

Securing the Cloud

A Review of Cloud Computing, Security Implications and Best Practices



Table of Contents

Executive Overview3

What Is Cloud Computing?3

Different Types of Cloud Computing3

Cloud Computing Benefits4

VMware vCloud Initiative: Open, Flexible Cloud Computing5

Enabling a Federation of Internal and External Clouds5

Security in the Cloud6

Integrated Cloud Security6

Cloud Burst Security6

Compliance Concerns6

Defense in Depth6

Security Best Practices in the Cloud7

Cloud Provider Best Practices7

1) Isolate networks7

2) Isolation of management networks7

3) Isolation of VMware VMotion and IP storage networks7

4) Isolation of customer data networks7

5) Secure customer access to cloud-based resources8

6) Secure, consistent backups and restoration of cloud-based resources8

7) Strong authentication, authorization and auditing mechanisms8

8) A library of secure and up-to-date templates of base OS and applications8

9) Resource management to prevent denial of service (DoS) attacks8

Customer Security Best Practices8

1) Follow standard best practices for securing operating systems9

2) Encrypt critical data9

Cloud Security Reference Architecture9

1) Security profile per compute profile10

2) Security DMZ for vApp10

3) OS management10

4) Resource management10

5) Security profile per network10

6) Data security10

7) Security authentication, authorization and auditing10

8) Identity management (SSO, entitlements)11

Summary11

Executive Overview

Today's IT budgets are tighter than at any time in recent history. But despite severe budget constraints, user demands are still escalating—as they always will. To survive in today's economy, businesses must carefully scrutinize investments in IT infrastructure to ensure that they match key business needs and deliver intended results in the most efficient and cost-effective way. To meet these challenges, IT organizations are increasingly moving away from a device-centric view of IT, to a view that is application-, information- and people-centric. Cloud computing aligns with this new world view.

Cloud computing technology is enabling IT to do more with the infrastructure that already exists, as well as adding new ways to expand capacity quickly and economically by using external cloud computing resources. This technology is enabling IT managers to treat infrastructure as a common substrate on which they can provision services to users faster in a much more flexible and cost-effective way –without having to re-design or add to the underlying infrastructure. Given the benefits of cloud computing, its broad appeal is not surprising. However, this new approach does raise some concerns. Chief among them is securing data in the cloud.

This white paper, jointly developed by VMware and Savvis, will briefly review the basic fundamentals of cloud computing and describe how virtualization and the VMware vCloud™ (“vCloud”) initiative are enabling enterprises to move toward a flexible, federated computing model with a cohesive mix of private external and internal cloud environments. It then discusses the security implications of cloud computing and provides insights into addressing them, and offers a view of security best practices to adopt when considering cloud services.

What Is Cloud Computing?

Cloud computing refers to the use of networked infrastructure software and capacity to provide resources to users in an on-demand environment. With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other devices.

Cloud infrastructure can reside within the company's datacenters (as internal clouds or on-premise solutions) or on external cloud computing resources (off-premise solutions available through service providers). It encompasses any subscription-based or pay-per-use service that extends existing IT capabilities.

Typically, Clouds utilize a set of virtualized computers that enable users to start and stop servers or use compute cycles only when needed (also referred to as utility computing). By design, cloud computing is scalable, flexible and elastic –offering IT staff a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure, training new personnel or licensing more software.

Different Types of Cloud Computing

Companies can leverage cloud computing for access to software, development platforms and physical hardware. These assets become virtualized and available as a service from the host:

- 1. Application and Information clouds** – Sometimes referred to as Software-as-a-Service, this type of cloud is referring to a business-level service. Typically available over the public Internet, these clouds are information-based.
- 2. Development clouds** – Sometimes referred to as Platform-as-a-Service, cloud development platforms enable application authoring and provide runtime environments without hardware investment.
- 3. Infrastructure clouds** – Also referred to as Infrastructure-as-a-Service, this type of cloud enables IT infrastructure to be deployed and used via remote access and made available on an elastic basis. Savvis Cloud Compute is an example of this type of cloud.

Cloud Computing Benefits

Cloud computing is enabling the enterprise to:

Expand scalability – By utilizing cloud computing, IT staff can quickly meet changing user loads without having to engineer for peak loads.

