The Strategic Guide to
VIRTUALIZATION
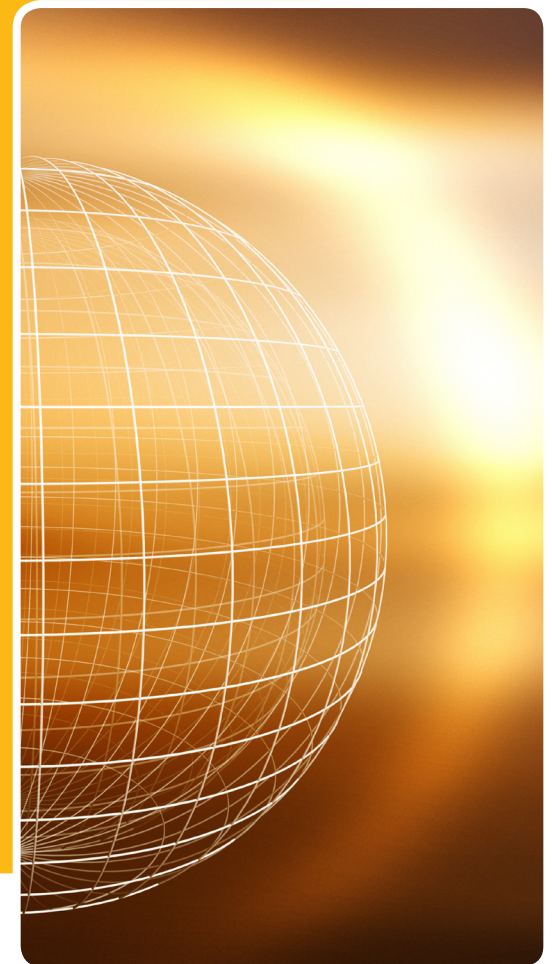
Complete the Promise of Virtualization

Confidence in a connected world.

symantec™

Virtualization: Simple concept, profound implications

Virtualization can help lower costs, and increase agility. It can also introduce new challenges and complexities in IT environments that are increasingly both physical and virtual. So, how can you ensure maximum return on investment (ROI) from your virtualization strategy, while preserving best practices for efficiency and cost savings?

This guide explores the opportunities and limitations you should be aware of as you implement virtualization - from the desktop to the data center - and is designed to help you make the best decisions for your organization.

Table of Contents

Virtualization promises to radically transform IT for the better by reducing costs and increasing agility. But without an effective strategy that addresses both physical and virtual environments, the benefits of virtualization can be offset by the challenges of new requirements that affect key service level processes such as backup, high availability, storage management, and endpoint management, to name a few.

This guide outlines best practices that help you manage and protect your physical and virtual environments - from the desktop to the data center – and deliver outstanding service to your business, and ultimately, to your customers.

Virtualization changes everything

Virtualization impacts many components in your IT portfolio and changes everything—from the way you make purchasing decisions to the way you implement technologies. The widespread adoption of virtualization is significantly altering IT management, deployment, licensing, and pricing. And with the availability and maturity of an increasing number of x86 and non-x86 virtual platforms, most organizations will need to plan for and manage multiple hypervisors.

Your virtualization strategy needs to include management solutions to address the new requirements that affect key service level processes in a heterogeneous physical and virtual environment.

Did you know?

• According to IDC, of the customers who are implementing virtualization in their data centers today, 22 percent have already virtualized their servers. That number is expected to increase to 45 percent by April 2009.[1]

• According to Gartner, "now that the hypervisor is becoming inexpensive and pervasive, the focus, business models, and costs are shifting to management tools." The rate of this change is more and more apparent in 2008 as the shift continues "from virtualization for consolidation, to virtualization management and agility through virtualization."[2]

• "For many organizations, the question is not if they will do a global rollout of x86 server virtualization, but when and who can provide them the service they need to make the rollout a success," said Matt Healy, research manager of IDC's Software and Hardware Support Services program.[3]

1 Brian Berliner, blog entry entitled "IDC Virtualization Forum West—Part 2," www.brianberliner.com, posted April 9, 2008.

