



Antivirus Practices for VMware® View™ 5

BEST PRACTICES

Table of Contents

Introduction	3
Problems with Standard Antivirus Protection.....	3
The VMware Solution to Antivirus Protection.....	4
VMware vShield Endpoint Architecture in Brief.....	4
Antivirus Protection for the Entire Virtual Desktop Infrastructure	5
Antivirus Protection for VMware View Virtual Machines.....	6
Install Only the Core Virus Scanner.....	6
With vShield Endpoint.....	6
Without vShield Endpoint.....	6
Use Random or Staggered Scan Scheduling.....	6
With vShield Endpoint.....	7
Without vShield Endpoint.....	7
Update Virtualization and Other Software.....	7
With vShield Endpoint.....	7
Without vShield Endpoint.....	7
Configure Virus Scanner Exclusion Lists	8
Resolve Virus Scanner Deployment Issues in Linked Clones.....	8
Potential Issue 1: Unique SIDs for Virus Scanning	8
Required Workaround for Some Legacy Antivirus Software	9
Potential Issue 2: Reacting to Virus Infections Depending on Whether the Master Image or a Cloned Desktop Is Infected.....	10
Protect the View Desktop During ThinApp Package Use.....	10
Background Information on ThinApp Isolation Modes and the Role of the Sandbox.....	10
Recommendations for View Desktop Scanning When Using ThinApp Packages ...	12
Antivirus Protection for the View Security Server	13
Antivirus Protection for Storage in the View Environment.....	13
Scanning Mapped Drives or Shared Folders	13
Protecting User Data Disks (UDD)	13
Protection Strategies for Storage Related to ThinApp Packages	13
Protection of the ThinApp Executable and Primary Data Container During Package Creation	14
VMware Partnership with eEye Retina.....	15
Protecting the ThinApp Repository in a VMware View Environment	15
Outbound.....	15
Inbound	16
Scanning the ThinApp Application Sandbox	16
Protecting External Drives Involved with the ThinApp Application.....	16
Scanning the Persona Repository of User Profile Files.....	17
Conclusion	17
About the Authors and Contributors	17

Introduction

Desktop virtualization is a transformative platform technology that can deliver cost-effective, manageable network and desktop access to workers with diverse computing needs. However, with security threats becoming more sophisticated, more frequent, more targeted, and potentially more profitable to those who seek to inflict damage, IT administrators must increase their vigilance and find security solutions for the virtual desktop environment. Solutions such as log analysis, host-based intrusion-prevention system (HIPS) technology, firewalls, and antivirus software need to evolve and adapt to desktop virtualization.

This paper focuses on the best practices for protection against viruses in the VMware View™ 5 virtual desktop environment. Antivirus software is one of the largest segments in today's computer security market. Nearly every enterprise deploys antivirus software on every desktop. As services such as security, mobility, access control, and line-of-business applications are all rolled up into the datacenter or cloud, antivirus practices need to be rolled up as well.

Problems with Standard Antivirus Protection

The typical top-down virus scanning model involves desktop antivirus scanning and signature file updates, with access to an auto-update server. During these operations, it is not uncommon for system resource usage to spike or become overly committed. Performance in the desktop environment is severely impacted by these “antivirus storms.”

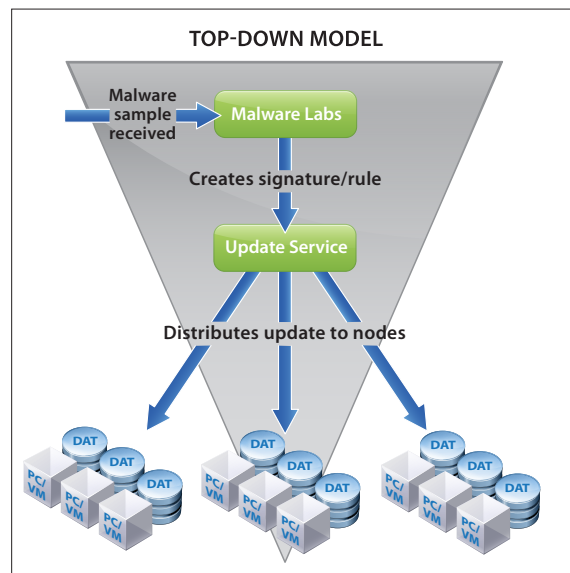


Figure 1: Top-Down Model

With VMware View, you can examine the system bottleneck during an antivirus storm, when virus scanners are running at the same time as users are accessing virtual desktops. Antivirus storms can cause 100% saturation in shared compute (CPU) and SAN/NAS (storage I/O) environments. In addition, the memory footprint is significant when antivirus software is installed on each virtual machine. Traditional antivirus agents are resource-intensive and not optimized for highly utilized, efficient clouds.

Antivirus storms can defeat the cost-cutting achievements of a virtual desktop implementation. To answer the need to eliminate antivirus storms and to maximize performance and consolidation ratios in the virtual desktop environment, VMware offers a solution.