Lower infrastructure costs – With external clouds, customers do not own the infrastructure. This enables enterprises to eliminate capital expenditures and consume resources as a service, paying only for what they use. Clouds enable IT departments to save on application implementation, maintenance and security costs, while benefiting from the economies of scale a cloud can offer compared to even a large company network.

Increase utilization – By sharing computing power between multiple clients, cloud computing can increase utilization rates, further reducing IT infrastructure costs.

Improve end-user productivity – With cloud computing, users can access systems, regardless of their location or what device they are using (e.g., PCs, laptops, etc.).

Improve reliability – Cloud computing can cost-effectively provide multiple redundant sites, facilitating business continuity and disaster recovery scenarios.

Increase security – Due to centralization of data and increased security-focused resources from cloud computing providers, cloud computing can enhance data security. Cloud computing can also relieve an IT organization from routine tasks, including backup and recovery. External cloud service providers typically have more infrastructure to handle data security than the average small to midsize business.

Gain access to more sophisticated applications – External clouds can offer CRM and other advanced tools that were previously out of reach for many businesses with smaller IT budgets.

Downsize the IT department – By moving applications out to a cloud, IT departments can reduce the number of application administrators needed for deployment, maintenance and updates. IT departments can then reassign key IT personnel to more strategic tasks.

Save energy – Going “green” is a key focus for many enterprises. Clouds help IT organizations reduce power, cooling and space usage to help the enterprise create environmentally responsible datacenters.

Challenges of Existing Cloud Computing Solutions

Like any new trend or technology, we must address some challenges that cloud computing poses before we can recognize its full value. These include:

A lack of interoperability – The absence of standardization across cloud computing platforms creates unnecessary complexity and results in high switching costs. Each compute cloud vendor has a different application model, many of which are proprietary, vertically integrated stacks that limit platform choice. Customers don't want to be locked into a single provider and are often reluctant to relinquish control of their mission-critical applications to hosting service providers.

Application Compatibility – Most of the existing public compute clouds are not interoperable with existing applications and they limit the addressable market to those willing to write new applications from scratch.

Difficulty in meeting compliance regulations – Regulatory compliance requirements may limit the use of the shared infrastructure and utility model of external cloud computing for some environments. Achieving compliance often requires complete transparency of the underlying IT infrastructure that supports business-critical applications, while cloud computing by design places IT infrastructure into a ‘black box’ accessible only through well-defined interfaces. As a result, internal compute clouds may be a better solution for some applications that must meet stringent compliance requirements.

Inadequate security – By design, cloud vendors typically support multi-tenancy compute environments. IT managers must look for a balance between the security of an internal, dedicated infrastructure versus the improved economics of a shared cloud environment. Security can be a key inhibitor to adoption of cloud computing and will be the primary focus of the remainder of this whitepaper.

VMware vCloud Initiative: Open, Flexible Cloud Computing

The VMware vCloud initiative brings to the industry a new platform for cloud computing that addresses the key inhibitors, allowing companies of all sizes to realize the benefits of enterprise-ready private compute clouds. It brings together applications, flexible infrastructure, a service provider ecosystem, and VMware vCloud technologies to enable a broad array of new services.

The VMware vCloud initiative provides the software and services to build complete internal and hosted clouds and connect the two together in a federated environment. VMware vCloud is built on the industry leading VMware® technology, ensuring high reliability, compatibility with any application, high scalability and extreme performance. VMware vCloud brings three unique characteristics to cloud computing :

- **Choice:** The VMware solution uses the Open Virtualization Format (OVF) standard, a platform-independent, efficient, extensible and open packaging and distribution format for virtual machines. VMware vCloud supports any application or operating system with a seamless ability to combine cloud services with in-house infrastructure.
- **Mobility and Technology:** Leveraging key VMware technology advancements, including VMware VMotion™, VMware Storage VMotion, VMware Distributed Resource Scheduler (DRS), and VMware vCenter™ Server, users know they can easily move virtual machines without downtime. This gives users the ability to manage, move and operate applications in the cloud as easily as they are in more traditional IT environments.
- **Application Support:** VMware vCloud is compatible with all applications, so no rewriting is required. The applications that run in the business today will work the same in the cloud, without recoding or building them on a cloud-only platform, saving time and valuable development resources.

