GameChanger

GAME CHANGING TECHNOLOGY TO MEET AGENCY MISSIONS

When the Hybrid Cloud Model Makes Sense

There are many good reasons why agencies choose to put their data, infrastructure or applications in a private cloud; resources are dedicated only to that agency or group of agencies, and security and content are fully controllable. In fact, the majority of federal cloud projects rely solely on private clouds.

Yet there are many situations when the hybrid cloud model makes more sense, both from the financial and flexibility perspective. As its name suggests, a hybrid cloud model is a mixture of features from both private and public clouds, either on or off premise. There are many ways that agencies can leverage hybrid clouds, such as:

Managing assets and dealing with demand spikes. An agency can rely on its internal resources until those resources are at full capacity, and at that point, automatically switch to a secure public cloud instance to gain capacity as needed. Once the demand has slowed, the workload would automatically revert back to private resources.

Saving money. While sensitive data should always remain on private resources, agencies often have computing workloads that aren't sensitive. By keeping these

on the public cloud, agencies can save money, since public cloud resources tend to cost less than private. Another way to save money with the hybrid model is by moving standard business applications like collaboration software and email to a secure area of a public cloud.

Testing and development. Testing and developing new applications and services requires a great deal of capacity, but only for a short time. This is a situation ready-made for the hybrid cloud, because it gives developers access to the resources they need when they need it, yet doesn't require the agency to pay for the resources for longer than necessary.

Disaster recovery/business continuity/ remote storage. If primary resources go down, having a secure area of a public cloud as a backup ensures that business can continue as usual. In addition, agencies often benefit from moving archived information that must be kept for compliance purposes but rarely accessed to a secure area of a public cloud.

Security concerns shouldn't be an inhibiting factor when considering the hybrid cloud model. In addition to choosing FedRAMP-certified cloud providers, agencies should know that cloud service providers today use dedicated network connections and enforce cloud encryption.different server or device in real time.

GOVERNMENT CLOUD, BY THE NUMBERS

18
The percentage that agencies could save, on average, by fully incorporating cloud into their overall strategy.[1]

18.48
The number, in billions, that government agencies will invest in cloud computing by 2018.[2]

41
The percentage of feds who say they are more likely to consider and select a hybrid, community, or public cloud solution because of FedRAMP certification.[3]

44
The percentage of feds who believe their agency is missing out on potential savings by using private clouds instead of public, hybrid or community clouds.[4]

58
Percentage of federal IT professionals who believe that federal initiatives designed to encourage cloud adoption have improved security.[5]

75
Nearly this percentage of large enterprises expect to have hybrid cloud deployments by 2015.[6]

2014
The first year when the majority of workloads will be in the cloud instead of a traditional IT environment.[7]

[1] www.meritalk.com/cloudconfusion
[2] www.marketsandmarkets.com/pressreleases/government-cloud.asp
[3] www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Government-Business-Council-Road-Ahead-Three-Years-After-Cloud-First.pdf
[4] www.meritalk.com/cloudconfusion
[5] www.tripwire.com/state-of-security/top-security-stories/cloud-computing-adoption-federal-agencies-increases-400/
[6] www.govtech.com/library/papers/Why-Expand-to-Cloud-Hybrid-Cloud-Market-Research-IDC-Analyst-Whitepaper.html
[7] www.cisco.com/c/en/us/solutions/service-provider/global-cloud-index-gci/index.html

For the Cloud, Safety Rules

For government agencies looking to take advantage of the cost, scalability and flexibility benefits that cloud computing provides, there has never been a safer time to get started.

The first reason is the Federal Risk and Authorization Management Program (FedRAMP). The program, which started in 2012, provides agencies and contractors with a series of steps regarding security assessment, authorization and continuous monitoring for cloud products and services. It includes more than 300 security controls.

FedRAMP recently took a giant leap forward. Starting in June 2014, cloud service providers working with the federal government must have their cloud services certified as compliant. So far, about a dozen cloud vendors have been authorized to operate cloud services on behalf of the federal government, and more are working toward certification. In addition, more than two dozen third-party assessment organizations have passed the requirements to verify cloud vendors' FedRAMP compliance.

There are other reasons why agencies can be more confident that cloud security is assured. One way is by relying on the National Institute of Standards and Technology's (NIST) guidelines on security and privacy, including its Cloud Computing Security Reference Architecture. The architecture helps agencies choose cloud-based services that address an agency's specific requirements in the most secure manner. And defense agency clouds can now rely on FedRAMP in addition to DOD requirements, instead of also having to comply with the DOD Information Assurance Certification and Accreditation Process (DIACAP).

In addition to working only with cloud service providers whose offerings have been certified as FedRAMP-compliant, agencies should ask these questions before making a decision:

- Does your system meet our other security requirements? These may include SOC, ITAR; HIPAA; FISMA Low, Moderate or High; any number of other federal security regulations, or specific state regulations.
- Have your personnel all passed background checks?
- Are your data centers on U.S. soil?
- Can you meet our specific requirements?
- Does your security policy include provisions that require notifying customers of security breaches?
- How do you guarantee your Service Level Agreement (SLA)?
- What is your disaster recovery plan?
- Do you have other government customers? Can we talk to them?

WHAT IS MULTI-TENANCY, ANYWAY?

