The Business Case for Desktop Virtualization

INFORMATION GUIDE

Why Choose VMware View?

Are You Considering Virtual Desktops?

Introduction

The end user computing landscape is evolving from an environment based primarily on personal computers running Windows applications to an environment where users:

- Move between endpoint devices during the work day (desktop computers, laptops, tablets, and cell phones)
- Expect to be able to stay connected to their professional and personal networks via mobile electronic devices
- Want their data to be available from any of their devices
- Want their applications to be available from any device. These applications include not only legacy Windows applications, but also web applications, SaaS applications, and server-based applications.

In this mobile user- and device-centric environment, IT must protect data security and control user access to data at the same time as it manages the range of applications and devices for all users. The single operating system and single device per user is a model of the past. VMware offers an end user computing solution that meets the challenges of providing for a mobile workforce, without compromising IT control or the operational efficiencies of existing management processes. VMware products incorporate the needs of both IT and end users.

Video: Building the Platform for the Post-PC Era. Vittorio Viarengo, Vice-President of Desktop Product Marketing at VMware, gives an overview of the VMware End User Computing vision for the journey to the cloud.

Why Choose VMware View?

Are You Considering Virtual Desktops?

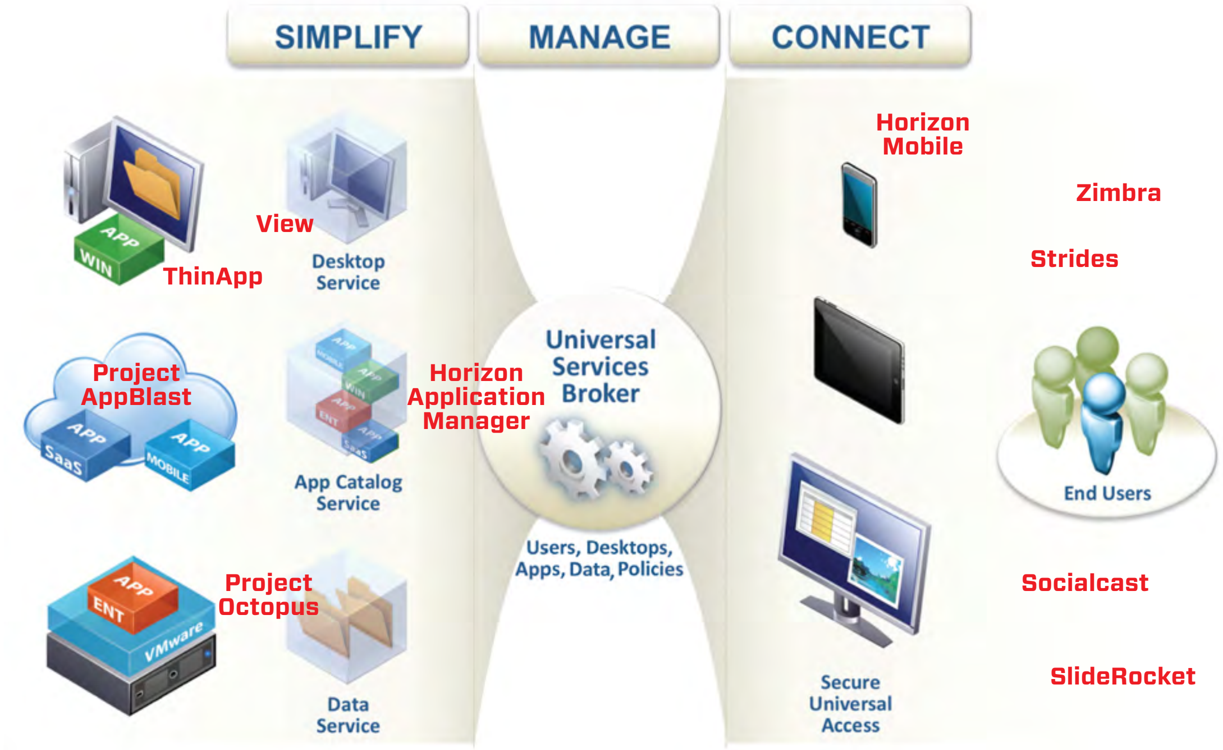

Figure 1: VMware End User Computing Journey to the Cloud

In this diagram of the VMware End User Computing journey to the cloud, end users have secure universal access via their chosen devices to their desktops, applications, and data in the cloud. A universal services broker connects users to this cloud with policies that control access and protect data.

At VMworld 2011, VMware announced this vision for the post-PC era. The vision recognizes the need to deliver legacy Windows and enterprise client/server applications alongside newer application technologies.

Why Choose VMware View?

Are You Considering Virtual Desktops?

VMware has a product for each of the steps of the End User Computing journey to the cloud. Some of these products are part of the VMware product set already, and others are under development. Following are the specific VMware products:

- **VMware View:** Virtual desktops as a managed service
- **VMware ThinApp:** Virtual applications as a managed service
- **Project AppBlast:** HTML5-based delivery of legacy applications via a web browser
- **Project Octopus:** Secure data share and sync
- **Horizon Application Manager:** Now, policy-based management of applications (SaaS, web applications, ThinApp virtualized Windows applications, and enterprise applications). Soon, policy-based management of all public and private cloud services (desktops, applications, and data).
- **Horizon Mobile:** A secure, managed, and policy-driven virtual smartphone for work, isolated and protected inside a personal smartphone

Cloud-based social/collaborative applications, designed for mobility:

- **Zimbra:** Open-source email and collaboration
- **Strides:** Social task management
- **Socialcast:** Enterprise social networking
- **SlideRocket:** Online presentation software

Why Choose VMware View?

Are You Considering Virtual Desktops?

The first step in the journey to the cloud is to integrate VMware View and ThinApp into your datacenter. View is the broker between end users and the cloud of desktops, applications, and data.

