

# Operational Aspects of Desktop Virtualization



# Contents

<b>Introduction</b> .....	<b>1</b>
<b>Endpoint Security</b> .....	<b>1</b>
Current Challenges with Endpoint Security.....	1
Virtualization Impact on Endpoint Security.....	2
<b>Desktop Patch Management</b> .....	<b>2</b>
Current Challenges for Desktop Patch Management.....	2
Costs of a Manual Approach to Patching .....	3
Costs of Automated Patching.....	4
Patch Management Workflow .....	4
Virtualization Impact on Desktop Patch Management.....	4
<b>Image and Application Management</b> .....	<b>6</b>
Current Challenges for Image and Application Management.....	6
Virtualization Impact on Image and Application Management.....	7
<b>Disaster Recovery and Data Protection</b> .....	<b>8</b>
Current Challenges for Disaster Recovery and Data Protection .....	8
Virtualization Impact on Disaster Recovery and Data Protection .....	9
<b>Desktop Help Desk and Support</b> .....	<b>10</b>
Current Challenges for Desktop Help Desk and Support.....	10
Virtualization Impact on Desktop Help Desk and Support .....	10
<b>Resources</b> .....	<b>11</b>
<b>About the Authors</b> .....	<b>11</b>

## Introduction

Built on the industry-leading VMware virtualization platform, VMware® View enables you to deliver rich, personalized virtual desktops to any device with all the benefits of centralized enterprise desktop management. The VMware View portfolio of products lets you run virtual desktops in the datacenter while giving end users a single view of all their applications and data in a familiar, personalized environment on any device at any location.

VMware View transforms the way you use and manage desktop operating systems. You can deploy desktop instances rapidly in secure data centers to facilitate high availability and disaster recovery, protect the integrity of enterprise information, and remove data from local devices that are susceptible to theft or loss. By isolating each desktop instance in its own virtual machine, you eliminate typical application compatibility issues and deliver a more personal computing environment.

This paper provides a guide to assessing the operational impact of deploying View. In planning for a View deployment, you must do more than evaluate the technology. You must also re-evaluate your current desktop management processes. To gain the greatest operational benefits from the move to virtual desktops under View, you might need to re-engineer some of those processes. This paper analyzes and quantifies operational efficiencies you can achieve in several key areas by deploying a View solution.

For each key area, the paper outlines the challenges with current desktop management processes and then offers best practice recommendations on how to be modify, update, or completely change these processes in a View environment. These recommendations are based on VMware best practices and on the experiences of successful customer deployments of View.

This paper is for desktop administrators and architects who are currently designing a View deployment or actively engaged in deploying View. To get the most from this paper, you should be familiar with the general architecture and concept of a View solution. In particular, you should be familiar with the *VMware View Manager Administration Guide*. (See the Resources section for a link.)

## Endpoint Security

As frequent news reports attest, lost laptop computers and compromised desktop PCs can compromise sensitive corporate or personal data all too easily. With the ever-increasing mobility of desktop environments and a higher percentage of users working on laptops, data security at the endpoint is becoming an increasing concern.

### Current Challenges with Endpoint Security

With traditional PCs and laptop computers, administrators attempt to mitigate a variety of security concerns. Securing a company's proprietary data on desktops and laptops is one of the primary efforts. Some organizations implement disk-based encryption solutions that can be costly and hard to scale.

As companies begin to outsource more and more of their workforce and use part-time contractors, they must be concerned about providing these individuals with corporate assets such as loaner laptops. If they use loaners, they risk seeing the equipment stolen or compromised after they leave the company's site. Other significant risks to corporate assets come from the intentional or unintentional actions of employees. These risks include data being copied to USB

flash drives and removed from the company site. They also include the introduction of a malicious virus into the corporate environment in the same fashion, via a USB flash drive.