The VMware Solution to Antivirus Protection

VMware vShield™ Endpoint is the solution to the problems inherent in antivirus scanning in a large-scale virtual desktop implementation. In a VMware View environment, vShield Endpoint consolidates and offloads two antivirus operations into one centralized virtual appliance:

- Checking for virus signature update files
- Antivirus scanning

VMware has partnered with antivirus software vendors to provide this bundled solution to antivirus problems in the VDI environment. VMware partners supply a dedicated, secure virtual appliance. This virtual appliance integrates with vShield Endpoint APIs to protect VMware virtual desktops against viruses and other malware. Instead of installing antivirus agents on each virtual desktop, you connect one virtual appliance to each virtual machine host.

The vShield Endpoint product offers the following benefits for large-scale antivirus protection:

- Enables VMware partners to eliminate antivirus storms that affect performance of virtual machines in a virtual desktop environment. Signature file updates and antivirus scanning are isolated and offloaded to a virtual appliance.
- Improves consolidation ratios of virtual desktops by offloading antivirus functions to a separate security virtual machine. The enterprise antivirus engine and the signature file are located on the virtual appliance, instead of on each virtual machine. This frees up virtual desktop system resources.
- Agentless solution: Instead of an antivirus agent installed on each desktop to be protected, vShield Endpoint utilizes a small-footprint driver on each desktop. This driver is part of VMware Tools, and no additional provisioning is required. The antivirus scanner and virus signatures are installed only in the virtual appliance. This saves space on each desktop.
- Ease of maintenance of the desktops to be protected: Any changes to the antivirus software are configured only in the virtual appliance, not in each desktop. You can change the configurations for the antivirus solution in the virtual appliance without reconfiguring the desktop driver. You do not have the responsibility of maintaining, patching, and updating antivirus agents on all of the desktops; you direct all changes to the virtual appliance instead.
- Simple addition or subtraction of AV vendors: You can add or change partner solutions by adding or removing the virtual appliances. You do not need to reconfigure the desktop driver.
- Satisfies audit requirements by providing detailed logging of antivirus (AV) tasks.

VMware vShield Endpoint Architecture in Brief

Instead of installing the antivirus and antimalware software on each virtual machine, you install it only on the single security virtual machine assigned to the vSphere host. Each virtual machine to be protected requires only a small-footprint vShield Endpoint driver.

VMware vShield Endpoint plugs into vSphere and protects virtual machines against viruses. Administrators can centrally manage VMware vShield Endpoint through the included vShield Manager console, which integrates with VMware vCenter™ Server for unified security management in the virtual datacenter.

Isolating the antivirus scanning engine on the virtual appliance makes it easier to protect the scanning engine than if it were placed on every virtual machine. In addition, detailed logging of activity from the antivirus or antimalware service satisfies auditor compliance requirements.

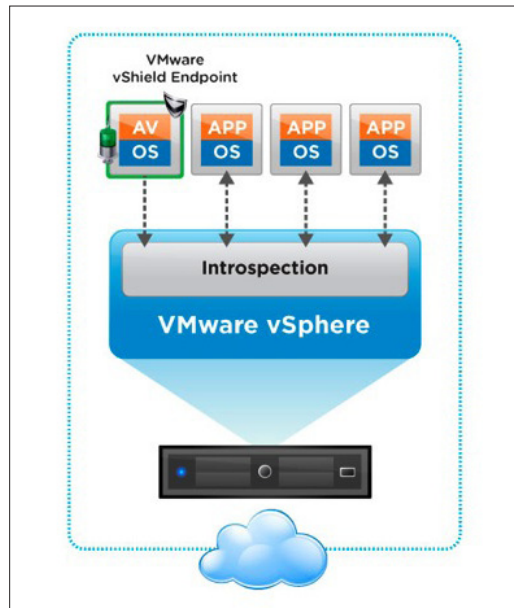


Figure 2: vShield Endpoint

When viruses or malware are detected, the partner antivirus solution manages the remedial action to the affected virtual machines, based on the administrator's specifications.

Antivirus Protection for the Entire Virtual Desktop Infrastructure

In a VMware View environment, you have three focal points for antivirus protection:

- Virtual machines
- View Security Server
- Storage

The vShield Endpoint solution from VMware partners provides complete protection for virtual machines running in a production VMware View environment. For storage and other servers connected to the virtual desktop infrastructure, the complementary solution is VMware partner antivirus software. The following sections provide best practices for managing antivirus protection for these three components—the virtual machines, the Security Server, and storage.

Antivirus Protection for VMware View Virtual Machines

For protection of virtual machines in a View virtual desktop environment, VMware recommends the vShield Endpoint solution offered by VMware partners. VMware partners who have integrated their antivirus solutions with vShield Endpoint are:

- [Trend Micro](#)
- Bitdefender (See: [Bitdefender Datasheet](#) and [Bitdefender: Security for Virtualized Environments](#))

VMware has also announced the following additional partners who are integrating their antivirus protection with vShield Endpoint for View:

- [Kaspersky Security for Virtualization](#)
- [McAfee MOVE AV 2.5](#)
- [Symantec](#)

To keep apprised of additional VMware partners integrating their antivirus solutions with vShield Endpoint for View, see:

[VMware vShield Endpoint](#)

Both nonpersistent and persistent desktops need antivirus protection. Infections can corrupt files even within a single user desktop session, so IT professionals need to set up antivirus protection for nonpersistent desktops, too. A distinct advantage of nonpersistent desktops is that they make remediation of infection easier: In the event of a security outbreak or breach, with proper configuration of Refresh on logout or reboot, a nonpersistent desktop can resume its original state.

