Avoiding Common Pitfalls in Hybrid Cloud Environments

Moving to the cloud is virtually inevitable for a majority of modern enterprises. Cloud-based solutions and tools with cloud elements like Google's G-suite, Microsoft Office 365, and Salesforce present several organizational benefits and improve productivity to exponential levels. Organizations often utilize a hybrid cloud environment, which entails a mix of private cloud solutions used on the premises and third-party public cloud services with orchestration between the two platforms.

However, there are several considerations that need to be made from an IT perspective before deciding on a solution and groundwork that should be done at the organizational level prior to implementation. Hybrid cloud environments present a host of benefits, but since the convenience and productivity aspects of the cloud are front and center in the evaluation phase, potential technological risks have to take a backseat. Here are the common pitfalls you need to consider when implementing hybrid cloud environments to reduce the likelihood of problems in the future.

1. Understand how you are going to predict, control, and allocate costs of implementing a hybrid cloud solution.

Initial and ongoing costs must be assessed. How much of the IT budget will go toward supporting and maintaining a hybrid cloud environment compared to implementing cloud applications? Personnel costs like new employees or temporary contractors whose skills are needed to introduce the application should be considered, as your current staff may not have the skills or enough hands-on deck to carry out this integration.

It's crucial to understand these costs upfront and also make a long-term plan for how maintenance expenses will be accounted for in the IT budget.

2. Create a defined criteria for your workloads and determine which cloud to allocate them to.

There are several privacy concerns when it comes to cloud storage. Storing employee data, customer data, intellectual property, and other sensitive information in the cloud poses an enormous risk. With the right infrastructure, though, some cloud systems can actually provide a more secure solution than on-premises security. Hybrid cloud environments can assuage many privacy concerns for organizations considering cloud migration as a result.

Tasks and workloads need to have well-defined criteria to manage this risk. The hybrid cloud model can effectively move some workloads to the public cloud, while the data with the most sensitivity and privacy constraints can remain on-premises but with the same portability that the cloud presents. In the planning stage, this must be accounted for to ensure the smooth deployment of applications and data remaining in the organization's control opposed to a data center.

3. Understand how you are going to monitor and manage your hybrid cloud.

More efficient resource management is one of the most-cited benefits of shifting to a hybrid cloud environment: It can take a lot of strain out of managing servers, operating systems, and networks on-premises. In building a hybrid cloud solution, though, decisions still need to be made as to how your technical resources will be utilized. How will ongoing monitoring be managed? Disaster recovery? Which of these aspects will be outsourced to technology partners, and which ones will be developed in-house?

When implementing a hybrid cloud environment, you'll have to determine which technical points will be self-managed and what will be outsourced so that you can focus on putting the cloud system to use and carrying out your tasks.

4. Take security seriously and ask the right questions.

While hybrid cloud environments are primarily designed to alleviate security risks, they still carry plenty of them that your organization needs to recognize and prepare for. Unprotected APIs, DDoS attacks, and poorly constructed cross-platform tools are among the most common technological risks that organizations face. Compliance, data redundancy, lack of data ownership, and inadequate risk assessment also factor into the security risks that hybrid cloud environments entail.

On the human resources side, there are also additional risks posed by disgruntled employees who could have malicious intent and poorly defined management strategies that can turn your hybrid cloud system into a ticking time bomb. Whether your concerns are technological or pertaining to the humans who use and manage the cloud system, they should factor into your security assessment and come up during the design and construction phases.

5. Understand what your compliance requirements are and how you will fulfill those requirements.

Cloud systems offer so much convenience, but they also pose a drastic compliance risk. Industry standards and regulations from all manner of governments need to factor into your hybrid cloud model's design, planning, and implementation. In addition to complying with the laws in which your business is incorporated, you will also need to comply with regulations where you have servers, other physical locations, or even significant amounts of remote employees. Since just one cloud environment already presents challenges with respect to compliance, all of the components of a hybrid model need to be evaluated as both a singular environment and as separate environments in all stages of planning and deployment.

Deploying hybrid clouds through a data center can ease meeting these requirements as the data center also needs to look out for its own compliance risk. Regardless of the method you choose, you must be aware of your requirements and determine how you fulfill them at all stages.

6. Do not underestimate the impact that hybrid cloud deployment may have on your internal team.

Your employees will need training and support at all stages, from planning to deployment, not just so that they can use the new hybrid cloud tools with ease, but because change can be jarring for people. Your tech talent has gotten used to their tools and methods, and a sudden upheaval to their daily routines can cause a major disruption or even unhappiness.

Make sure to provide ongoing training and support with both IT change management experts and trainers who are well-versed in hybrid cloud models.

7. Understand that not all cloud providers are created equal: Understand where they specialize.

Come prepared and with a long list of questions about the types of hybrid cloud environments they have previously built. What industries has the cloud provider specialized in, and what problems are they best known for solving? Which type of enterprise do they serve the most? While all cloud providers have a great deal of talent and experience to contribute to the tech sector and problems they can solve in your organization, you need to find a cloud provider who can design the hybrid cloud model that distinctly fits your organization's needs and challenges. Cloud providers frequently have specific industries they focus on, such as healthcare or retail, as well as enterprise size: A cloud provider who designs solutions for Fortune 500 companies may have solutions for smaller organizations, but be less apt to understand their day-to-day technology issues at this scale.

Comport offers years of trusted expertise in the cloud integration sphere and can set your organization on the right path with an effective hybrid cloud strategy and deployment plan. We can design a hybrid cloud environment that is devised to your specifications and assist you with every step of the design process. Contact us today to speak to one of our cloud computing experts.