# Enabling VMware® vShield Endpoint™ in a VMware Horizon View™ Environment

VMware vShield Endpoint 5.x and Horizon View 5.x

WHITE PAPER

## Table of Contents

# Introduction

In the early days of virtual desktop infrastructure (VDI), it was important to run an antivirus (AV) software agent on every virtual machine because each and all were subject to the same threats as physical PCs. These agents performed a useful function, but they consumed CPU, memory, and storage resources to the point where AV scans could interfere with users' ability to work.

The performance problems caused by AV software are compounded in large implementations. When many people log in around the same time, waking up dormant virtual machines and triggering simultaneous antivirus signature updates, the resulting I/O problems—login and AV storms—become time-consuming and inconvenient, to say the least. Even with improved scheduling and other techniques designed to mitigate their effects, these I/O problems downgrade the typical user experience and precipitate expensive service calls. They are capable of bringing VDI performance to a grinding halt.

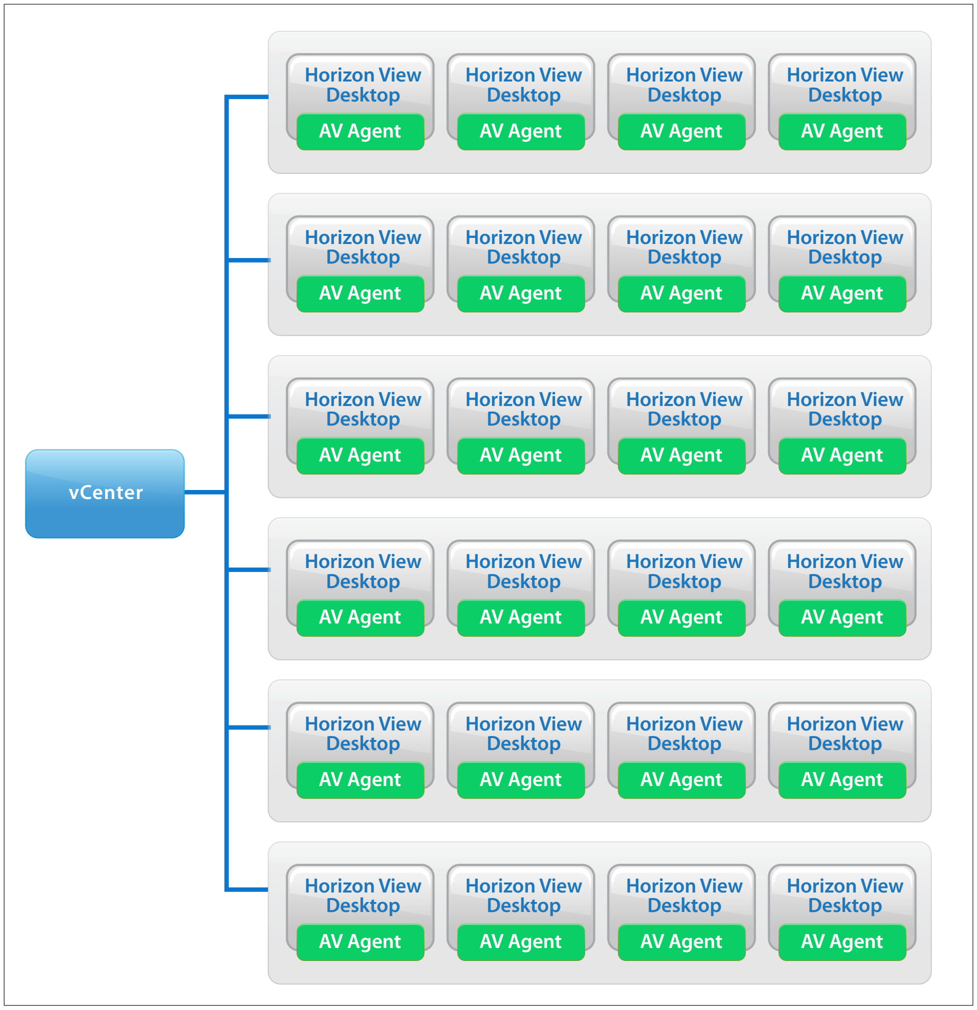

**Figure 1:** AV Agents on the Desktop Consume Resources

VMware® vShield Endpoint™ addresses the problems of antivirus scanning in a large-scale virtual desktop implementation with a better solution: It consolidates and offloads all antivirus and associated operations into a centralized security virtual appliance (SVA), supplied by a VMware partner. The SVA runs and manages antivirus software as a dedicated virtual machine on the hypervisor, with very small desktop drivers. This replaces dozens or hundreds or thousands of large AV agents on individual virtual desktops.

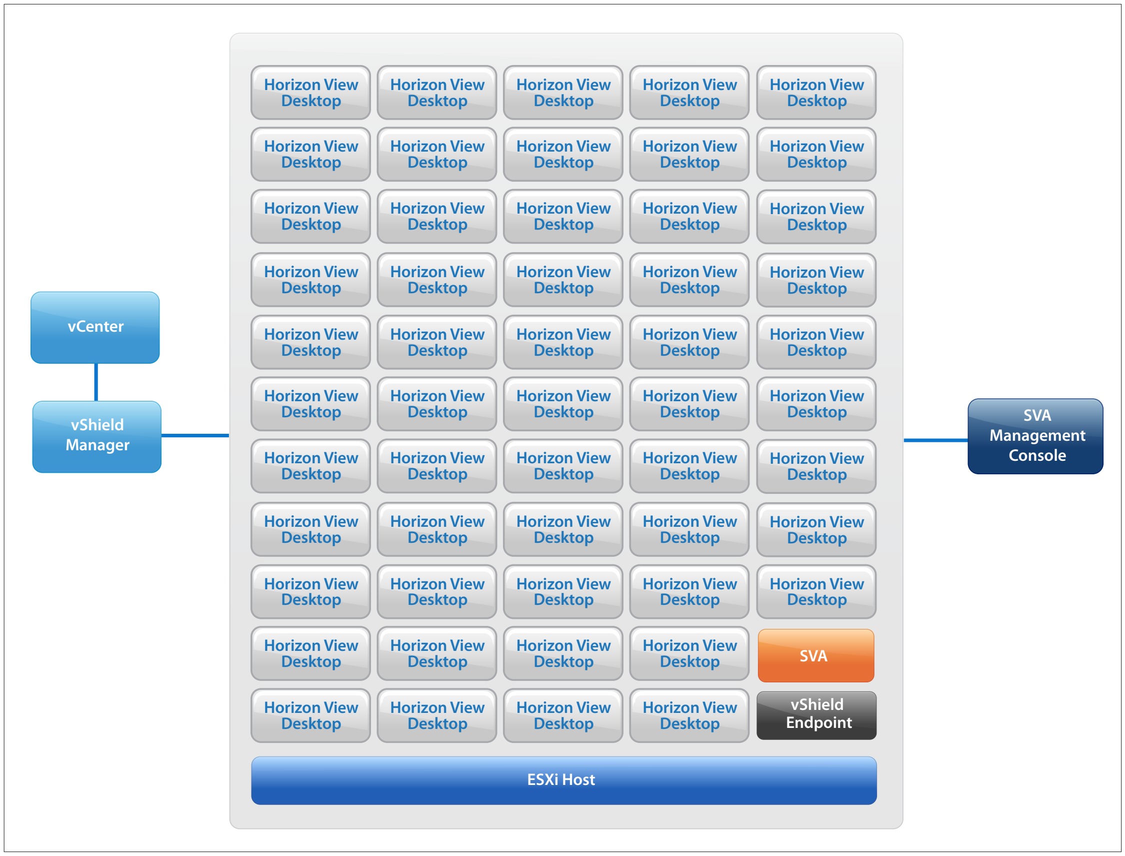

**Figure 2:** vShield Endpoint: One SVA per Host Instead of One AV Agent per Desktop

VMware vShield Endpoint is included in VMware vSphere® 5.1 and later as well as in VMware Horizon View™ 5.3. The vShield Endpoint API provides the hooks that enable the SVA to run on the hypervisor and pull information from the individual desktops.