For persistent desktops in VMware View, you need to install the vShield Endpoint driver in the virtual machine before it is converted by View Composer into a parent virtual machine for linked clones. If you do not use vShield Endpoint, you need to install the antivirus agent on the virtual machine before it becomes the parent virtual machine. The feasibility of including the antivirus agent in the parent virtual machine is determined by your choice of antivirus protection suite.

The vShield Endpoint product is the best approach to securing both persistent and nonpersistent desktops in the View environment.

Following are some best practices when you are protecting virtual machines in a VMware View environment.

Install Only the Core Virus Scanner

Top antivirus vendors offer not only the core virus scanner, but also optional features such as personal firewalls, antispymware, data shredders, PC clean-up utilities, and host-based intrusion-prevention system technologies. Depending upon whether you are utilizing vShield Endpoint or not, you can consider these optional features.

With vShield Endpoint

If you have vShield Endpoint installed, the footprint is already reduced on the desktops because the antivirus engine and signature file are on the virtual appliance. Therefore, you have more opportunity to add other options offered by the antivirus vendor.

Without vShield Endpoint

When you install an antivirus software package without vShield Endpoint, install only the core virus scanner on desktops, not the full-featured virus scanner package. Bundles of features may be appropriate for a freestanding PC but are less so for virtual machines in a contained datacenter. Installing only the core scanner helps to reduce the desktop agent memory and CPU footprint.

Use Random or Staggered Scan Scheduling

There are two common types of antivirus scans:

- **On-Demand Scanning (ODS):** User-activated scanning of all or part of a computer for malware
- **On-Access Scanning (OAS):** Automatic protection, or real-time protection, against viruses, spyware, or other malware. Scanning is automatically started when a file is opened or executed. OAS proactively prevents the spread of malware infections that may have entered the computer, but which have not yet been eliminated with an antivirus solution

With vShield Endpoint

If you employ vShield Endpoint, the burden of simultaneous signature file updates is eliminated because only the virtual appliance is updated. In addition, the vShield Endpoint architecture promotes staggered scanning of virtual machines managed by the vShield Endpoint virtual appliance. The vShield Endpoint solution provides information to the antivirus engine about which host the virtual machine is running on, and the antivirus scanner is then able to stagger the on-demand scans on the same host.

Without vShield Endpoint

However, if you do not use vShield Endpoint in your View virtual desktop implementation, you need to carefully schedule random or staggered scans.

In most organizations, IT administrators enable OAS for inbound (write) and outbound (read) file access scenarios. In organizations that are very sensitive about security, customers may prefer to perform additional frequent on-demand scans. With most antivirus solutions, you can perform ODS on a scheduled basis and always have OAS enabled. A best practice is to consider the impact on the storage and hypervisor resources, and to randomize the ODS scan times based on the hypervisor or storage LUN.

You may or may not be allowed by the antivirus software vendor to stagger scans with an antivirus agent installed on each virtual machine. Randomizing the scan schedule may be more viable, which would allow you to reduce the number of same-host virtual machines that are running their signature file updates simultaneously. However, you are only *randomizing* the signature file updates, not *eliminating* concurrent updates. Most antivirus software defaults to immediate updating when there is a new signature file available, which ensures immediate virus scanning when a new virus is circulating. With virtualization visibility, you can gather I/O load data by comparing the increased ratio between a clean virtual machine and a virtual machine with antivirus installed. Prevent virus scanning activities from saturating the I/O, and make sure that host CPU utilization is lower than 80 percent of your host capacity.

Update Virtualization and Other Software

Update your virtualization software and apply security patches. As with any software, desktop virtualization software on guest or local systems may contain security vulnerabilities, so it is important to keep all of your known virtualization software and applications updated with appropriate security patches. The common reasons to update software are to resolve functional bugs and leverage optimized or improved code, and to close vulnerabilities opened by security bugs.

With vShield Endpoint

One of the advantages of the vShield Endpoint solution is that you update the AV software only in the virtual appliance for each host, not in each desktop. This eliminates the AV storms that can occur when virtual machines that have been offline are powered on, which triggers an immediate update check for the signature file. In addition, you do not need to update AV software in each nonpersistent desktop image; the update on the virtual appliance suffices.

Without vShield Endpoint

If you do not use vShield Endpoint, you must update the AV software on each View desktop image. This clearly takes more time than updating a dedicated virtual appliance that holds the antivirus software, and there is more possibility of error.

Configure Virus Scanner Exclusion Lists

Almost all enterprise-grade virus scanners allow you to set up exclusion lists for the scanning process. We highly recommend that administrators configure these lists to exclude certain types of files from scanning.

Research which files are safe to exclude from scanning. Database and encrypted types of files should generally be excluded from scanning to avoid performance and functionality issues. The following are sample exclusions to consider for hosted desktops.