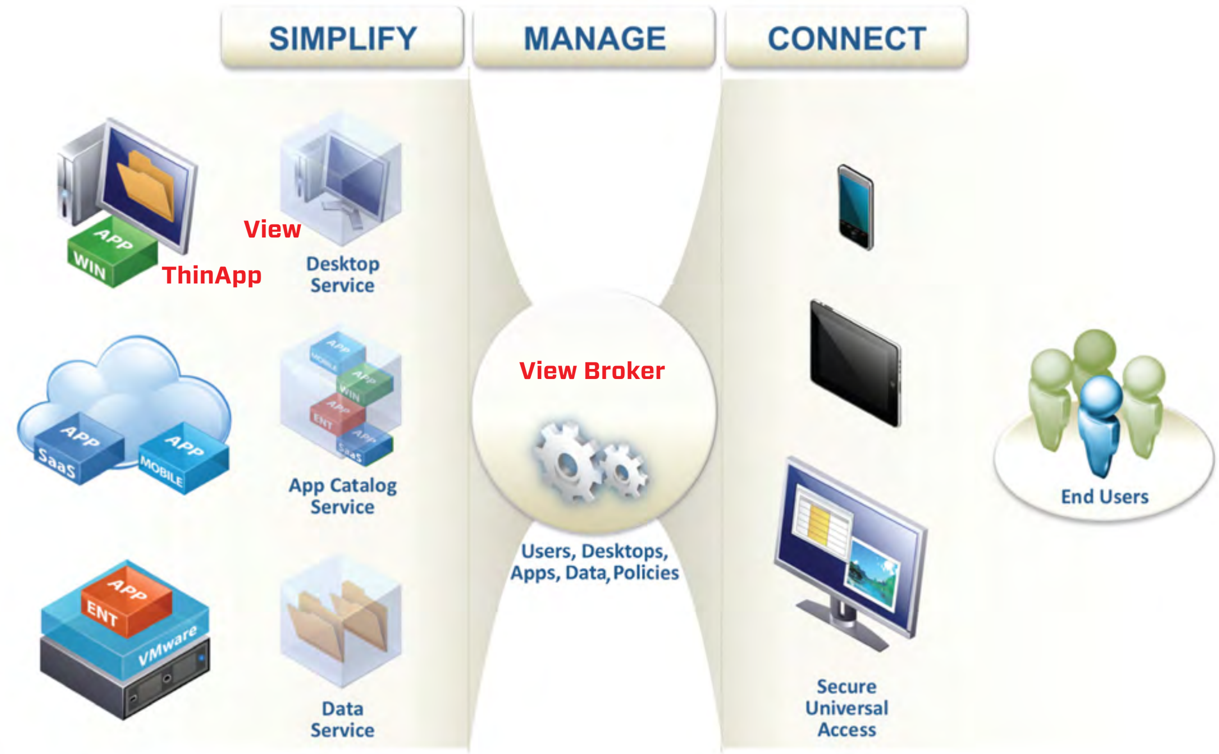

Figure 2: The First Step in the End User Computing Journey to the Cloud

Video: VMware View 5.0 and End-User Computing. Chris Young, former Vice-President and General Manager, End User Computing, VMware, discusses how the new version of VMware View meets the needs of IT and end users.

Why Choose VMware View?

VMware's journey to the cloud for End User Computing satisfies the needs of both IT and end users:

- IT is concerned with security, compliance, and efficiency of the desktop and needs to manage and set policies for users, applications, and data
- End users, in local and remote offices and working from home or while traveling, require access to their data and applications from a large variety of mobile devices

Built on the industry-leading virtualization platform, VMware vSphere™, VMware View enables you to deliver virtual desktops to any device with all the benefits of centralized enterprise desktop management. You can deploy desktop instances rapidly from secure datacenters 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.

The key benefits of VMware View to keep in mind are:

- The power of the underlying VMware infrastructure, vSphere, with all of its functionality
- Ease of setup and management: one management console
- PCoIP remote desktop protocol: optimized out of the box to give you high performance over a LAN or WAN, with automatic adjustment to network speed and latency
- Integrated user profile management system (View Persona Management)
- Application virtualization software (ThinApp)
- Offloading of antivirus protection to a virtual appliance (vShield Endpoint)
- Management of linked-clone desktop images (View Composer)
- Access to View desktops from all popular mobile devices: Windows and Mac laptops, Android tablets, and iPads

By including VMware's application virtualization software, ThinApp, with your View implementation, you not only eliminate typical application compatibility issues, but also deliver a more reliable computing environment. As an added bonus, View and ThinApp are compatible with your existing automated distribution technologies for application and patch deployment.

> *"Understanding that our clinical delivery teams are one of the most mobile set of users, I knew we had to look outside the traditional desktop delivery method. Having the ability for your desktop to securely follow you anywhere, while providing an uncompromised desktop experience, was a crucial requirement in making the decision to go with VMware View. When cost saving is an outcome, that makes my decision even easier."*
>
> – Trevor Derkatz, CIO,
> Prairie North Health Region,
> Saskatchewan, Canada

Why Choose VMware View?

Are You Considering Virtual Desktops?

Are You Considering Virtual Desktops?

This paper is for business decision-makers who are currently considering a virtual desktop implementation so they can continue their journey to the cloud. The focus is on time you can save in desktop administration by deploying a VMware View solution. Staff time saved in desktop management can be applied to other projects on your roadmap.

When is the right time to take the virtual desktop step? Many organizations find that instead of refreshing obsolete physical computers with new desktop computers, they can instead divert funds to a virtual desktop implementation. Legacy hardware can be repurposed as client devices, or you can purchase less expensive thin clients. The remaining funds can be devoted to the virtual desktop implementation.

The Numbers

Return on investment: IDC (Table 2) found a 367% median five-year return on investment (ROI) with a VMware View implementation. The payback period, the point at which dollars invested were equal to dollars saved, was 5.61 months following deployment.

Cost of infrastructure and labor: The cost of infrastructure and labor for a VMware View implementation is 50% of the cost for a physical PC implementation (IDC, Figure 3). (This is the average cost over a five-year period and includes user devices, hardware and software infrastructure, and labor.)

Labor costs: With the infrastructure costs eliminated from the equation, labor costs are reduced by approximately 57% per user per year with a VMware View virtual desktop implementation, compared to physical desktops (IDC, Table 1 *). This paper focuses on the labor saved with a VMware View implementation.