2 Gartner, Inc., Server Virtualization Trends in 2008: Everything Changes; by Thomas J. Bittman; March 2008.

3 IDC, Worldwide Virtualization Services Spending 2007–2021 Forecast, August 2008, by Matt Healey, Cushing Anderson, John Humphreys, and Elaina Stergiades; August 2008.

Virtualization: The end of the beginning

Today, virtualization is not just a possibility—it is becoming mainstream in data centers across the business world. Technology is evolving at a rapid rate, and virtualization is no longer just about consolidation and cost savings.

It is about the agility and flexibility needed for service delivery in your data center, including your production environment and the infrastructure that supports your most mission-critical applications. You can no longer approach your virtual environment in a tactical and isolated way, but rather as a part of the overarching IT fabric. This means that your strategy needs to include plans for broader service-level and management factors to ensure long-term success.

Did you know?

According to IDC, recent surveys found that "over 50% of all customers virtualizing servers are employing the technology in support of production applications, including components of some of the most mission-critical applications…." Furthermore, "those employing virtualization in their organization on average report that roughly one quarter of their production applications are running on virtual machines. Within the next 12 months, these same users expect nearly 50% of their applications will be hosted on a virtualized server."[4]

4 IDC, The Future of Virtualization: Leveraging Mobility to Move Beyond Consolidation, by John Humphreys; April 2008.

What they didn't tell you about virtualization

Congratulations! You may have just used virtualization to consolidate 25 applications running on 25 servers to run on just three servers. You will realize hardware cost savings over time, but the reality of virtualization is that it can also increase the complexity and thus the cost of managing those applications, desktops and servers. In addition, IT is tasked with meeting growing demands for anytime, anywhere, via-any-device access to desktops, applications, data and personal profiles. In heterogeneous, physical and virtual environments, it can be daunting:

• Virtualization can reduce physical server sprawl, but it actually increases virtual server sprawl because it's so easy and fast to provision new virtual machines.

• Management software and processes that work in the physical server environment don't always work in a virtual environment.

• Virtualization can actually decrease your visibility of the infrastructure and changes the requirements and approaches for backup and recovery, storage management, high availability, and disaster recovery.

• Virtualization increases management complexity – whether it's a desktop or server -especially when there are disparate tools to manage.

• The ease of deployment and workload mobility that virtualization enables can make security, configuration management, and compliance more challenging than in less dynamic physical environments.

Always begin with the end in mind

The business environment today is much different than it was 12 months ago, and it will certainly be different 12 months from now. With continuous innovation in technology and evolving business needs, the only constant in IT is change. One thing, however, never changes: the need to meet the service level goals on which your business depends. Approach your virtualization investments with these goals in mind, and you will be more likely to make the right management decisions.

Plan now

Things that don't begin well tend not to end well. Planning is the single most important step in generating the greatest returns. You will be successful with virtualization if you spend the time necessary up-front to discover your requirements, learn about all of your options, and plan with best practices in mind. Whether you are managing physical or virtual infrastructure in a test or production environment, the goal is always the same: delivering the expected service to your organization.

If you plan well, you can enjoy the benefits of virtualization without being derailed by the risks. When deciding on best practices, keep the following in mind:

• Make sure that as you adopt virtualization, your technology decisions continue to be focused on meeting service level agreements (SLAs), recovery point objectives (RPO), and recovery time objectives (RTO).

• Your management infrastructure should serve as a common platform across heterogeneous storage, server, desktop and application environments. Beware of technology providers who claim to provide robust feature sets for virtual environments if they only support their own proprietary technology platforms.

• Most organizations will want to take advantage of multiple hypervisor platforms over time; make sure you don't get locked into any single one. Make decisions that will enable your company to remain flexible, maintain freedom of choice, and ensure that what you have today will work with what you deploy in the future.

• Look for production-proven management solutions. Test and development are different from production environments; you cannot afford to take any risks in production when it comes to the data that is the lifeblood of your organization.

• Learn which IT processes are most impacted by the architectural and other changes that virtualization introduces, and adjust your strategy accordingly.

Understand the impact of virtualization on high availability and disaster recovery

Whether you are managing a physical or virtual infrastructure, or both, your RPO and RTO are still the biggest factors in managing planned and unplanned downtime. Virtualization can reduce planned downtime by providing the flexibility to move application workloads from one server to another during maintenance operations, without impacting the end user.