The SVA remains on when desktops are shut down or recomposed, so that desktops receive the latest protection as soon as they are powered on. The SVA also logs AV tasks to satisfy audit requirements.

Although AV agents provide granularity—such as registry and buffer overflow protection, process monitoring, and vendor-specific kernel hooking—at the level of the individual virtual desktop, they need to be managed individually. Local agent management is conducive to additional problems, such as duplicate clients and orphaned clients. It requires a lot of effort. Removing traditional AV agents from virtual desktops frees up memory and storage and reduces peak IOPS consumption, and multiple levels of caching help to reduce stress on system resources. These factors improve resource utilization and desktop performance.

From a system administrator's point of view, it is much easier to monitor and defend a single enforcement point than a multiplicity of individual desktops. Also, the ability to add or remove partner SVAs without having to reconfigure desktop drivers is convenient as well as useful for a defense-in-depth strategy.

So, agentless SVAs effectively remove the I/O-storm problem and improve the overall VDI user experience. They help to reduce operating expenses by centralizing maintenance and management functions and by pre-empting the need for service calls. They replace space- and memory-hogging AV agents and improve consolidation ratios. These are important business benefits, but they are not the only considerations.

## Visibility

With previous generations of AV software, it was often impossible to view or monitor all desktops in a given implementation. For example, in a typical Horizon View implementation of 150 desktops per ESXi host, some desktops would be configured with AV agents. These desktops would show up in a management console, while other desktops might not be visible at all. These unauthorized, rogue desktops might result, for instance, from an administrator's choice not to deploy agents on all virtual machines or pools, from failover or load-balancing events, or, less commonly, from users installing unauthorized virtual machines or disabling AV scans to improve performance.

In addition, malware can target AV agents and turn them off. Users, who may patch on a weekly or monthly or random basis, can unwittingly provide exposure to rootkits and memory exploits. Finally, allowing both production and test networks to run on the same host or moving virtual machines to different hosts can also create blind spots.

These problems are all effects or consequences of agent-based AV solutions.

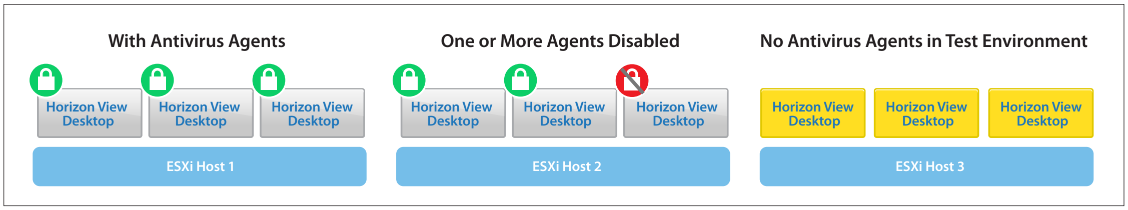

**Figure 3:** Agent-Based Solutions Do Not Provide 100 Percent Visibility

Security virtual appliances from VMware partners, however, pull data from the hypervisor instead of from individual desktop agents. This gives the administrator full visibility into the virtual desktop environment.

## Vigilance

Another threat to security has as much to do with the attitude of the administrator as with scanning or network topology. Overconfidence can lead an administrator to be complacent, to "rest assured." Putting complete faith in a firewall, an authentication procedure, or an existing agent-based AV solution, for example, while leaving perhaps a few individual desktops or pools unprotected, provides a convenient attack surface for intruders. With an agentless SVA solution and proper configuration of VMware Tools™, all desktops become visible to the administrator, who can also set SVA policies to scan all relevant files. These are huge improvements, but the administrator still needs to maintain a vigilant attitude toward an evolving threat landscape.

