



# Why Choose VMware?

WHITE PAPER

Table of Contents

Introduction ..... 3

**Best Virtualization Platform ..... 3**

VMware vSphere: The Recognized Leader in Virtualization..... 3

VMware Solutions: Most Proven, Trusted and Widely Deployed..... 6

VMware Ecosystem: The Most Flexibility and Choice ..... 8

Access to Broad Application Support ..... 13

**More Choice for Your Cloud ..... 13**

VMware vCloud: The Most Pragmatic Approach to Cloud Computing ..... 13

vCloud Partners: Greater Choice and Compatibility for Public Cloud ..... 16

**Better Security for Your Cloud ..... 16**

Simple: Centralized, Cost-Effective Security ..... 17

Strong: Adaptive Security Optimized for Virtualization ..... 17

Better Compliance at a Lower Cost ..... 19

**Lowest Total Cost of Ownership ..... 20**

Maximize Virtual-Machine Density per Physical Server..... 21

Save on Operational Costs ..... 23

## Introduction

Cloud computing enables IT as a Service, a vastly more efficient, flexible, and cost-effective way for IT to meet escalating business needs. VMware offers the most pragmatic path to this new model, with solutions that harness the power of the cloud while ensuring security and preserving the value of existing technology investments.

VMware is the best cloud infrastructure vendor because it provides the following:

- **Best virtualization platform** – VMware vSphere® forms the rock-solid platform on which all other solutions are built. Over the past decade, vSphere has emerged as the industry’s leading virtualization platform. Today, more than 250,000 customers have chosen to build their virtual and cloud infrastructures on vSphere, trusting their mission-critical applications and production environments to the advanced capabilities and reliability that only vSphere provides. With VMware vSphere® 5.0, VMware has raised the bar even higher with enhancements that make it clearly the best virtualization platform.
- **More choice for your cloud** – VMware brings the benefits of cloud computing to its customers in an evolutionary and pragmatic way with solutions that are built on top of and designed especially for vSphere. The VMware cloud model requires that customers make only incremental technology changes in order to achieve the agility and other benefits the cloud has to offer. Whether it is an internal private cloud, a public cloud or a hybrid model, VMware provides customers with the greatest choice in building a cloud that best suits their needs.
- **Better security for your cloud** – Cloud computing and highly virtualized environments introduce new security challenges that traditional security solutions, on their own, cannot address. VMware has a better approach to cloud security than other virtualization and cloud vendors with a new set of virtualization-aware security products that work with existing solutions to enable adaptive and cost-effective security and compliance within a single management framework. VMware’s new security model for the cloud is the foundation for trusted and scalable cloud infrastructures.

Best of all, VMware delivers all of this while providing a low total cost of ownership (TCO).

## Best Virtualization Platform

As the foundation for cloud computing, the virtualization platform must be reliable, secure, easy to manage, and deliver the highest performance. vSphere is the best virtualization platform and the best platform for cloud computing for these reasons:

- vSphere is the recognized leader in virtualization.
- VMware solutions are the most proven, trusted and widely deployed.
- The VMware ecosystem offers the most flexibility and choice.

### VMware vSphere: The Recognized Leader in Virtualization

---

*“VMware is the clear and obvious leader in virtualization products. We tried both the Microsoft and Oracle virtualization products and found them lacking in features and performance compared to the VMware product.”*

— David Greer, Director of Information Services, HelioVolt Corporation

---

Over a decade of innovation has firmly established vSphere as the virtualization industry leader as recognized by customers, press and analysts.

Among the [hundreds of awards given to VMware products](#) over the past years, the 2011 InfoWorld Best [Technology of the Year award for Best Virtualization Platform](#) stands out. It further validates the position of VMware as the best platform for IT and clearly illustrates the technology gap between VMware and its competitors.

The foundation for cloud computing is a robust and production-proven hypervisor, and not all hypervisors are equal. VMware ESXi™ is—and will continue to be—the industry’s most robust and production-proven hypervisor and is a better choice than other hypervisors for building your cloud.

**Hypervisor Architectures Do Matter**

ESXi—the industry’s first “bare-metal” hypervisor for x86 systems—is the most reliable and robust virtualization platform. Launched in 2001 and now in its fifth generation, the VMware purpose-built, thin hypervisor is designed for the sole purpose of virtualization. A smaller hypervisor disk footprint reduces the attack surface for external threats and can drastically lower the number of patches required, giving you a more reliable product and a more stable datacenter. With the ESXi hypervisor at the core of vSphere, VMware has achieved by far the smallest code size of any virtualization product by completely eliminating any dependence on a general-purpose operating system or management console. By stripping out the tens of millions of lines of code required by a management operating system, ESXi 5 delivers a full x86/x64 virtualization platform in a tiny 144MB disk footprint.

Competing hypervisors treat virtualization as an add-on to a general-purpose operating system that serves as a “parent partition.” This thicker architecture introduces reliability concerns, because the parent operating system has a much larger attack surface and more unrelated code to patch and maintain. Windows Server 2008 R2 with Hyper-V, Xen and KVM all have architectures that depend on a large general-purpose server operating system. That dependency means that a flaw or vulnerability anywhere in the management OS—even in components unrelated to virtualization—puts the entire virtualization platform at risk. It also means that users of those products must cope with the more numerous and frequent patches issued to secure Windows and Linux operating systems, resulting in more downtime and disruption.

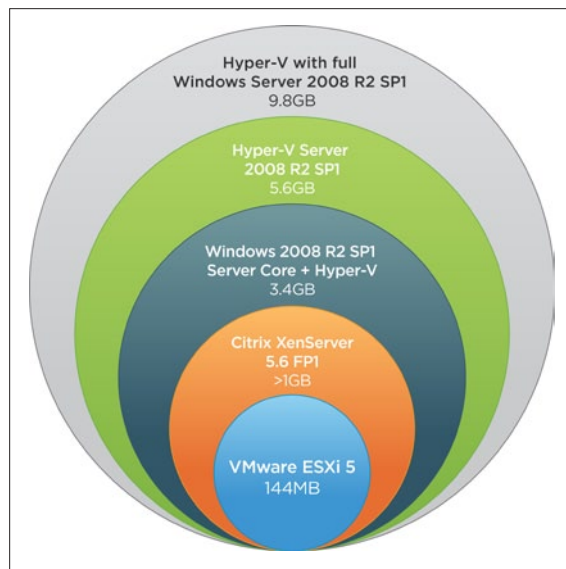


Figure 1. Relative Disk Footprint of Various Hypervisors

Additionally, competing hypervisors use an indirect I/O design that routes all virtual-machine network and storage traffic through the management OS, relying on generic I/O drivers. This configuration means that all virtual machines are fighting to use the same drivers within the general-purpose OS, and that these generic

drivers are not optimized for virtualization. VMware ESXi employs a direct driver model, whereby certified and hardened I/O drivers are contained directly within the ESXi hypervisor. To ensure optimal performance, these drivers must pass rigorous testing and optimization steps performed jointly by VMware and the hardware vendors before they are certified for use with ESXi. With the drivers in the hypervisor, ESXi can optimize performance through management of CPU scheduling and memory resources that drivers need to process I/O loads from multiple virtual machines. This architecture enables all virtual machines to directly leverage drivers and to “talk” directly to external devices.

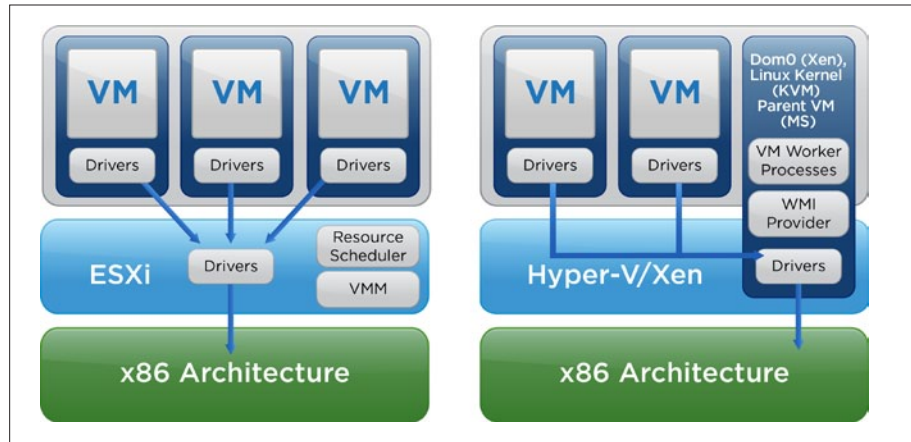


Figure 2. Comparing Driver Models of Competing Hypervisors

For more comparisons among hypervisors, see <http://www.vmware.com/technical-resources/advantages/robust-foundation.html>.

