

9

Common Cloud Deployment Myths **DEBUNKED...**

and a Pair of Strategies to Start You on Your Way to the Cloud!

By **Mark Gordon**, Enterprise Architect, Aptera

Whether you know all about the cloud or you're still investigating its applicability to your business, chances are good that you have caught wind of some common myths circulating about cloud deployment. Following is a straightforward look at nine common misperceptions about the cloud, followed by two strategies for integrating the cloud into your work environment:



Myth #1: The cloud is mysterious and not well-defined.

Like any new technology, the cloud is mysterious until you learn more about it. Rather than thinking about the totality of the cloud, which can be overwhelming, you might instead think in terms of specific services that could benefit your business. It's easiest to start with the services you already use, such as collaboration tools like e-mail, document management, and communications. Another easy place to start is with file shares and data backups.

But those are just the tip of the iceberg when it comes to what the cloud can ultimately do for your business. Other services that are relatively simple to implement include Windows Azure, which allows you to manage your servers from the cloud and even automatically move your virtual machines to the cloud if you have a local outage. On the desktop and mobile device front, services like Windows Intune give you great control and reporting while allowing you to deploy your software to your machines automatically or on-demand no matter where your people are.

Myth #2: The cloud is always cheaper.

Cloud services are usually less expensive, but not always. For instance, if you already have a service that is running well, paid for, secure, and robust, then it might be hard to justify the expenses associated with moving that service to the cloud and operating it there.

Let's look at some scenarios where operating on the cloud can definitely be cheaper. The cloud is a good option if you need to upgrade or expand your services, or if you need to make them available everywhere. It can also make financial sense if you need to implement disaster recovery, since those offerings are built in to the cloud, and the cost of building a disaster recovery environment can be sizable.

Consider how your current functions are working and where you need to change or expand. There are definitely scenarios where moving to the cloud can save you money, such as offsetting the hard costs of upgrading or growing your current systems.

Myth #3: I lose control in the cloud.

While it is true that you cannot customize many of the services offered in the cloud, most are easily configurable to meet your needs. There are times when you may need to host some parts of your environment yourself because some custom third-party applications aren't available in the cloud. At the same time, savvy application vendors are changing how they integrate their applications with services like Exchange and SharePoint. The top vendors in e-mail archive and Enterprise workflow engines are already shipping cloud compliant versions of their products.

It is also true that you lose the ability to physically see your servers and data centers when you move to the cloud. But having your data physically on the premises doesn't necessarily give you any more control than you have with the cloud. Generally, with the cloud you get a set of well-known interfaces, along with choices about how you want to manage your security, user environment, applications, and data. Most cloud providers provide web interfaces and robust scripting interfaces that make it possible to manage your services from anywhere and to easily automate common tasks through scripting.

You may not be able to see the physical server, but you may end up gaining control through the ability to easily manage your environment from anywhere.

Myth #4: The cloud limits my choices.

You may be limited by the parameters of programs on the cloud, but those choices are often superior to what you are accustomed to. Security policy is a good example. Cloud providers have developed their security environments and policies from the ground up, using insights from some of the best minds in the business. By choosing your cloud vendors carefully, it is very possible that you will actually be increasing your security when you move to the cloud.

Audits are another good example of more effective solutions in the cloud. You may currently do very specific kinds of security audits that aren't possible for you to run in the cloud. But your cloud provider should be able to provide you with their own audits. Many companies such as Microsoft hire very effective third-party auditors to test their environments on a regular basis, and these audits will quite likely be cheaper and more complete than what you were running before.

Scale is another area where people are often confused by cloud services. The notion is that cloud services are designed for one size, which will either be too big or too small. But when it comes to scale, cloud services have several advantages over building an on-premises environment. Platform services like Azure allow you to pay only for the computing cycles you use, to automatically scale from one small server to scores of huge servers on demand, and only pay for what you use when you use it. Application Services like Exchange Online also allow you to pay only for the mailboxes you use and have anywhere from one to tens of thousands of mailboxes in the cloud.

Myth #5: The cloud is all or nothing.

The truth is that you can use the cloud to the extent that you need. Many cloud providers offer services that easily integrate with your on-premises environment. It has become common to integrate the cloud with on-site solutions – like joining archival data storage on the cloud with your on-premises system to free up local storage space, or keeping your PBX on premises while putting voice mail into Exchange Online to save money and make it easier for your people to get their voice mail.