# Architecture

Instead of installing the antivirus and antimalware software on each virtual desktop, you install a security virtual appliance on the ESXi host. Each desktop to be protected requires only a vShield Endpoint driver, which is bundled with the custom installation of VMware Tools for the virtual machine. The driver, which has a tiny footprint compared with an AV agent, communicates with the SVA to notify it of file events on the desktop and to enforce remediation.

For more information on this topic, see *Install VMware Tools on the Guest Virtual Machine* in the vShield Installation and Upgrade Guide.

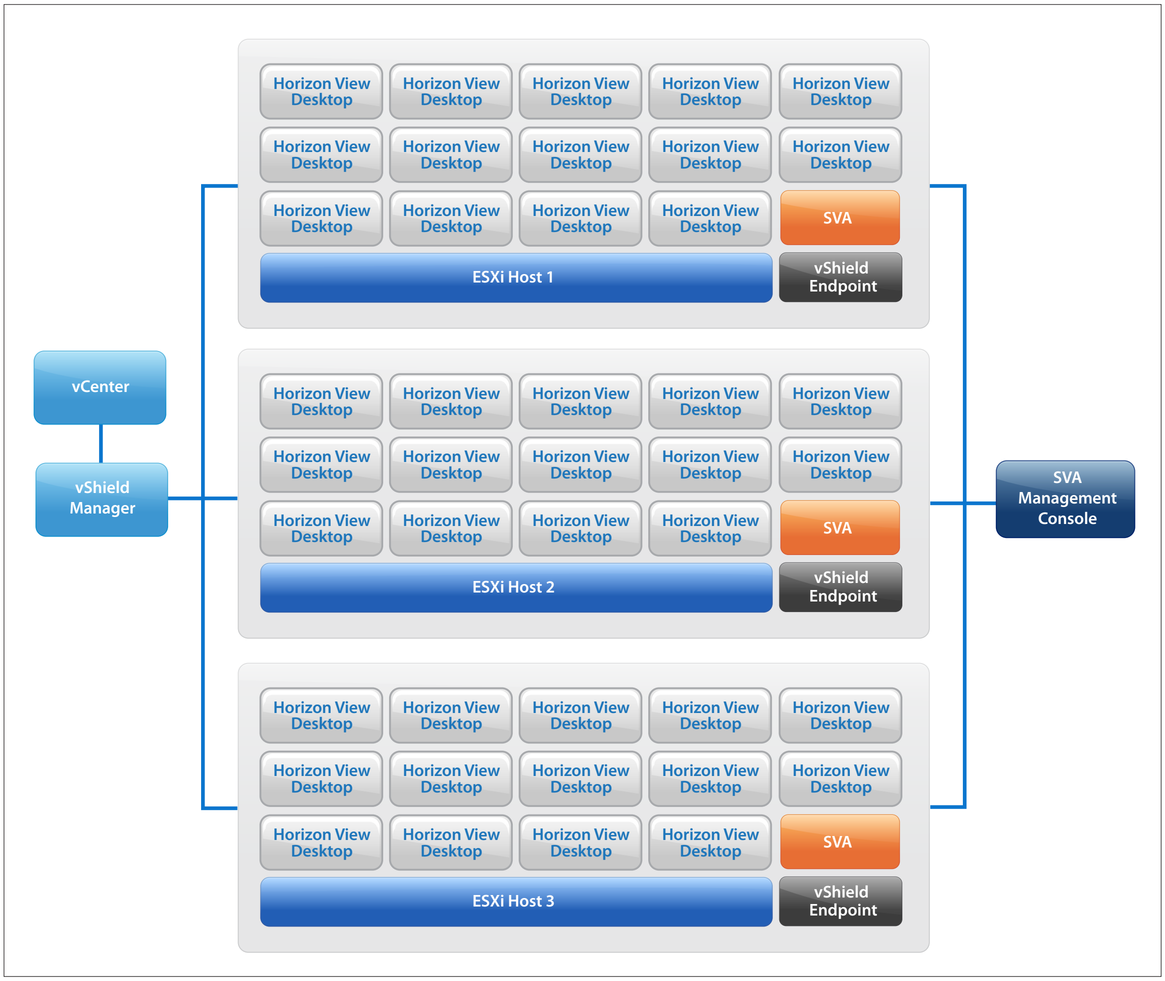

**Figure 4:** vShield Endpoint and an SVA Installed on Each ESXi Host in a Cluster

When viruses or malware are detected, the SVA manages the remedial action to the affected virtual machines, based on the administrator's settings. The exact policy settings and procedures, which vary somewhat for each SVA, are described in the partner documentation (see Table 2).