> *"We wanted to find a solution that didn't require us to stay on that three-year refresh cycle to keep up with student technologies and student application needs... we were able to take all of the money that we would use for desktops and apply them towards a server and VMware View infrastructure. We were able to continue using our old hardware and really prolong the life of that hardware."*
>
> – Matt Byers, Systems Administrator, SunGard Higher Education at Seattle University, Seattle, Washington

Video: Seattle University. Seattle University moved to a VMware View virtual desktop solution instead of replacing obsolete physical desktop computers. The IT department repurposed legacy hardware as View Clients. In addition, they provided students with the ability to access their data and applications from their own devices, from wherever they are.

Why Choose VMware View?

Are You Considering Virtual Desktops?

This discussion outlines the challenges in current desktop management processes and then describes how a View implementation can change these processes and save time. These recommendations are based on VMware best practices and on the experiences in successful customer deployments of View.

We will frequently refer in this paper to a study carried out by IDC: Quantifying the Business Value of VMware View. This study focused on a set of VMware View customers who have reaped the financial benefits of a View virtual desktop implementation. *

Video: Improving the Physician Experience Through Desktop Virtualization, Metro Health. Metro Health in Michigan implemented a VMware View solution delivered in partnership with Open Systems Technologies. The video showcases the mobile end user experience of Dr. Bradley J. Clegg, DO, Metro Health Hospital.

> *"With VMware View, I can honestly say that there are months that go by where I don't have to think about the infrastructure because it just works. The scalability and the performance are really there, and I am very grateful not to have to worry about it."*
>
> — Chris House, Senior Network Analyst, Metro Health, Michigan

* Total hours spent per desktop in a traditional PC implementation were calculated from IDC figures given in Table 1 of the May 2011 version of Quantifying the Business Value of VMware View. The figures used in the calculations were 1) labor hours saved with View and 2) the percent reduction in labor required for View, as compared to a traditional PC infrastructure. Related rows in the IDC table were combined to result in the larger categories discussed in this paper.

Managing Traditional Personal Computers

Although the capital expenditure required for traditional personal computers and storage has decreased over time, the operational cost of managing individual physical desktop computers has increased because of rising labor costs and the escalating complexity of desktop maintenance tasks. The operational cost of personal computing is the most sensitive area of expenditures for IT departments, and this is also the area where a VMware View virtual desktop implementation can reduce the total cost of ownership.

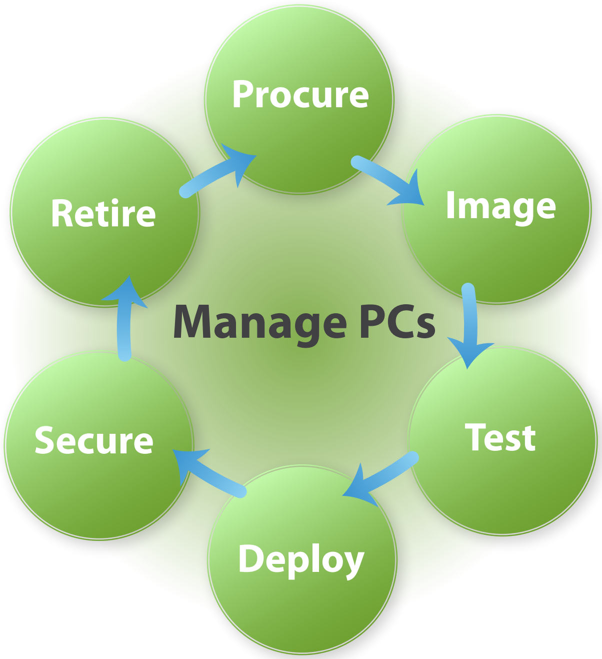

Figure 3: Managing the Personal Computer Lifecycle Stages

The repeating stages of a personal computer life cycle, as illustrated, are:

- Procure
- Image
- Test
- Deploy
- Secure
- Retire

The management of the physical PC life cycle consumes a great deal of time for IT departments. A VMware View virtual desktop solution can shortcut and even eliminate some of this desktop management and thereby reduce the operational costs of desktops. With a virtual desktop solution, the amount of time saved per desktop is multiplied by hundreds or thousands of users.

The Advantages of Virtual Desktops

We will discuss each of the following desktop management activities with regard to the cost challenges and how a VMware View virtual desktop solution can relieve those costs:

- Desktop hardware and software deployment
- User administration
- Image and application management
- Desktop patch management
- Desktop data security
- Desktop disaster recovery and data backup
- Desktop help desk and support

Desktop Hardware and Software Deployment

Most enterprises have a heterogeneous desktop computing landscape, with a mix of different hardware types, peripheral devices, drivers, screen resolutions, applications, and application versions. A single IT organization typically supports the configuration and rollout of hardware and software in this mixed environment.

Current Challenges of Desktop Hardware and Software Deployment

Deploying a desktop computer to each user involves ordering, receiving, tagging, and checking the computer, and then configuring applications and corporate settings. Testing and securing the desktop computer add to the deployment time. After the user receives the desktop computer, more time is spent in initial setup and support until the new computer is fully productive for the user.

Virtualization Impact on Desktop Hardware and Software Deployment

The time difference between configuring and deploying a physical desktop and deploying a virtual desktop to a user is significant. For example, with View, it can take only eight minutes to deploy a View virtual desktop to a user. The process of copying a virtual image and assigning it to a user is much faster and more foolproof than setting up an individual physical desktop. In addition, you can repurpose legacy hardware to access the virtual desktop image. This extends the useful life of the hardware, reduces the initial cost of desktop virtualization, and results in a user device that is simpler to maintain than a physical desktop.

Time Saved in Deploying a Desktop to a User with VMware View

Traditional Physical PC Implementation *	Time Saved per User per Year with VMware View **	Percent Reduction in Labor Costs **
.78 hours	**.51 hours**	**65%**

* Calculated from IDC figures ** From IDC figures

Provisioning: The process of providing users with access to data and technology resources.

– Webopedia.com,
14 February 2012

"With View Composer, we can create new desktops on the fly. If we have a Wyse terminal ready to go, it takes us about 15 minutes to create a new desktop, whereas before, it was taking us two to three hours to load a desktop image. That makes IT much more responsive to the overall needs of the organization."