**Leading Innovation in Virtualization**

VMware has a culture of innovation that continues to propel virtualization and cloud computing into the future. VMware was first to market with time- and money-saving technology such as VMware vMotion®, VMware Distributed Resource Scheduler (DRS), and VMware vSphere Storage vMotion. Competitors are mainly copying

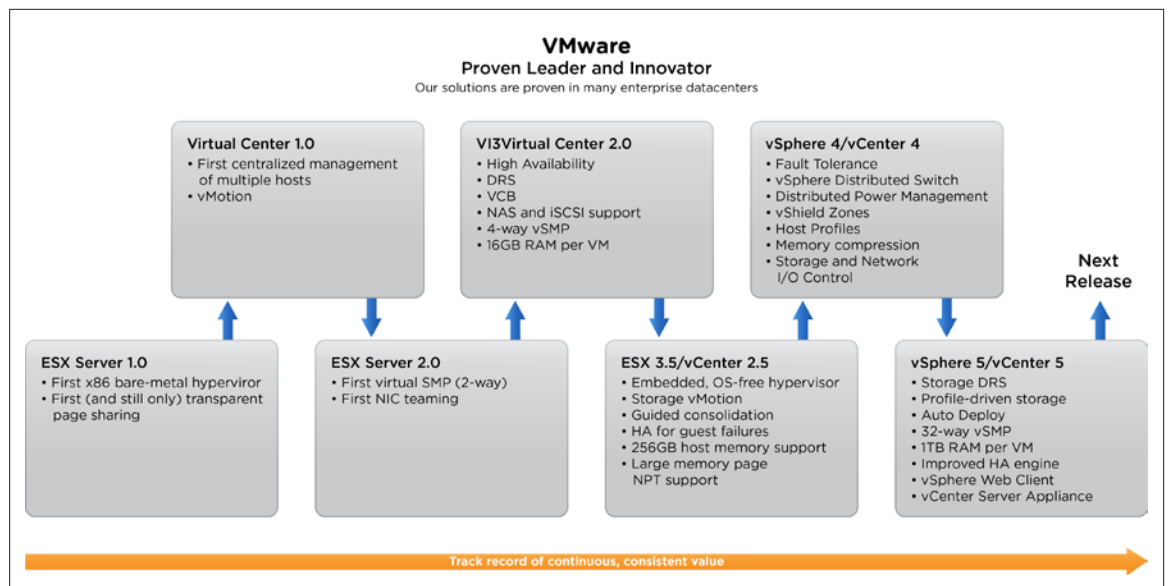


Figure 3. VMware Innovation Through the Years

these VMware features and roadmap or trying to graft technology best suited for a physical environment onto a virtual one, but VMware has not been resting on its laurels. With vSphere 5.0, VMware introduced VMware vSphere Storage DRS™, Profile-Driven Storage, Auto Deploy and more than 200 other enhancements, further extending the company’s lead and ensuring that VMware customers obtain unparalleled levels of performance and reliability.

One example of VMware’s technology leadership is in the area of storage management. VMware introduced VMware vSphere VMFS back in 2001. VMFS (Virtual Machine File System) leverages shared storage to allow multiple instances of ESXi to read and write concurrently to the same storage while using disk locking to allow only the hosts owning each individual virtual machine to write to the virtual disk files. This is a fundamental building block of achieving storage virtualization and creating a pool of storage resources. The competitors have recognized the need for more advanced storage management and have released their own storage management improvements, mainly Cluster Shared Volumes (CSV) for Hyper-V and StorageLink for XenServer, both released in 2009. However, VMware remains the only solution capable of live storage migration—the ability to move virtual machines from one storage array to another with no downtime. VMware has taken this concept even further with vSphere Storage DRS—automated load balancing of virtual machines across multiple storage arrays to avoid I/O bottlenecks and meet stringent service-level agreements. Finally, VMware has streamlined storage provisioning and improved agility with Profile-Driven Storage—a method of classifying storage tiers and managing initial and ongoing placement of virtual machines according to predefined virtual-machine requirements.

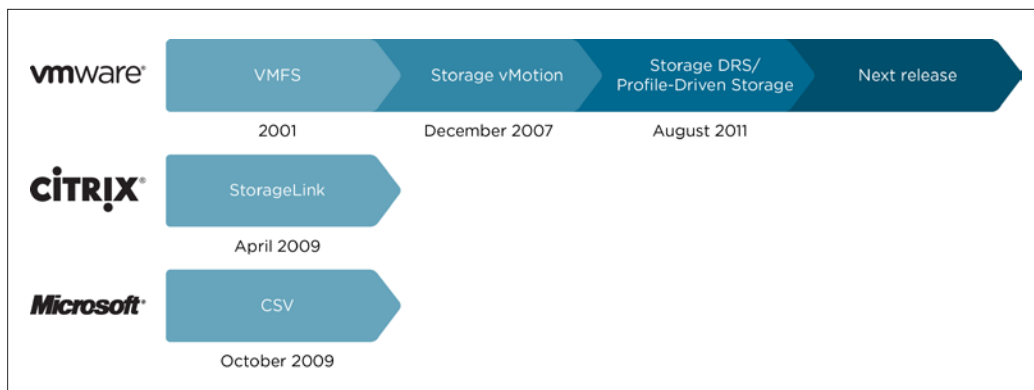


Figure 4. Advanced Storage Management Solutions by Different Virtualization Vendors

Storage management is just one of several areas in which VMware has demonstrated innovative thinking and technology leadership. VMware’s unique developments with virtualization- and cloud-aware security are discussed in “Better Security for Your Cloud,” later in this paper.

### VMware Solutions: Most Proven, Trusted and Widely Deployed

When selecting a cloud infrastructure platform, it is important to have one that is being deployed in production in a variety of customers, industries, and segments.

#### World’s Most Successful Companies Run VMware

VMware is the proven choice for virtualization from the desktop through the datacenter to the cloud. More than 250,000 customers of all sizes have chosen VMware as their cloud infrastructure platform, including

- 100 percent of Fortune 100
- 100 percent of Fortune Global 100
- 99 percent of Fortune 1000
- 97 percent of Fortune Global 500

Among the world’s leading Fortune 1000 companies, VMware has been adopted across all industries, including

- 100 percent of manufacturers
- 100 percent of healthcare companies
- 100 percent of technology companies
- 100 percent of retailers
- 100 percent of transportation companies
- 97 percent of financial services companies
- 95 percent of telecommunications/media/entertainment

**Customers Trust VMware with Business-Critical Applications**

*“The university has virtualized 50,000 Exchange 2007 mailboxes on VMware Infrastructure. We not only have a more manageable and flexible Exchange environment, but we have replaced Microsoft clustering with VMware’s built-in high availability solutions such as HA and vMotion. We couldn’t be happier with the uptime and performance of our Exchange implementation on VMware. VMware technology works for small companies all the way up to massive financial institutions. And clearly, it has worked for us.”*

— Adrian Jane, Infrastructure and Operations Manager, University of Plymouth

Customers trust vSphere and its advanced capabilities to virtualize business-critical applications, which enable them to respond to business needs faster. In just over one year, customers have increased the virtualization of tier 1 applications such as Microsoft SharePoint and Oracle DB significantly.