However, virtualization can also increase availability risks by consolidating the points of failure on fewer servers. In addition, ensuring high availability and disaster recovery for multi-tier and other complex applications that are deployed on a combination of physical and virtual server nodes introduces additional complexities. For example, an ERP application may have middleware components running in a virtual server, but the underlying database is on a physical server.

Virtualization by itself is not a panacea for high availability and disaster recovery. To leverage virtualization in demanding production environments, you will need to ensure that your architecture and management processes address the requirements of dynamic virtual environments without sacrificing service-level commitments.

Understanding the impact of virtualization on storage management

As customers adopt virtualization strategies, they discover that virtualization actually increases the complexities of storage management related to monitoring, reporting, and managing a virtual environment. With physical storage now separated by two or more degrees from the logical storage an application consumes, traditional storage management approaches are no longer valid. The task of understanding and monitoring how applications residing on virtual hosts are connected through the virtualization-layer to their storage resources can be a daunting one for the storage administrator. Having the ability to decompose logical storage through the virtualization layer all the way back to one or more physical resources, including SAN connectivity, is imperative. This is the case not only for accurate root cause analysis (RCA) but, more importantly, for establishing and maintaining application service levels as well.

The impact of virtualization

Virtualization makes problem isolation challenging. Virtualization encapsulates application components (operating system, database, middleware, drivers, network gateways, and so forth) to make it easier to move application workloads between servers. However, this same encapsulation also reduces visibility into the state of those components, which can make the identification and remediation of disaster recovery issues challenging.

Virtualization is not a replacement for clustering. Virtualization can reduce planned downtime, but the consolidation of multiple applications and virtual machines onto fewer servers increases the risk of unplanned downtime. Individually monitoring and managing the physical and virtual servers is not enough; it is essential to have management tools that provide visibility and remediation for the variety of network, database, application, and other application resource dependencies that make up a typical production environment. And for maximum architectural flexibility and cost avoidance, you need an infrastructure that can support heterogeneous failover

configurations—including physical-to-virtual, virtual-to-physical, virtual-to-virtual, and physical-to-physical—locally, over metropolitan distances, or over a wide area network.

Application disaster recovery solutions must be storage aware. In a disaster recovery scenario, recovering the application is one part of the equation, and recovering and restoring access to the application data is the other. Disaster recovery solutions for virtual environments have to be data replication aware so that in the event of a failure, applications are automatically failed over and remounted to the underlying storage and data on which they depend. In virtual environments, this can be difficult because application components become more dispersed and dynamic, causing greater complexity when it comes to mapping application resources to their underlying storage. Architect a high availability and disaster recovery solution that supports storage aware recovery in virtual environments to ensure business continuity.

Best practices

• Set policies to monitor virtual and physical servers as well as application resources within the virtual machines.

• Avoid the challenge of problem isolation in a virtual deployment by leveraging management tools that provide visibility and monitoring of not only the physical servers and virtual machines, but also all the application components inside those virtual machines and the availability of storage allocated to the applications and virtual hosts.

• Select tools that automate the detection of failures and the recovery of application components across any combination of physical and virtual servers and over any distance.

• Incorporate data replication as well as application clustering to enable coordinated failover and migration of both application resources and storage resources in heterogeneous physical and virtual environments.

HA/DR Diagram
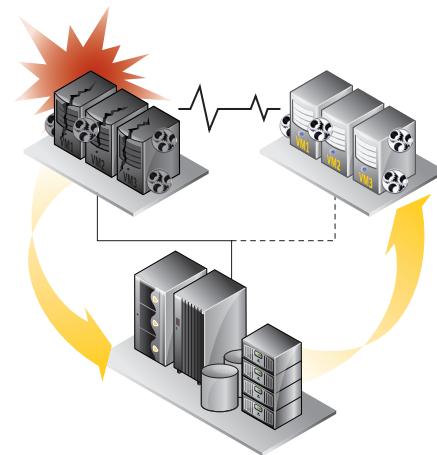
Symantec delivers market-leading Veritas™ high availability and disaster recovery technology that detects and automates the failover of applications on virtual servers.

