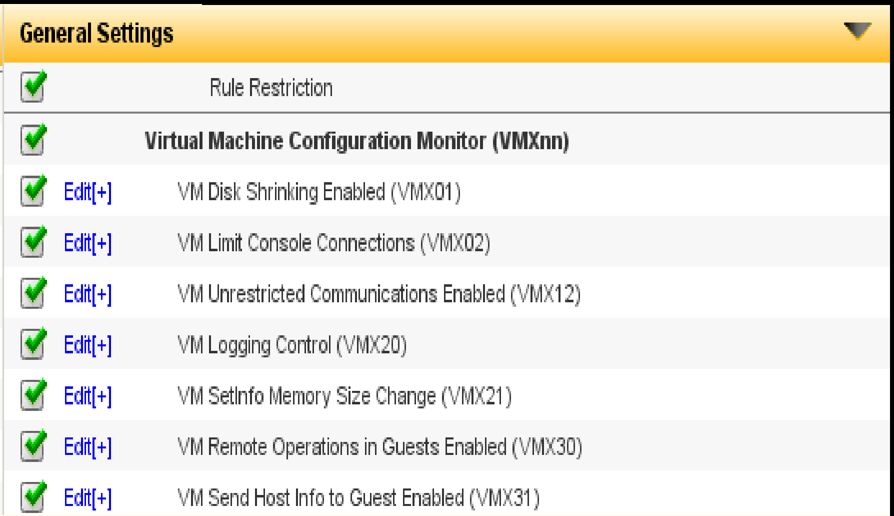
☑ Edit[+] User Login Detection (Console)

☑ Edit[+] User Login Detection (SSH)

☑ Edit[+] User Login Detection (SSH public key)

☑ Edit[+] Login Detection Based On Time of Day or Week

☑ **ESXi Logoff Monitor**



General Settings

☑ Rule Restriction

☑ **Virtual Machine Configuration Monitor (VMXnn)**

☑ Edit[+] VM Disk Shrinking Enabled (VMX01)

☑ Edit[+] VM Limit Console Connections (VMX02)

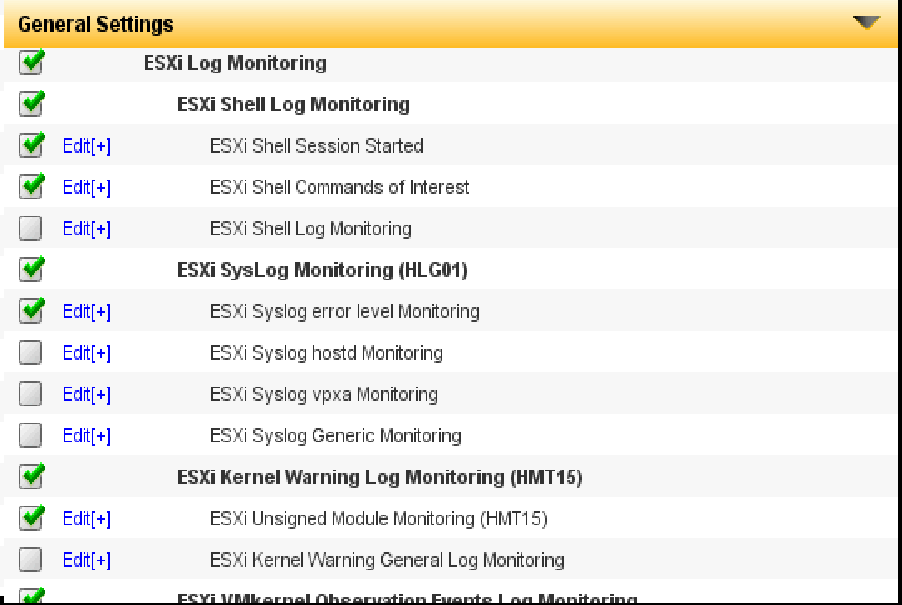
☑ Edit[+] VM Unrestricted Communications Enabled (VMX12)

☑ Edit[+] VM Logging Control (VMX20)

☑ Edit[+] VM SetInfo Memory Size Change (VMX21)

☑ Edit[+] VM Remote Operations in Guests Enabled (VMX30)

☑ Edit[+] VM Send Host Info to Guest Enabled (VMX31)



General Settings

☑ **ESXi Log Monitoring**

☑ **ESXi Shell Log Monitoring**

☑ Edit[+] ESXi Shell Session Started

☑ Edit[+] ESXi Shell Commands of Interest

☐ Edit[+] ESXi Shell Log Monitoring

☑ **ESXi SysLog Monitoring (HLG01)**

☑ Edit[+] ESXi Syslog error level Monitoring

☐ Edit[+] ESXi Syslog hostd Monitoring

☐ Edit[+] ESXi Syslog vpxa Monitoring

☐ Edit[+] ESXi Syslog Generic Monitoring

☑ **ESXi Kernel Warning Log Monitoring (HMT15)**

☑ Edit[+] ESXi Unsigned Module Monitoring (HMT15)

