



Symantec Endpoint Protection and Virtual Environments

Marcus Brownell, CISSP

Sr. Regional Product Manager, SEP

Agenda

1

Virtualization Features in Symantec 12.1

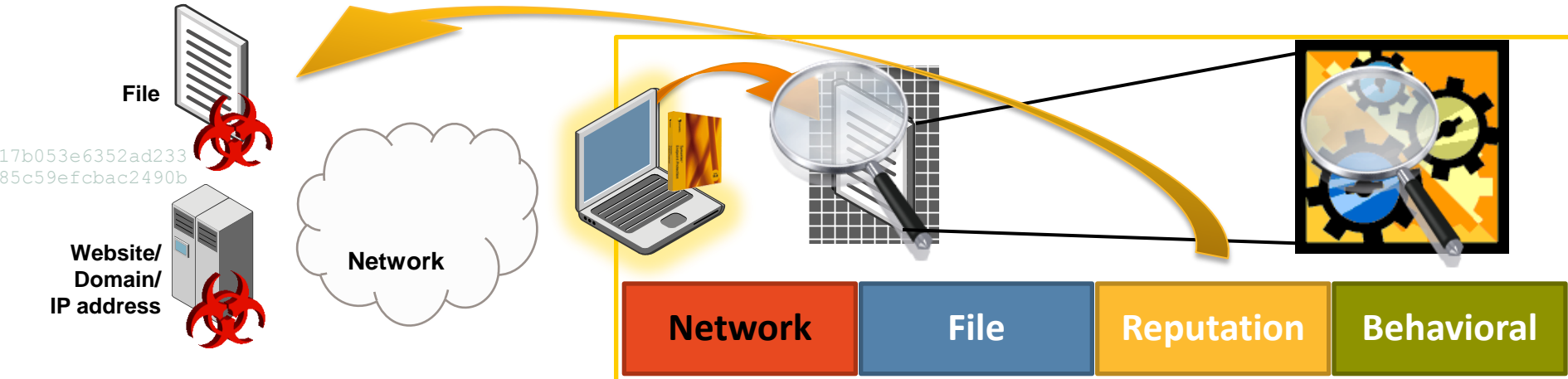
2

vShield Integration in SEP 12.1.2 (RU2)

Virtualization Features in Symantec 12.1

Symantec Protection Model

Defense in Depth



1 Network-based Protection

Stops malware as it travels over the network and tries to take up residence on a system

- Protocol aware IPS
- Browser Protection
- IPv6 Support

2 File-based Protection

Looks for and eradicates malware that has already taken up residence on a system

- Antivirus Engine
- Auto Protect
- Malheur Heuristics

3 Reputation-based Protection

Establishes information about entities e.g. websites, files, IP addresses to be used in effective security

- Insight
- Domain Reputation
- File Reputation
- Prevalence
- Age

4 Behavioral-based Protection

Looks at processes as they execute and uses malicious behaviors to indicate the presence of malware

- SONAR
- Behavioral Signatures

Optimised Performance in Virtual Environments

Without sacrificing protection...

- **Eliminate** scan activity with *Virtual Image Exception*
- **De-duplicate** remaining scan activity with *Shared Insight Cache*
- **Smooth out** remaining scan and update activity with *Resource Leveling*