Plan now for a common storage management infrastructure

Thanks to virtualization, deploying new applications and moving application workloads dynamically has never been easier. Storage management, however, becomes more challenging as it becomes more difficult to maintain the visibility and control that you are used to having in non-virtual environments. Tracking the dependencies between applications deployed on virtual servers and their underlying storage resources can be difficult, so automating

this process is an essential step in realizing the agility benefits that virtualization promises.

Beware of the storage management issues that virtualization introduces. Architect your environment to deliver overall manageability across heterogeneous physical and virtual platforms without compromising the storage management capabilities you currently rely on for your physical server platforms.

The impact of virtualization

Storage management complexity. Most organizations have been moving toward more manageable storage infrastructures by eliminating storage silos and leveraging technologies such as networked storage, storage virtualization, and standardized tools and processes for managing heterogeneous storage platforms. Server virtualization introduces new storage management challenges. Organizations need to address these challenges in a way that does not create new silos of storage management tools and processes that are in conflict with their overall storage management objectives.

Storage and server resource visibility. The encapsulation of application resources in virtual machines makes it difficult to map applications to

the storage resources on which they depend, and this difficulty is further compounded by the dynamic nature of virtual environments. Storage virtualization adds another layer of abstraction that is beneficial for storage management but presents greater complexity in managing the relationships between servers and storage. You can overcome these obstacles by leveraging tools that provide end-to-end visibility of your virtual and physical environment so that you increase storage utilization and reclaim over-provisioned but under-used storage.

File-level versus block-level storage. Inherently, virtualization adds a layer of abstraction to a physical resource. There are two approaches to storage management in virtual environments: a file-level approach (using a file system) and a block-level approach. A file-system based approach is suitable for low-end workloads such as file, print, and Web services. A block-level approach that allows granular and advanced storage management becomes more important for mission-critical workloads—in particular, production database environments. The block-level storage access renders greater visibility between applications and their underlying storage, which is needed to remediate problems quickly, effectively manage storage capacities, and meet application service levels.

Online storage management. Many storage administration and management tasks, such as growing and shrinking volumes and deploying RAID configurations, can be performed in a physical server and storage environment without taking applications offline. Unfortunately, some virtual environments eliminate this capability because of the way they interact with storage subsystems. Planned downtime to perform these day-to-day management tasks should not be necessary, and can be avoided if you deploy storage management tools that are optimized for both physical and virtual environments.

Best practices

• Leverage management tools that enable you to perform advanced storage management tasks such as storage pooling, online migrations, I/O load balancing, and failover without having to take applications offline.

• Provide the diverse applications that are running on different machines the right tier of storage based on your business requirements.

• Make sure you have holistic monitoring that provides storage visibility across all physical, logical, and virtual components of your data center, so that you can take automatic and corrective action based on user-defined policies.

• Choose tools that are capable of centrally monitoring and managing hundreds of virtual machines and their underlying storage.

• For effective storage capacity management, look for tools that provide end-to-end, in-depth storage reports that detail the dependencies and correlations of physical and virtual components.
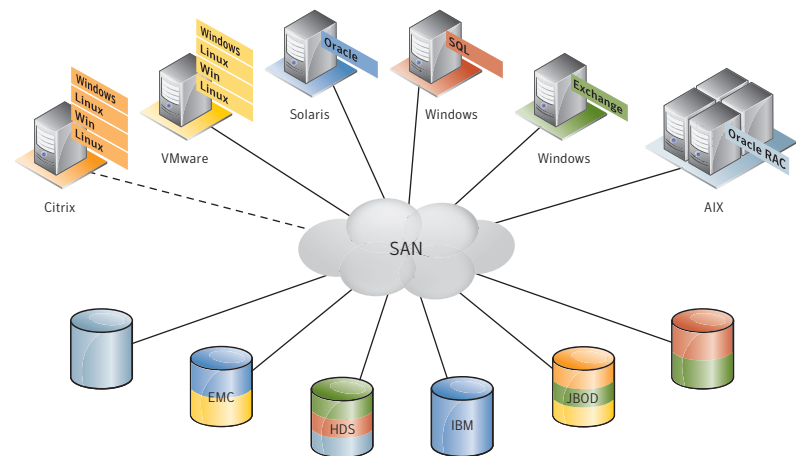
Veritas storage management technology from Symantec delivers tools to optimize storage utilization and provide management and flexibility across physical and virtual environments.