# Partners

The following VMware partners have integrated their antivirus solutions with vShield Endpoint for Horizon View:

- Bitdefender
- Kaspersky
- McAfee
- Sourcefire
- Symantec
- Trend Micro

SVAs from these partners require licenses. For documentation and download links, see Table 2. Knowledge Base articles and other items that may be of interest are listed under Additional Resources.

To keep apprised of additional VMware partners integrating antivirus solutions with vShield Endpoint for Horizon View, see the latest version of VMware Integrated Partner Solutions for Networking and Security.

# Packaging and Licensing

Horizon View is available as a bundle that includes vSphere Desktop and VMware vCenter™ Desktop, as an add-on to an existing vSphere infrastructure, or as part of the VMware Horizon™ Suite. All Horizon View options include vShield Endpoint.

If purchased as part of the Horizon Suite, Horizon View inherits the licensing of the Suite, which can be by concurrent user or by named user. If purchased outside of the Horizon Suite, Horizon View is licensed by concurrent connection. VMware vShield Endpoint for Horizon View inherits the licensing of Horizon View. In most cases, adding vShield Endpoint to a Horizon View implementation requires no extra licensing except for the partner SVA.

For a fuller description of components and licensing, see the following resources:

- VMware Horizon Family Pricing, Packaging, and Licensing white paper
- Purchasing tab of the Horizon View product page
- VMware Horizon View Product Evaluation Center

For more information on VMware security products, see the VMware vCloud® Suite and vCloud Networking and Security product pages.

# Installation and Configuration

This document does not repeat the detailed installation and configuration instructions presented in the VMware and partner documentation. The instructions vary somewhat for different SVA vendors and may vary considerably based on site architecture. However, the following diagram outlines the major steps needed to set up a security virtual appliance in a Horizon View environment:

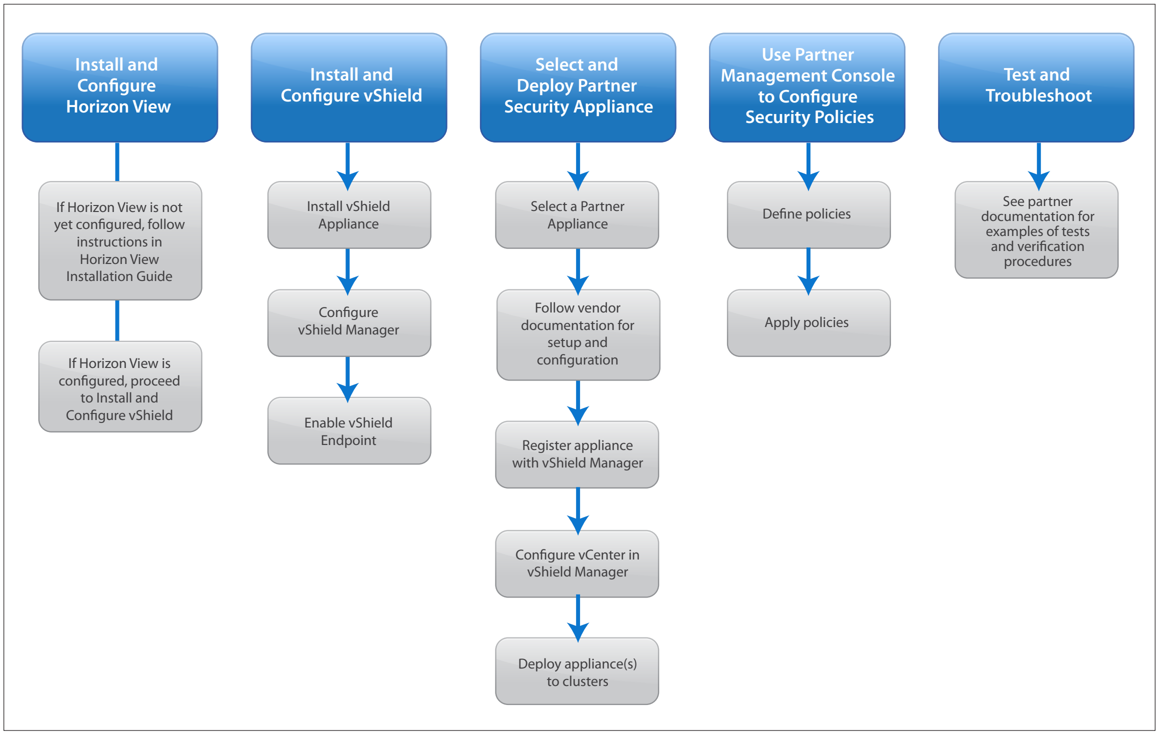
Install and Configure Horizon View
If Horizon View is not yet configured, follow instructions in Horizon View Installation Guide
If Horizon View is configured, proceed to Install and Configure vShield
Install and Configure vShield
Install vShield Appliance
Configure vShield Manager
Enable vShield Endpoint
Select and Deploy Partner Security Appliance
Select a Partner Appliance
Follow vendor documentation for setup and configuration
Register appliance with vShield Manager
Configure vCenter in vShield Manager
Deploy appliance(s) to clusters
Use Partner Management Console to Configure Security Policies
Define policies
Apply policies
Test and Troubleshoot
See partner documentation for examples of tests and verification procedures

**Figure 5:** Major Installation and Configuration Steps

## Install and Configure Horizon View

In most cases, Horizon View is already installed. If not, follow the instructions in VMware Horizon View Installation.

**Note:** The installation procedures for Horizon View 5.2 are also valid for Horizon View 5.3, but some important changes are logged in the Release Notes.

The following table summarizes compatibility of various versions of vShield Endpoint with different Horizon View versions. For the most up-to-date information, see the VMware Product Interoperability Matrixes page.

| VMWARE PRODUCT | HORIZON VIEW 5.3 | HORIZON VIEW 5.2 | VMWARE VIEW™ 5.1.3 | VMWARE VIEW 5.1.2 | VMWARE VIEW 5.1.1 | VMWARE VIEW 5.1 | VMWARE VIEW 5.0.1 | VMWARE VIEW 5.0 |
|---|---|---|---|---|---|---|---|---|
| VSHIELD ENDPOINT 5.5 | ✓ | | | | | | | |
| VSHIELD ENDPOINT 5.1.2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| VSHIELD ENDPOINT 5.1.1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| VSHIELD ENDPOINT 5.1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| VSHIELD ENDPOINT 5.0.2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| VSHIELD ENDPOINT 5.0.1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| VSHIELD ENDPOINT 5.0 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**Table 1:** Compatibility Matrix for Horizon View and vShield Endpoint Versions

## Install and Configure vShield

After the Horizon View implementation is set up and provisioned, install and configure the vShield components you need. VMware vShield Manager™ and vShield Endpoint are required for this solution. The other components are valuable but optional, especially if other products or solutions, such as firewalls, are already in place. In any case, defense in depth is always desirable.

Follow the instructions in the vShield Installation and Upgrade Guide. This manual contains instructions for vShield Manager, VMware vShield Edge™, and vShield Endpoint.  See especially Chapter 3, *Installing the vShield Manager*, and Chapter 4, *Installing vShield Edge*, *vShield App, vShield Endpoint*, *and vShield Data Security.* For more in-depth information, see the vShield Administration Guide. For earlier versions of Horizon View and vShield Endpoint listed in Table 1, find the correct versions of the product documentation by searching the VMware Support portal.