Virtual Image
Exception

Shared
Insight Cache

Resource
Leveling

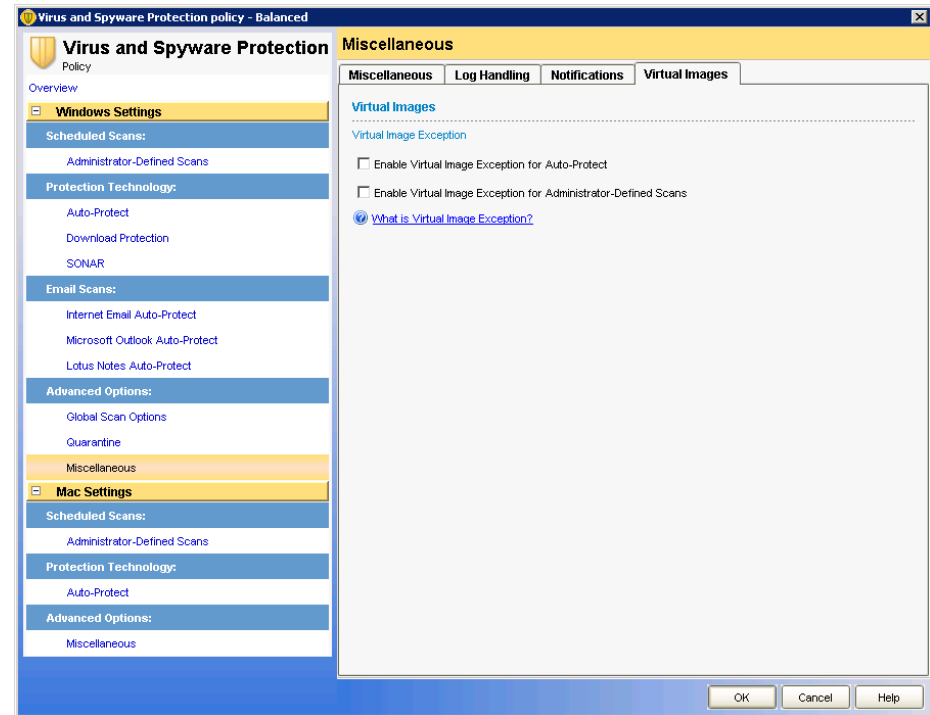
Key benefit: reduction in disk I/O

Virtualization Features: Virtual Image Exception

Virtual Image Exception (VIE):

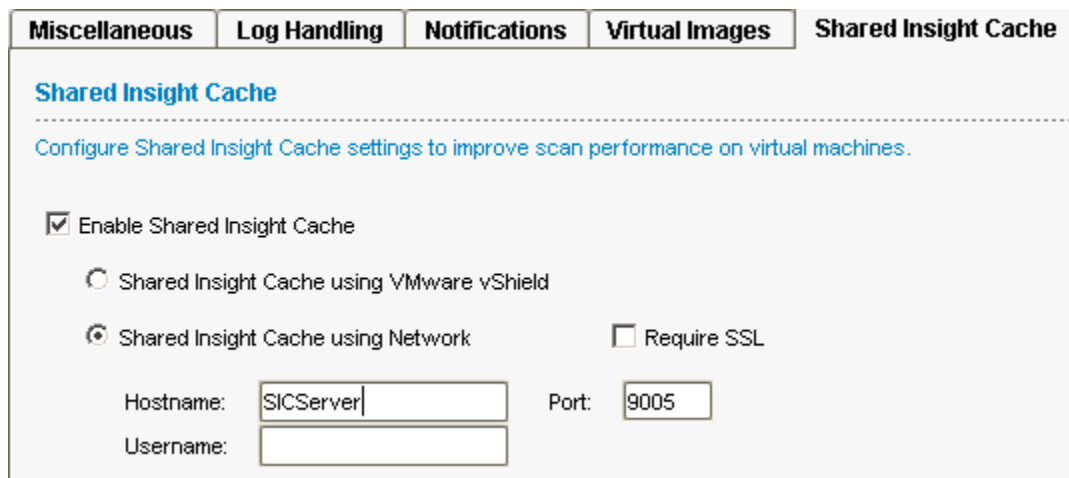
gives administrators the ability to exclude files in a base VM.

- Runs as a stand alone application in a guest VM (VMware, Citrix, of Hyper-V)
- Configurable in SEPM for Admins to enable/disable VIE exceptions for auto-protect and administrator defined scans.
- Ideal for excluding a Gold Image in linked clone and non-persistent VDI environments