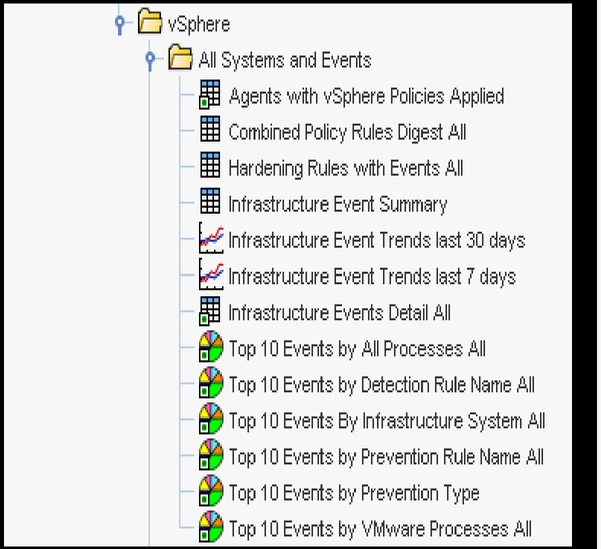
☐ Edit[+] ESXi Kernel Warning General Log Monitoring

☑ **ESXi VMkernel Observation Events Log Monitoring**

vSphere Reporting Content Overview

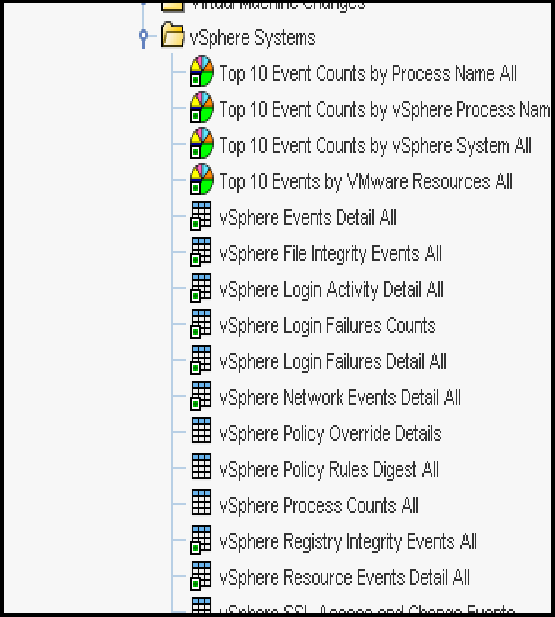
Queries

All VMware Systems



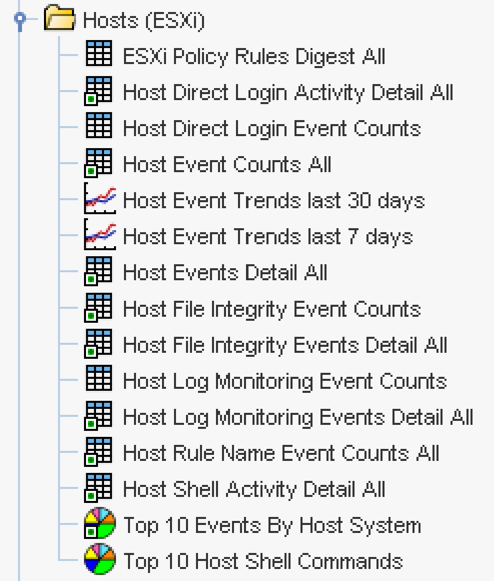
- vSphere
  - All Systems and Events
    - Agents with vSphere Policies Applied
    - Combined Policy Rules Digest All
    - Hardening Rules with Events All
    - Infrastructure Event Summary
    - Infrastructure Event Trends last 30 days
    - Infrastructure Event Trends last 7 days
    - Infrastructure Events Detail All
    - Top 10 Events by All Processes All
    - Top 10 Events by Detection Rule Name All
    - Top 10 Events By Infrastructure System All
    - Top 10 Events by Prevention Rule Name All
    - Top 10 Events by Prevention Type
    - Top 10 Events by VMware Processes All

vSphere Mgt Systems



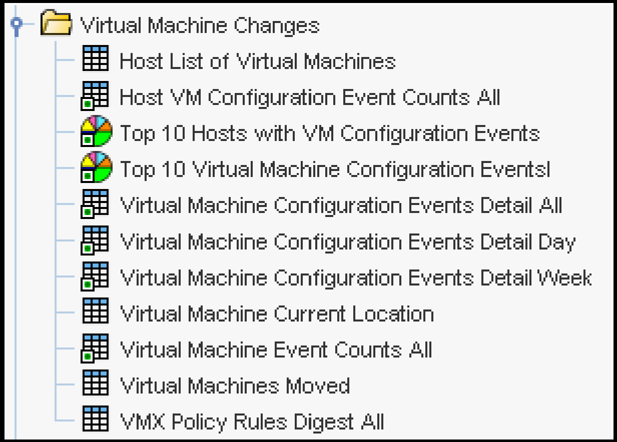
- Virtual Machine Changes
- vSphere Systems
  - Top 10 Event Counts by Process Name All
  - Top 10 Event Counts by vSphere Process Nam
  - Top 10 Event Counts by vSphere System All
  - Top 10 Events by VMware Resources All
  - vSphere Events Detail All
  - vSphere File Integrity Events All
  - vSphere Login Activity Detail All
  - vSphere Login Failures Counts
  - vSphere Login Failures Detail All
  - vSphere Network Events Detail All
  - vSphere Policy Override Details
  - vSphere Policy Rules Digest All
  - vSphere Process Counts All
  - vSphere Registry Integrity Events All
  - vSphere Resource Events Detail All
  - vSphere SSL Access and Change Events