Bottom line: you can move just the parts of your environment to the cloud that you want to and still have everything work together.

Myth # 6: I have to do it all at once.

It often makes sense to move services to the cloud one at a time and also to move users from on-premises servers to the cloud in groups, not all at once. Consider starting by moving e-mail to the cloud for a group of users who need the increased functionality. These users will act as your pilot group. Because of the deep integration possible in services like Exchange Online, it is easy to conduct a proof of concept, move to a pilot, and then implement a phased migration of your users.

Myth #7: The cloud is not secure.

Since people cannot see where their data resides – no rows of servers or physical hard drives – it seems logical for them to have security concerns with the cloud. But the reality is that security on the cloud is much better than you could provide in your own data center. Cloud providers have very stringent security regulations to which they must adhere. And they're working at an enormous scale to build state-of-the-art physical, logical, and human security systems that most companies would never be able to implement on their own.

If your business works with highly confidential data, you also have the option of encrypting the data before storing it on the cloud. Since you would control which individuals at your organization would hold the encryption key, if the data were ever exposed, it would not be readable without your permission and your knowledge.

Myth #8: I can't use the cloud because of industry regulations.

This is true in certain industries, but in the past few years cloud providers have been working with regulatory bodies to do two things: first, develop standards that make sense in the 21st century and can be met in the cloud, and second, build services that comply with these standards that the governing bodies certify. The result is that today, data being highly regulated doesn't mean that it cannot be stored on the cloud.

One of the most notable moves in industry regulations that has allowed for data storage on the cloud is the Health Insurance Portability and Accountability Act (HIPAA), which protects individuals' healthcare information. Microsoft has worked with the Department of Health and Human Services to get Office 365 certified. Now you can co-sign the HIPAA business associate agreement that Microsoft has with HHS. This means that the data you put in Office 365 can meet HIPAA regulations. Microsoft has similar agreements you can co-sign that cover you for FISMA, EU privacy, and Safe Harbor laws.

There are some regulations such as ITAR that require that sensitive data may not leave US soil and control the nationality of the people allowed into the data center. Microsoft does also have specific plans that can cover you for these.

Bottom line: you should not assume that just because you have regulated data that you cannot use the cloud.

Myth #9: I will have to retrain my staff.

If your employees are currently using a particular service, then using that same service hosted in the cloud may be no different; in fact, they may (and likely should) not know where the service is hosted. There may be some new interfaces for your administrators to use in managing the service, but there should be much less to manage as you will likely not have to bother with hardware, disaster recovery, backup, or other standard components of the service. Overall, it will likely shorten the time it takes you to train a new IT employee.

STRATEGIES

Now that some common misperceptions have been covered, let's investigate some strategies for evaluating and using the cloud in your workplace.

Strategy #1: Evaluate your costs and validate your plans.


The first step in assessing whether to move a service to the cloud is evaluating the true costs. Most cloud websites have some rudimentary cost analysis tools that will help you analyze both capital and recurring costs. While these can be helpful, they may or may not offer a complete picture of your financial scenario. When evaluating a major change from a capital to an operational model, it can make sense to consult with a third party who has experience with the financial models and framework you will need to conduct an accurate analysis and sell it internally to the decision makers.


You may also want to conduct a pilot for the services you are considering. For instance, identify a sub-set of your population that can begin using cloud services. A pilot will help you vet your assumptions and make sure you have the right services and plan for moving to the cloud.

Strategy #2: Divide and Conquer

Avoid changing everything at once if at all possible. One of the easiest services to move to the cloud is email. Email can be labor-intensive to manage, maintain, backup, and cover for disaster recovery. As a result, this is where most companies start their move to the cloud. Your company may have a specific need that you want to meet with a cloud service like data storage, client/mobile management, etc.

Always consider starting with something that will translate into large financial savings in the cloud and require few changes to other systems. Services you're just launching can also be good candidates for initiating your cloud project. Rather than investing in new hardware, it may make sense to place that service in the cloud.

 facebook.com/apterasoftware

 youtube.com/apterainc

 twitter.com/apterasoftware