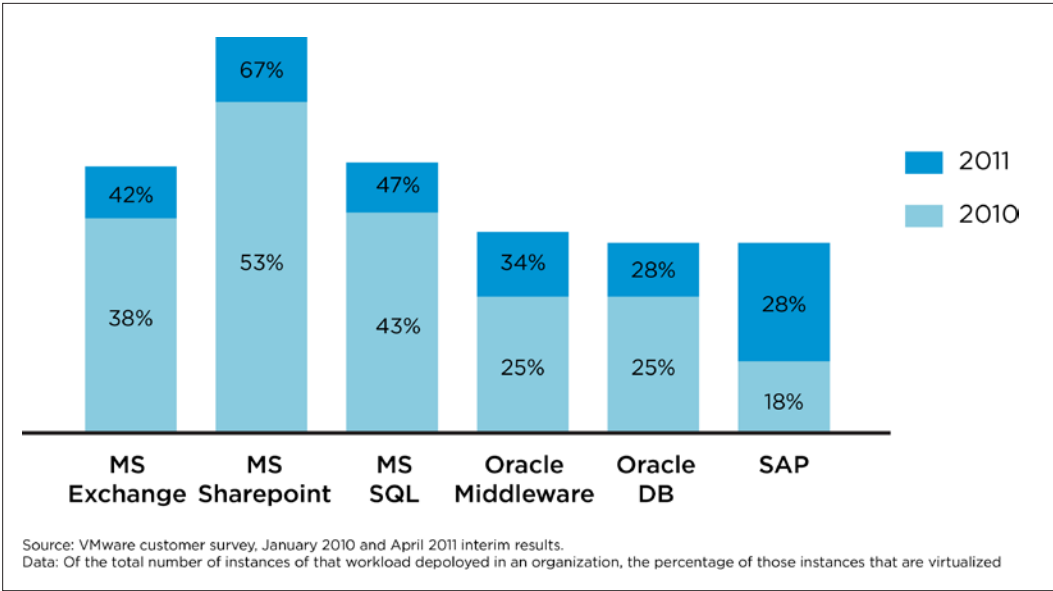


Figure 5. Percentage of Workload Instances Running on VMware in Customer Base

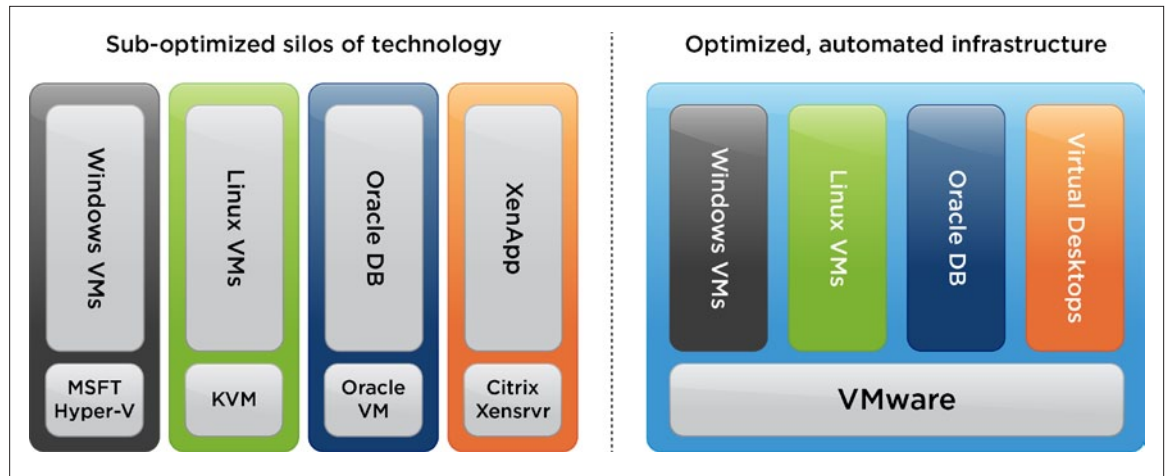


Figure 6. Comparing VMware Workload-Agnostic Approach to the Competitors

In addition to customers, independent technology analysts have also recognized VMware as being the leaders in virtualization. In fact, Gartner has placed VMware in the leaders quadrant of its x86 Virtualization Magic Quadrant—and VMware is the only vendor to receive that ranking each year the Magic Quadrant has been published.

### VMware Ecosystem: The Most Flexibility and Choice

The VMware approach to cloud infrastructure provides customers with the most choice and flexibility in selecting hardware and application components that best suit their needs, and customers know that VMware solutions integrate well with their existing technology investments. VMware follows a workload-agnostic approach with no “preferred” workload, delivering uniformly high performance across all virtualized applications. This makes it possible to have one platform instead of multiple silos.

VMware works closely with its large ecosystem of partners (software vendors, system OEMs and peripheral manufacturers) to certify their products with the VMware vSphere platform—usually delivering certification when those products are first released. The result of working with such a wide variety of technology vendors is that VMware technology works across the broadest array of IT environments. vSphere supports more guest operating systems than any other x86 virtualization platform; in fact, it supports more versions of Windows than Microsoft does. vSphere is certified on more than 1,000 server models for very broad hardware support, and over 1,600 software providers have explicitly issued support statements for 3,000 applications running on the vSphere platform.

#### VMware Supports the Largest Number of Guest Operating Systems

vSphere has a unique multimode capability that allows it to support the broadest range of guest operating systems and processors. vSphere takes full advantage of the latest hardware acceleration features built in to recent Intel and AMD processors, yet it can also run older guest OSs on earlier processors. With VMware’s exclusive technology, vSphere can run off-the-shelf operating systems at near-native performance. Other hypervisors suffer serious performance degradation with unmodified guests, and they require nonstandard guest modifications such as paravirtualization (Xen) or “Enlightenments” (Hyper-V) in order to deliver acceptable performance. The need for modifications also means those hypervisors do not support as many operating systems.

vSphere supports all guest operating systems in a consistent, unbiased manner. For example, the advanced memory management techniques of vSphere 5.0, including memory ballooning, transparent page sharing and memory compression, are applied to all guest operating systems. In comparison, Hyper-V Dynamic Memory—a new feature included in Windows Server 2008 R2 with SP1—works only with a limited number of Windows guest operating systems (Windows Server 2003, Windows Server 2008, Windows Vista, and Windows 7) and no Linux guest operating systems.



See the VMware Guest Operating System Installation Guide on [www.vmware.com](http://www.vmware.com) for full details on support for guest operating systems.

<b>GUEST OPERATING SYSTEM SUPPORT</b>	<b>VMWARE VSPHERE 5</b>	<b>MICROSOFT WINDOWS 2008 SERVER R2 SP1 WITH HYPER-V</b>	<b>CITRIX XENSERVER 5.6 SP1</b>
TOTAL	83	25	29
Windows NT 4.0	✓	✗	✗
Windows 2000	✓	✗	✓
Windows Server 2003 64-bit	✓	✓	✓
Windows Server 2003	✓	✓	✓
Windows Server 2008 64-bit	✓	✓	✓
Windows Server 2008	✓	✓	✓
Windows 7 64-bit	✓	✓	✓
Windows 7	✓	✓	✓
Windows XP 64-bit	✓	✓	✗
Windows XP	✓	✓	✓
Windows Vista 64-bit	✓	✓	✗
Windows Vista	✓	✓	✓
Windows 98	✓	✗	✗
Windows 95	✓	✗	✗
Windows 3.1	✓	✗	✗
MS-DOS 6.22	✓	✗	✗
Windows Preinstallation Environment 2 64-bit	✓	✗	✗
Windows Preinstallation Environment 2	✓	✗	✗
Windows Home Server 2011	✗	✓	✗
Windows Storage Server 2008 R2	✗	✓	✗