ESXi Hosts



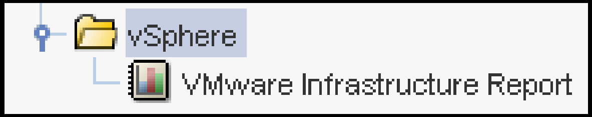
- Hosts (ESXi)
  - ESXi Policy Rules Digest All
  - Host Direct Login Activity Detail All
  - Host Direct Login Event Counts
  - Host Event Counts All
  - Host Event Trends last 30 days
  - Host Event Trends last 7 days
  - Host Events Detail All
  - Host File Integrity Event Counts
  - Host File Integrity Events Detail All
  - Host Log Monitoring Event Counts
  - Host Log Monitoring Events Detail All
  - Host Rule Name Event Counts All
  - Host Shell Activity Detail All
  - Top 10 Events By Host System
  - Top 10 Host Shell Commands

Virtual Machines



- Virtual Machine Changes
  - Host List of Virtual Machines
  - Host VM Configuration Event Counts All
  - Top 10 Hosts with VM Configuration Events
  - Top 10 Virtual Machine Configuration EventsI
  - Virtual Machine Configuration Events Detail All
  - Virtual Machine Configuration Events Detail Day
  - Virtual Machine Configuration Events Detail Week
  - Virtual Machine Current Location
  - Virtual Machine Event Counts All
  - Virtual Machines Moved
  - VMX Policy Rules Digest All