MUCH LIKE MULTIPLE TENANTS share an apartment building, a multi-tenant cloud is one where several organizations share a computing resource in the cloud. A multi-tenant architecture distributes a single instance of software or other resource among multiple users. Each organization's data is separated from the rest and fully secure. Here is what you need to know:

Q: Why is it called multi-tenancy?
A: A tenant is an application that requires its own separate, secure computing environment. In a multi-tenant environment, a cloud service is shared among several organizations and managed by all of the organizations together or a third party managed service provider.

Q: How is multi-tenancy different from the hybrid cloud?
A: A hybrid cloud is a mix of public and private clouds, while a multi-tenant cloud is an infrastructure shared by several organizations that can include several private clouds, a combination of public and private clouds, or only the public cloud.

Q: How secure is a multi-tenant cloud?
A: Since multiple organizations are sharing resources, security is critical. In addition to being FedRAMP-certified, a secure multi-tenant cloud will encrypt data both at rest and in motion, fully separate the data of each group sharing the resource, and require usernames and passwords. Nobody—not even the hosting provider—can access an organization's data.

Q: Is a multi-tenant cloud the same as a community cloud?
A: Basically, yes. The idea is the same; a cloud service model shared by several organizations with similar requirements. It's ideal for organizations collaborating on projects, research or applications. In the case of government, several agencies that need to operate under a HIPAA-compliant infrastructure might use this model.

Q: What are the benefits of a multi-tenant environment?
A: Because you're sharing resources, costs are lower. And even though you're all sharing one instance of an application, for example, you can still customize your instance.

Secure, Compliant Hybrid Clouds with Government in Mind

Whether spurred by the need to increase efficiency, meet government mandates or deal with rapidly expanding data sets and workloads, more and more agencies are moving some or all of their applications or infrastructure to the cloud.

And for many agencies, the most cost-effective, secure and efficient solution is a hybrid cloud model that allows them to not only leverage their existing investments in IT infrastructure, but also extend their systems seamlessly to the technology platform that best meets their needs.

VMware vCloud® Government Service provided by Carpathia® is helping agencies do just that—accelerating federal cloud adoption by providing a familiar platform that combines a dedicated private cloud with a secure government community cloud designed specifically to meet the needs of agency workloads, while satisfying stringent security requirements such as FedRAMP.

Most agencies today are already using VMware in some way, whether it's vSphere to manage data centers, vCloud Director for software-defined data center services, or other VMware products. By choosing to host systems on the vCloud Government Service platform, agencies can leverage their existing investment in VMware solutions and more easily operate a hybrid cloud solution under a common management umbrella.

"With VMware vCloud Government Service provided by Carpathia, agencies can seamlessly run both legacy and new applications on site, off site and in the cloud, using a more supportive and integrated cloud infrastructure that meets FedRAMP security requirements" says Stu Fleagle, Vice President, Carpathia Government Solutions.

vCloud Government Service provides a simple platform for migrating and managing workloads between dedicated virtualized environments using native VMware tools such as vCloud Connector, and affords agencies the highest level of flexibility and control when it comes to how their applications are deployed and managed. It also allows agencies to leverage their IT staff's existing skillsets, easing concerns over the cost and effort required to leverage a hybrid cloud model.

SECURITY AND EXPERTISE, TOGETHER

Carpathia, a leading provider of cloud services and managed hosting for government agencies and enterprises, has partnered with VMware to deliver vCloud Government Service to the market. Together, Carpathia and VMware provide the only enterprise-class hybrid cloud service that provides VMware capabilities with the added security and compliance assurance of FedRAMP authorization.

"An agency can put its dedicated infrastructure for a certain program or for the entire enterprise inside our IBX Vault data center and, over a Layer 2 cross-connection, connect right into the vCloud Government Service platform, never losing the security, compliance or standardization," Fleagle explains.

VMware vCloud Government Service provided by Carpathia affords agencies the ability to host their private and community cloud workloads in the same compliant facilities, providing a consistent and secure platform for servicing their users.

For agencies that experience cyclical spikes in capacity requirements, this setup is ideal. If an agency collects fees from its constituency on a quarterly basis or processes program applications at certain times, for example, it can quickly expand beyond its dedicated infrastructure to additional resources on a secure portion of the government community cloud. Once that spike is resolved, all resources can be returned to the dedicated infrastructure.

Running workloads on vCloud Government Service also lowers overall cost. Not only can agencies avoid the cost of training or retraining IT staff because they are already proficient with VMware technology, but the availability of additional capacity on-demand means that agencies don't have to pay for that capacity when they don't need it.

Nearly two-dozen defense and federal agencies, as well as systems integrators, are currently testing the service for workloads such as development and testing, seasonal or event-driven workloads and disaster recovery. These organizations are now discovering the efficiencies, cost savings and security of running workloads on VMware's vCloud Government Service provided by Carpathia. •

SECURITY AND COMPLIANCE

vCloud Government Service provided by Carpathia maintains compliance across a broad range of regulations, standards and best practices, including:

- FedRAMP
- FISMA
- DIACAP
- ITAR
- FIPS
- HIPAA

carahsoft. | vmware®

CARPATHIA.

Learn more about Carpathia's secure, compliant, enterprise-class hybrid cloud solutions built on VMware at **www.carpathia.com/partner-solutions/vmware.**