vmware®

Five Biggest Cloud Challenges Today

How to Solve Them with a Hybrid Cloud

The cloud has taken the enterprise by storm. The numbers tell the story. A $59 billion industry in 2009, cloud computing hit $150 billion in 2014, according to recent research from IT advisory firm Gartner. And IT industry association CompTIA reported recently that 90 percent of companies are using cloud computing in some form.

Everyone is doing it, but that doesn't mean they're doing it right. Many enterprises are failing to prepare properly for cloud migration, and that's inflicting disastrous results on their business, including prolonged downtime, decreased productivity, even the dreaded data security breach.

Here are the five most serious challenges to cloud implementation and ways for technology executives to ensure success by considering a hybrid cloud environment that uses both internal and external clouds.

1. Wrong Type of Cloud

The cloud is not a one-size-fits-all proposition. That means CIOs must figure out what type of cloud computing architecture best suits their particular business. Are you in a heavily regulated industry? If so, you'll need a cloud solution that meets your compliance and data security requirements before making the transition. Do your homework. Research the various types of cloud services out there and determine which one is best for your business model.

Most companies still think the cloud is just ... one big cloud. In reality, there are private clouds, public clouds, and hybrid clouds. Know which one, or which combination, is right for your business. The hybrid cloud model can maximize the value of all clouds by balancing the use of internal assets and external services. Organizations also benefit from this environment by acknowledging that not all of their IT resources should exist in public clouds.

2. False Sense of Security

While public cloud providers are responsible for the security of their clouds, they're not usually responsible for the security of your servers, applications, and data. In the CDW 2013 State of the Cloud Report, 46 percent of respondents cited "security of proprietary data or applications" as a key challenge. Also, keep in mind that just because a public cloud provider says it is in full compliance with a particular regulation, it doesn't mean your data is 100 percent compliant. You're still required to encrypt and protect your data. To do that, you might need to invest in a suite of tools, including antivirus, malware, and secure Web gateways from multiple security vendors.

Before engaging with a cloud vendor, ask the following questions: What are you doing to protect the confidentiality of my data? What are you doing to ensure my data is not corrupted? Will my data be continuously available? How will you help me if something goes wrong?

If your data is compromised, the loss to your company could far outweigh the amount saved by migrating to the cloud. One of the key benefits of using a hybrid cloud is that you are able to maintain in-house storage for sensitive operations.

3. Miscalculation of ROI

Paying only for what you use is one of the chief attractions of the cloud, so many companies assume a move to the cloud means instant savings. They think they won't need an IT staff, will never need to buy hardware again, and that servers will magically run themselves. That's not the case. When judging ROI, your first task is to calculate the total cost of ownership over a three-to-five-year period to see if moving to the cloud makes financial sense for your business. This means calculating not only the potential savings but the costs associated with cloud migration and management. For instance, how many servers will you need? How much bandwidth? What's your backup plan? How will your system be maintained?

With a hybrid cloud, organizations can achieve the infrastructure automation benefits of a public cloud without sacrificing their existing investments in applications, operations, and management. And be cautious of obscure pricing frameworks some companies use that can negatively impact the pay-per-use benefits of the cloud. For example, some providers publish low usage rates but charge hefty data ingress/egress fees.

4. Inadequate Strategy and Plan

Lack of a change-management strategy as well as poor planning and testing are some of the biggest mistakes firms make when migrating to the cloud. For instance, organizations continue to have trouble implementing cloud systems and demonstrating their value because they have not made the necessary changes around people, processes, and business management.

Implementing a cloud environment requires proper planning. Of course, some systems can have you up and running in a matter of minutes, but that doesn't mean they are perfectly configured for your business. For instance, you should be able to tweak security settings and service levels to better meet the needs of your organization. Also, don't forget to conduct adequate testing prior to launch. This includes running through a variety of use-case scenarios and checking data storage and retrieval capabilities.

You should also look for projects where you can score quick wins to demonstrate credibility. The beauty of the hybrid cloud is that it makes it easier to introduce new functionality quickly and more flexibly.

5. Vendor Lock-in

Vendor lock-in often refers to the migration costs if ever you need to walk away from your current service provider. This lock-in happens when an organization becomes reliant on one vendor and the cost of switching to a new technology platform is so prohibitive that the customer is effectively unable to make a change. A hybrid cloud, with its common infrastructure, management, and security is the ideal choice to avoid lock-in because it offers a capability for seamless migration to and from clouds.

By moving to a hybrid cloud, businesses large and small are reaping the benefits of increased flexibility, faster application deployment, better collaboration, and greater cost savings. Now it's your turn to make the most of the cloud.

vmware®