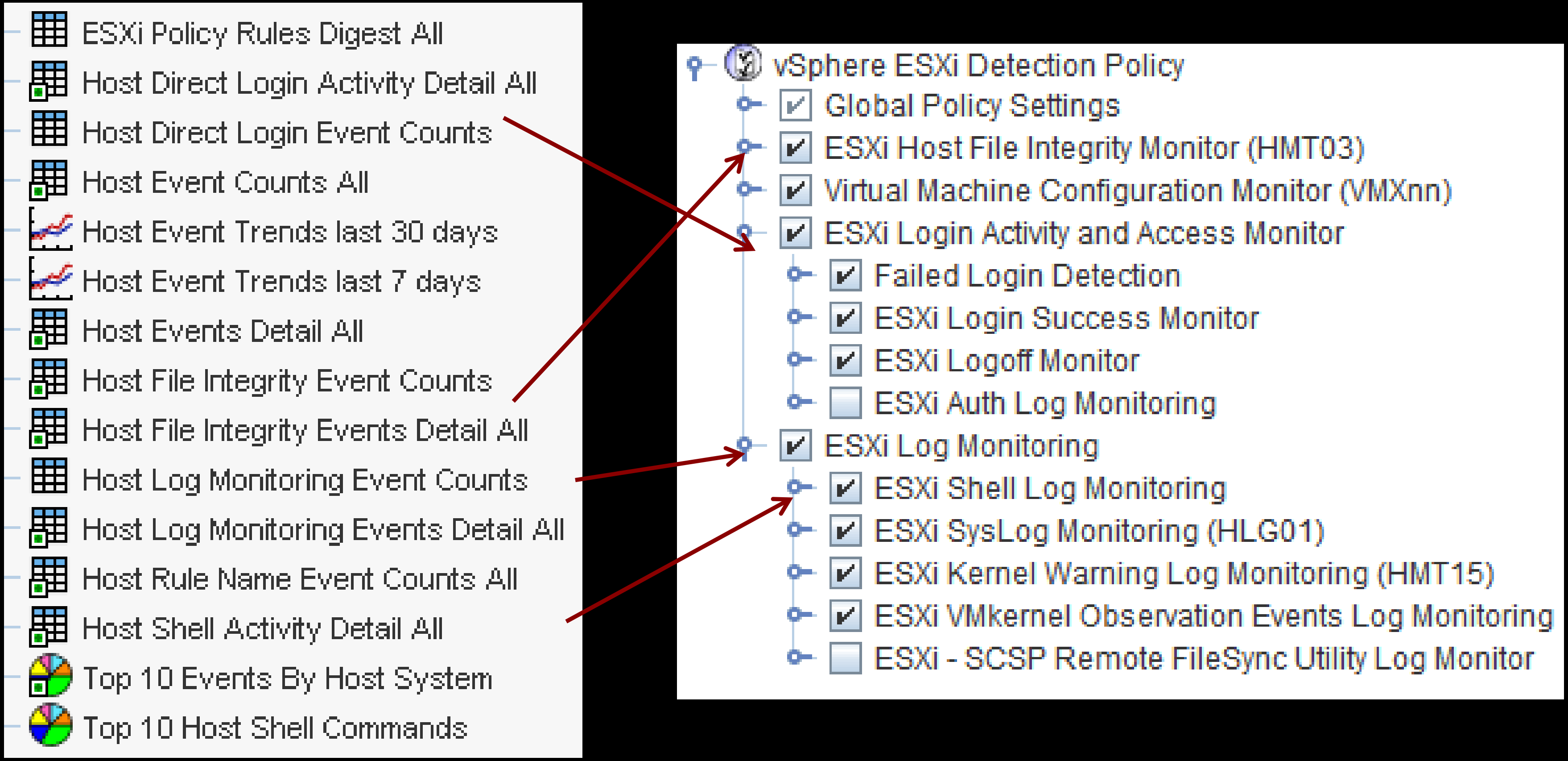
Dashboard Report



- vSphere
  - VMware Infrastructure Report

ESXi Hosts

- Filtered Queries for ESXi policy events (minus any VMX configuration changes) and drill downs to specific policy activity as shown below:

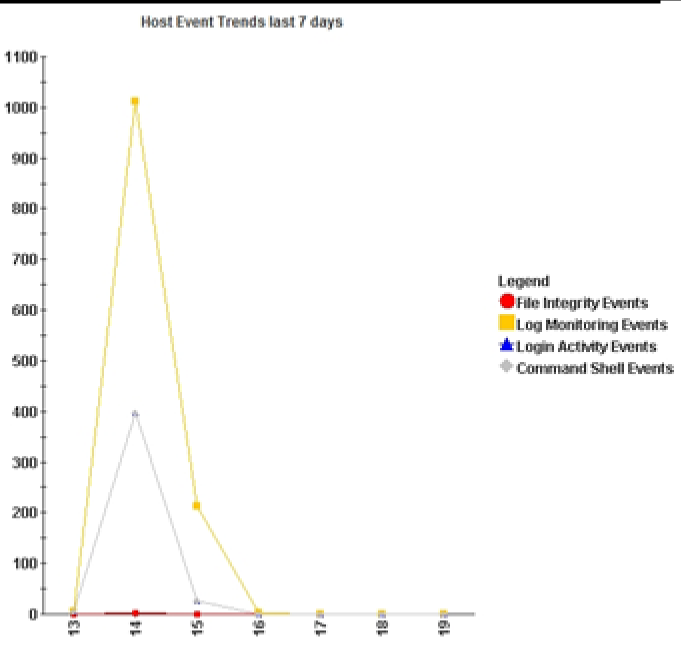


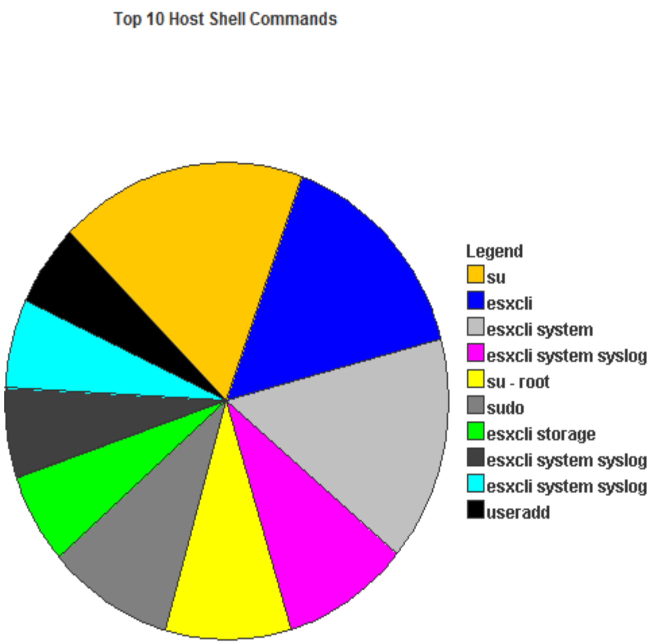
- ESXi Policy Rules Digest All
- Host Direct Login Activity Detail All
- Host Direct Login Event Counts
- Host Event Counts All
- Host Event Trends last 30 days
- Host Event Trends last 7 days
- Host Events Detail All
- Host File Integrity Event Counts
- Host File Integrity Events Detail All
- Host Log Monitoring Event Counts
- Host Log Monitoring Events Detail All
- Host Rule Name Event Counts All
- Host Shell Activity Detail All
- Top 10 Events By Host System
- Top 10 Host Shell Commands