Ensure your backups are ready for virtualization

Although the business requirements are the same whether you are protecting data in a physical or a virtual environment, the technology and processes for backup and recovery of virtual machines and their data are not. Virtualization, as effective as it is for maximizing server utilization, can create problems for data protection. For example, the proliferation of servers can make backup configuration more time-consuming, increase storage requirements, and add complexity to backups and restores. In addition, the consolidation of multiple backup processes onto fewer systems also increases the amount of processing power required per server, a problem that is further exacerbated when there are fewer idle CPUs available per server.

The impact of virtualization

Performance. Running backup processes on the same server that is running an application workload is usually not a problem for the typically underutilized physical production server. However, one of the benefits of virtualization is the significant increase in the utilization of CPU resources, which can leave fewer CPU cycles available for backup processes. And, even when there are enough CPU resources to handle the backup processes, there is still the issue of I/O bandwidth between guest virtual machines and the underlying physical server and network infrastructure. Sometimes there is just too much data traffic to handle efficiently. Therefore, support for advanced technologies such as off-host backup or block-level incremental backup becomes critical to overcoming the performance and bandwidth constraints associated with virtual environments.

The performance versus recovery trade-off. Advanced technologies like off-host backup and block-level incremental backup address performance challenges highlighted above, but introduce additional challenges for recovery. When you implement these technologies to alleviate performance problems, you can lose the ability to recover individual files from the backup. Typical alternatives to the lack of granular file recovery, such as multiple backup jobs or recovery of the full machine, inevitably consume more storage resources and administration time. Implement a backup strategy that allows administrators to control, or better yet, overcome the challenges associate with advanced storage technologies.

Backup configuration and management. In a typical physical server environment, administrators define and configure server-specific backup jobs assuming that the underlying application and server topology is relatively static. In a virtual environment, where applications are being moved between servers and brought online and offline dynamically in response to changing requirements, managing backup policies can be much more challenging. You need the ability to automatically discover virtual machines, track their movement, and instantly find files for recovery, especially as the number of virtual machines deployed increases into hundreds or thousands. Finally, don't under-estimate the value of centralizing both alerts and reporting for all backup activity (both physical and virtual).

Storage and bandwidth utilization. In your quest for maximizing server utilization, don't forget about maximizing storage utilization. Source- based deduplication during the backup process minimizes the amount of data transferred over the network which improves backup performance and storage consumption. Target-based deduplication can be used without backup agents in the virtual guest, but occurs after the backup data has been moved over a SAN or LAN. Both approaches reduce the backup storage required for backups and disaster recovery.

Best practices

• Centralize operational management and reporting of backup and recovery for both physical and virtual environments. Ensure that you can easily identify and report on virtual machines with data protection policies.

• Demand solutions that tightly integrate your backup and recovery processes with your virtualization platform (e.g., automating the discovery of virtual machines at backup configuration time). This will eliminate the need for manual scripting and streamlining administration.

• Get the best of both worlds: Leverage tools that offer you two types of recovery from one type of backup. Traditionally, customer needed to perform an image based backup for full server recovery (virtual or physical) and a file level backup to respond to individual recovery requests.

• Seek to minimize the impact of backup operations on the virtual hosts with advanced technologies such as off-host, block-level incremental backup, and client-side deduplication.

• Understand and test how advanced technologies such as block level incremental backups affect the speed and efficiency of your recovery operations (e.g., Can you recover individual files from an incremental backup? How long does it take to find a file you want to recover?)

• Deduplicate your virtual machine backup data and consider solutions that support both source and target-based deduplication. Client-side deduplication approaches deliver more value in environments without shared storage resources. Target-based deduplication approaches work well when network bandwidth (SAN or LAN) is not a constraint and allow you to eliminate duplicate data. Some solutions let customers deploy and manage both approaches.