—John Meharg, Director of Health Information Technology, Norman Regional Health System, Oklahoma

Desktop Hardware and Software Deployment

User Administration

Image and Application Management

Desktop Patch Management

Desktop Data Security

Desktop Disaster Recovery and Data Backup

Desktop Help Desk and Support

User Administration

Maintaining and managing user profiles and logins takes a good deal of IT management time. The time savings with virtual desktops is significant.

Current Challenges of User Administration

Users join an organization, change roles, change user account data, and leave the organization. User administration on desktops involves creating user accounts and changing user accounts to accommodate office moves, departmental transfers, and departures from the organization. Maintaining policies within Active Directory for application entitlement adds to the complexity of user administration. The IT group has a constant flow of work to maintain user accounts on physical desktops.

Virtualization Impact on User Administration

User administration is simplified with a View deployment. View provides an easy-to-use administrative interface to assign desktops to Active Directory users. In addition, desktop administrators do not need to physically visit the desktop; they can simply change parameters of desktop assignment from the datacenter.

Time Saved in User Account Administration with VMware View

Traditional Physical PC Implementation *	Time Saved per User per Year with VMware View **	Percent Reduction in Labor Costs **
1.31 hours	**.89 hours**	**68%**

* Calculated from IDC figures ** From IDC figures

> *"What probably used to take us two to three weeks from procurement to provisioning of a system, now we can do in five to ten minutes. It used to take us probably an hour or two to customize and tailor for an associate. Now we can do that as well in just several minutes."*
>
> —Shane Martinez, Director of Global Infrastructure, ADP Dealer Services, Illinois

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 downtime and mitigating any potential user data loss.

Current Challenges for Image and Application Management

Desktop images configured for end users are not usually tailored for specific 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. The need to standardize management of physical desktops can result in a "one-size-fits-all" approach, where a common image is used to support multiple job roles. The result is that most users have a more complex image and more applications than they need.

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 need to develop can grow very quickly. The operational costs of desktop imaging and reimaging are significant, which further drives the "one-size-fits-all" approach.

You face a similar challenge when you need to migrate to a newer desktop operating system. Many organizations are migrating to the Windows 7 operating system. The migration from Windows XP to Windows 7 in a physical environment is time-consuming and expensive.

The processes of upgrading and migrating operating systems, as well as packaging, testing, and provisioning applications, can burden an organization so much that they remain years behind the available technology. In addition, end users can be tied to devices and images that may be obsolete for their job roles.

Virtualization Impact on Image and Application Management

When you implement a remote desktop strategy based on VMware 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:

- Operating system
- Applications
- User data and user persona

To manage the operating system layer of the desktop image, VMware View provides the choice between nonpersistent and persistent desktops. View Composer is an option to manage linked-clone desktops.

To manage applications, the best choice is to virtualize as many applications as possible with VMware ThinApp and to place those virtual application packages on the VMware View base images.

To manage the user data and user persona, you can use View Persona Management.

> *"Right now, we've got over 1,700 desktops and laptops out around the college with different images on them. With VMware View, we can have one 'golden image' instead of having to manage 30 to 40 different images—and that makes turnaround time for updates on drivers and software much quicker."*
>
> —Dave Hunter, Associate Director,
> IT Services, Red Deer College,
> Red Deer, Alberta, Canada

Application Virtualization with ThinApp

To further simplify desktop management, you can virtualize the application layer with VMware ThinApp. ThinApp virtual application packages separate the application from the operating system layer by encapsulating a virtual operating system within the ThinApp package. A ThinApp package is not installed in the operating system, but instead placed on the desktop as an isolated executable. As a result, ThinApp application packages do not conflict with each other in ways that native applications can.

A July 2010 Forrester Research report on the economic impact of ThinApp application virtualization presents a case study of a ThinApp implementation with a risk-adjusted payback period of one year and a return on investment of 185% over four years. The customer in the case study cited the following economic benefits:

- Faster application packaging
- Decreased or eliminated regression testing
- Faster application and update deployment
- Reduction in or elimination of level one and level two help desk calls
- Increased user productivity

You can take one of two approaches to distributing ThinApp executables to users:

- **Streaming** execution mode, where the user launches the ThinApp virtualized application from a desktop shortcut. Blocks of application data are streamed from a central file share into memory on the desktop for local execution. There is no disk footprint on the desktop for the virtualized application.
- **Deployed** execution mode, where the user runs the ThinApp virtualized application from a copy of the ThinApp executable placed on the desktop

You choose streaming or deployed execution mode based on the needs of your users and the speed and latency of the users' network connections.

> *"Once an application has been virtualized with VMware ThinApp, it's very, very predictable. We know we can be confident that we will not have to go back later and fix things."*
>
> —Dewand Neely,
> Tier 3 Support Manager,
> Indiana Office of Technology,
> Indiana state government,
> Indianapolis, Indiana.
> Indiana Office of Technology Drives Cost-Effective Application Management with VMware ThinApp.

In a View environment, you create a central file share, or ThinApp Repository, to store your ThinApp virtualized applications. Figure 3 shows the ThinApp Repository connected to View Composer. You can copy ThinApp packages from the repository to the parent image so that each linked clone has the virtualized applications on the desktop, or each linked clone can have desktop shortcuts to run the applications in streaming mode from the repository.