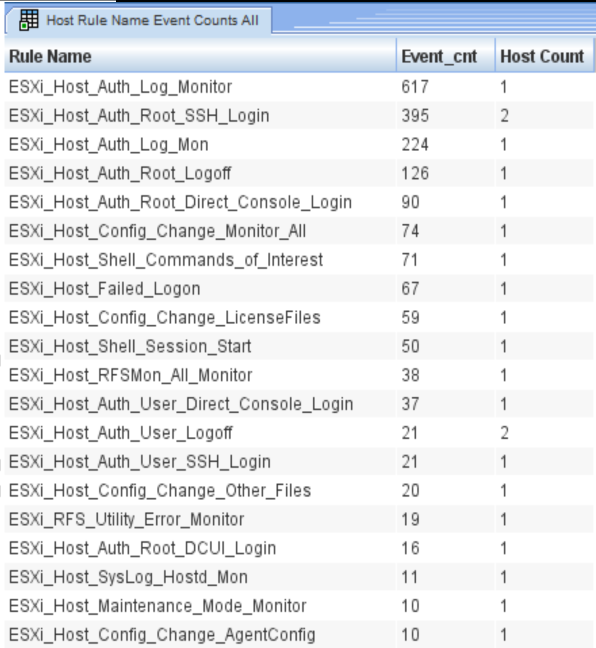
vSphere ESXi Detection Policy
- ☑ Global Policy Settings
- ☑ ESXi Host File Integrity Monitor (HMT03)
- ☑ Virtual Machine Configuration Monitor (VMXnn)
- ☑ ESXi Login Activity and Access Monitor
  - ☑ Failed Login Detection
  - ☑ ESXi Login Success Monitor
  - ☑ ESXi Logoff Monitor
  - □ ESXi Auth Log Monitoring
- ☑ ESXi Log Monitoring
  - ☑ ESXi Shell Log Monitoring
  - ☑ ESXi SysLog Monitoring (HLG01)
  - ☑ ESXi Kernel Warning Log Monitoring (HMT15)
  - ☑ ESXi VMkernel Observation Events Log Monitoring
  - □ ESXi - SCSP Remote FileSync Utility Log Monitor

ESXi Trends, Top 10, Event Counts

- Events specific to ESXi configuration changes and log monitoring including direct console logins and shell activity

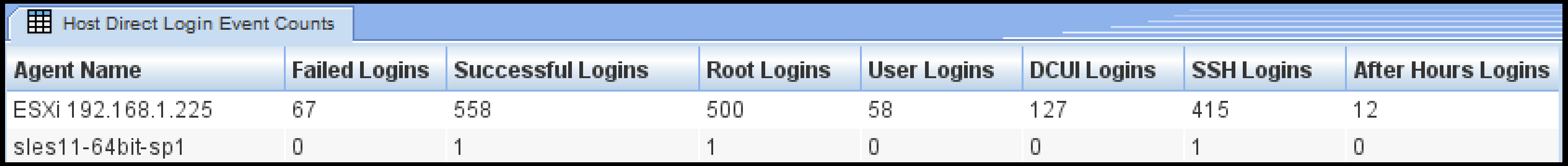






Host Rule Name Event Counts All

Rule Name	Event_cnt	Host Count
ESXi_Host_Auth_Log_Monitor	617	1
ESXi_Host_Auth_Root_SSH_Login	395	2
ESXi_Host_Auth_Log_Mon	224	1
ESXi_Host_Auth_Root_Logoff	126	1
ESXi_Host_Auth_Root_Direct_Console_Login	90	1
ESXi_Host_Config_Change_Monitor_All	74	1
ESXi_Host_Shell_Commands_of_Interest	71	1
ESXi_Host_Failed_Logon	67	1
ESXi_Host_Config_Change_LicenseFiles	59	1
ESXi_Host_Shell_Session_Start	50	1
ESXi_Host_RFSMon_All_Monitor	38	1
ESXi_Host_Auth_User_Direct_Console_Login	37	1
ESXi_Host_Auth_User_Logoff	21	2
ESXi_Host_Auth_User_SSH_Login	21	1
ESXi_Host_Config_Change_Other_Files	20	1
ESXi_RFS_Utility_Error_Monitor	19	1
ESXi_Host_Auth_Root_DCUI_Login	16	1
ESXi_Host_SysLog_Hostd_Mon	11	1
ESXi_Host_Maintenance_Mode_Monitor	10	1
ESXi_Host_Config_Change_AgentConfig	10	1