Enabling a Federation of Internal and External Clouds

Obtaining the benefits of cloud computing does not need to be an “all-or-nothing” proposition. The most effective scenario is a federated environment of internal and external clouds. With this model, IT managers can make intelligent and flexible decisions about what parts of their application loads they want to run internally and what parts externally – and then have the ability to change their minds quickly and easily as the business goals evolve.

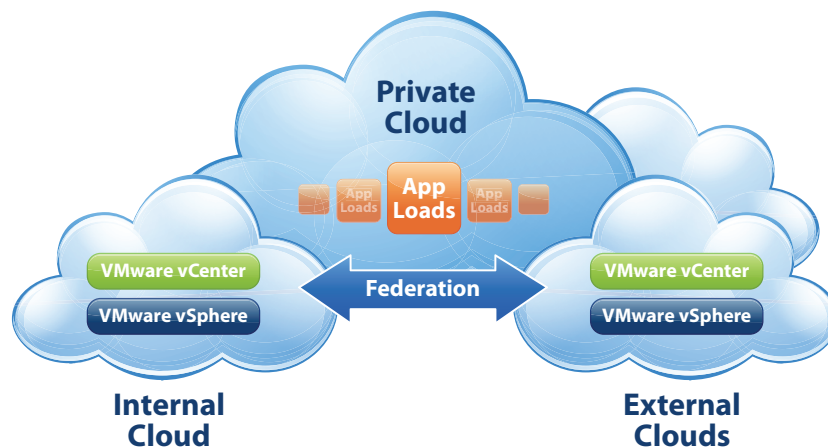


Figure 1. VMware vCloud Components

Security in the Cloud

Conventional infrastructure security controls designed for dedicated hardware do not always map well to the cloud environment. Cloud architectures must have well-defined security policies and procedures in place. Realizing full interoperability with existing dedicated security controls is unlikely; there has to be some degree of compatibility between the newer security protections specifically designed for cloud environments and traditional security controls.

Integrated Cloud Security

Traditional environments segment physical servers with VLANs. Cloud environments should take this same approach and segment virtual machines by VLANs through Port Group configurations. Since these are physical servers, traffic flows are visible to traditional network-based security protection devices, such as network-based intrusion prevention systems (IPSs). The concern in cloud environments is that IPS systems provide limited visibility to inter-virtual machine traffic flows. These are the flows between virtual machines on the same VLAN. By default, those traffic flows are not visible to traditional network-based security protection devices located in the datacenter network. Administrators must make specific architecture and configuration decisions either to make the virtualization solution work with current security tools or to integrate security appliances into the virtualization architecture.

IT teams can also leverage a virtual infrastructure aware IPS solution, integrated with the hypervisor, to provide the needed visibility and security to prevent communication directly between hosted partitions within the virtual server. These directly integrated solutions employ hypervisor-based APIs, and can also be used to ensure that even offline virtual machines are protected and can stay up to date with patches, AV/IDS signatures filters and rules while they are in an offline or mobile state.

Cloud Burst Security

One of the primary advantages of cloud computing is that enterprises can move applications that consist of several virtual machines to the cloud provider when the physical environment requires additional processor or compute resources. These bursting virtual machines need security policies and baseline histories to move with them. When a virtual machines moves, if the security policy does not accompany it, that virtual machines becomes vulnerable. In addition, when virtual machines move, they lose their performance histories and administrators must re-evaluate the virtual machine performance baselines.

Compliance Concerns

The auditing community is aware that current practices for auditing cloud environments are inadequate. As compliance grows in importance, enterprises implementing clouds need to satisfy their auditors' concerns, especially since creating an identity for an individual virtual machine and tracking that virtual machine from creation to deletion creates challenges for even the most mature virtualized environments. Virtual machine sprawl— when the number of virtual machines being created is growing more quickly than an enterprise's ability to manage them— adds complexity.

Defense in Depth

Strategies for ensuring perimeter security have evolved significantly over the last few years. Today, most enterprises have deployed layered defense strategies, but server virtualization can complicate matters. In an attempt to consolidate servers, many organizations have left themselves vulnerable to the inter-virtual machine communications that exist, because if one virtual machine is compromised, then all the other virtual machines that are part of the virtual network can be compromised without anyone detecting it.