- Cisco CallManager
 - Drive:\Program Files\Call Manager
 - Drive:\Program Files\Call Manager Serviceability
 - Drive:\Program Files\Call Manager Attendant

- VMware

Other file extension types that should be added to the exclusion list include large flat files such as VMware virtual machine disks. Scanning VMware virtual machine disks while attempting to access them can affect session-loading performance and the ability to interact with the virtual machine. The antivirus software may already exclude these file types because they do not recognize the format.

- Exclusions can be configured for the directories that contain the virtual machines, or by excluding *.vmdk and *.vmem files

These are sample scanning exclusions. The security administrator needs to solicit recommendations from the antivirus vendor and carefully consider each proposed exclusion.

Resolve Virus Scanner Deployment Issues in Linked Clones

Linked clones present some special considerations for antivirus scanners. One issue is that some virus scanners require unique SIDs for the desktops. The other issue is determining where to remedy a virus infection: on the master image or on the linked clones.

Potential Issue 1: Unique SIDs for Virus Scanning

Each computer desktop in an environment needs a unique identity on the network so that a virus scanner can keep track of the machines that have been scanned. When you create a pool of linked-clone desktops with View Composer in a VMware View environment, each linked clone has the same Security Identifier (SID). To give each linked clone a unique identifier on the network, you can then use either Microsoft Sysprep or VMware QuickPrep. VMware recommends QuickPrep for this operation.

You can create a Sysprep script to give each linked clone a unique *local* SID. This local SID is used only until the computer is a member of a Windows Active Directory domain. As soon as you add the desktop to an Active Directory domain, Windows creates a new SID for the desktop, and the *local* SID is no longer in use. The Sysprep operation needs several minutes to change the local SID on a Windows OS because Sysprep must change all files on the hard disk drive. When you Refresh the desktop, the unique ID is retained. When you Recompose the desktop, a new unique ID is generated, which takes some time and leaves unused entries in Active Directory that you need to clean up.

The VMware QuickPrep tool comes with VMware View and applies only to linked clone desktop pools. QuickPrep assigns the same SID to all linked clones of the parent virtual machine. After the linked clones are created, View Composer uses the Windows API to create a computer account in the Active Directory domain and thereby generate a unique SID for each linked clone in Active Directory. Quickprep is faster than Sysprep because it does not change all files on the hard disk. After a Refresh or Recompose, the unique ID in Active Directory is retained, which saves time. Generally, the unique ID in Active Directory is sufficient for antivirus scanning.

Required Workaround for Some Legacy Antivirus Software

VMware recommends using QuickPrep to generate unique SIDs for linked clone desktops because the personalization process is faster. However, with legacy antivirus software, a few complicating factors may require action in addition to using QuickPrep. Some antivirus software products need a unique *local* SID *if they do not leverage VMware vShield Endpoint*. These products use the local SID to generate a Globally Unique Identifier (GUID) for tracking during the scanning process.

If the antivirus software you choose for your environment is not integrated with vShield, and the software needs a local SID to generate its own GUID for each endpoint, or if for any other reason you need a unique local SID for your linked clone desktops, you can use a workaround to avoid running Sysprep. The workaround is to use Recompose on each desktop to force the system to create a new local SID. This takes a long time, depending on the number of files in the virtual machine. However, you may find that spending this time to Recompose is more acceptable than time spent with Sysprep during creation of the desktops.

If you decide to use the Recompose approach, you must make sure that:

- The View Composer component is installed on the virtual machine. (This is standard.) The View Agent needs to use View Composer for the Recompose.
- The Active Directory controllers are reachable from all of the desktops.

To automate the Recompose, you can create a power-off script to save the SID before shutting down the virtual machine. VMware View Administrator allows you to provide a custom script to interact with View Composer. For more information on how to configure View Composer, refer to the [VMware View Administration guide](#).

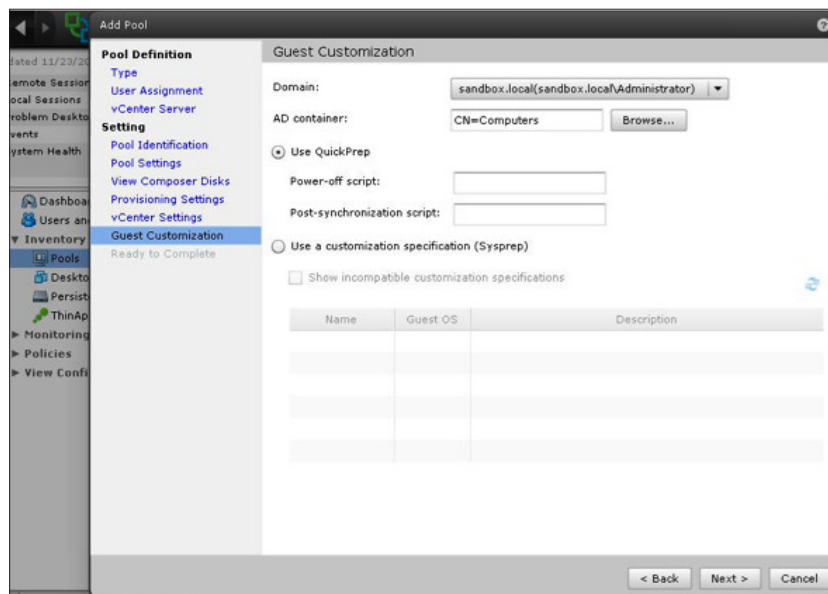


Figure 3: QuickPrep Settings and a Power-Off Script

Important: Remember that if you integrate the vShield Endpoint antivirus solution with your View implementation, you do not need this workaround. The vShield Endpoint product passes the virtual machine BIOS UUID on to the partner antivirus software. The BIOS UUID is not always unique, so vShield Endpoint also provides to the partner antivirus software the full path to storage for the virtual machine. This differentiates two virtual machines with the same BIOS UUID.