## Virtualization Impact on Endpoint Security

The immediate improvement that a virtual desktop solution offers for data security is the fact that you house all desktop data in virtual machines your corporate datacenter. You protect access to this data by datacenter-level security mechanisms, such as firewalls, DMZs, Web proxies, and VPNs. When users have thin clients at their desks, they no longer keep data locally. Such a configuration is ideal for providing contractors or offshore developers access to secure desktop environments without having to worry about proprietary data being removed.

Another benefit of replacing the devices at users' desks with thin clients is the ability to be very selective with the types of USB devices that you allow to connect to the secure virtual desktop environment. You gain the ability to prevent users from connecting USB flash drives, iPods, or iPhones to their desktops, reducing the opportunity for those users to use company resources for unproductive activities. By restricting use of USB devices, you can also mitigate concerns about the introduction of malicious software or the removal of sensitive data.

For users who are not always connected to the corporate network — traveling sales people or executives who are issued laptops, for example — View includes an experimental feature called Offline Desktop. This feature allows end users to access their virtual desktops in their datacenter when they are online in the office. If they have upcoming business trips and expect network access will be intermittent, they can check out their desktops to their local devices. An instance of a user's desktop is copied to the local device, it is encrypted, and the user has offline access to the applications and data in the virtual desktop. When the user comes back on line the, local copy of the desktop is synchronized with the datacenter copy. This approach means you always have a last known good state of the desktop data secure in the datacenter. If this user loses the laptop computer or has it stolen, you can ship a new device to the user, who can then connect to the corporate network and download the most recent version of the desktop that was synchronized to the datacenter. The data on the missing device is encrypted and has a remote kill setting that disables it if it does not communicate to the corporate network within a specified time.

## Desktop Patch Management

Today's traditional patch management processes and solutions pose many challenges. A great deal of a desktop administrator's time is spent testing and distributing patches and troubleshooting patch distribution issues.

### Current Challenges for Desktop Patch Management

The distributed nature of desktop and laptop computers has made centrally managed software distribution mechanisms — such as Windows Server Update Services, Systems Management Server, and Altiris Deployment Solution — an important part of the IT infrastructure in many organizations. Usually these solutions are very distributed in nature and are complex to manage and maintain. They also do not guarantee successful distribution, because they rely on client-side agents, which must be running and on the network to receive any updates. The more distributed the desktop environment, the more complex this environment is, and the lower the first-pass success ratio is. This problem becomes even more significant if the desktop environment is widely dispersed. If you need to deliver patches and service packs to desktops at remote branch or regional offices, where network connectivity is limited, you can encounter connectivity issues, and it can take much longer to deploy the updates.

Another key challenge in the conventional patch management process is validating patches to assure that applying a patch will not have a negative impact on an end user's PC or applications. This process is time consuming and subject to failure. After PCs are deployed, they are subject to significant configuration drift. This configuration drift can be attributed to hardware replacements, upgrades, or application installations that vary from the core corporate image. Thus, certifying a patch against your organization's base image does not ensure that it works on all users' computers. Because the validation process is not 100 percent successful, a patch or service pack you distribute may cause problems on some computers and not on others. It is then very difficult to revert to the last known clean state and back out the changes.

With all of these complexities, it can take a very long time to patch all the computers in your organization. The delays make it difficult to maintain good security.

A study by Qualys showed that over the past five years, the average time to patch desktops has improved by only one day, from 60 to 59 days on average. This is not nearly fast enough to handle the increasing number of vulnerabilities and the speed with which they are being exploited. On average, 10 percent of desktops are never patched, and the number of vulnerabilities has jumped from 3 million five years ago to 680 million today. Of these 680 million vulnerabilities, 72 million were deemed critical. If you are a desktop administrator, the odds are squarely against you.

An additional concern is the time it takes companies to patch 50 percent of the reported vulnerabilities. A metric reference in the same Qualys study called this the "half-life" for patching desktops. In 2004 this half-life was measured at 30 days on average, and in 2008 this metric has only improved to 29.5. This slow progress can be attributed in large part to the lack of innovation in both products and methodologies that companies use to manage their desktops.