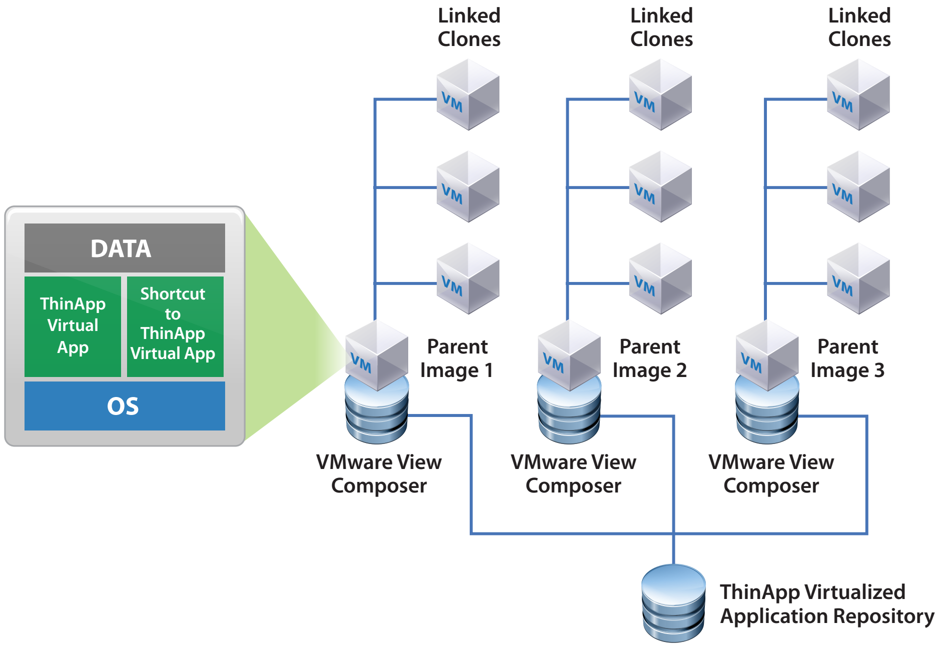

Figure 4: View Composer Adds ThinApp Packages to Desktops

The ideal in a VMware View implementation is to have as many of your applications as possible virtualized with ThinApp. You can easily mix “native” Windows applications with ThinApp virtualized applications on the View desktop. Fortunately, ThinApp applications can be managed through the same tools and processes as your native Windows applications, and you can take advantage of the efficiency of your current application management system.

By virtualizing applications, you also gain a dynamic mechanism to roll out new or patched versions of an application. For streamed applications, you substitute the updated package for the original on the ThinApp Repository. For applications residing on the parent images, you can use the ThinApp AppSync feature and place an updated application on an update server in the datacenter, and users automatically download the new version of the application.

VMware ThinApp is especially suited to migrating applications to a new version of the Windows operating system, such as Windows 7 or later. Your VMware View Windows 7 desktops can include ThinApp packages of legacy applications. If an application is supported on the later version of the operating system, you can virtualize the legacy application and run it on a Windows 7 desktop. In addition, with ThinApp, you can virtualize Internet Explorer 6 along with a legacy application that runs only on IE6, and run that virtualized application on Windows 7. The natively installed Internet Explorer browser runs alongside the virtualized IE6 browser on a Windows 7 desktop.

Customers in the IDC study said that the centralized packaging, testing, provisioning, and updating of applications in a VMware View implementation was the reason for the cost savings in application support. These benefits are magnified when desktop applications are virtualized with ThinApp.

Time Saved in Managing Applications on the Desktop with VMware View

Traditional Physical PC Implementation *	Time Saved per User per Year with VMware View **	Percent Reduction in Labor Costs **
2.62 hours	**1.41 hours**	**54%**

* Calculated from IDC figures   ** From IDC figures

> *“VMware ThinApp has helped us keep our legacy applications functioning and move forward with new technologies, even when we are faced by budget constraints.”*
>
> —Paul Baltzell,
> Deputy CIO Delivery Services,
> Indiana Office of Technology,
> Indiana state government,
> Indianapolis, Indiana

Desktop Hardware and Software Deployment
User Administration
Image and Application Management
Desktop Patch Management
Desktop Data Security
Desktop Disaster Recovery and Data Backup
Desktop Help Desk and Support

Rolling Out New Base Images of Operating Systems and Applications

VMware View provides the options of nonpersistent (stateless) and persistent (stateful) desktops, as well as View Composer to manage linked clones. The View image management system provides options to meet your organization's needs.

If you are migrating to a new operating system version, such as Windows 7 or later, you can use View Composer and the Recompose function for a much simpler transition. You can build the new desktop image to include virtualized applications to separate the applications from the operating system.

VMware View desktops based on master images stored in the datacenter can be easily distributed to remote or branch offices, without the need for desktop administrators to travel.

View customers in the IDC study said that the reduction in the number of images, plus the faster time to change each image, were instrumental in reducing the operational costs of imaging in a View environment. For example, one View enterprise user in the IDC study found that a desktop reimage took 5 minutes with View, but 120 minutes with the traditional imaging approach.

Time Saved in Desktop Imaging with VMware View

Traditional Physical PC Implementation *	Time Saved per User Per Year with VMware View **	Percent Reduction in Labor Costs **
2.13 hours	**1.26 hours**	**59%**

* Calculated from IDC figures   ** From IDC figures

> *"With VMware there is a lot of cost savings that people overlook. One of the biggest things that I can say about VMware, and it's just flabbergasting, is that it used to take two technicians three to four days to set up a lab of 40 thick machines, and now it takes one technician three hours. Software upgrades or new installations can be pushed out in two hours, as opposed to eight hours for a lab of 100 machines."*
>
> —Georges Khairallah,
> Network Specialist,
> Chino Valley Unified School District,
> Chino, California

Desktop Hardware and Software Deployment

User Administration

Image and Application Management

Desktop Patch Management

Desktop Data Security

Desktop Disaster Recovery and Data Backup

Desktop Help Desk and Support

User Data and User Persona in a View Environment

VMware provides user data and persona management with View Persona Management. With Persona Management, you can store persistent user profile information and user data in a separate location from the desktop image and optimize performance by taking advantage of the access and update algorithms of View Persona Management.

Persona Management downloads user profile information on an as-needed basis, thus avoiding login bottlenecks. In addition, updates to user data and the user persona are uploaded on an intermittent basis to the persona repository, which avoids a logout bottleneck. For more information on implementing View Persona Management, see the VMware View Persona Management Deployment Guide.

View Persona Management was not in place when IDC did their study, so we have no figures yet for the savings in labor time with View Persona Management.

Video: ADP Dealer Services, Illinois. ADP Dealer Services, a division of ADP (Automatic Data Processing), offers human resource, payroll, tax, and benefits administration to automobile dealerships. In this video, Bill Naughton, Chief Information Officer, and Shane Martinez, Director of Global Infrastructure, discuss their VMware View implementation. View desktops are used in remote locations, on mobile devices, and in call centers by software developers and end users.