• Consider how your virtual machine backup and recovery plans could be affected by a decision to use tape media as a backup target. Can you perform the same fast recovery of data from tape as from disk?
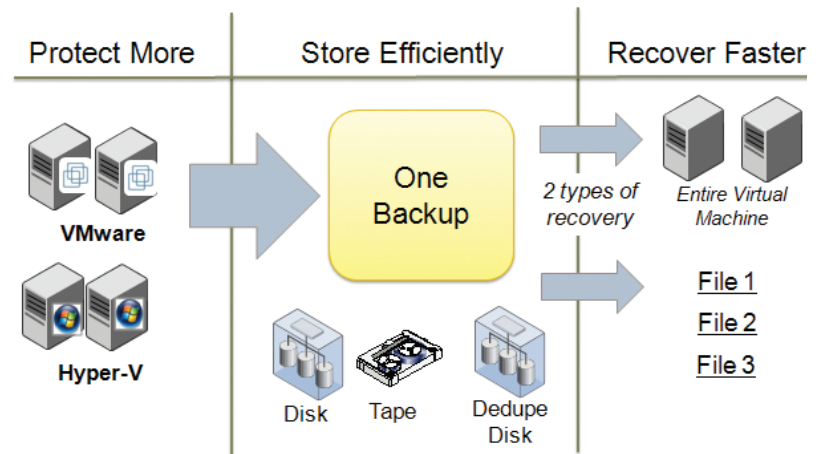
Symantec granular recovery technology lets you protect virtual machines without compromise

Don't let security be an afterthought

Virtualization may change some things, but the need to stay protected from malicious threats and data loss always stays the same. Every endpoint on the network, whether physical or virtual, has to be secured. Since virtualization makes it significantly easier and faster to deploy new systems, it is not uncommon to forgo the security best practices you worked so hard to establish in your physical environment. Centralize and standardize the definition and enforcement of security policies across physical and virtual server environments and, where possible, automate configuration, deployment, maintenance, and other processes critical to your overall risk posture.

## The impact of virtualization

Automation. Unless your provisioning process incorporates security best practices, it can be easy to overlook security requirements, leaving some virtual machines and endpoints at risk. Automate this process to ensure that you will meet your compliance requirements and keep your business secure.

Overhead. Security approaches that work well in a physical server environment may need to be modified for virtual servers. Because virtualization consolidates more applications and resources onto fewer physical servers, performing security scans and updates simultaneously can overload the system. Adjust your security policies to be virtualization-aware through techniques such as randomized scan times or sending patch updates at different times rather than all at once.

Security zones. Virtualization projects sometimes end up circumventing or collapsing the traditional roles and responsibility matrices that IT operations have established to support their existing infrastructure. As your computing environment becomes more consolidated and virtualized, administrators may become responsible for setting and enforcing policies that they are not trained to perform. Your security strategy should ensure that existing best practices and expertise are leveraged across these new virtual architectures.

Best practices

- Automate the process of keeping track of security configurations on virtual machines and perform remediation when components are out of policy.

- Ensure host integrity and compliance across heterogeneous platforms by implementing proactive, behavior-based host intrusion protection and strict system lockdown, along with advanced log analysis and response capabilities.

- Plan to adopt hypervisor extensions, when available, that will enable existing forms of security to be more robust and efficient as well as to optimize new forms of advanced security.
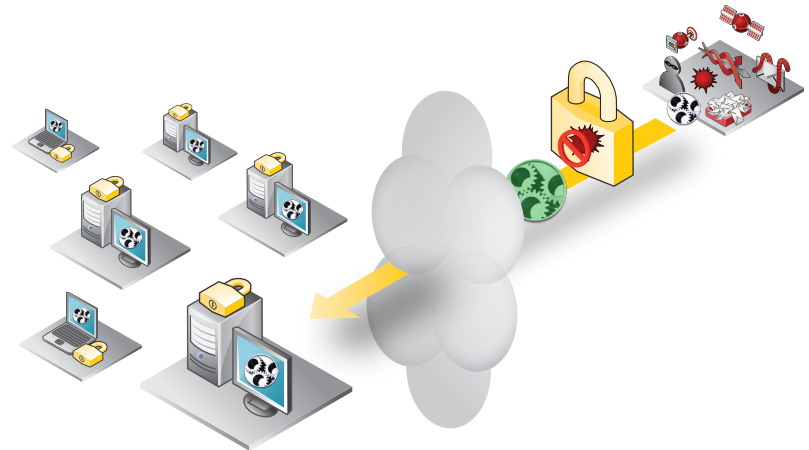
Symantec security software automates the process of protecting your endpoint systems and servers from spam, malware, and other threats.