A bigger issue is that hackers are releasing exploits for vulnerabilities at much faster pace than administrators can patch systems. On Microsoft's patch Tuesday in April 2008, of the 21 fixes that Microsoft published, 10 repaired vulnerabilities for which exploits were already in circulation.

Another result of this complex combination of considerations is that you may find it difficult or impossible to focus on timely patches for the tier-one applications that are most important to your organization's activities. Examples of these key applications include Microsoft Office and Adobe Acrobat.

You can quantify the cost of failing to mitigate software vulnerabilities using the following equation:

$$\text{Cost not to mitigate} = D * T * R$$

In this equation,  $D$  is the number of desktops,  $T$  is the time needed to fix systems and lost productivity, and  $R$  is hourly cost of the time spent and productive time lost.

For an organization with 1,000 desktops to be fixed, each taking eight hours of downtime (four hours for one administrator to repair the PC and four hours that the end user is nonproductive) at a rate of \$70 per hour in wages and benefits, the cost of responding after an attack is:

$$1,000 \text{ computers} * 8 \text{ hours} * \$70/\text{hour} = \$560,000$$

### Costs of a Manual Approach to Patching

Compare the cost of recovering from an attack to the cost of manual monitoring and prevention. Assume the vulnerability exploited by a worm and the corresponding patch are announced before the worm is created. This has been the case for most exploits. True zero-day attacks are not frequent. Manually monitoring for new patches for a single type of desktop image takes as little as 10 minutes each day, or 60.8 hours per year. Applying a desktop patch generally takes no more than 10 minutes. This makes the cost equation for the annual monitoring cost:

$60.8 \text{ hours monitoring} * \$70/\text{hour} = \$4,256$

The cost to apply each patch manually is:

$0.16 \text{ hours patching} * 1,000 \text{ computers} * \$70/\text{hour} = \$11,200$

The total cost to maintain the systems is:

$(\$4,256 + (\$11,200/\text{patch})) * (\text{number of different desktop image types})$

Based on Microsoft security bulletins for 2006, 2007, and 2008, the company has averaged about six patches per month, or 72 patches per year. The cost to maintain just one desktop image is  $\$4,256 + (\$11,200 * 72) = \$810,656$ . Most organizations maintain more than one desktop image, so this number grows in a linear fashion as the number of supported desktop images increases.

### Costs of Automated Patching

A third option is to invest in an automated patching solution. These solutions automatically check for required patches and deploy them. Both free and commercial solutions are available. Assume that a commercial solution costs \$15,000 and charges \$20 per computer for annual maintenance. This approach is much less expensive than the manual solution, even though it might be necessary to dedicate all of a person's time to maintaining, updating, and patching using the automated solution.

Annual cost for the administrator to run the patching solution:

$40 \text{ hours/week} * 52 \text{ weeks/year} * \$70/\text{hour} = \$145,600$

Annual patching cost for the automated solution:

$\$145,600 \text{ administrator cost} + (1,000 \text{ computers} * \$20/\text{computer}) = \$165,600$

### Patch Management Workflow

The basic process workflow that most organizations follow or attempt to follow when they implement patch management is similar to the following:

1. Inventory
2. Identify need
3. Prioritize
4. Plan
5. Test
6. Remediate
7. Report
8. Maintain and assure

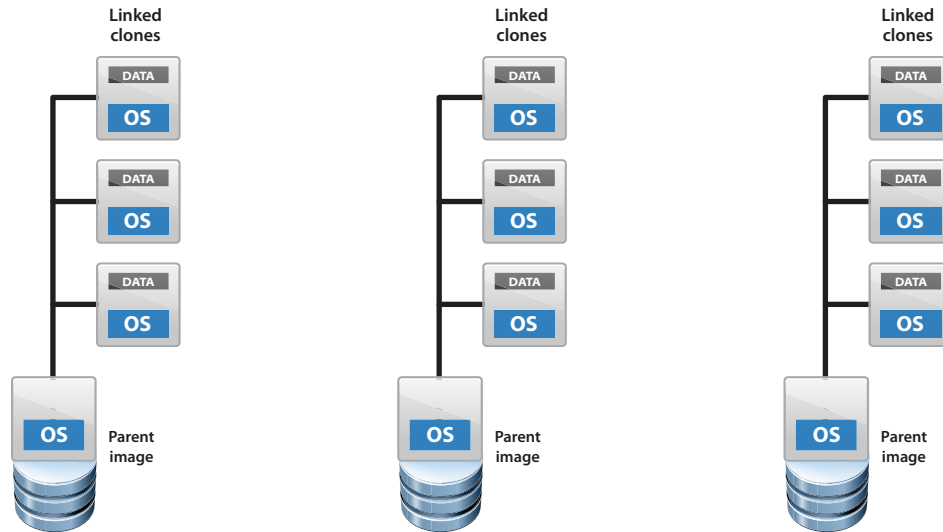
This process is cyclical. After step 8 is completed, the process begins again. This process can be complex and subject to many challenges, which can lessen the effectiveness of the patch management process.

### Virtualization Impact on Desktop Patch Management

Implementing a virtual desktops solution does not eliminate the need for solid processes and organizational resources to manage patching and other security issues. However, you can make the patching process more efficient using the tools that a View solution provides. In a typical View environment, updates you apply to a single virtual machine instance automatically affect multiple

end-user desktops. As a result, you spend less time patching and update more end-user desktops on the first pass.

As shown in Figure 1, the composer technology in View enables you to create a catalog of desktop types to meet the needs of particular categories of users. You create a parent virtual machine image for each desktop type, and View provisions a desktop to each end user by creating a linked clone based on the appropriate parent image.



**Figure 1 — End-user desktops based on parent images**

View creates the operating system disks for these end-user desktops as linked clones of the parent virtual machine. Initially, the desktops read data from the parent disk. When a desktop writes data, View saves it in storage that is unique to that desktop. Future reads come from the desktop's unique data or from the parent image as appropriate. Taking advantage of the properties of linked clones, View gives you new management functions for these desktops, including recompose, refresh, and rebalance.

The refresh operation allows you to reset a linked clone desktop back to its original deployment state. You can use this feature to mitigate performance issues that result from operating system bloat. It is also useful for desktops that are not assigned persistently to any particular user and are reset every time a new user logs in. The recompose function allows you to migrate an end user from one desktop to another, maintaining the user's data disk and making the data disk available to the user from the new desktop. The rebalance feature is a way to move virtual desktops from one storage array LUN to another in order to balance the disk usage load.

You can use the recompose function to streamline patching and make the process more efficient. Rather than managing a patching process for each individual desktop, you can patch the parent desktop and use the recompose function to distribute that patch automatically to end users' desktops. You implement your existing patching processes for the subset of parent desktops, a small fraction of the total number of instances you would need to patch with the traditional approach of patching each individual instance.

You manage all of these parent images directly, and they are located in the datacenter on the corporate network. Because they are in the datacenter, you avoid the traditional problems that patching software encounters, such as network latency and bandwidth issues as well as issues with desktops and laptops being on the network at the time of the remediation. The centralized nature of the virtual desktops ensures that these parent images are always at the latest patch

level. You can leverage your existing investment in automated distribution technologies to patch the master images.

Another approach you can take is to use vCenter Update Manager as the patch mechanism for the parent images. Using Update Manager, you can create different patch baselines for each category of desktop. This approach allows you to assign the appropriate level of priority to patching categories of desktops based on how critical they are to your business, rather than using the traditional broadcast approach. Another advantage of vCenter Update Manager is that it automatically takes a snapshot of each desktop before applying the patches. This snapshot provides a revert point if your validation tests uncover any issues with the patches. Because all the individual desktop instances are anchored to replicas of the parent image, your installation and validation activities have no impact on your end users.