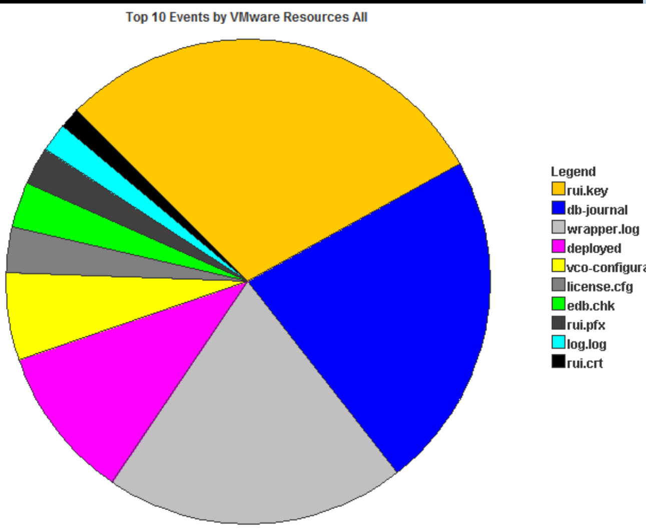


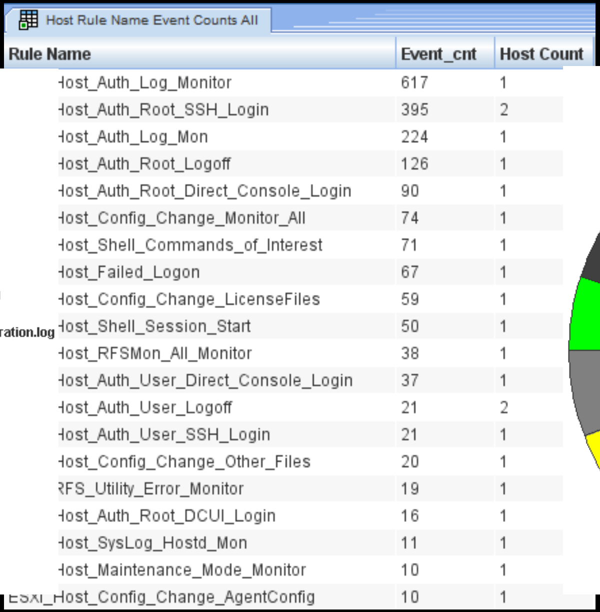
Host Direct Login Event Counts

Agent Name	Failed Logins	Successful Logins	Root Logins	User Logins	DCUI Logins	SSH Logins	After Hours Logins
ESXi 192.168.1.225	67	558	500	58	127	415	12
sles11-64bit-sp1	0	1	1	0	0	1	0

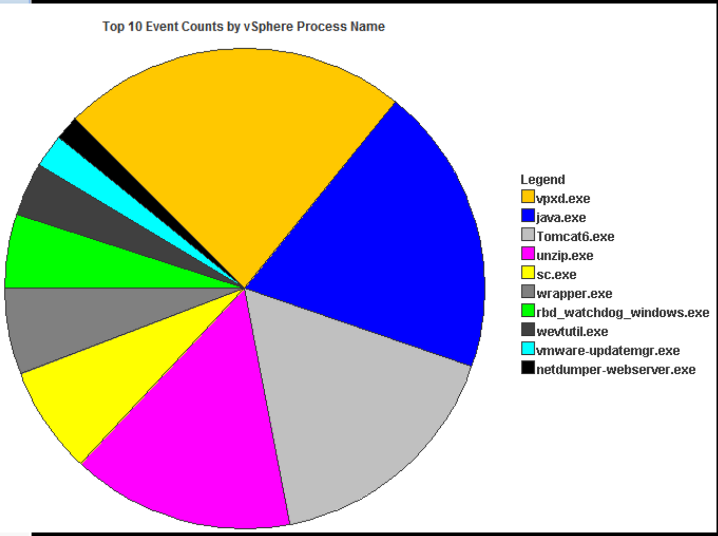
Top vSphere Resources and Processes and Event Counts

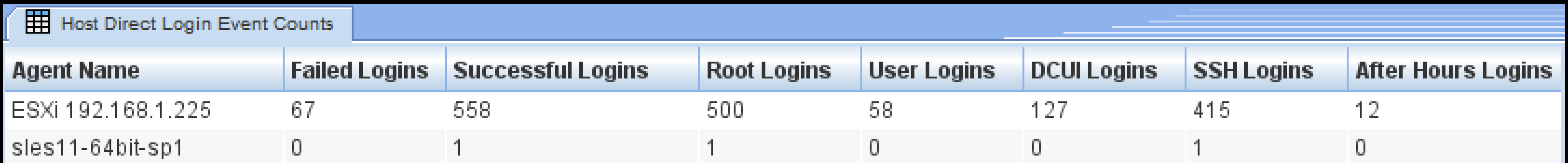
- Events related to vSphere configuration changes, resource accesses and log monitoring





Rule Name	Event_cnt	Host Count
Host_Auth_Log_Monitor	617	1
Host_Auth_Root_SSH_Login	395	2
Host_Auth_Log_Mon	224	1
Host_Auth_Root_Logoff	126	1
Host_Auth_Root_Direct_Console_Login	90	1
Host_Config_Change_Monitor_All	74	1
Host_Shell_Commands_of_Interest	71	1
Host_Failed_Logon	67	1
Host_Config_Change_LicenseFiles	59	1
Host_Shell_Session_Start	50	1
Host_RFSMon_All_Monitor	38	1
Host_Auth_User_Direct_Console_Login	37	1
Host_Auth_User_Logoff	21	2
Host_Auth_User_SSH_Login	21	1
Host_Config_Change_Other_Files	20	1
RFS_Utility_Error_Monitor	19	1
Host_Auth_Root_DCUI_Login	16	1
Host_SysLog_Hostd_Mon	11	1
Host_Maintenance_Mode_Monitor	10	1
ESXi_Host_Config_Change_AgentConfig	10	1