If you do not use vShield Endpoint, determine if your antivirus software requires this workaround for QuickPrep. The necessity for the workaround depends upon how the antivirus software generates the GUID. Instead of using the local SID to create a GUID, some antivirus products leverage the MAC address or the hostname stored in DNS to create the GUID.

If the antivirus software leverages the MAC address or the DNS entry of the endpoint to generate a GUID, and if no other software installed on each virtual desktop needs the local SID to distinguish endpoints, QuickPrep is sufficient, with no need to use Sysprep or the Recompose workaround described above.

If you are concerned about duplicate local SIDs on linked clones, refer to [The Machine SID Duplication Myth \(and Why Sysprep Matters\)](#).

Potential Issue 2: Reacting to Virus Infections Depending on Whether the Master Image or a Cloned Desktop Is Infected

If a virus is found, the first and immediate step is to perform the virus scanning on the master image. Scanning the master image first is the best option because it is a template and not in use. If an infection is found, clean it and then perform a Recompose.

If the master image is clean, but the cloned desktop is infected, the best course of action is to Refresh the cloned desktop. If the cloned desktop cannot be refreshed for some reason (or if the infection happened in a UDD – see next subsection), then use the antivirus solution to clean up the malware on each clone individually.

Protect the View Desktop During ThinApp Package Use

ThinApp virtualized applications present no special virus and malware vulnerabilities. In fact, ThinApp virtualized applications provide some added security because of the isolation of the running application from the VMware View desktop environment. If you are using View nonpersistent desktops, you need only be concerned with viruses and malware as they affect a session before the user logs out. If you are using View persistent desktops, you must consider antivirus protection more carefully.

Running ThinApp virtualized applications on a View desktop is similar to running native applications on the desktop. Malware may find a way to infect the desktop, and you need to protect the desktop. ThinApp is not a security technology, although application virtualization can provide a layer of protection against runtime modifications to files and registry keys. ThinApp virtual applications help to reduce exposure to malware and viruses by isolating the application, user data, and user settings inside a “virtual bubble.” This virtual bubble includes the application sandbox, where data and settings may be written.

As background, the following section gives an overview of ThinApp isolation modes and the role of the application sandbox. After this background discussion, we present [recommendations for desktop antivirus protection when using ThinApp packages](#). A separate section focuses on [protecting storage related to ThinApp packages](#) (the ThinApp packages, the ThinApp Repository, the ThinApp application sandbox, and related external drives).

Background Information on ThinApp Isolation Modes and the Role of the Sandbox

The isolation mode of a ThinApp package determines how much is written to the sandbox, and how much is written to the host desktop. VMware ThinApp sets up the default isolation mode for the virtual application by restricting some desktop directories from writes. During Setup Capture, you can set the isolation mode of directories that ThinApp has not already set. You can choose from two directory isolation modes, as in the following picture.

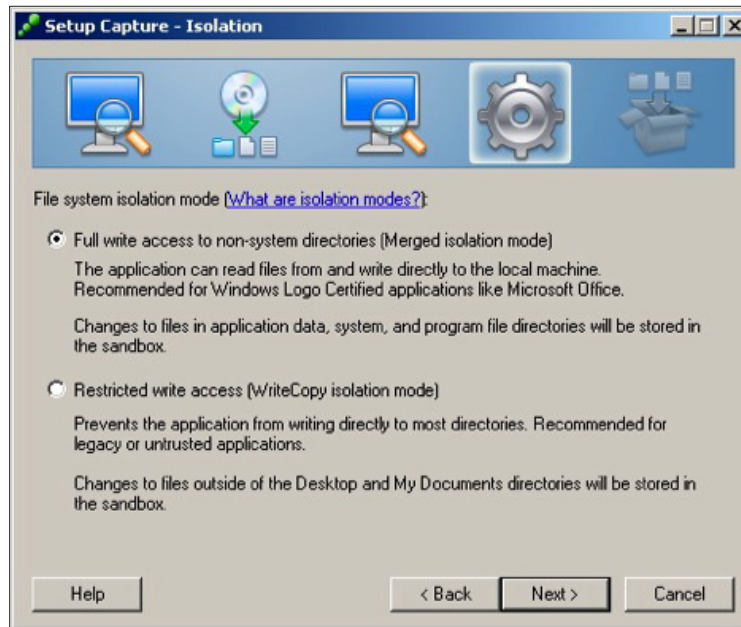


Figure 4: Isolation Window During ThinApp Setup Capture

These directory isolation mode choices are:

- **Full write access to non-system directories (Merged isolation mode):** During application use, the user can read from and write to directories on the desktop system hosting the ThinApp package. Writes to system directories are automatically excluded, and changes to those directories are stored instead in the ThinApp application sandbox. This is the default isolation mode.
- **Restricted write access (WriteCopy isolation mode):** The user can read from the system hosting the ThinApp package. The user cannot write to any directory on the host system, except for a few automatically specified user directories:
 - %Desktop%
 - %Personal% (My Documents)
 - %SystemSystem%\spool

All other writes to files and registry keys are saved to copies of these files in the ThinApp application sandbox.