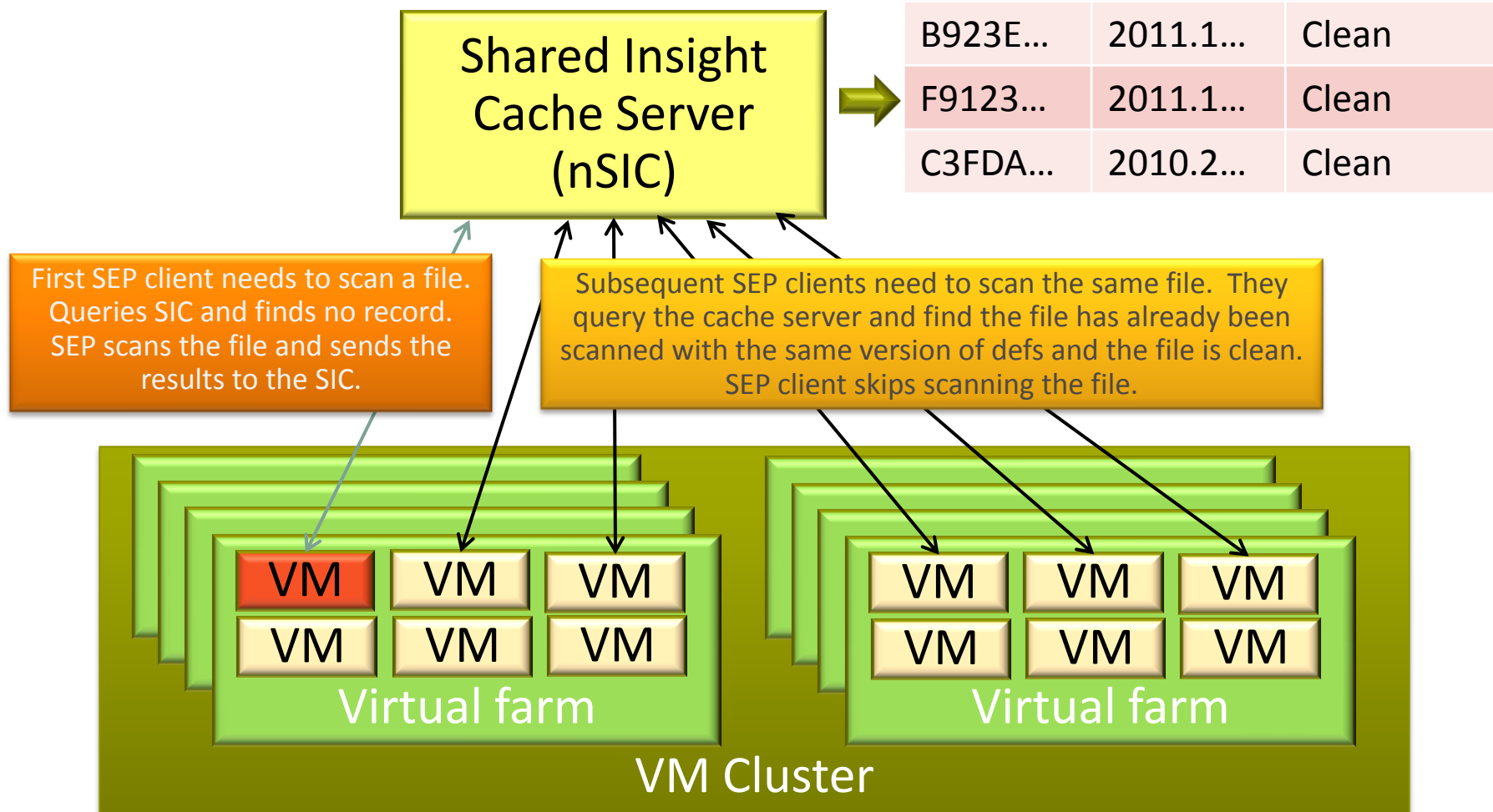
Shared Insight Cache (nSIC)

- Shared Insight Cache (nSIC) is a server application which caches hashes of known clean files to optimize **scheduled scan** performance.
- nSIC server keeps a record in memory of files determined to be clean by guests performing scans
- Communication between clients and nSIC uses http (or https)



The screenshot shows the 'Shared Insight Cache' configuration window. At the top, there are tabs: 'Miscellaneous', 'Log Handling', 'Notifications', 'Virtual Images', and 'Shared Insight Cache'. The 'Shared Insight Cache' tab is selected. Below the tabs, the title 'Shared Insight Cache' is displayed in blue. A subtitle reads: 'Configure Shared Insight Cache settings to improve scan performance on virtual machines.' The main configuration area includes a checked checkbox 'Enable Shared Insight Cache'. Below this, there are two radio button options: 'Shared Insight Cache using VMware vShield' (unselected) and 'Shared Insight Cache using Network' (selected). To the right of the 'Shared Insight Cache using Network' option is a checkbox 'Require SSL' which is unchecked. Below the radio buttons, there are input fields for 'Hostname' (containing 'SICServer'), 'Port' (containing '9005'), and 'Username' (empty).