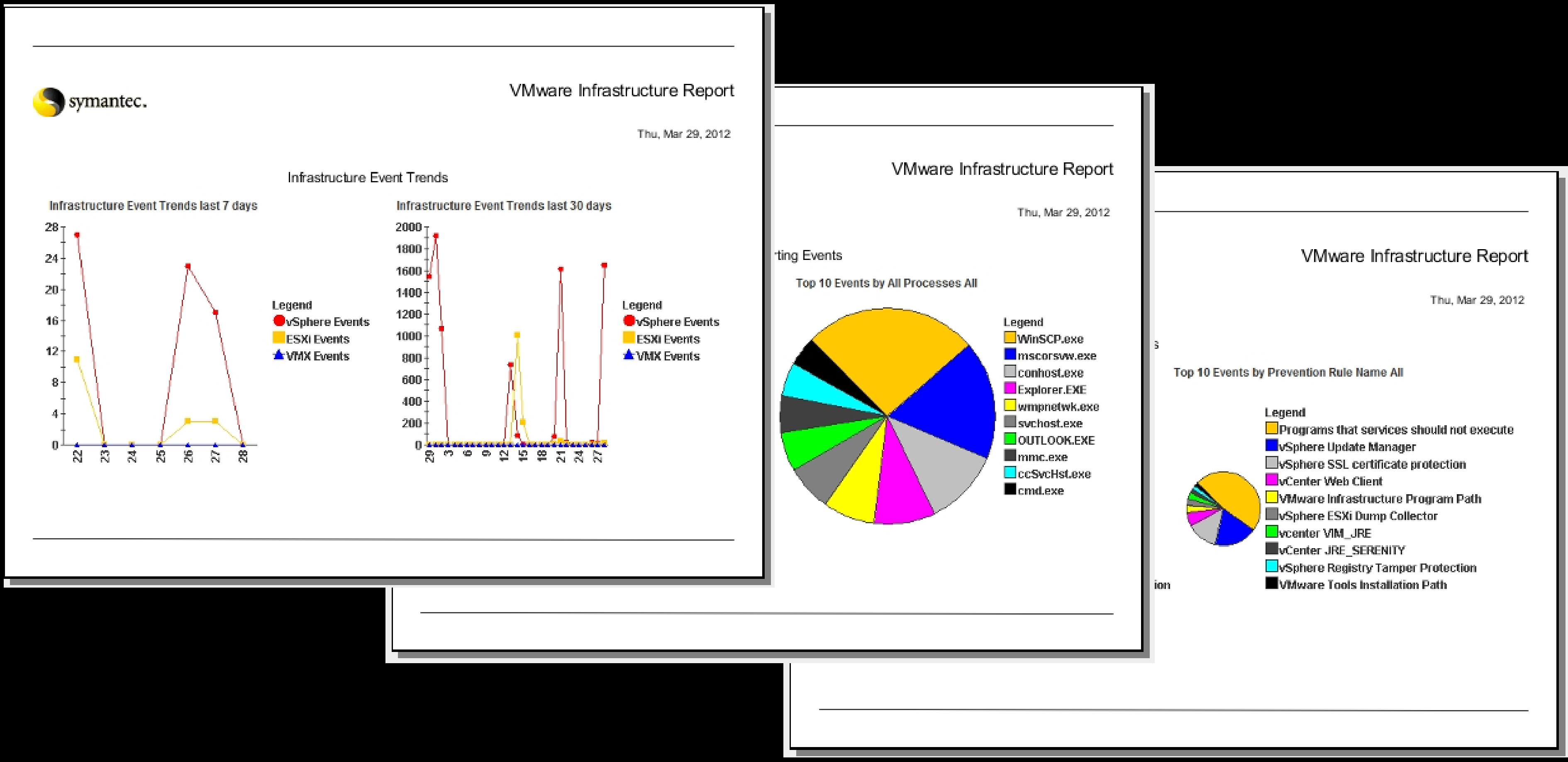




Agent Name	Failed Logins	Successful Logins	Root Logins	User Logins	DCUI Logins	SSH Logins	After Hours Logins
ESXi 192.168.1.225	67	558	500	58	127	415	12
sles11-64bit-sp1	0	1	1	0	0	1	0

Multi-Page VMware Infrastructure Report Example

- Trends and Top n Dashboard View



symantec.