A third isolation mode choice is available only from the `Package.ini` configuration file:

- **Full isolation mode:** The user cannot read from or write to the system hosting the ThinApp package. Reads are from the files and registry keys within the virtual bubble. All writes are stored in the application sandbox. ThinApp itself sets this isolation mode for only a few directories, and ThinApp packagers should never choose Full isolation mode for the entire virtual application. A virtual application must be able to read and utilize the underlying operating system, and Full isolation mode would prevent that. The virtual application would not be able to run.

Registry isolation mode defaults to WriteCopy, unlike the default for directory isolation mode, which is Merged. You can change the default registry isolation mode in the `Package.ini` configuration file for ThinApp.

For details on isolation modes, see [Configuring Isolation Modes for the File System and Registry in ThinApp \(Video Included\)](#).

Recommendations for View Desktop Scanning When Using ThinApp Packages

You need to be aware of how ThinApp package isolation mode can possibly expose your system to malware or viruses. If the virtualized package is fully isolated from the desktop system, data and settings changes remain within the ThinApp sandbox. However, ThinApp sets only a few directories to Full isolation mode. The general isolation mode for most directories is either Merged or WriteCopy, and some runtime changes are therefore saved directly to the host desktop system. Any application can bring in viruses or other malware to the system.

System files in a ThinApp package are always protected from writes by both Merged and WriteCopy isolation modes. If malware attacked a system, changes to system files would be stored and isolated in the sandbox, instead of on the host desktop system. For recommendations about scanning the sandbox, see [Scanning the ThinApp Application Sandbox](#).

Changes to non-system files may be written to the desktop system, so you need to routinely run a scheduled, on-demand virus scan on the desktop system that hosts the ThinApp package, just as you would for any system hosting native applications. Even if the desktop is nonpersistent and deleted upon user logout, you must scan the desktop for viruses during a user session.

Antivirus Protection for the View Security Server

Servers that run in the demilitarized zone (DMZ), including a View Security Server, need to be hardened. Run an antivirus scan regularly on the Security Server.

Antivirus Protection for Storage in the View Environment

The vShield Endpoint product is the solution to antivirus protection in running virtual machines. A View implementation invariably contains storage devices for such purposes as storing user data, user profiles, ThinApp virtual application packages, and more. The solution for securing storage devices is agent-based antivirus software from VMware partners.

This section discusses best practices in antivirus protection for:

- Mapped drives or shared folders
- User data disks (UDD)
- ThinApp-related storage
- The Persona Repository for View Persona Management

Scanning Mapped Drives or Shared Folders

Disable the mapped drives or shared folders option in the antivirus agent for best performance. If this option is enabled, it may create unnecessary network traffic when end users access remote paths or mapped network drives. This can severely impact the user's experience. If you need to scan mapped drives or shared folders, consider disabling scans in all but one endpoint (make that one endpoint the "designated scanner" for network shares, and make sure it always has the latest signatures).

Protecting User Data Disks (UDD)

When you compose a linked clone, you can also create a user data disk (UDD) to store and preserve user settings and data. You can create the UDD on the same storage location where the virtual machine resides or on a different preferred storage device. You need to use antivirus software to scan the UDD.

If a virus infection occurs, and the infected files are on the UDD, recomposing the linked clone will not clean up the infection. You need to use the antivirus product to clean the infection on each UDD.

Protection Strategies for Storage Related to ThinApp Packages

When working with ThinApp virtualized applications in a View implementation, you need to protect the ThinApp package itself and storage areas related to ThinApp. This section discusses protecting the

- [ThinApp package](#)
- [ThinApp Repository for virtual application packages](#)
- [ThinApp application sandbox](#)
- [External drives involved in the ThinApp implementation](#)

Protection of the ThinApp Executable and Primary Data Container During Package Creation

You will store ThinApp virtualized applications within your View environment in a ThinApp Repository. Before you place the executables and primary data containers in the repository, you need to ensure that the ThinApp packages you created are free from malware.

Consider the environments during the two phases of package creation:

- Capture machine
- Build machine

To protect against incorporating malware into a ThinApp package as you *capture* the application, you must use a clean capture machine. A **clean capture machine** is a generic installation of the lowest version of the operating system that will be in your deployment scenario. ThinApp uses a Delta snapshot algorithm. The ThinApp prescan takes a snapshot of the clean machine. Then you install the application you want to capture. The postscan takes a snapshot of the machine with the application installed, and ThinApp uses the difference between the snapshots to create the virtual application.