After you update the parent images and validate the patches, one administrator can run a scheduled recompose operation for all the individual desktop instances you have deployed. You can schedule this recompose operation outside business hours to minimize any impact on end users' productivity. Because the desktops all reside in the datacenter, you avoid the problem of systems remaining unpatched because particular desktops are powered off or not on the network. Also, because you have a revert point for the parent images, if you discover a compatibility issue after deploying the new desktop instances, you can trigger a revert recompose operation on demand to return users to their last known good desktop.

You can schedule recompose operations or execute them on demand, forcing users off of their desktops in the event that you need to apply a critical patch immediately.

## Image and Application Management

As new versions of applications and desktop operating systems are released, you need to have an efficient way to update end users' desktop environments. You need to achieve this while minimizing end user down time and mitigating any potential user data loss.

### Current Challenges for Image and Application Management

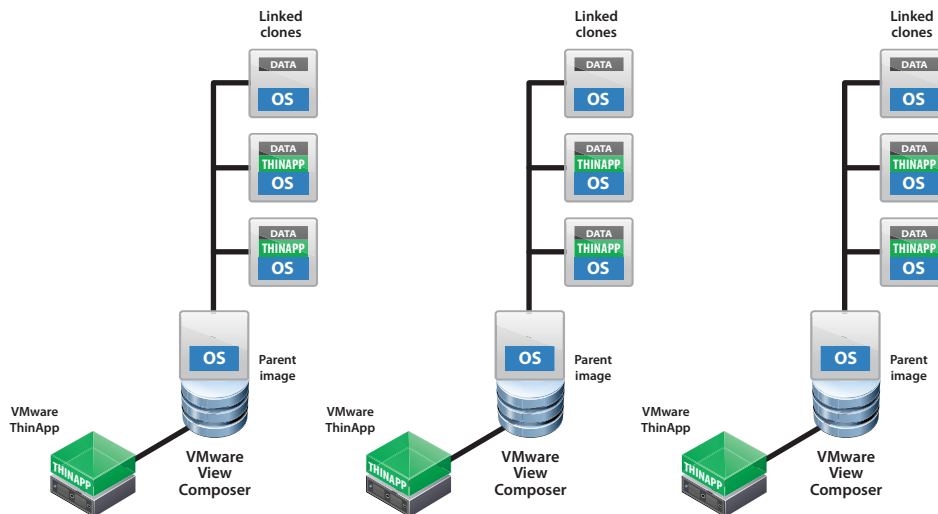
Desktop images configured for end users are usually very heavy and not carefully tailored for various user roles. In addition, the applications in these images are tightly coupled with the operating system. It is very difficult to manage just one application or to maintain the operating system without affecting some other component of the installed software, sometimes negatively. For example, you might need to update an image with a newer version of Java or the .NET Framework. Such updates often have trickle-down effects on other applications in the image. This tight coupling of applications and the underlying operating system can significantly hamper image maintenance. Images also must include compatible desktop and laptop hardware drivers. To ensure compatibility, organizations tend to engineer and certify desktop images for each of their desktop hardware types. Because most organizations refresh their desktop hardware every three to five years, the number of new images that they might have to develop could grow very quickly.

You face a similar challenge when you need to migrate to a newer desktop operating system. Windows XP has been the de facto standard desktop operating system for the past four to five years. Many organizations did not adopt Windows Vista, but they are likely to move to the upcoming Windows 7 release. The migration from Windows XP to Windows 7 in a physical environment is likely to be very painful.

## Virtualization Impact on Image and Application Management

When you implement a remote desktop strategy based on View, you can decouple the various layers that make up a desktop image and manage each of these desktop layers independently. This allows you to use more efficient management processes and minimizes the impact a change at one layer has on the other layers and ultimately on end users.

The layers of a virtual desktop are the operating system, applications virtualized using ThinApp, and user data. As shown in Figure 2, when a user connects to a virtual desktop, these three layers are joined dynamically to present a fully functioning desktop to the user.



**Figure 2 — View Composer adds ThinApp applications to desktops**

For each category of users, you create a lowest common denominator operating system image as a virtual machine. VMware recommends that you create fresh images rather than importing images from physical PCs. When you convert images from physical PCs, it is difficult to break the bond between the operating system and the applications.