Shared Insight Cache - High Level



nSIC Vs VIE: Reducing I/O

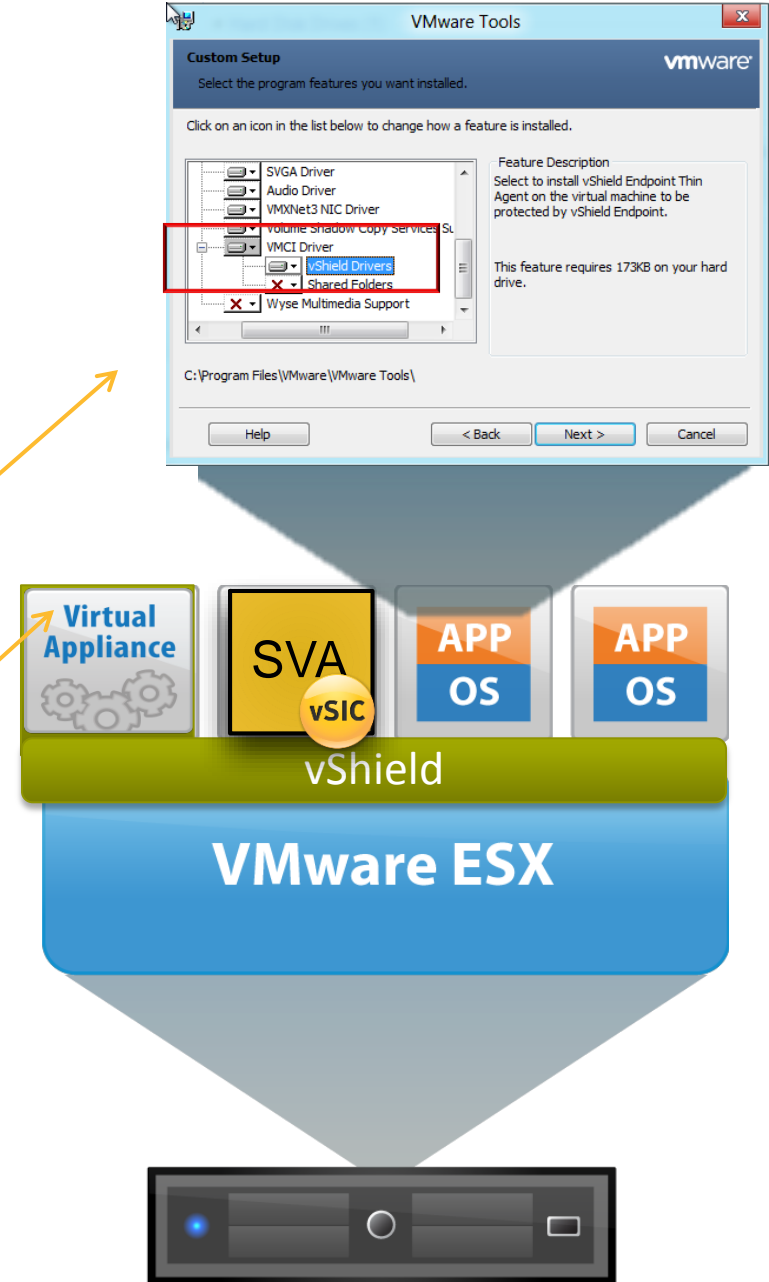
nSIC	VIE
Caches clean file hashes not yet trusted or white listed by another technology	Whitelist ALL files on a VM template
Applies to scheduled scans only	Applies to scheduled scan and real-time scans
Requires a SIC server on Windows with .Net 4.0	N/A
Platform agnostic (VMware, Citrix, Microsoft)	