GUEST OPERATING SYSTEM SUPPORT	VMWARE VSPHERE 5	MICROSOFT WINDOWS 2008 SERVER R2 SP1 WITH HYPER-V	CITRIX XENSERVER 5.6 SP1
Windows Small Business Server 2003	✗	✗	✓
Windows Small Business Server 2011	✗	✓	✗
Red Hat Enterprise Linux 6 64-bit	✓	✓	✓
Red Hat Enterprise Linux 6	✓	✓	✗
Red Hat Enterprise Linux 5 64-bit	✓	✓	✓
Red Hat Enterprise Linux 5	✓	✓	✓
Red Hat Enterprise Linux 4 64-bit	✓	✗	✗
Red Hat Enterprise Linux 4	✓	✗	✓
Red Hat Enterprise Linux 3 64-bit	✓	✗	✗
Red Hat Enterprise Linux 3	✓	✗	✓
Red Hat Enterprise Linux 2.1	✓	✗	✗
SUSE Linux Enterprise Server 11 64-bit	✓	✓	✓
SUSE Linux Enterprise Server 11	✓	✓	✓
SUSE Linux Enterprise Server 10 64-bit	✓	✓	✓
SUSE Linux Enterprise Server 10	✓	✓	✓
SUSE Linux Enterprise Server 9 64-bit	✓	✗	✗
SUSE Linux Enterprise Server 9	✓	✗	✓
SUSE Linux Enterprise Server 8	✓	✗	✗
Ubuntu 10 Linux 64-bit	✓	✗	✗
Ubuntu 10 Linux	✓	✗	✗
Ubuntu 9 Linux 64-bit	✓	✗	✗
Ubuntu 9 Linux	✓	✗	✗
Ubuntu 8 Linux 64-bit	✓	✗	✗

<b>GUEST OPERATING SYSTEM SUPPORT</b>	<b>VMWARE VSPHERE 5</b>	<b>MICROSOFT WINDOWS 2008 SERVER R2 SP1 WITH HYPER-V</b>	<b>CITRIX XENSERVER 5.6 SP1</b>
Ubuntu 8 Linux	✓	✗	✗
Ubuntu 7 Linux 64-bit	✓	✗	✗
Ubuntu 7 Linux	✓	✗	✗
Novell NetWare 6	✓	✗	✗
Novell NetWare 5	✓	✗	✗
OS/2 Warp 4	✓	✗	✗
Oracle (Sun) Solaris 10 x86 64-bit	✓	✗	✗
Oracle Solaris 10 x86	✓	✗	✗
Oracle Solaris 9 x86	✓	✗	✗
Oracle Solaris 8 x86	✓	✗	✗
SCO OpenServer 5	✓	✗	✗
SCO UnixWare 7	✓	✗	✗
CentOS 6 64-bit	✓	✓	✗
CentOS 6	✓	✓	✓
CentOS 5 64-bit	✓	✓	✓
CentOS 5	✓	✓	✓
CentOS 4 64-bit	✓	✗	✗
CentOS 4	✓	✗	✓
Oracle Linux 6 64-bit	✓	✗	✗
Oracle Linux 6	✓	✗	✗
Oracle Enterprise Linux 5 64-bit	✓	✗	✓
Oracle Enterprise Linux 5	✓	✗	✓
Oracle Enterprise Linux 4 64-bit	✓	✗	✗

GUEST OPERATING SYSTEM SUPPORT	VMWARE VSPHERE 5	MICROSOFT WINDOWS 2008 SERVER R2 SP1 WITH HYPER-V	CITRIX XENSERVER 5.6 SP1
Oracle Enterprise Linux 4	✓	✗	✗
Debian 6 64-bit	✓	✗	✓
Debian 6	✓	✗	✓
Debian 5 64-bit	✓	✗	✗
Debian 5	✓	✗	✓
Debian 4 64-bit	✓	✗	✗
Debian 4	✓	✗	✗
FreeBSD 8 64-bit	✓	✗	✗
FreeBSD 8	✓	✗	✗
FreeBSD 7 64-bit	✓	✗	✗
FreeBSD 7	✓	✗	✗
FreeBSD 6 64-bit	✓	✗	✗
FreeBSD 6	✓	✗	✗
Asianux 4 64-bit	✓	✗	✗
Asianux 4	✓	✗	✗
Asianux 3 64-bit	✓	✗	✗
Asianux 3	✓	✗	✗
Serenity Systems eComStation 2	✓	✗	✗
Serenity Systems eComStation 1.2R	✓	✗	✗
Apple Mac OS X 10 64-bit	✓	✗	✗
Apple Mac OS X 10	✓	✗	✗
TOTAL	83	25	29

Table 1. Comparing Guest Operating System Support Among Virtualization Platforms  
Data collected September 12, 2011

## Access to Broad Application Support

VMware has also garnered extensive support from enterprise application vendors. In fact, independent analysts have concluded that VMware has the broadest support for applications, with almost 3,000 applications supported.

More and more independent software vendors (ISVs) test their software on VMware even before they release it. Most major global software vendors support customers running their applications in and with VMware environments, including

- Adobe
- Avaya
- BMC Software
- Borland Software Corp.
- Cisco Systems
- Computer Associates
- Dell
- EMC
- HP
- IBM
- Juniper Networks
- McAfee
- Microsoft
- MySQL
- Oracle
- Red Hat
- Research in Motion
- SAP
- Symantec
- TIBCO

## More Choice for Your Cloud

Cloud computing is the antidote to inflexible, overly complex IT infrastructures. It separates applications and information from the complexity of underlying infrastructure, so IT can focus on the support and enablement of business value. While there are different models of cloud computing to choose from—private cloud, public cloud, or hybrid cloud—virtualization provides the first layer of abstraction away from the physical infrastructure. With VMware, customers can progress toward the cloud-computing model of their choice, knowing that they all share vSphere as the common virtualization engine.

The flexibility of the VMware cloud can be summarized in two points:

- VMware vCloud® is the most pragmatic path to cloud computing.
- vCloud partners offer greater choice and compatibility for the public cloud.

### VMware vCloud: The Most Pragmatic Approach to Cloud Computing

---

*VMware vCloud Director enables Siemens IT Solutions and Services to bring out a cloud service offering that combines outstanding self-service features with robust security in a multitenant environment.”*

— Jordan Janeczko, Global Technology Manager for Cloud Computing, Siemens IT Solutions and Services GmbH

---

Many vendors have a narrow vision of what their cloud looks like, or they claim to have a cloud solution when their products can't deliver the necessary elements of true cloud computing. Some have a one-size-fits-all

approach that locks customers into a single cloud provider. They force customers to keep their applications hosted with that provider with no way to change that decision as business needs dictate, and they often ignore private clouds in the customer’s datacenter as an ongoing option. Other vendors require burdensome application rewrites, which are very costly and time consuming.

Rather than imposing vendor lock-in or forcing customers to completely re-engineer their application infrastructures, VMware brings the benefits of cloud computing to its customers in an evolutionary and pragmatic way. The VMware cloud model requires that customers make only incremental technology changes to achieve the agility and other benefits the cloud has to offer. VMware’s goal is to enable customers to benefit from the full spectrum of cloud computing while maximizing their existing infrastructure investments.

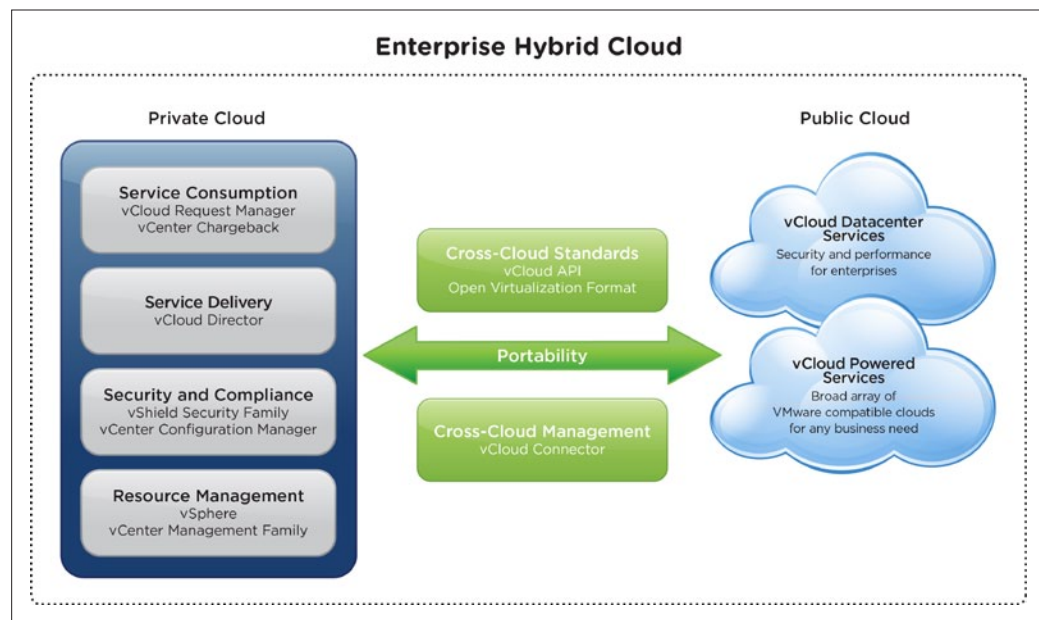


Figure 7. vCloud Solution

**Complete Cloud Infrastructure Solution**

The VMware cloud infrastructure solution is built on top of vSphere and provides all the components needed to transform an internal datacenter into a secure private cloud with extensibility to public clouds. By integrating with and extending the capabilities of vSphere, VMware cloud infrastructure solutions deliver all the benefits of cloud computing:

- Increased business agility through rapid self-service of on-demand resources
- Reduced costs through efficient delivery of resources and consolidation of infrastructure
- Improved security and compliance
- Application portability and interoperability between private and public clouds

Competitor solutions fall short in their ability to deliver on all aspects of setting up a secure cloud environment.

	VMWARE V CLOUD	MICROSOFT HYPER-V AND SYSTEM CENTER	CITRIX XENSERVER AND CLOUDSTACK
Cloud Consumption	<p>✓</p> <p><b>VMware vCloud Director™ and VMware vCenter Chargeback™</b></p> <ul style="list-style-type: none"> <li>•Secure multitenancy</li> <li>•Virtual datacenters with pooled resources</li> <li>•Policy-based self-service portal</li> <li>•Integrated chargeback with vSphere aware constructs</li> </ul>	<p>~</p> <p><b>SCVMM Self-Service Portal</b></p> <ul style="list-style-type: none"> <li>•No multitenancy</li> <li>•Third-party tools required for monitoring consumption</li> <li>•Limited automation; administrator intervention required</li> </ul>	<p>~</p> <p><b>CloudStack</b></p> <ul style="list-style-type: none"> <li>•Manual segregation for multitenancy</li> <li>•No virtual datacenter constructs</li> <li>•Recent acquisition, still integrating with Citrix</li> </ul>
Operations and Management	<p>✓</p> <p><b>VMware vCenter™ Operations</b></p> <ul style="list-style-type: none"> <li>•Actionable intelligence for rapid problem resolution</li> <li>•Patented analytics for preemptive identification of building problems</li> <li>•Powerful visualization of impending issues and risks</li> </ul>	<p>~</p> <p><b>System Center</b></p> <ul style="list-style-type: none"> <li>•Requires multiple System Center solutions</li> <li>•Complicated setup relies on static thresholds that trigger many false alarms</li> <li>•Does not scale well for large environments</li> </ul>	<p>✗</p> <p>Nothing comparable</p>
Security and Compliance	<p>✓</p> <p><b>VMware vShield™ and VMware vCenter Configuration Manager™</b></p> <ul style="list-style-type: none"> <li>•Virtualization-aware security</li> <li>•Built-in firewall, NAT, site-to-site VPN, DHCP, flow monitoring, and load balancing</li> <li>•Automated collection, analysis, remediation and patching with configuration templates</li> </ul>	<p>✗</p> <p>Nothing comparable</p>	<p>✗</p> <p>Nothing comparable</p>
Virtualization	<p>✓</p> <p><b>vSphere and vCenter</b></p> <ul style="list-style-type: none"> <li>•True, purpose-built thin hypervisor</li> <li>•Advanced business continuity solutions</li> <li>-VMware vSphere High Availability</li> <li>-VMware vSphere Fault Tolerance</li> <li>-NIC teaming</li> <li>-vMotion/Storage vMotion</li> <li>•Advanced storage management capabilities</li> <li>-Storage DRS</li> <li>-Profile-Driven Storage</li> </ul>	<p>~</p> <p><b>Hyper-V</b></p> <ul style="list-style-type: none"> <li>•Hypervisor is a feature of a general-purpose OS</li> <li>•No logical resource pools</li> <li>•Lacks many of the advanced capabilities available in vSphere</li> </ul>	<p>~</p> <p><b>XenServer</b></p> <ul style="list-style-type: none"> <li>•Hypervisor is a feature of a general-purpose OS</li> <li>•No logical resource pools</li> <li>•Lacks many of the advanced capabilities available in vSphere</li> </ul>

**Real Path to Hybrid Clouds**

Customers can use the VMware cloud infrastructure solutions to build their own private clouds, but what if they need to move workloads out to public clouds for capacity or cost reasons? Customers who choose VMware can be assured that their workloads are portable to public clouds because of VMware cross-cloud management tools and cross-cloud standards.

VMware is the only vendor today that provides cross-cloud management capabilities, delivering the ability to view and manage private and public cloud resources through a “single pane of glass” (with the vSphere Client) and making the hybrid cloud model a reality. Other private cloud vendors claim to support hybrid clouds, but they make it extremely difficult to move workloads around. For example, moving a virtual machine from

Microsoft Hyper-V to Microsoft Azure is a [complex operation](#) that requires preparation within the Hyper-V environment, the Azure environment and Visual Studio. With VMware vCloud Connector™, you can migrate workloads from internal datacenters out to compatible public clouds—no rework or re-architecting is necessary.

## vCloud Partners: Greater Choice and Compatibility for Public Cloud

---

*“VMware vCloud technology allows our customers to seamlessly migrate workloads to and from the public and private cloud, without having to reload data, change IP addresses or deal with domain name server issues.”*

— Tom Kiblin, Chief Technology Officer, Virtacore Systems

---

To make the move to public clouds easier, VMware has joined forces with leading service providers worldwide. These vCloud Powered service providers offer a broad range of cloud-based offerings based on vSphere and vCloud Director, while supporting vCloud APIs and Open Virtualization Format (OVF). Using the same set of intelligent cloud infrastructure solutions from VMware, these service providers offer compatible environments with the same UI and management capabilities customers are accustomed to in their private cloud environments.

More important, customers have the option to move workloads between different vCloud service providers. That means customers can choose a different service provider if they become unhappy with their current service, price or geography. No other cloud ecosystem can deliver that level of flexibility and choice.

Within vCloud service providers are two subgroups: VMware vCloud Datacenter Service and vCloud Express.

### vCloud Datacenter Service

vCloud Datacenter Service partners delivers a globally consistent, enterprise-class infrastructure cloud service. These public cloud providers offer seamless compatibility to users of VMware private clouds while guaranteeing performance, uptime, and auditable security and compliance. With Global Connect, you can work with your preferred service provider in your region and have access to other vCloud Datacenter Service partners in multiple geographies for end-to-end service-level confidence.

### vCloud Express

vCloud Express services provide reliable, on-demand, pay-as-you-go infrastructure aimed at developers. This class of service enables IT to reduce both capital expense and resource challenges associated with the fluctuating infrastructure requirements of development teams.

## Better Security for Your Cloud

Whether you are considering moving to the cloud today or sometime in the future, you will need to start thinking about securing your cloud infrastructure.

Currently, the most common way of securing virtualized environments is through the use of air gaps. The air gap security model segregates applications in different trust zones on dedicated virtualized hosts with layers of security—usually involving firewalls, load balancers and VPNs. This model is effective in lower density and static environments, but how can it be improved for dynamic datacenters or multitenant cloud environments?

VMware, with the vShield family of products, is the only vendor addressing the security requirements for cloud computing with solutions that improve existing security infrastructure. Competitors such as Microsoft, Citrix, Red Hat and Oracle have no answer to vShield. Only VMware is rethinking the old methodology to come up with a more efficient, less complex way to manage security that is better for your cloud. It's better because it is



- Simple – centralized, cost-effective security
- Strong – adaptive security optimized for virtualization
- Cost-effective – better compliance at a lower cost

**Simple: Centralized, Cost-Effective Security**

Legacy security solutions often require patching together various tools, but the lack of a common framework makes visibility and control a real challenge. vShield secures the datacenter at multiple levels, all within a single management framework that is integrated with VMware vCenter Server. This framework lets you deploy and manage security services from VMware as well as third parties to reduce complexity and improve operational efficiency.