Most application vendors recommend that antivirus software and other security technologies such as firewalls not be installed or running when you install their applications; the application installation during ThinApp capture follows these guidelines. If possible, do not install applications such as antivirus software on your clean capture machine. If anything is preinstalled on the clean capture machine, and the application being captured uses any of those items, the new application installation skips installing those items. When you later place the captured application on a host machine, and those items are missing, the virtual application will not run properly. If your organization's policies require you to install antivirus software on the capture machine, you must install the same version of the antivirus software on all of the machines where you expect the virtual application to run. The virtual application may rely on components of the antivirus software that were preinstalled on the capture machine. However, other factors may come into play that you cannot predict when you do not capture on a clean machine. For an accurate application capture, use a clean capture machine.

For similar reasons, if you do not need a network connection for the application, disable the connection or use host-only mode.

These are general recommendations for a clean capture machine, and your environment will have unique requirements. Be sure to consider the effects of those requirements on the creation of a clean captured application.

The machine on which you *build* the ThinApp package is another concern. You can build the virtual application on a different machine from the one where you captured the application. The build machine does not have to be a machine with only a clean, basic operating system—the build machine can be an environment with other applications installed. Therefore, a best practice is to run a virus scan against the ThinApp application project directory before you build, if you are not building on the clean capture machine. And because you may rebuild the virtual application after tweaking configurations, keep the project directory free of viruses by continuing to run scheduled on-demand virus scans on it.

With these proper safeguards, you will not be packaging malware into the ThinApp executable or primary data container. Occasionally your virus scanner may point to a ThinApp package as having a virus or malware, but this may be a false positive (an error). Contact your antivirus vendor to find out if the virus detection is accurate, or if the virus checker is giving a false positive because of the ThinApp package format.

Note: You might think that it would be a good idea to capture an application and an installation of an antivirus program with ThinApp so that you can protect the application. However, because you cannot virtualize a device driver with ThinApp, it is not possible to capture an antivirus package.

After you place the ThinApp virtualized application on a ThinApp Repository and run the application on a desktop, you must continue to be vigilant about protecting the executable and the deployment system. The executable itself is read-only to the user, but malware authors are clever, and no file is invulnerable to attack. You must properly secure both the read-only ThinApp executable and the desktop system.

VMware Partnership with eEye Retina

To protect against vulnerabilities in the application being virtualized, consider a solution from eEye Retina. Any application, including a virtual application, is vulnerable to hacking because it listens to ports and takes instructions from other files (including from malware or a virus). With ThinApp virtual applications, the location of the infection can be the host desktop or the ThinApp application sandbox. Other sections of this paper discuss how to protect the [desktop](#) and the [sandbox](#).

Traditional vulnerability assessment solutions are not able to look into a ThinApp package, examine its components, and expose vulnerabilities. [VMware and eEye Digital Security have partnered to create a vulnerability management tool](#) within eEye's Retina suite of products. This tool recognizes ThinApp virtualized application packages and lists known vulnerabilities for those applications so that you can patch these applications before distribution. You include an eEye Retina script in the ThinApp package, which notifies Retina where the application is on the system. Retina then uses the ThinApp SDK to audit application vulnerabilities, particularly the application version number, even when the application is not running. The tool does not identify viruses or malware, but instead warns you about known vulnerabilities for the application versions that you have packaged. This capability is particularly important to government agencies and other security-sensitive enterprises. The Retina suite of products also is able to secure ESX and ESXi virtual machines; vulnerability management for virtual applications extends this security surveillance.

Protecting the ThinApp Repository in a VMware View Environment

In a VMware View environment, ThinApp executables and primary data containers are stored in a ThinApp Repository (Windows application share). Consider how viruses or malware might travel to or from this file share:

- **Outbound:** As users access the ThinApp packages, malware can travel out to users
- **Inbound:** Malware could accompany a ThinApp package as it is copied to the file share, or as users connect to the file share to access applications

Outbound

If you properly packaged a virtual application with ThinApp on a clean machine, you do not need to be concerned about malware in the executable or primary data container which could travel out to the desktop.

Do not enable on-access scanning of executables in the repository, or user performance will be impacted on each access of a ThinApp package. If you are forced to scan the repository, choose on-demand scanning during periods of low use.

If you are required to use on-access scanning for the ThinApp repository, make sure that all ThinApp packages larger than a couple of megabytes have separate primary data containers. You can choose this option during Setup Capture. The primary data container includes the ThinApp runtime for each virtualized application. By isolating the ThinApp runtime from the executable for each package, you reduce the size of the executable and minimize the scan time at application launch. For more information on creating a separate DAT file, see the [ThinApp User's Guide](#).

At a minimum, try to exclude the DAT files from scanning because they are generally larger than the executables. Some virus scanners provide file-extension exclusion filters. Even if you cannot exclude DAT or EXE files from on-access scans, the impact of scanning these files is lessened if you separate the DAT file from the EXE.

These recommendations are for the purpose of decreasing application launch times and augmenting application performance. Of course, you may have regulations that require scanning the EXE and DAT files. In this case, try to use on-demand scanning at low-usage hours.

Inbound

If you properly set permissions on the ThinApp Repository to read-only, user access to ThinApp packages in the repository is read- and execute-only, so you do not need to be concerned about transfer of infections from user systems to the repository.

As you add ThinApp packages to the repository, scan them in case the process of copying the packages in has carried in viruses or malware. To do this, set up virus scanning of the repository only for inbound files, if this option is available in your virus checker. If specifying only inbound files for scanning is not possible with your virus checker, set up on-demand scanning of the repository at a regular, low-impact time of day, rather than use on-access virus scanning, which would impact user access to the files.