After you create the operating system images, you can use this baseline image as part of a persistent or nonpersistent desktop pool. The kind of pool you use depends on the role and business requirements of the end user.

For each category of desktop you manage, you choose one of two approaches to adding applications to this baseline image. The goal is to separate as many of these applications as possible from the base image. You can use ThinApp application virtualization to achieve this goal.

VMware recommends that you create a centralized ThinApp repository in the datacenter and then take advantage of Active Directory security policies to stream the appropriate applications to the each category of desktop users based on their requirements.

If network restrictions prevent you from using the first approach, you can add ThinApp applications to the base images. An example of an application that would be better suited to inclusion in the base image is Microsoft Office 2003 or 2007.

The inherent isolation that application virtualization provides makes it much easier to troubleshoot issues with applications and eliminate common conflicts between applications. By virtualizing the applications, you also gain a mechanism you can use to roll out new or patched versions of an application dynamically. You replace the source application package on the central file share, or you configure the applications installed in the images to use the ThinApp Application Sync feature to update automatically from a secure HTTPS site in the datacenter. Both

of these approaches give you a level of separation between the desktop operating system and the applications running in the desktop.

When you need to migrate to newer desktop operating systems, such as Windows 7, you can use View Composer and the recompose function for a much simpler transition. You can build the new desktop image following the recommendations above for separating the applications from the operating system.

After you have built the image and certified it in the lab, you can take either of two approaches to rolling it out.

You can choose a small subset of your user base for a pilot rollout, in order to carry out user acceptance testing. You can schedule this migration outside business hours and carry it out using a recompose function. Your pilot users log out of their desktops at the end of the day, you run the recompose function, and when your users log in the next day, they have their new desktop images. You do not need to touch an individual PC for each user or deploy a large image over the network to an end device that might or might not be on the network or might not have hardware that is compatible with the new operating system.

An alternative approach you can implement easily is to roll out the new desktop image in addition to the existing desktop your users are already using. In organizations that adopted Windows Vista, users encountered many differences and faced a difficult learning curve. A similar experience is likely in organizations that move directly from Windows XP to Windows 7. If you entitle users to desktops with both the old and the new operating systems, you can minimize the number of support calls from end users who do not know how to use the new desktop environment. These users can try out the new desktop until they are more comfortable with its new features and functionality but use the old desktop to ensure they remain productive. When they are ready to move completely to the new desktop, you can decommission the old one.

## Disaster Recovery and Data Protection

Organizations have a difficult enough time defining and implementing a disaster recovery strategy for their servers, so it is not surprising that they do not assign high priority to disaster recovery planning for desktop systems. This is in a large part because of the high cost of disaster recovery plans for environments that many organizations might not consider tier 1 environments. Data protection is also a challenge, especially with largely distributed environments. It often falls upon end users to implement their own desktop and laptop backup solutions if they want to protect against a severe failure or data corruption.

### Current Challenges for Disaster Recovery and Data Protection

Consider the next level of concern for an organization hit by a disaster that causes its servers to fail over to a disaster recovery location. Who now needs access to the applications running on those servers and how do these end users connect to the recovery infrastructure?

If a datacenter suffers a disaster outage, it is likely that the surrounding area, including the organization's office, is suffering some sort of outage or is inaccessible to end users. A disaster recovery plan must also recover end users' desktops and make them available so that the servers, which have failed over to the new location, can be used by anyone. In an environment that relies on hardware-dependent end-user desktops, the cost and sheer complexity of recovery can be prohibitively expensive and subject to limited success. The challenges include image backup, hardware availability at a disaster recovery site, and desktop data replication or transfer.

Desktop backup strategies provide one alternative to a complete disaster recovery plan. The main objective of a backup approach is to have certain key data backed up in the event that an end

user's desktop is damaged, infected with a virus, or retired. The goal is to be able to recover a user's critical documents and files. The distributed nature of the desktop environment makes this problem hard to solve. Most organizations that attempt this approach have to invest in agent-based backup solutions that they install on every desktop and laptop. They configure these agents to run scheduled file backups.