## Select and Deploy a Partner Security Appliance

VMware recommends the following third-party appliances, which have all been designed to work with the vShield Endpoint API. You can download, install, and configure more than one partner SVA, for instance, for evaluation. The typical evaluation period is 60 days, after which a license is required.

| PARTNER PRODUCT | DOWNLOAD | DOCUMENTATION |
|---|---|---|
| Bitdefender Gravity Zone Security for Virtualized Environments | http://enterprise.bitdefender.com/solutions/gravityzone/virtualization-security.html | http://download.bitdefender.com/resources/media/materials/business/en/datasheet-sve.pdf<br>http://download.bitdefender.com/SMB/SVE/SVE-1.2/Multi-Platform/Bitdefender_SVE_MultiPlatform_AdminsGuide_enUS.pdf |
| Kaspersky Security for Virtualization | http://support.kaspersky.com/ksv2#downloads<br>http://www.kaspersky.com/product-updates/virtualization-security | http://www.kaspersky.com/documentation/virtualization<br>http://docs.kaspersky-labs.com/english/ksv2.0mr1_adminguide_en.pdf |
| McAfee MOVE AntiVirus Agentless | http://www.mcafee.com/apps/downloads/free-evaluations/default.aspx?region=us&pid=16650 | http://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24625/en_US/MOVE_AV_Agentless_300_Product_Guide_final.pdf |
| Sourcefire Next-Generation Intrusion Prevention System (NGIPS) and FireAMP Virtual | http://www.sourcefire.com/purchase-products | Login required for access to official documentation but the following is commercially available:<br>https://info.sourcefire.com/NGIPSforDummies.html |
| Symantec Endpoint Protection Security Virtual Appliance | http://buy.symantec.com/estore/categoryDetailPage/productCode/SEP-EXP-LEM_V12.1_12MO_Px/skuType/Product | http://www.symantec.com/business/support/index?page=content&id=HOWTO81110#v730697 31 |
| Trend Micro Deep Security Antivirus and Deep Security Integrity Monitoring | http://forms.trendmicro.com/trials/ downloads/?dom=us&productID=123 | http://files.trendmicro.com/documentation/guides/deep_security/Deep_Security_9_SP1_Install_Guide_EN.pdf |

**Table 2:** Partner Security Virtual Appliances

After you download your choice of partner SVA listed in Table 2, follow the instructions in the partner documentation, register the SVA with vShield Manager, and register vShield Manager with vCenter. Then you can log in to vCenter with the Web Client and deploy an appliance (or appliances) to clusters.

The partner documentation describes how to perform setup and configuration tasks, such as defining security groups, defining and applying policies, and defining responses.

# Summary of Best Practices

Best practices have been developed over time and documented elsewhere. See, for example, Antivirus Best Practices for VMware Horizon View 5.x. In addition, the VMware partners suggest best practices in their own documentation.

## Protect the Whole Infrastructure

The vShield Endpoint solutions from VMware partners provide complete protection for virtual machines running in a production Horizon View environment. For storage and other servers connected to the virtual desktop infrastructure, VMware recommends a complementary solution from a VMware antivirus software partner.

## Protect All Desktops

All desktops need antivirus protection because infections can corrupt files even within a single desktop session, and active sessions are always vulnerable to some extent. Nonpersistent desktops are easier to remediate in the event of a virus outbreak or security breach; with proper configuration of Refresh on logout or reboot, a nonpersistent desktop can resume its original state.

Install VMware Tools before using VMware View Composer™ to create a parent virtual machine for linked clones.

## Do Not Run AV Software Agents on Individual Virtual Desktops

Use vShield Endpoint and a partner SVA instead of running AV agents on individual virtual desktops. With the vShield Endpoint solution, you update the antivirus software only in the virtual appliance for each host, not in each desktop.

## Keep Virtualization and Other Software Up-To-Date

As with any software, desktop virtualization software on guest or local systems may contain security vulnerabilities, so it is important to keep all virtualization software and applications updated with appropriate security patches. Always upgrade to the latest patch or update of the vShield Endpoint drivers included in VMware Tools.