Second, role-based access controls enable virtualization administrators, network teams and security teams to work together, each with visibility into changes and events within the infrastructure that affect their domains. This improves business agility as administrators can manage all security policies in the datacenter and quickly update these policies as needed, whether due to business needs or compliance changes.

Finally, with the unique introspection capabilities of VMware, third-party security vendors such as Trend Micro, Symantec, Luminous, Sophos, BitDefender, Kaspersky and McAfee are providing specialized security solutions that are delivered as virtual appliances, reducing the number of physical hardware appliances to maintain and manage.

These are just some of the ways that vShield makes datacenter security disruptively simple.

	<b>TRADITIONAL SECURITY TOOLS ALONE</b>	<b>SECURITY WITH VSHIELD</b>
Policy Frameworks	<p><b>Multiple rules</b></p> <ul style="list-style-type: none"> <li>•Separate policies and rules defined for each component of the datacenter (hosts, networking, applications, data, endpoint)</li> </ul>	<p><b>Simple, single pane of glass</b></p> <ul style="list-style-type: none"> <li>•Distinct components integrated into a single management framework</li> <li>•vShield Manager provides a central command center</li> </ul>
IT Roles and Responsibilities	<p><b>Multiple IT groups involved</b></p> <ul style="list-style-type: none"> <li>•Multiple stakeholders involved in security planning and implementation</li> <li>•Roles overlap, adding complexity and confusion</li> </ul>	<p><b>Clear distribution of roles</b></p> <ul style="list-style-type: none"> <li>•Role-based access provides clear separation of workflows for virtualization and security administrators</li> <li>•Administrative tasks delegated flexibly across resource pools and security groups</li> </ul>
Hardware Security Solutions	<p><b>Multiple physical solutions</b></p> <ul style="list-style-type: none"> <li>•Patchwork of multiple point solutions:                             <ul style="list-style-type: none"> <li>-Firewalls</li> <li>-VPNs</li> <li>-Load balancers</li> </ul> </li> <li>•Each device managed separately</li> <li>•Capacity limited by hardware appliance ports</li> <li>•Increased cost and complexity</li> </ul>	<p><b>Integrated virtual appliances</b></p> <ul style="list-style-type: none"> <li>•Built-in VPN, load balancer, NAT, DHCP and firewall</li> <li>•Centralized and integrated management</li> <li>•Lower cost</li> <li>•Overall management simplified</li> </ul>

Table 3. Comparing Security Complexity with and Without vShield

**Strong: Adaptive Security Optimized for Virtualization**

Traditional security models were built to support static, physical workloads: Security solutions are attached to the hardware where the applications reside, and applications with similar trust levels are segregated into rigid silos. But what happens in a cloud environment where an application may change its host location several times a day, or applications with different security levels reside on the same infrastructure?

### Adaptive Virtual-Machine Security

vShield can make traditional security solutions stronger by enabling a more dynamic and adaptive form of security. With vShield, network security policies are defined in the vCenter management console and applied at the hypervisor layer, meaning virtual machines no longer need to be “pinned” to a particular host or cluster, enabling customers to leverage dynamic mobility capabilities such as live migration, automated load balancing and automated virtual-machine restart. The centralized security model also enables customers to define security at the logical level instead of the physical level, making it possible for applications with different security requirements to coexist on the same infrastructure. These two capabilities make adaptive trust zones a reality—you can operate groups of virtual machines with different security requirements together in the same cloud infrastructure.

Without a comparable solution, competitors must rely solely on VLANs and port rules for the segregation of virtual-machine traffic. This approach can be too rigid for a cloud environment that is constantly changing, and it can create VLAN sprawl, which leads to gaps in enforcement points.

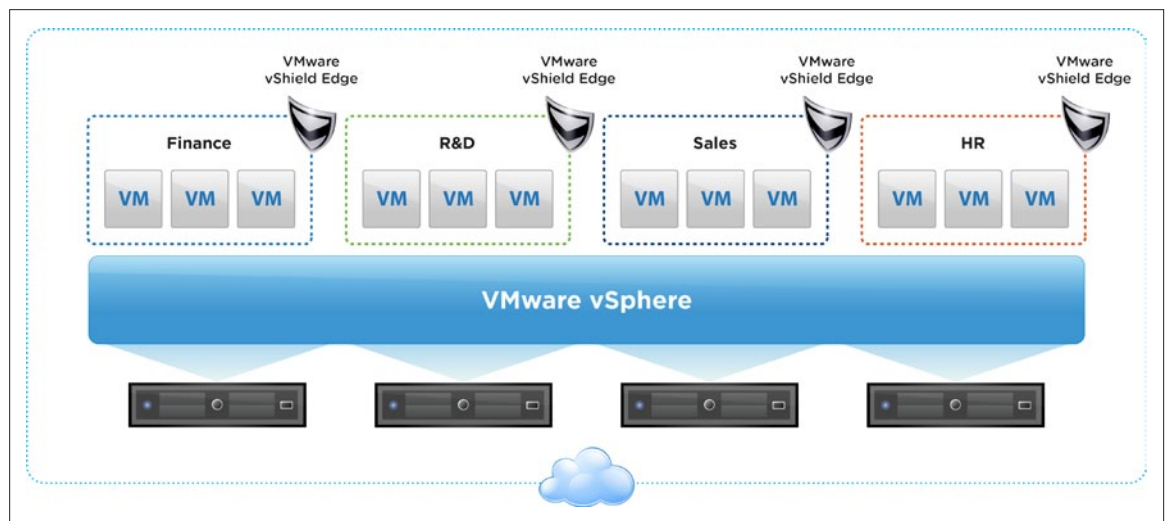


Figure 8. Adaptive Trust Zones with vShield

### Antivirus Protection

Antivirus (AV) is a crucial component of every company’s security plan. Conventionally, antivirus solutions rely on agents that are installed in every operating system. These agents communicate with a centralized server and ensure that the latest antivirus definition files have been updated and applied. The problem arises when multiple virtual machines are virtualized on the same host with an AV agent in every guest operating system. When all agents update their definition files or scan at the same time, an “AV storm” results, causing considerable performance degradation.

vShield has resolved this problem with its unique introspection capability. Instead of multiple agents, a single tamper-proof security virtual machine provided by VMware’s security partners communicates to each virtual machine and streamlines antivirus and anti-malware deployment. Independent testing has shown that offloading antivirus to one such appliance from Trend Micro demonstrated consistently lower demand for system CPU, memory and disk I/O over traditional agent-based solutions (Tolly Report: [Trend Micro Deep Security 7.5 vs. McAfee and Symantec](#)). The agentless antivirus protection of vShield provides customers with the scalability and flexibility they need to secure their environments.

Traditional security solutions were designed for physical server deployments and adapted for virtual environments. By combining these traditional security techniques with vShield, deployments on VMware are more secure than on physical devices.