One of the bigger challenges of this approach is the impact the backup process has on end users. If a window pops up in the middle of the workday and the agent starts to back up files, users are annoyed and their computers can slow to a crawl. As a result, users might cancel the processes and kill the backup agent window. In some cases, if users have administrative access to their PCs and are savvy enough, they even disable the backup agents on their PCs. If they lose their laptops or their desktop hard drives die — or if a disaster makes the office inaccessible — they have no backups from which to restore.

Some organizations implement agentless strategies in which they map desktop computers to centrally located file shares, and critical files are redirected using Active Directory group policy objects. This approach is somewhat more successful, but depending on the network topology and distribution of users, it can put a strain on the network infrastructure and is also somewhat dependent on end users knowing where to save their files.

## Virtualization Impact on Disaster Recovery and Data Protection

Implementing a View desktop strategy can help you achieve efficiencies both in disaster recovery for desktops and in desktop backups.

One key architectural characteristic of a View implementation is that all the data files and the virtual machines that provide the end-user desktops reside in a datacenter on shared storage. In many instances, the View desktops can and should reside on the same storage arrays you use to store your server virtual machines.

As a result, you can use array replication technologies to replicate the LUNs where the desktops are stored to your disaster recovery site along with the server virtual machines. You can use this approach in conjunction with a solution such as VMware Site Recovery Manager to automate recovery of the desktop virtual machines. Because you can set up all of the View infrastructure servers as virtual machines, you can also replicate them to the disaster recovery site.

With all the components of your View infrastructure available at your disaster recovery site, you can get your organization back to work much more easily after a disaster. Your end users can access their desktops from home via a corporate VPN or, depending on your configuration, just an Internet connection. Similarly, if a pandemic requires your organization to tell workers to stay at home, they can connect to their desktops and access the corporate resources they need to do their jobs without having to come into the office.

When you plan your desktop backup strategy, you can choose from several backup solutions for virtual machines that provide both image-level and file-level backups without any downtime or end-user impact. These solutions integrate with vCenter and provide deduplication capabilities to ensure greatest efficiency.

If you use the image management approach outlined in this paper, you no longer need to back up stateless operating system instances. Instead, you configure user data disks so they are on storage arrays that use the necessary array-based backup technology.

If a nonpersistent desktop fails or is not available, you do not need to try to recover the desktop from a backup, because the backup has no user-specific data. It is faster and simpler to deploy a new desktop created from the same base image and give the user access to the new desktop.

You can use the same approach with a desktop that is infected with a virus and is unusable. Because you have separated the operating system disk from the applications and user data, it is easy to recover the operating system partition quickly from a clean image that is not infected.

## Desktop Help Desk and Support

As a result of implementing a View-based desktop strategy, you can expect to achieve higher levels of service for your end users and increase the perceived level of service. You should also be able to take advantage of the centralized nature of the architecture to reduce the mean time to resolution of end user help desk issues.

### Current Challenges for Desktop Help Desk and Support

Desktop administration teams face a constant battle to meet established service level agreements for desktop end users and to maximize update speed. Help desks that support desktop users also focus on minimizing the mean time to resolution (MTTR) when a user's desktop fails. This in turn reduces the amount of time that end users are not being productive.

Some of the most common desktop support issues include the following:

- User wants a bigger or more powerful PC — “My desktop is slow or not snappy.”
- Desktop hardware has failed — Hard disk failure, network card failure, etc.
- User encounters an application-specific issue — Office, Visio, or AutoCAD is not working right.
- Network connectivity to corporate resources is not working.
- User's computer has a spyware or virus infection from malicious Web sites or email attachments.

Again, the distributed nature of a desktop environment also adds a level of complexity. How does a support technician troubleshoot an end user's PC that is miles away in another city, in some cases? This distance makes troubleshooting issues much more difficult and more costly. There are also many hardware-related issues that arise as a result of the varying types of drives and other hardware devices in a traditional desktop environment.