Transform workspace management with endpoint virtualization

In today's world, an exploding number of desktops, laptops, and mobile devices are being used by a mobile workforce, using company hardware or their own equipment, and demanding different applications and access requirements. IT has an ever-increasing responsibility to improve the end-user experience and enhance productivity so that businesses can fully leverage technology to maximize their competitive advantage. Against this continuous pressure for maximum user productivity, organizations must also balance demands for information security and compliance while lowering the total cost of infrastructure ownership.

Reducing endpoint management costs and increasing user end-point productivity have been historically opposing efforts. Today, organizations can optimize both with Symantec's endpoint virtualization technologies. Endpoint Virtualization offers new ways to meet these demands by enabling IT to deliver and provision essential applications and workspace components to anyone, from anywhere, at any time, to any type of endpoint, by separating information and applications from the underlying operating system delivery model. Endpoint virtualization solutions that include application virtualization, streaming, profile virtualization and resource brokerage technologies enable user-based workspace management and change the way software is managed, delivered, and consumed at the endpoint. According to Gartner, "Use of application virtualization — In this specific example, introducing virtualization for 30% of applications in use reduces overall TCO 9% for desktops and 9% to 14% for notebooks. Use of application virtualization has a positive impact on IT labor costs (reducing the time required to package, test and support applications) as well as on end

user costs (lost productivity attributable to users trying to solve problems related to conflicting applications)"[5]

The impact of virtualization

Application management. Today, most desktops do not remain stationary on the LAN or run the same applications every day. Instead, organizations are managing multi-user desktops; laptops; virtual, streamed, and frequently updated applications; and remote offices in a virtual environment. As a result, inventory, delivery, and management methods that can span both traditional and virtual computing environments become critical to IT's ability to manage the endpoints.

License compliance. Traditional inventory scans of desktop computers simply identify installed software, but are insufficient for identifying which software is active or most commonly needed. Virtual desktops can be inaccessible, offline, or suspended, preventing normal tracking from taking place. As a result, license compliance can be a risk in any environment with virtual desktops, especially where users have access to multiple desktops simultaneously. A delivery mechanism that targets the role and needs of the end-user, rather than the device, is needed to ensure that licenses are not pre-consumed, but rather, consumed in the most efficient model permitted by your license agreement.

5 Source: Troni, Fredrica and Brian Gammage and Michael Silver. "How to Reduce Your PC TCO 30% in 2011". March 20, 2009"

Asset management. License compliance for applications in use is critical, but it can be equally important for an organization to salvage licenses that are no longer being used. Make sure you can automatically and efficiently discover and manage application consumption at the endpoint to help reduce the cost and complexity of traditional software management.

Delivery of service. The productivity of your users depends on their ability to access what they need when they need it, be it on their laptop, at virtual and terminal-server desktops, or on their mobile devices. In turn, your productivity depends on your ability to automatically deliver just-in-time service for your applications through the cloud without having to guess, anticipate, or preplan for unique user behavior. the cloud without having to guess, anticipate, or preplan for unique user behavior.

Best practices

• Increase end-user productivity with anytime, anywhere, any-device access to desktops, applications, data and personal profiles. The Symantec Endpoint Virtualization Suite takes a unique end-user-centric approach that builds dynamic workspaces centered on the end-user, their role, device, location and connection method.

• Reduce the total cost of ownership (TCO) associated with managing diverse and complex client computing models. Symantec Endpoint Virtualization Suite is an agnostic virtualization solution that works independently or in conjunction with other desktop virtualization infrastructure products and compliments multiple desktop computing models.

• Virtualize your applications and data into managed units so that you can instantly activate, deactivate, or reset applications and completely avoid

conflicts between applications without altering the base operating system installation of your endpoints.