By providing security services from within the cloud provider infrastructure, enterprises are able to deploy security policies and rules between each virtual machine (or between virtual machine centers) as they would in the physical world. A feature of the cloud provider infrastructure is that enterprises can maintain corporate security policies and the data collected about them with the virtual machines. This allows them to enforce security services in the enterprise and the cloud provider consistently

Security Best Practices in the Cloud

Like any technology, best practices exist to ensure the secure processing and storage of data. In this section, we will discuss a number of best practices that should be followed when housing critical systems and data in a cloud environment. For the purposes of this paper, we categorized best practices by cloud provider and the data owner.

Cloud Provider Best Practices

The cloud provider is going to take on most of the responsibility of employing the best practices as it is providing the infrastructure for the customer. The primary theme of the service provider's responsibility is around providing a secure and isolated environment for each customer. Each customer should only be able to access his or her own environment and no other customer's environment in any way. No customer should have any visibility into the structure, systems, data or any other attributes of another customer's environment.

1) Isolate networks

The first responsibility of the cloud provider is to provide a level of isolation between all of the different networks that are a part of the virtualization infrastructure. These networks include management networks, VMware VMotion or Live Migration networks, IP storage networks, and individual customer networks. All of these networks should be segmented from each other. Administrators can use a couple primary methods to achieve isolation. First, they can use separate virtual switches for each of the networks, which also requires using separate physical NICs to uplink the virtual switches to the physical network. Additionally, they can use 802.1Q VLANs, which allows for much greater scaling of the virtual environment and the most flexibility. The last option is a combination of the two methods and using a virtual switch and 802.1Q VLANs for management, VMware VMotion and IP Storage networks, and a virtual switch and 802.1Q VLANs for the customer networks. A firewall between networks helps to prevent any potential of traffic being routed accidentally between each other.

Next, we will talk about each of the different types of networks and focus on why it is important to isolate them.

2) Isolation of management networks

Cloud infrastructure management networks are how cloud providers access the infrastructure and manage the different components within that infrastructure. Only authorized administrators should have access to this network because control of the management interfaces of the individual virtualization hosts allows for complete control of all of the virtual machines on that host. Root access on this interface is analogous to having the keys to a physical rack of servers within a datacenter. Administrator access to the central management console that manages all of the different virtualization hosts within the cloud is analogous to having the keys to the datacenter and every rack within that datacenter. Therefore, protection of these interfaces is of paramount importance, and a customer should never need direct access to any of the systems within this network.

3) Isolation of VMware VMotion and IP storage networks

Both VMware VMotion and IP Storage networks should be on isolated and non-routable networks. There is no reason why any outside connectivity is needed into this network. The reason for isolating this traffic is two-fold. First, both VMware VMotion and IP storage traffic need very fast data rates for optimal performance. Furthermore, traffic travels over the network in clear text and is susceptible to an attacker sniffing sensitive information off the network. By fully isolating this network, an attacker would need physical access to this network to have any chance of successfully compromising this data.

4) Isolation of customer data networks

Companies should isolate customer data networks from each other and from any management networks. This can be accomplished in both a secure and scalable way using 802.1Q VLANs and firewalling between the networks to ensure that no traffic is routed between networks. Administrators can employ either physical or virtual appliance firewalls/IDS/IPS to provide powerful security between networks.

5) Secure customer access to cloud-based resources

Customers will need to have a way to access their resources that are located within the cloud and be able to manage those resources in a secure manner. Therefore, it is incumbent upon the cloud provider to supply the customer with a management portal that is encrypted. SSL Encryption would be the most common tool for this task.

6) Secure, consistent backups and restoration of cloud-based resources

The service provider should be able to supply the customer with a transparent and secure backup mechanism to allow the customer's cloud-based resources to be backed up on a consistent basis and enable fast restoration in the event of downtime. Snapshot and cloning capabilities of VMware virtualization technology make it possible to backup and restore data, and also complete operating systems and applications running within those operating systems.

7) Strong authentication, authorization and auditing mechanisms

It is very important in this type of shared environment to properly and securely authenticate system users and administrators, and provide them with access to only the resources they need to do their jobs or the resources that they own within the system. It is also very important in a cloud environment to know who is doing what within the system, when they did it, and what exactly they did.

Separating duties and enforcing least privilege applies for both the cloud provider and the customer. The cloud provider should ensure that only authorized administrators have access to resources. They should also provide the customer with a mechanism for giving internal administrators access to necessary resources. Any access to the cloud resources by either the customer or the cloud provider needs to be logged for auditing purposes. It's critical to follow industry best practices to harden the cloud infrastructure. Both vendors and third parties such as STIG or CIS provide these best practices.