## Tune Partner SVA Settings

Adjust the SVA settings based on the number of virtual machines and workloads, and make sure that permissions are set correctly. Refer to the individual partner documentation (see Table 2) for details.

# Additional Resources

- Antivirus Best Practices for VMware Horizon View 5.x
- Bitdefender Enterprise Security Solutions
- Deep Security Comprehensive Server Security Platform
- How to deploy the [Bitdefender] Security Virtual Appliance in your VMware vSphere environment
- How to install Bitdefender Security Console Appliance in your VMware vSphere environment
- How to install Security for Virtualized Environments
- Kaspersky Security for Virtualization 2.0
- McAfee Move 3.0 and vShield – Deployment and Tips
- McAfee Product Documentation page
- Symantec Endpoint Protection Integration with VMware Horizon View
- Symantec Virtualization Solutions
- The Technology Foundations of VMware vShield
- Toward Guest OS Writable Virtual Machine Introspection
- Trend Micro Deep Security 9.0 SP1 Installation Guide
- Trend Micro End User Licensing Agreements and Terms
- Trend Micro Deep Security 9 data sheet
- Trend Micro Deep Security white paper
- VMware KB Article 2045513, Using VMware ThinApp packages with non-persistent Floating Pools in VMware Horizon View
- VMware KB Article 340, Overview of VMware Tools
- VMware KB Article 2020338, Support for McAfee MOVE AntiVirus [Agentless] 2.5 with VMware vShield Endpoint 5.0
- VMware KB Article 2036875, Downloading and enabling vShield Endpoint on supported vSphere platforms
- VMware KB Article 2042015, Using Sourcefire FireAMP Virtual with VMware vShield Manager 5
- VMware Horizon Family: Pricing, Packaging, and Licensing
- VMware Horizon View 5.3: Pricing, Licensing and Support
- VMware Horizon View product page
- VMware Integrated Partner Solutions for Networking and Security
- VMware Licensing Help Center
- VMware Product Interoperability Matrixes
- VMware vCloud Networking and Security Documentation
- VMware vShield Endpoint data sheet
- VMware vShield Endpoint product page

# Glossary

blind spot

Agent-based AV solutions can allow unmonitored communication across virtual machines on the same host, creating blind spots. Hypervisor-based solutions address this problem.

consolidation ratio

The number of virtual machines that can be hosted on a given hypervisor. For instance, a vShield Endpoint driver has a memory footprint typically around 250MB smaller than an AV agent. The extra memory freed up by an agentless solution dramatically increases the number of virtual machines that can be supported per host.

defense in depth

The use of multiple layers of security controls to provide redundant protection in case one aspect or technique is compromised.

introspection

Virtual machine introspection pulls the guest OS state into the hypervisor and performs external monitoring of its runtime state. This gives an administrator the ability to see, among other things, file activity at the hypervisor level.

rogue desktop

A virtual machine that is installed without proper authorization is usually considered to be a rogue. A vShield Endpoint solution cannot prevent rogue desktops from occurring, but it does make them visible to the administrator through the SVA.

rootkit

Malware designed to get privileged access to a computer, whether physical or virtual. The solution proposed here cannot prevent rootkit attacks, but it can mitigate their effectiveness and endurance.

## About the Author

Gary Sloane is a consultant for VMware End-User Computing. He has been writing about VDI and security-related topics since 2007.

## Acknowledgements

The following people offered technical advice, encouragement, and reviews:

Kofi Ahulu, Systems Engineer in VMware End-User Computing

Kevin Berger, Information Security Analyst in VMware Corporate IT

Jeremiah Cornelius, Alliances Partner Architect in the VMware Global Strategic Alliances

Tina de Benedictis, Senior Technical Marketing Manager in VMware End-User Computing

Azeem Feroz, Senior R&D Manager in VMware Networking and Security Product Development

Amit Patil, Senior R&D Manager in VMware Networking and Security Product Development

Steve Sledzieski, Member of the Technical Staff in VMware Cloud Security Product Development

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com