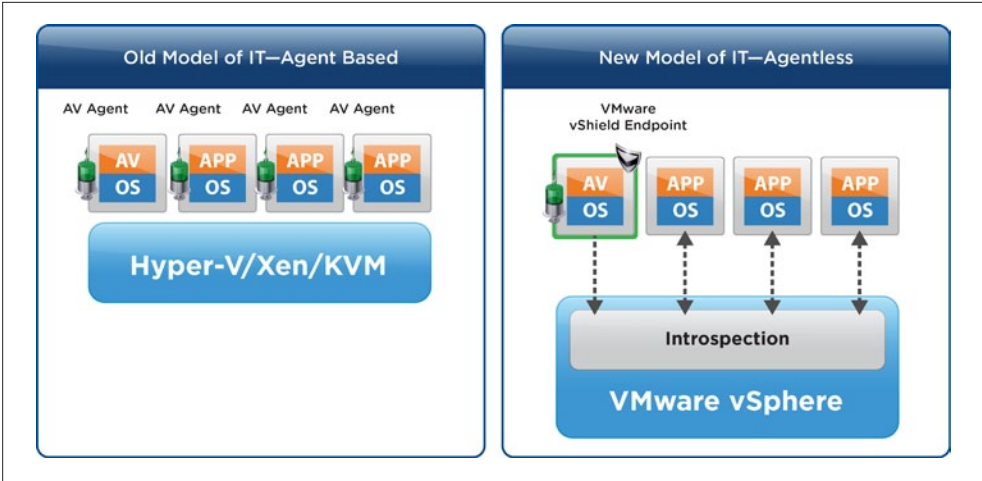


Figure 9. Comparing Antivirus Deployment Methods

	TRADITIONAL SECURITY TOOLS ALONE	SECURITY WITH VSHIELD
Adaptive Virtual-Machine Security	<p><b>Rigid policies, tied to server</b></p> <ul style="list-style-type: none"> <li>•Security limited to the server itself</li> <li>•Virtual machines cannot migrate freely to other hosts</li> <li>•Virtual machines must be segregated by trust</li> <li>•Virtual machines that are compromised have access to everything within the trust zone</li> </ul>	<p><b>Adaptive trust zones</b></p> <ul style="list-style-type: none"> <li>•Security groups become a logical construct rather than physical server construct</li> <li>•Security groups enforced with virtual-machine movement</li> <li>•Mix of virtual machines from different groups on the same host</li> <li>•Instant quarantining of compromised virtual machines to protect other applications</li> </ul>
VM-to-VM Security	<p><b>Limited to VLAN rules</b></p> <ul style="list-style-type: none"> <li>•Security breaks when virtual machines move</li> <li>•Not scalable; creates “VLAN sprawl”</li> <li>•Gap in enforcement points</li> </ul>	<p><b>Hypervisor-level firewalls</b></p> <ul style="list-style-type: none"> <li>•Unlimited scalability</li> <li>•Change-aware</li> <li>•Virtualization-aware</li> </ul>
Antivirus Protection	<p><b>Agent-based</b></p> <ul style="list-style-type: none"> <li>•Agents are resource-intensive; difficult to scale for virtual desktop infrastructure (VDI), large cloud deployments</li> <li>•Susceptible to “AV storms,” which can cause 100% saturation of CPU and storage appliance ports</li> </ul>	<p><b>Agentless</b></p> <ul style="list-style-type: none"> <li>•Agentless architecture improves performance and scales well for large environments</li> <li>•AV storms eliminated</li> </ul>

Table 4. Comparing Security Strength with and Without vShield

**Better Compliance at a Lower Cost**

Ensuring a secure environment often requires meeting compliance rules for privacy and isolation. Assessing compliance and remediating compliance gaps in a single server is a manual process; it is labor-intensive and requires highly specialized knowledge. In a cloud environment, the challenge is even greater as the volume of workloads increases and workloads are not static.

VMware helps you manage and improve compliance with two different solutions: vCenter Configuration Manager and VMware vShield App with Data Security.

**vCenter Configuration Manager**

vCenter Configuration Manager enables you to patch and manage both physical and virtual environments with out-of-the-box templates (such as Sarbanes-Oxley, HIPAA, DISA, PCI DSS and NIST). With a single centralized view, you can detect configuration drift, remediate configuration problems and fix security vulnerabilities automatically.

**vShield App with Data Security**

vShield App with Data Security reduces security and compliance risk with continuous dynamic discovery and classification of sensitive business information. It scans your virtualized workloads for sensitive data—such as credit-card information—and reports violations of regulations. With more than 80 out-of-the-box templates corresponding to government and industry information policy regulations, vShield helps you identify and segment virtual machines with sensitive data into a separate trust zone.

	TRADITIONAL SECURITY TOOLS ALONE	SECURITY WITH VSHIELD
IT Resources	<p><b>Specialists required</b></p> <ul style="list-style-type: none"> <li>•Experts in various security compliance issues required</li> <li>•Multiple experts needed to cover multiple security standards</li> </ul>	<p><b>Prebuilt templates</b></p> <ul style="list-style-type: none"> <li>•More than 80 built-in templates for the most common types of sensitive data</li> <li>•One administrator can deploy compliance checks for multiple standards</li> </ul>
Compliance Process	<p><b>Manually intensive</b></p> <ul style="list-style-type: none"> <li>•Each physical and virtual instance must be investigated against multiple standards</li> <li>•Multiple solutions required to complete compliance checks</li> </ul>	<p><b>Automatic discovery</b></p> <ul style="list-style-type: none"> <li>•Continuous assessment performed on both physical and virtual infrastructure</li> <li>•Protection of sensitive business data improved, and compliance to regulatory frameworks validated</li> </ul>
Compliance Visibility	<p><b>Limited</b></p> <ul style="list-style-type: none"> <li>•Reports on compliance come in different formats from different specialists</li> <li>•Compliance reporting occurs during certain intervals of time</li> </ul>	<p><b>Compliance reports</b></p> <ul style="list-style-type: none"> <li>•Compliance results presented in a single, clear report</li> <li>•Compliance tracked over time</li> <li>•Systems brought back to compliance with one-click remediation</li> </ul>

Table 5. Comparing Compliance Methods with and Without vShield

## Lowest Total Cost of Ownership

VMware delivers the best cloud infrastructure solution in the market—a solution that is based on a rock-solid virtualization platform, a pragmatic path to the cloud of your choice, and a better security model.

But what about cost? Other vendors would like you to believe that VMware is too expensive. In fact, they commonly claim that VMware is three to five times more expensive than their own offerings. They also claim that the vRAM entitlements introduced with vSphere 5.0 will cause most customers' vSphere deployments to increase in cost. However, they base their claims on comparisons of upfront licensing with unrealistic vRAM profiles and without taking advantage of pooling. This presents an incomplete story.

Instead, comparisons should be based on total cost of ownership (TCO). Looking beyond the upfront license costs, any company doing a TCO analysis for cloud computing must include the following in its calculations:

- Virtual-machine density per physical server** – How many virtual machines can run per host, and how many servers and software licenses do you need to buy?
- Operational cost savings** – IT administration and maintenance costs dominate IT budgets today. How does each solution improve your IT staff efficiency and reduce operational costs?

*“We’ve already saved \$2.1 million since moving to VMware vSphere, and expect to see these savings grow over the next few years. We’ve consolidated our servers at a 20:1 ratio, significantly reducing hardware costs. We’ve saved energy and space. We’ve even saved time because VMware technology has eliminated the extra time, steps, and costs of procuring and provisioning physical servers. From an operational and capital expense standpoint, going with VMware vSphere made a lot more sense.”*

— Tom Hines, Chief Information Officer, Trilliant

### Maximize Virtual-Machine Density per Physical Server

Before virtualization, IT organizations would run one application per physical server, so cost-per-server was a quick way to compare costs—it was a one-to-one relationship.

But in a cloud environment, many applications (each in its own virtual machine) run on each physical server—it is now a many-to-one relationship. Consequently, cost-per-server comparisons no longer make sense. A much more accurate metric is cost-per-application, because you want to know the cost of running the entire set of applications required to maintain business operations. This is like asking, “Which is more cost-effective, a 4-door sedan or a 50-passenger bus?” The sedan may cost less up front, but if you need to transport a football team, the 50-passenger bus is clearly more cost-effective! The cost per passenger is much lower because the bus has a higher passenger-per-vehicle density. In a many-to-one relationship, density matters.