### Virtualization Impact on Desktop Help Desk and Support

By centralizing the desktops in the datacenter using View, you bring the desktops closer to the administrators and support teams. This eliminates the challenges of working with remote desktops such as those in branch offices. In a View environment, administrators have direct access to end users' desktops via vCenter, so they can see what is happening without using a remote management tool, such as VNC or Remote Control.

If the problem with the desktop is not something that is wrong with the parent image, you can quickly provision a new desktop for the end user, either permanently or temporarily. You create a temporary or backup desktop pool (similar to the approach you would use for hotel or kiosk PCs) and entitle the end user to use a desktop from that pool. The user logs out and logs back in, gaining access to a basic desktop that provides some level of productivity for the end user while the administrator tries to resolve the problem with the user's normal desktop.

Because virtual machines use standard and generic virtual hardware devices, issues with driver compatibility are sharply reduced. VMware has a well staffed operating system certification team that ensures there are no driver issues with virtualized operating systems.

For architectures that include the replacement of end users PCs with thin clients, support for those end-user devices becomes very simple. In many instances, end users themselves can install

and set up their thin clients without a technical support engineer on site. If a hardware problem occurs, the end user can try to fix the problem by simply resetting the device. If a reset does not resolve the issue, the support technician can deliver a replacement thin client, and the user is up and running again. Typical thin client devices have a fraction of the moving parts that a traditional PC or laptop has. Therefore, the mean time between failures for these devices is very high. In the long run, the simplicity of these devices leads to fewer support calls related to hardware failure.

## Resources

- "The challenges of desktop management"  
<http://it.toolbox.com/blogs/enterprise-design/the-challenges-of-desktop-management-8498>
- "Challenges of remote desktop management"  
<http://www.computerweekly.com/Articles/2008/07/01/231314/challenges-of-remote-desktop-management.htm>
- "Cloud security will supplant patching, says report author"  
<http://www.networkworld.com/news/2009/050409-cloud-security-will-supplant-patching.html>
- "Companies still dragging their feet with patches"  
<http://www.networkworld.com/news/2009/042809-companies-still-dragging-their-feet.html>
- "Creating a Patch and Vulnerability Management Program"  
<http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>
- "Essentials of Patch Management Policy and Practice "  
<http://www.patchmanagement.org/pmessentials.asp>
- "Image Engineering"  
<http://technet.microsoft.com/en-us/library/bb456442.aspx>
- "Laptop & PC Backup"  
[http://www.peersoftware.com/solutions/data\\_retention/laptop\\_pc\\_backup.aspx](http://www.peersoftware.com/solutions/data_retention/laptop_pc_backup.aspx)
- "Microsoft Solution Accelerator for Business Desktop Deployment 2007"  
<http://technet.microsoft.com/en-us/library/bb490308.aspx>
- "Update Management"  
<http://technet.microsoft.com/en-us/library/bb466251.aspx>
- *VMware View Manager Administration Guide*  
[http://www.vmware.com/pdf/viewmanager3\\_admin\\_guide.pdf](http://www.vmware.com/pdf/viewmanager3_admin_guide.pdf)

## About the Authors

Joseph Horsey is a staff systems engineer at VMware based in Atlanta, Georgia. He has been with VMware for four years and has more than nine years of experience architecting and selling desktop and server management solutions.

Anjan Srinivas is a senior technical marketing manager in the desktop business unit at VMware. Srinivas' time is primarily spent in developing content and customer architectures that help customers adopt View. In the past Srinivas worked for Cisco Systems and Aruba Networks.

Revision: 20090709 Item: IN-098-PRD-01-01



**VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 [www.vmware.com](http://www.vmware.com)**  
© 2009 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,961,941, 6,961,806, 6,944,699, 7,069,413; 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, 7,356,679, 7,409,487, 7,412,492, 7,412,702, 7,424,710, 7,428,636, 7,433,951, and 7,434,002; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