8) A library of secure and up-to-date templates of base OS and applications

One of the biggest security risks with any type of technology is the potential for misconfiguration that results in opening a security hole within that system. To prevent misconfiguration, using securely configured templates or "gold image" of operating systems and applications is an excellent practice. However, the key to this being effective is keeping the templates up to date with all of the necessary security patches and anti-malware signatures. The responsibility to provide these "gold images" can fall on either the service provider or the customer. Along with using a "gold image," administrators should implement a multi-step approval process for putting virtual machines into production. Lifecycle management tools not only require that proper approval be obtained before a virtual machine can be provisioned, but it also can require virtual machines not to be provisioned from a known, good template, and add another level of approval once it is ready to be moved into production.

9) Resource management to prevent denial of service (DoS) attacks

Many think of resource management as a way to separate the cloud-based resources between customers within the cloud based on what the customer has paid for. Resource management also has a very important security function, which is to prevent the potential for DoS attacks. For example, if resource management is not in place, a compromised virtual machine could allow an attacker to starve all of the other virtual machines within that cloud of their needed resources. By using resource management, a compromised virtual machine can only affect itself and none of the other virtual machines within the cloud.

Customer Security Best Practices

While the burden of securing the cloud goes to the service provider, the customer collocating resources should keep in mind the following:

1) Follow standard best practices for securing operating systems

Administrators should secure operating systems that run in the cloud in the exact same manner as the OS running within the customer's datacenter using the same practices for such tasks as hardening the OS, keeping up to date with the latest patches, and installing endpoint based antivirus, IDS/IPS, and firewalls. Using gold images as described earlier simplifies this process.

2) Encrypt critical data

Data encryption adds a layer of protection, even if a system is compromised. Encrypting data in transit is especially important, as that traffic will be traversing a shared network and could potentially be intercepted if an attacker gains access at a critical point in the network. Encrypting the data as it traverses the network makes it much more difficult for an attacker to do anything with intercepted traffic.

Encrypting critical data “at rest” within the virtual disk file is also very important. This will protect critical data from “walking off,” and will make it much more difficult for an attacker to compromise data, even if they are able to compromise an endpoint.

Cloud Security Reference Architecture

Reference architectures are useful for understanding how various recommendations come together to provide a complete solution. Enterprises that are interested in cloud computing models should consider the following reference architecture to ensure adequate security and optimal functionality.

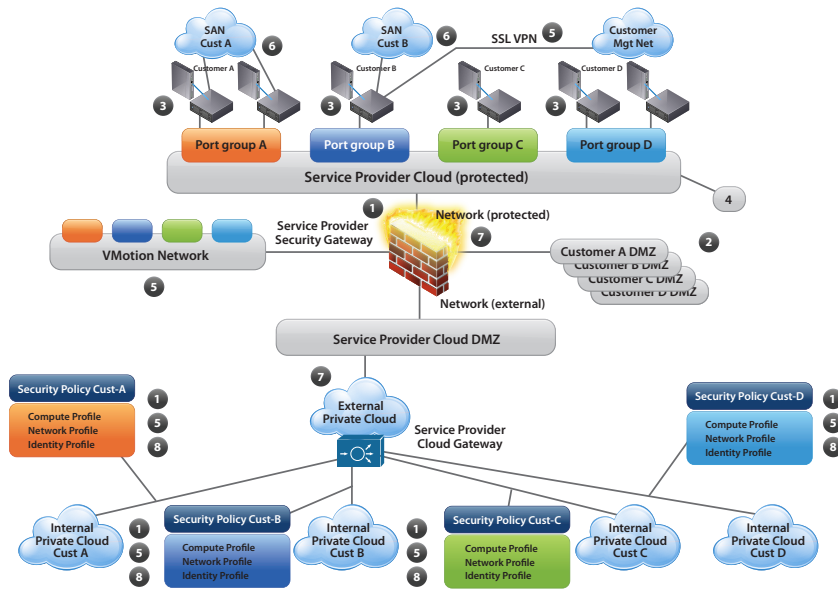


Figure 2. Cloud Security Reference Architecture

Diagram Key:

- 1) Security profile per compute profile
- 2) Security DMZ per vApp
- 3) OS Management
- 4) Resource Management
- 5) Security profile per network
- 6) Data Security
- 7) Security Authentication, Authorization, and Auditing
- 8) Identity Management

1) Security profile per compute profile

Administrators should communicate enterprise corporate security policy and server tier firewall rules that are defined within a vApp to the service provider. This should include corporate server security patch levels, anti-virus status and file-level access restrictions. The VMware vCloud reference architecture provides a method to communicate the policies and server tier firewall rules for the vApp.