Desktop Patch Management

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

Current Challenges for Desktop Patch Management

Both operating systems and applications need to be patched to keep up with security enhancements, bug fixes, and more. The basic process workflow that most organizations follow or attempt to follow when they implement patch management is the following:

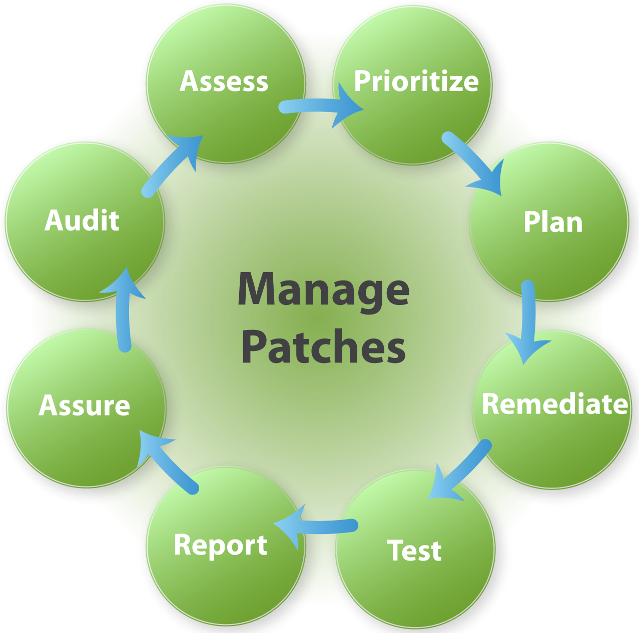

Figure 5: Managing the Patch Maintenance Stages

This repeating process of Assess, Prioritize, Plan, Remediate, Test, Report, Assure, and Audit can be complex and subject to many challenges, which reduces the effectiveness of the patch management process. The number of vulnerabilities that hackers exploit each year increases at a rate that is too fast for IT administrators to remedy. As the number of necessary patches increases, the time needed to patch all desktop systems in an organization expands, and by the time one patch or set of patches is rolled out, other vulnerabilities are exposed, which also need to be patched.

The distributed nature of desktop and laptop computers has made centrally managed software distribution mechanisms an important part of the IT infrastructure in many organizations. Usually these solutions are highly distributed in nature and 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 patch management is, and the lower the first-pass success ratio. If you need to deliver patches and service packs to desktops at remote branches or regional offices where network connectivity is limited, you can encounter connectivity issues, and it will take much longer to deploy the updates. Some user systems never receive patches because of infrequent connection to the network.

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 other applications. This process is time-consuming and subject to failure. After PCs are deployed to users, they are subject to significant configuration drift. This configuration drift can be attributed to user-initiated hardware replacements, hardware 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. 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 of the user's desktop and to back out the changes.

With all of these complexities, it can take a very long time to patch all of the computers in your organization. The delays make it difficult to maintain adequate enterprise security, and the cost of remediating the gaps in security is significant. The traditional patch management process involves high IT labor costs and notable user downtime and inconvenience.

Virtualization Impact on Desktop Patch Management

Implementing a virtual desktop 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 by using the tools that a View solution provides. In a typical View environment, updates you apply to a single parent virtual machine instance automatically affect multiple end-user desktops. As a result, you spend less time patching and can update more end-user desktops on the first pass.

View Composer offers enhanced image management in a View environment. As shown in Figure 6, the View Composer technology 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 Composer provisions a desktop to each end user by creating a linked clone based on the appropriate parent image.

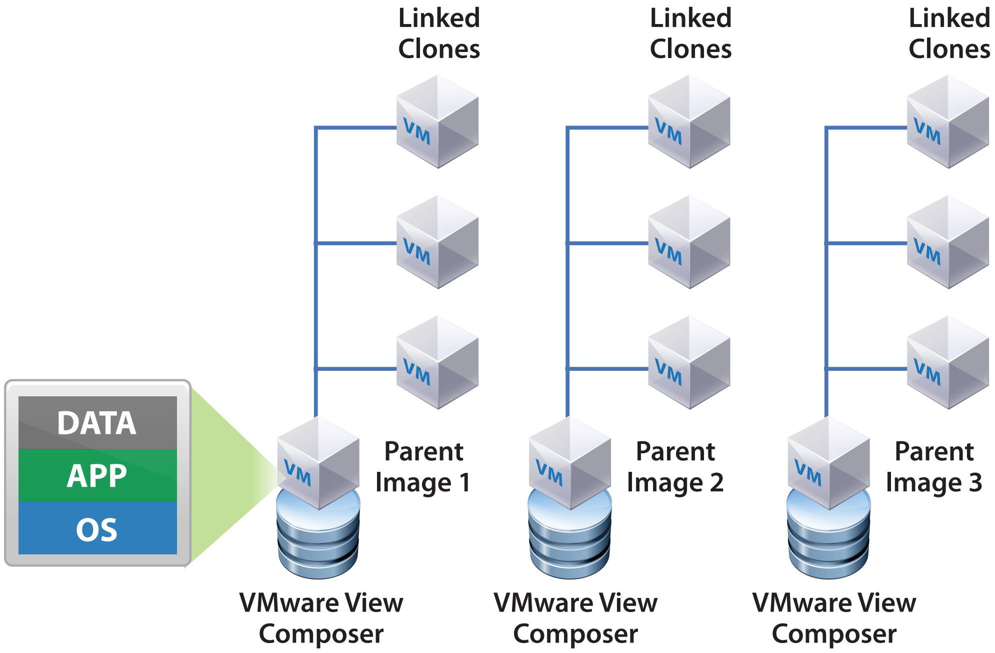

Figure 6: End-User Linked-Clone Desktops Based on Parent Images

Desktop Hardware and Software Deployment
User Administration
Image and Application Management
Desktop Patch Management
Desktop Data Security
Desktop Disaster Recovery and Data Backup
Desktop Help Desk and Support

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 on a persistent disk that is unique to that desktop. Future reads come from the desktop's persistent disk, or from the rebuilt desktop image, as appropriate.