VMware Infrastructure Report

Thu, Mar 29, 2012

Infrastructure Event Trends

VMware Infrastructure Report

Thu, Mar 29, 2012

rting Events

Top 10 Events by All Processes All

VMware Infrastructure Report

Thu, Mar 29, 2012

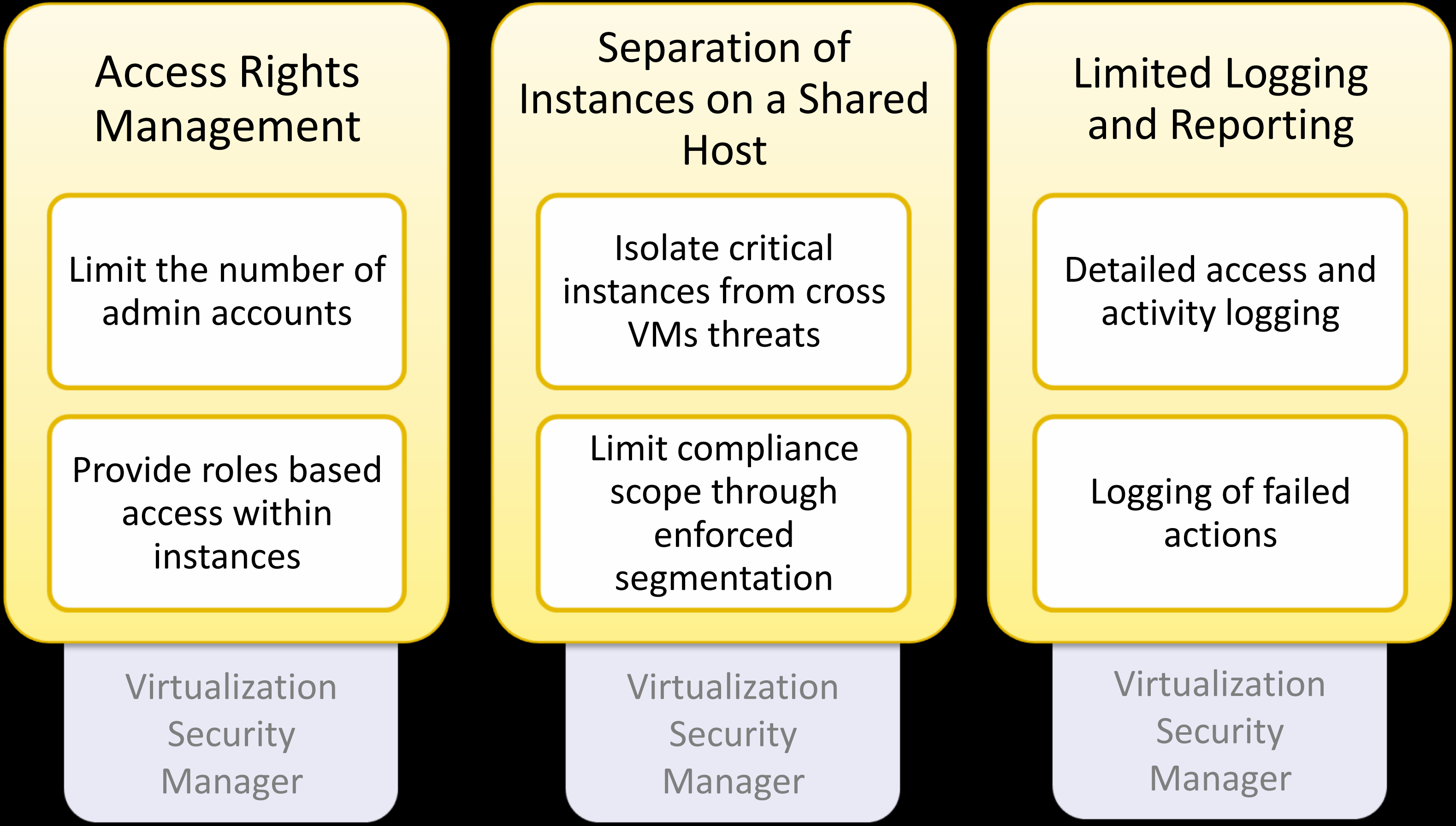
s

Top 10 Events by Prevention Rule Name All

Legend
■ Programs that services should not execute
■ vSphere Update Manager
■ vSphere SSL certificate protection
■ vCenter Web Client
■ VMware Infrastructure Program Path
■ vSphere ESXi Dump Collector
■ vcenter VIM_JRE
■ vCenter JRE_SERENITY
■ vSphere Registry Tamper Protection
■ VMware Tools Installation Path

ion

Control Compliance Suite Virtual Security Manager



Access Rights Management

- Limit the number of admin accounts
- Provide roles based access within instances

Virtualization Security Manager

Separation of Instances on a Shared Host

- Isolate critical instances from cross VMs threats
- Limit compliance scope through enforced segmentation

Virtualization Security Manager

Limited Logging and Reporting

- Detailed access and activity logging
- Logging of failed actions

Virtualization Security Manager

Critical Systems Protection + CCS VSM

CSP: Protect & Prevent

- Exploit prevention of both internal and external threats
- Targeted protection based on data and function
- Ensure availability of critical systems
- Configuration and access change monitoring

CCS VSM: Comply & Report

- Regulatory and security guidelines
- Configuration assessment & reporting
- Logical separation to limit compliance scope
- Detailed activity reporting
- Single view of risk across physical & virtual assets
- Configuration assessment

*CCS Virtualization Security Manager available by end 2012

Securing the Virtual Data Center: Key Takeaways

- Security Threats Continue To Evolve That Can Impact All Components That Are Part Of Your Virtual Data Center (e.g. Hosts/Hypervisors, Guests, Console/vCenter, etc.)
- Governmental, Regulatory And Manufacturer Virtual Infrastructure Guidelines Continue To Create Business Drivers For Securing All Elements Of A Virtual Data Center.
- Symantec Endpoint Protection v 12.1.2 Provides Features/Options To Secure Guest Virtual Machines For VMware And Other Virtual Guest Environments.
- Symantec Critical System Protection Provides Features/Options To Secure and Monitor All Components Of A Virtual Data Center.

Thank you!

Peter A. Starceski and James A. Kelly