2) Security DMZ for vApp

The service provider needs to validate the patch level and security level prior to bringing a vApp into the production environment. The VMware vCloud reference architecture should include a DMZ area for validating the vApp and mitigating any security violations according to each enterprise's security profile.

3) OS management

It is important to understand the security hardening performed around the service provider's library of OSs and patching policies. Administrators should update traditional security policies that govern the service provider's hosting environment to ensure that virtual machines are hardened and patched within the standard enterprise policies. Administrators should update virtual machines that are not at the correct patch level to the correct patch level through a DMZ, for example.

4) Resource management

The service provider needs to separate and isolate the resources each customer virtual machine uses from other customers' virtual machine resources to prevent DDoS attacks. These attacks are usually caused by log files not having limits or CPU or memory utilization increasing on a single virtual machine through memory leaks or poorly behaving applications.

5) Security profile per network

In addition to the vApp having a compute security profile, there should also be a network security profile to ensure perimeter and Web access security. This includes functionality like switch and router Access Control Lists (ACLs), perimeter firewall rules, or Web application security (Application Firewall, URL Filtering, whitelist and blacklists). The VMware vCloud reference architecture provides a method to communicate the network security profile.

A critical component of the reference architecture is the isolation of networks; enterprises need to ensure that service providers implement separate management networks and data networks per customer. In other words, there needs to be complete isolation between each customer's virtual machine and the data traffic connecting to their virtual machines. In addition, service providers should have a separate network for VMware VMotion and VMware VMsafe™. Enterprises should request that service providers encrypt all management traffic, including VMware VMotion events.

Many enterprises will require encryption of data packets via SSL/IPSec, or management connectivity via SSL or SSH. Some service providers offer only shared or open connectivity. At a minimum, all management connectivity should be provided via SSL.

6) Data security

Enterprises should request service providers provide access paths to only the physical servers that must have access to maintain the desired functionality. Service providers should accomplish this through the use of zoning via SAN N-Port ID virtualization (NPIV), LUN masking, access lists and permission configurations.

7) Security authentication, authorization and auditing

Cloud service provider environments require tight integration with enterprise policies around individual and group access, authentication and auditing (AAA). This involves integrating corporate directories and group policies with the service provider's policies. Service providers should offer stronger authentication methods to enterprises, such as 2-factor hard or soft tokens or certificates. The enterprise should require a user access report, including administrative access as well as authentication failures, through the service provider portal or via a method that pulls this data back to the enterprise. The VMware vCloud reference architecture provides a method to communicate the access controls and authentication needs to the service provider.

8) Identity management (SSO, entitlements)

Cloud environments require control over user access. Cloud providers must define a virtual machine identity that ties each virtual machine to an asset identity within the provider's infrastructure. Based on this identity, service providers are able to assign user, role and privilege access within the extended infrastructure to provide role-based access controls.

Enterprises also want to prevent unauthorized data cloning or copying from a virtual machine to a USB device or CD. Service providers can prevent cloning and copying of virtual machines using a combination of virtual machine identity and server configuration management policies.

Summary

Enterprises that are looking for ways to streamline internal IT operations, to expand on-premise infrastructure and add capacity on demand, or to fully outsource the infrastructure are all investigating the many advantages of cloud computing.

While cloud computing offers a fundamentally new way to cost-effectively and quickly deploy new services and augment existing capabilities, it's not without its challenges. Chief among these challenges is security. IT staff can readily address security concerns by deploying the appropriate solutions and following best practices as they relate to each company's unique business requirements.

For more information on VMware vCloud initiative, please visit

- www.vmware.com/vcloud

For more information on Savvis Cloud Security Solutions, please visit

- www.savvis.com/en-US/Solutions/Pages/Cloud.aspx



VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2009 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. VMW_09Q2_WP_Savvis_P12_R3