View Composer gives you management functions for these linked-clone desktops, including Refresh, Recompose, and Rebalance:

- **Refresh:** The Refresh operation allows you to revert a linked clone desktop to its original deployment state.
- **Recompose:** The Recompose function allows you to migrate an end user from one desktop to another, maintaining the user's persistent disk and making the user data available to the user from the new desktop.
- **Rebalance:** 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.

For more information on Refresh, Recompose, and Rebalance, see the VMware View Administration guide.

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 manage all of these parent images directly. Because parent images are in the datacenter, you avoid the problems that the traditional patching process encounters, such as network latency and bandwidth issues, and 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 in a View implementation. This way, your current, standardized operations are not affected. 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 patching priority to categories of desktops based on how critical the desktops are to your business, rather than with the traditional broadcast approach.

Video: Blue Cross Blue Shield of Kansas City, Missouri. This video highlights some of the benefits of a VMware View solution: the power, space, and cost savings; disaster recovery; and View Clients on mobile devices such as iPads.

After you update the parent images and validate the patches, one administrator can run a scheduled Recompose operation for all of 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 rollback 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 access, forcing users off of their desktops in the event that you need to apply a critical patch immediately.

Customers in the IDC study stated that the locked-down image of Windows on the desktop made patching much easier.

Time Saved in Patch Management with VMware View

Traditional Physical PC Implementation *	Time Saved per User per Year with VMware View **	Percent Reduction in Labor Costs **
.77 hours	**.50 hours**	**65%**

* Calculated from IDC figures   ** From IDC figures

In addition, we have already mentioned the ease of updating applications with VMware ThinApp. Either with copies of the ThinApp packages on the View base images, or with desktop shortcuts to virtualized applications stored on the ThinApp Repository, ThinApp provides a means of updating applications automatically, without interruption to application use. Either way, updated versions of applications are centralized, and you can enforce user migration to the updated versions.

Desktop Data Security

As frequent news reports attest, lost laptop computers and compromised desktop PCs can endanger 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. Both unauthorized access to data in the datacenter and data loss through theft or loss of the desktop device must be prevented.

Current Challenges with Desktop Data Security

To prevent unauthorized access to datacenter data through laptops, some organizations implement disk-based encryption solutions that can be costly and difficult to scale.

Also, with an increasingly mobile and remote workforce, laptops and other devices are easily lost or stolen. Employees may also copy data to USB flash drives and remove data from the company site. USB flash drives can also introduce viruses, which can corrupt data.

If a security breach or leak occurs in an organization, the productivity lost and the cost to fix the breach are significant.

Virtualization Impact on Desktop Data Security

The immediate improvement that a virtual desktop solution offers for data security is that you store all data in virtual machines that are hosted in 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 store data locally. IT can meet expectations about security and compliance with regulations.

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, iPhones, or other USB-based personal devices to their desktops, thereby reducing the opportunity for data leaks. By restricting use of USB devices, you can also mitigate concerns about the introduction of malicious software.

For users who are not always connected to the corporate network, VMware View includes a feature called View with Local Mode. Local Mode allows end users to check out their desktops—including applications and data—from the datacenter to their local devices. This instance of a user 's desktop is encrypted. If the user loses the laptop computer, or the laptop is stolen, the data on the missing device is encrypted and has a remote-erase setting that disables it if it does not communicate to the corporate network within a specified amount of time.

You also have the option of including VMware vShield Endpoint in your View deployment, to manage antivirus scanning. The vShield Endpoint product handles antivirus scanning of View desktops from a centralized virtual appliance. See the VMware website for more information about vShield Endpoint.

Customers in the IDC study stated that the cost savings in security were largely due to the ability to push patches onto desktop images without waiting for individual machines to be available. The benefits of vShield Endpoint were not yet available at the time of the IDC study.

Time Saved in Security Administration with VMware View

Traditional Physical PC Implementation *	Time Saved per User per Year with VMware View **	Percent Reduction in Labor Costs **
.80 hours	**.24 hours**	**30%**

* Calculated from IDC figures ** From IDC figures

> *"Security is very important. Being in healthcare, we want to make sure that we have no information whatsoever residing on the local machine. With VMware, our Security Department gets to manage security in the way they need to, and at the same time,our policies are kept…in place, and also our responsibilities with HIPAA [Health Insurance Portability and Accountability Act] and the federal regulations are completely in compliance as well."*
>
> —Greg Wolverton,
> Chief Information Officer,
> ARcare healthcare, Arkansas

Desktop Disaster Recovery and Data Backup

Disaster recovery plans for end-user devices can be highly costly, so some organizations focus on server disaster recovery plans and neglect recovery plans for desktops. End users must often implement their own desktop and laptop backup solutions if they want to protect against a severe failure or data corruption. And few users are diligent about their backups.

Current Challenges for Desktop Disaster Recovery and Data Backup

If an organization is hit by a disaster that causes its servers to fail over to a disaster recovery location, end users need access to the applications running on those servers. In addition, users need to connect to centralized data stored at the recovery location. A disaster recovery plan must connect end users to the recovery infrastructure so that they can continue being productive.

Another disaster scenario is the failure or theft of an end user's physical desktop. In an environment that relies on hardware-dependent end-user desktops, the cost and complexity of recovery can be prohibitively expensive and subject to limited success. Desktop backup strategies provide one method of desktop recovery, but few backup plans are fully implemented or accepted. The goal is to be able to recover a user's critical documents, files, applications, and personal settings. Most organizations that attempt this approach have to invest in agent-based backup solutions that they install on every desktop and laptop.

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 may cancel the processes and quit the backup agent window. In some cases, if users have administrative access to their PCs and are savvy enough, they can disable the backup agents on their PCs. If they lose their laptops, or their desktop hard drives fail, 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 Desktop Disaster Recovery and Data Backup

Implementing a VMware View desktop strategy can help you to achieve efficiencies in disaster recovery. These efficiencies are evident both in recovery of desktop connections to an alternate datacenter location, as well as recovery of desktop images.