Scanning the ThinApp Application Sandbox

The ThinApp application sandbox stores changes to data and settings that are not writable to the host desktop because of isolation mode settings. Therefore, the sandbox may contain infected files. If the sandbox is not persistent (that is, you delete it upon logout), you may think that you do not need to scan it for viruses. However, an infection can spread quickly even within one user session. If the sandbox is persistent, you do need to scan it. So, in either case—persistent or nonpersistent—you need to develop a strategy for scanning the sandbox.

The ThinApp application sandbox is a standard, readable folder in Windows, and therefore is easy to include in virus scans. However, scanning the sandbox on access would impair application performance: users access their data and settings throughout application use. If possible, exclude the sandbox from on-access scanning. If you are required to scan the sandbox, use on-demand scanning during periods of low use. You might want to test how scanning impacts performance to choose the best time of day.

If a virus is discovered in the sandbox, you can either clean or delete the sandbox. A fresh sandbox is automatically regenerated the next time the user runs the virtualized application.

During ThinApp packaging, you determine where to locate the ThinApp sandbox for each application. If you use View Persona Management, you would most commonly locate the ThinApp application sandbox within the persona user profile location so that Persona Management includes it in the user profile. See the [Persona Management](#) section for advice on scanning the Persona Management user profile location. If you are required to scan the sandbox, and the sandbox resides outside of the user's profile, it is a best practice to set the sandbox location to a local drive to avoid incurring extra network traffic.

The ideal is to use a nonpersistent View virtual desktop with a local ThinApp application sandbox because the sandbox is included in the automatic deletion on logout. A new sandbox is generated upon starting the application. If you use View Persona Management, the ThinApp application sandbox is by default included in the Persona Repository; if you do not want to retain the sandbox, you must exclude the sandbox from roaming. Refer to the [VMware View Administration guide](#) and the [VMware View Persona Management Deployment Guide](#) for implementation details.

Protecting External Drives Involved with the ThinApp Application

Your directory isolation mode setting for the ThinApp virtual application applies not only to directories on the local desktop, but also to virtual drives. However, your isolation mode setting does *not* apply to external drives connected to the host desktop system. By default, users can write to network drives and removable disks. Therefore, you need to be aware that viruses and malware can travel to these drives. Be sure to scan them with your antivirus checker, or guard against writes to these drives.

For information about how to restrict virtual application writes to network drives and removable disks, see [The SandboxNetworkDrives Parameter in Package.ini in ThinApp](#) and [The SandboxRemovableDisk Parameter in Package.ini in ThinApp](#).

Scanning the Persona Repository of User Profile Files

Instead of creating a user data disk for user profile data, in View 5 you can implement View Persona Management to provide users with a place for their personal data.

UDDs and Persona Management both provide user profile management, but they operate differently, and it is actually possible to have both. View Persona Management has several advantages in terms of manageability. For more information about these advantages and about how to implement Persona Management in a View deployment, see the [VMware View Persona Management Deployment Guide](#).

View Persona Management presents some opportunities for streamlining antivirus scanning. Persona Management downloads user profile files from the centralized Persona Repository as the user needs them. If on-access virus scanning were to occur within the user's virtual desktop as the files got copied from the central repository, the IOPS load would be increased. The performance of the user's desktop would be slowed.

The best practice for View deployments with Persona Management is to turn off on-access scanning of the local user persona files and to set up on-demand scanning of the Persona Repository file share at periods of low usage. An alternative to on-demand scans of the Persona Repository is to create power-off or logout scripts to scan the repository. This would protect the user from malware for the next time they log in to their desktop. This guards against missing a virus between periodic Persona Repository scans.

These are recommendations only. Your strategy for scanning profile files is at your own discretion. You must strike a balance between security and performance.

Conclusion

Virus and malware prevention in virtual desktops creates some challenges that need to be taken into consideration when architecting the virtual desktop environment. However, these challenges can be properly tackled, either by deploying a vShield Endpoint integrated solution in the View environment or by taking some small steps during initial deployment and configuration. VMware View provides a modern, high-performance, flexible virtual desktop that is both better secured than a physical desktop and also more easily cleaned of any infection that does get through the antivirus software.

About the Authors and Contributors

Tina de Benedictis, Technical Marketing Manager for Enterprise Desktop at VMware, revised and updated this document for View 5. Tina's background at VMware includes writing Knowledge Base articles and developing Technical Support training on ThinApp, Fusion, and Capacity Planner. Her previous background is in customer training, technical support, and technical publications at companies including Mobileum (Roamware), Scopus (Siebel), and ASK/Ingres (Computer Associates).

Tina acknowledges the contributions of Afonso Infante for View 5 and vShield Endpoint information. Peter Bjork, Dean Flaming, Travis Sales, and Blake Watts refined the ThinApp information. Sam Larsen, Joshua Schwartz, and Lionel Litty reviewed the vShield Endpoint content.

Cynthia Hsieh wrote the View 4.5 version of this document. Dean Flaming, John Dodge, Marios Leventopoulos, and Mason Uyeda provided review and information for the View 4.5 version.