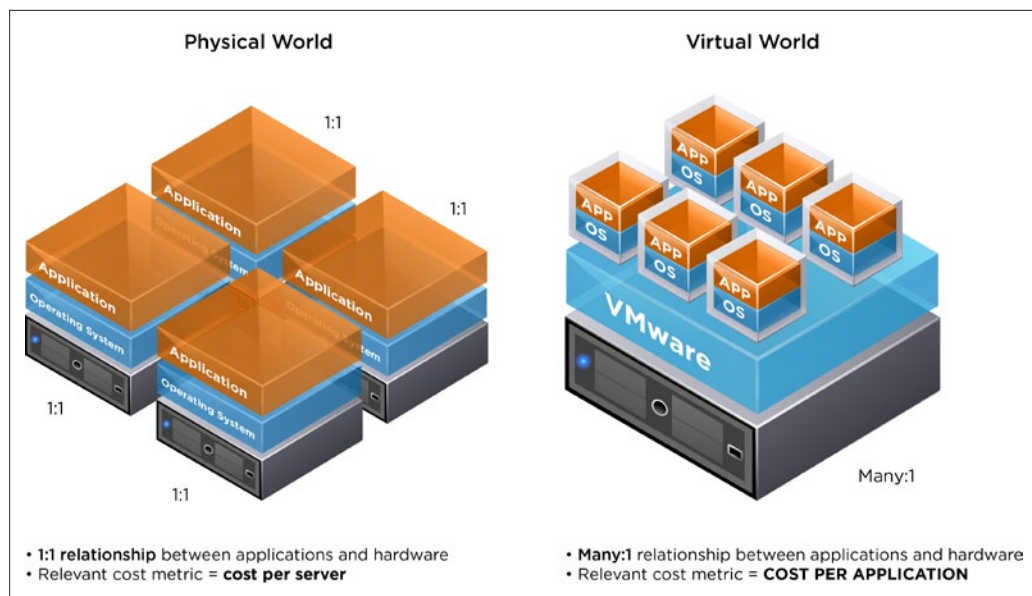


Figure 10. Comparing Metrics for Physical and Virtual Environments

VMware has invested in technologies to achieve very high virtual-machine density on vSphere:

- **Memory oversubscription** – More efficient use of physical RAM enabled by multiple levels of technology: page sharing, reclaiming unused memory, memory compression.
- **DRS with resource pools** – Dynamic load balancing of virtual machines across a cluster enables applications to get required resources when they need them—a “safety net” that lets administrators run individual servers at higher utilization levels while meeting service-level agreements.

- **High-performance “gang” scheduler** – Ability to account for CPU and I/O needs of virtual machines by dynamically allocating more resources and larger processor time slices to virtual machines.
- **Direct driver model** – VMware ESXi can achieve very high I/O throughput and can handle the I/O requirements for more virtual machines simultaneously requesting hardware resources.
- **Logical resource pools** – Ability to divide host clusters into pools of CPU, memory, networking and storage resources, and assign pools to business units, so they can manage resources independently and without wasteful dedication of hardware.

No other cloud infrastructure platform achieves the high virtual-machine density of vSphere and still maintains consistent, high application performance across all running virtual machines.

Virtual-machine density per host (number of concurrent virtual machines that can run on a physical server) directly affects cost per application and is not affected by the new vRAM entitlements. That is because vRAM is measured as a pooled resource across all hosts managed by vCenter, and a typical environment includes virtual machines of various sizes. As an example, a multitiered Web application is generally based on a database server, one or more application servers, and multiple Web servers. Although a virtualized database may require a larger virtual machine (8GB or more of vRAM), Web servers are typically smaller (less than 4GB of vRAM). Because there are more Web servers than database servers deployed in a Web application, the effective average vRAM used is less than 8GB of vRAM.

A typical workload distribution consists of 60 percent small virtual machines (2–4GB of vRAM), 30 percent medium-sized virtual machines (4–8GB of vRAM), and 10 percent large virtual machines (8GB or more of vRAM) for an effective average of 4.8GB of vRAM per virtual machine. As Table 6 shows, the VMware solution can virtualize 200 applications at a lower cost per application and without any effect from the vRAM entitlements.

	<b>VMWARE VSPHERE ENTERPRISE PLUS</b>	<b>VMWARE VSPHERE ENTERPRISE</b>	<b>VMWARE VSPHERE STANDARD</b>	<b>WINDOWS SERVER 2008 R2 WITH SP1 (HYPER-V) + SYSTEM CENTER</b>	<b>CITRIX XENSERVER 6 ENTERPRISE</b>
Number of Applications Virtualized	200	200	200	200	200
vRAM Required	960GB	960GB	960GB		
Number of VMs per Host	29	29	29	24	24
Number of Dual-Socket Hosts	7	7	7	9	9
vRAM Entitlement	14 CPUs * 96GB = <b>1,344GB</b>	14 CPUs * 64GB = <b>896GB</b>	14 CPUs * 32GB = <b>448GB</b>		
Infrastructure Costs	\$256,971	\$256,971	\$256,971	\$328,575	\$300,671
Software Costs	\$147,220	\$138,716	\$123,405	\$123,449	\$122,176
Total Costs	\$404,191	\$395,687	\$380,375	\$452,024	\$422,846
<b>Cost per Application</b>	<b>\$2,021</b>	<b>\$1,978</b>	<b>\$1,902</b>	<b>\$2,260</b>	<b>\$2,114</b>

Table 6. Cost Per Application to Virtualize 200 Applications<sup>1</sup>

## Save on Operational Costs

IT management and operational costs can be several times greater than hardware and software acquisition costs over the lifetime of a server and must be factored into any TCO analysis.

You can directly reduce your operational costs by using the dynamic IT services built in to vSphere, which most competitors do not offer. These services include the following:

- **vSphere Storage vMotion** enables storage array maintenance and upgrades with no downtime impact to end users. In a VMware environment with 200 virtual machines where the opportunity cost of an hour of downtime is \$100 per hour, a company can save an estimated \$40,000 each year with vSphere Storage vMotion.
- **VMware DRS** saves IT from having to manually monitor virtual machines and manually move them to ensure proper resource reallocation. In a VMware environment with 200 virtual machines, a company can save an estimated \$17,500 each year in IT administrative costs by using VMware DRS instead of manually monitoring workload and responding to customer calls.
- **VMware vShield Zones™** enables IT to set up application firewalls for dynamic protection of virtual machines as they migrate. Because it is a software-based firewall built in to vCenter and vShield Manager, vShield Zones saves IT from having to install separate hardware security appliances or respond to virtual-machine migrations as they occur. In a VMware environment with 200 virtual machines, a company can save an estimated \$8,300 in IT administrative costs each year by using vShield Zones.
- **VMware vSphere Distributed Switch and Host Profiles** reduce the complexity involved in setting up and managing the network attached to a VMware virtual environment. Host Profiles simplify how you configure new ESXi hosts by using prevalidated configurations. vSphere Distributed Switch abstracts configuration of individual virtual switches and provides a centralized point of control for cluster-level networking. The two combined can save an estimated \$11,200 in IT administrative costs in a VMware environment with 200 virtual machines.
- **Auto Deploy** enables you to dynamically provision new hosts from bare metal by simply powering on the new server without scripting or intervening in vCenter. Auto Deploy can save an estimated \$10,200 in IT administrative costs in a VMware environment with 200 virtual machines.
- **vSphere Storage DRS and Profile-Driven Storage** are storage management solutions that enable you to streamline storage provisioning, improve application performance by avoiding storage resource bottlenecks, and ensure that application SLAs are met with programmable storage I/O control. These solutions resolve a major IT administrative headache and can save an estimated \$11,200 in IT administrative costs.

By adopting another solution that does not offer these dynamic IT capabilities, your organization would lose these savings.

---

1. Note: The virtual-machine density advantage of VMware over Microsoft Hyper-V with Dynamic Memory and Citrix XenServer with Dynamic Memory Control is based on third-party testing of SQL Server-based workloads on the same physical hosts. For details, see the full reports:

• <http://www.principledtechnologies.com/clients/reports/VMware/vsphere5density0811.pdf>

• <http://www.vmware.com/files/pdf/vmware-maximize-workload-density-tg.pdf>

Being able to run your applications on fewer physical servers directly affects your bottom line by dramatically reducing hardware, software, power, cooling and datacenter space costs.

Don't be misled by other cloud and virtualization vendors claiming they are "free" and less expensive than VMware. Vendors base these claims on only one factor: license price comparison. Such comparisons are oversimplified and misleading. Run your own comparisons with your own numbers using the VMware Cost-Per-Application Calculator ([www.vmware.com/go/costperappcalc](http://www.vmware.com/go/costperappcalc)).



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 [www.vmware.com](http://www.vmware.com)

Copyright © 2011 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-WP-WhyChoose-USLET-103