Management of View virtual desktops by VMware vSphere and vCenter is key. One 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 easily replicate both the desktop and the server virtual machines to your disaster recovery site. You can use this approach in conjunction with a solution such as VMware Site Recovery Manager to fully automate the 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 of 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.

The time and productivity savings in these areas are significant with a VMware View solution. IDC has not yet calculated the time saved for disaster recovery and data backup in a View implementation.

> *"It's not just the initial cost of hardware, it's also that the failure of that hardware takes quite a bit of time to troubleshoot and fix—not to mention the possibility of losing data, say if somebody drops a laptop. With VMware View, we can reduce hardware dependency and store all that data in a protected datacenter. That's good for the user and good for the company, since it will mean we won't have sensitive data wandering around on desktops and laptops and USB keys. And because a virtual desktop is an appliance, if a device fails, we can swap it out and get the user back up and running very quickly. We can even tie it in with [VMware vSphere] Site Recovery Manager to enable more dynamic recovery, so if we lose a call center in one location, its data is protected and we can start up again in another."*
>
> —Tom Van Harn, Systems Support Advisor, Amway, regarding the security and disaster recovery benefits of moving from physical desktops to VMware View virtual desktops

Desktop Help Desk and Support

As a result of implementing a VMware 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 struggle constantly to meet established service level agreements for desktop end users. Help desks that support desktop users focus on minimizing the mean time to resolution (MTTR) when a user's desktop fails. A lower MTTR reduces the amount of time that end users are not being productive.

End users usually present IT with a problem, but not a cause. Common user issues include obsolete hardware, faulty hardware, application failures, lack of network connectivity, and viruses and malware. Only by communicating with the end user and discovering the cause can the desktop administrator solve the problem. More complex problems must be escalated to more experienced desktop administrators, which adds to the cost and delay.

The distributed nature of a desktop environment adds a level of complexity to desktop administration. End users may telecommute or work in remote offices or buildings, which can make desktop troubleshooting more difficult and more costly. Sometimes desktop administrators must travel to other buildings or sites.

Virtualization Impact on Desktop Help Desk and Support

By centralizing the desktops in the datacenter with VMware View, you bring the desktops closer to the desktop administrators. This eliminates the challenges of working with desktops in branch or remote 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.

Searching for a cause to the problem can be limited in time; if discovery takes more than five minutes, desktop administrators can simply provision a new desktop for the end user and deliver it over the network.

> *"Our department has lost 20 percent of its funding and staff in the past year. By using VMware View and HP Mobile Thin Clients, we've found a more cost-effective and efficient way to deliver computing resources to our students. We're containing our operating costs, while supporting 40 percent more machines. The desktops require less support, the teachers get a more reliable platform, and the students get a better educational experience. Everybody wins."*
>
> —Jeremy Woods,
> Technology Planning Coordinator,
> Ontario-Montclair School District,
> Ontario, California

For architectures that include the replacement of end users' PCs with thin clients or zero clients, support for these end-user devices is very simple. In many instances, end users themselves can install and set up their thin clients without a technical support engineer onsite. 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 productive 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 (MTBF) for these devices is very high. In the long run, the simplicity of these devices leads to fewer support calls related to hardware failure.

Time Saved in Desktop Help Desk and Support with VMware View

Traditional Physical PC Implementation *	Time Saved per User per Year with VMware View **	Percent Reduction in Labor Costs **
3.75 hours	**2.17 hours**	**58%**

* Calculated from IDC figures ** From IDC figures

Summary

The time saved in the management of user desktops is significant with a VMware View virtual desktop implementation. Time saved in desktop management means that your IT staff can devote themselves to other projects on your IT horizon.

A VMware View virtual desktop solution resolves many of the economic and user satisfaction issues of a desktop environment. A View deployment saves an average of 7 hours of labor per user desktop per year, out of 12.2 hours labor per user on a physical desktop per year. This is a 57% decrease in labor costs with a VMware View implementation. Multiply the 7 hours by your number of users, and the time available for other projects is a convincing argument for virtual desktops.

Time Saved in Desktop Management with VMware View Virtual Desktops

Desktop Management Task	**Hours Saved per User per Year**	**Percentage of Time Saved per User per Year**
Desktop hardware and software deployment	.51	65%
User administration	.89	68%
Application management	1.41	54%
Image management	1.26	59%
User profile management *	Not calculated by IDC	Not calculated by IDC
Desktop patch management	.50	65%
Desktop data security **	.24	30%
Desktop disaster recovery and data backup	Not calculated by IDC	Not calculated by IDC
Desktop help desk and support	2.17	58%
TOTAL time saved per user per year	**6.98 hours**	**57%**

Note: This total is a very conservative estimate of time saved with VMware View. It does not include the time saved with View Persona Management or vShield Endpoint antivirus protection.

* IDC has not yet studied the time saved with View Persona Management. ** IDC has not yet studied the time benefits of vShield Endpoint for antivirus protection.

In addition to the labor-saving benefits of desktop virtualization, View desktop virtualization solution is the first step in the journey to the cloud. By placing user desktops in the cloud along with ThinApp virtualized applications, you are poised to fill in the other VMware solutions for the post-PC era.

Additional Resources

Quantifying the Business Value of VMware View, IDC white paper, May 2011

Desktop Total Cost of Ownership: 2011 Update, Gartner research note, February 2011

10 Reasons to Modernize the Desktop, CIO Custom Solutions Group white paper

The Total Economic Impact of VMware ThinApp, Forrester Research study, September 2010

VMware View documentation

View Technical Resources: Decide, Design, Deploy

About the Authors and Contributors

Tina de Benedictis wrote the current version of this paper. Tina is a technical marketing manager in the End User Computing group at VMware. She writes papers on VMware View, ThinApp, and other enterprise desktop products.

Special thanks to Ridwan Huq and Brian Gammage for contributions to this version of the paper.

The authors of the original version of this white paper were Joseph Horsey and Anjan Srinivas. Joseph Horsey is currently a manager of systems engineering for VMware and has vast experience architecting and selling desktop and server management solutions. Anjan Srinivas was formerly a group product marketing manager for desktop products at VMware.

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

Copyright © 2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark 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. Item No: VMW-IG-BUSINESSCASE-USLET-20120302-WEB