• Move applications and data on demand from the network to the endpoint more efficiently with application streaming. Applications are not installed in the traditional sense, but still provide the same features and functionality, allowing the applications to be viewed and used as a service. This self-provisioning of applications helps lower license and support costs.

• Virtualize profiles and data to reduce lengthy log-on and log-off times and to give end-users instant access to their documents and personal settings

• Centralize management of users, applications, and workstations through a desktop connection broker that allows LAN and remote access for any endpoint.

Symantec Endpoint Virtualization puts the user at the center of the IT process, separating the information that matters (OS, applications, profiles, data) to simplify management and allow automated workspace configuration.

Standardization is a precursor to successful virtualization

Standardizing key infrastructure processes such as backup and data protection, high availability and disaster recovery, storage management, security, and client and application management will not only help you control and reduce costs, but will also help you improve service levels. As these key processes are standardized, you will be able to realize cost savings from virtualization as well as from the standardization process itself.

The benefits of standardizing your mixed physical and virtual environment include the following:

- **Reduced training costs.** Just because you are introducing virtualization in your environment, it does not mean you have to introduce new tools. You can leverage common software solutions for both infrastructures without introducing new and disparate tools that your administrators will have to learn how to use.

- **Improved service levels through automation.** Automation not only results in less administrative overhead, but it also enables you to deliver better service to your customers so that they will get what they need when and where they need it.

- **Reduced implementation costs through interoperability.** If you could make purchasing decisions based on business needs and budgetary allowances rather than on interoperability restrictions, your business efficiency and your purchasing power could increase. Not to mention the fact that the time to implementation can significantly decrease if you subtract the need for heavy scripting and integration to make disparate applications and processes work.

- **Consistent operations.** As you introduce virtualization into a physical infrastructure, you can leverage the same tasks and processes across both your physical and virtual infrastructure to ensure consistent operations across heterogeneous workloads.

You need production-proven, industry-leading capabilities that work in both physical and virtual environments. Complete heterogeneous support of these capabilities will enable you to achieve the standardization you need to get the largest ROI possible from your investments.

Symantec offers solutions for virtual environments

Symantec offers solutions that span both virtual and physical, heterogeneous environments to help organizations of all sizes get the most of out their virtualization in support of their mission-critical applications. Symantec provides an information-driven approach that leverages virtualization to manage, secure, and protect all information resources that matter—data, applications, images, configurations, user profiles, and more—across any server, storage, and any virtual machine. Through a common management environment that is hypervisor, operating system, machine (server and desktop), and platform (physical and virtual) agnostic, Symantec solutions help to ensure that critical information resources can be protected completely, managed easily, and controlled automatically, with greater visibility, cost savings, and confidence.

Visit www.symantec.com/virtualization for more information.

Protect completely

- Protect information and applications across physical and virtual platforms.

- Back up and recover systems and data in heterogeneous physical and virtual environments with precision.

- Keep applications and their storage resources highly available across heterogeneous physical and virtual environments.

- Secure information, systems, and virtual environments, from the data center to the desktop.

Manage easily

- Manage infrastructure consistently, independent of the physical or virtual platform.

- Manage physical and virtual servers, storage, and clients with one multiplatform toolset.

- Maximize utilization and uptime with virtualization-aware storage.

- Deliver and manage applications and end-user workspaces through endpoint virtualization.

Control automatically

- Control and automate processes to help ensure compliance and service-level quality.

- Automate management workflows across physical and virtual environments.

- Centrally define and automatically enforce security and compliance policies consistently across physical and virtual environments.

- Control access to applications and data and manage application software licensing through centralized administration of end-user policies.

About Symantec
Symantec is a global leader in providing security, storage
and systems management solutions to help businesses
and consumers secure and manage their information.
Headquartered in Cupertino, Calif., Symantec has operations
in more than 40 countries. More information is available at
www.symantec.com.

symantec.™

Symantec has worldwide operations
in more than 40 countries. For specific
country offices and contact numbers
please visit our website. For product
information in the U.S., call toll-free
1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043, United States
Phone: +1 650-527-8000
1 (800) 721 3934
www.symantec.com