New Virtualization Features in SEP 12.1.2 RU2 – vShield integration

vShield Endpoint components

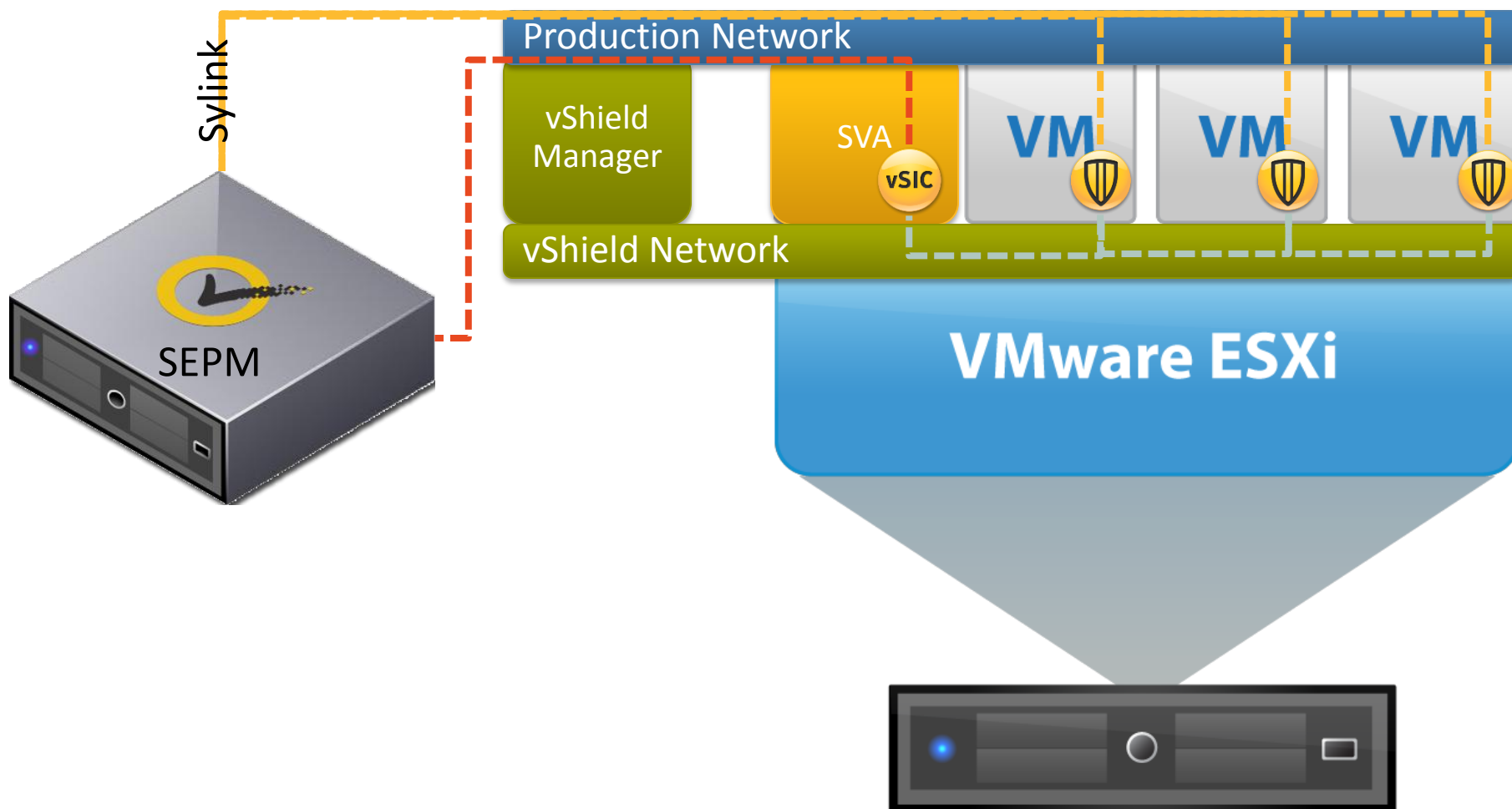
vShield Endpoint plugs directly into vCenter and consists of three components:

- 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 hypervisor layer



© VMware, Inc.

vSIC components overview



© VMware, Inc.

vShield enabled Shared Insight Cache (vSIC)

- vShield Endpoint enabled scan cache to optimize performance for scanning
- Moves the SEP 12.1 Shared Insight Cache into a Security Virtual Appliance
- Uses vShield as the communication channel between SEP and the cache
- Same performance benefit as SEP 12.1 nSIC

The screenshot shows the 'Shared Insight Cache' configuration page. It has tabs for 'Miscellaneous', 'Log Handling', 'Notifications', 'Virtual Images', and 'Shared Insight Cache'. The 'Shared Insight Cache' tab is active. Below the tabs, there is a section titled 'Shared Insight Cache' with a description: 'Configure Shared Insight Cache settings to improve scan performance on virtual machines.' There are two radio buttons: 'Enable Shared Insight Cache' (checked) and 'Shared Insight Cache using VMware vShield'. Under 'Enable Shared Insight Cache', there are two radio buttons: 'Shared Insight Cache using VMware vShield' (selected) and 'Shared Insight Cache using Network'. There is a checkbox for 'Require SSL'. Below these are input fields for 'Hostname', 'Username', and 'Port' (set to 9005). There is a 'Change Password...' button. At the bottom, there is a link 'What is Shared Insight Cache?'.

The screenshot shows the 'Security Virtual Appliance' status table. It has tabs for 'Summary', 'Logs', 'Command Status', 'Notifications', and 'Security Virtual Appliance'. The 'Security Virtual Appliance' tab is active. Below the tabs, there is a section titled 'Security Virtual Appliance' with links for 'Export' and 'Details'. Below this is a table with columns: Status, Hostname, Version, Clients, Last Checkin, and Last Restart.

Status▼	Hostname▼	Version▼	Clients▼	Last Checkin▼	Last Restart▼
Online	Symantec-SVA-esx11-symclab-local	93.1.128.128	0	18/01/2012 16:34:43	01/12/2011 14:55:17

If vSIC doesn't provide better performance than nSIC then what is the point?

- Auto-discovery
- No network traffic (physical)
- vMotion support for GVM's
- Monitoring SVA via SEPM
- Monitor vSIC protected Clients via SEPM



Q&A



Thank you!

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.