ITWC

CanadianCIO WHITEPAPER

Moving to the Cloud: Beyond the Myths

CARBON60
THE MANAGED CLOUD COMPANY

The move to the cloud is one that businesses are making with increasing frequency. And many are reaping the benefits. But others are experiencing the challenges generated by their misconceptions about what the cloud can do for them, what they can do in the cloud, and what resources they will need to make it all work. Spoiler: it's not just about the tech.

This paper will help businesses move past the myths into a factual world where cloud implementations succeed.

MYTH #1

You sign up and the provider takes care of everything

One of the biggest myths about moving to the cloud was perpetrated by providers marketing in the early days of the technology. That myth was that you provide the credit card and they do the rest.

Nothing could be farther from the truth. Providers today offer many different models, some in which they do more than in others, and each requiring a different level of skill and involvement from the customer.

At the basic level there's **Infrastructure as a Service (IaaS)**. It delivers access to the vendor's compute, network, and storage resources on an on-demand, pay-as-you-go basis. Users can quickly scale up and down, helping them deal with surges – say, Black Friday for a retailer – and then scale back down to save money. But the downside for many is that the customer is responsible for everything other than the hardware (or virtual hardware). The customer provides and manages the operating system, middleware, runtimes, data, and applications. Security, patching and backup? The customer takes care of those too. They need skilled IT folks – an often scarce and thus expensive resource — to run this setup, or they can engage a managed service provider (MSP) or managed cloud provider (MCP) to do so on their behalf.

Canadian businesses are adopting cloud at an increasing pace. But it can get complex to cover all the angles — from security, scaling and cost optimization — which pose challenges for companies of all sizes.

John Witte, President & CEO, Carbon60

Next up is **Platform as a Service (PaaS)**. For (obviously) more money, the vendor provides and manages everything offered by IaaS, plus the operating system, middleware, and runtime, including security, patching, and backups. The customer just has to worry about its application software and data.

Finally, there's **Software as a Service (SaaS)**. With SaaS, the vendor handles everything — or almost everything. Think of services like Salesforce.com, for example. But there's a price to pay, other than the subscription fee — customization is limited or impossible. The customer has to adapt its business processes to the service; the service will not adapt to the business. The customer also needs to clearly understand its responsibilities. For example, will user data be backed up by the provider (the answer is often no), or does the customer have to implement its own solution?

MYTH #2

Cloud always saves money

This myth also began with marketers anxious to lure in customers. And sometimes it's true. For example, it is likely cheaper for a retailer to burst to the cloud during peak periods than it is to build out its datacentre to accommodate those peaks. A startup can use the cloud and the pay-as-you-go model to conserve capital rather than spending on datacentre infrastructure and maintenance.

In addition, depending on the chosen operating model, the provider may be the one who will worry about mundane but critical things like software licensing, sparing scarce corporate IT resources for more value-added work. The provider's expertise can also be leveraged to handle functions such as security that require expensive, hard-to-find talent.

However, over time cloud can become more expensive than on-prem if the customer isn't paying attention. Read the terms and conditions and pricing models carefully — you'll likely be paying for data movement that, on-prem, is covered in your network costs. And the base price may be low, but you may be expected to pay for add-ons. Your MSP or MCP can guide you to cloud provider plans and incentives that help avoid expensive surprises.

MYTH #3

One cloud rules them all

One ring may rule them all, but one cloud probably can't cut it for every business. Not all clouds are created equal — some are better at some functions than others or offer specialized services the others don't. Existing technology investments also come into play. If one cloud vendor supports specific workloads better than others, it makes sense to place that workload on that cloud. Other workloads may run better/cost less/ be easier to manage on another cloud.

Yes, multi-cloud can make technical and business management more complex, but increasingly there are tools that work across clouds, providing a single dashboard. A good MSP or CSP can also help keep the complexity to a minimum.

Also consider IT staff's skills and expertise. Cloud operations require different knowledge. Not only do the staff have to be involved in vendor management, they need to acquire expertise in technologies they may have never used. This means training (or even replacing people), adding to costs, and possibly delaying migrations until the right people are onboard.

MYTH #4

The cloud is (or isn’t) more secure than on prem

There are as many opinions on cloud security as there are people expressing them. In the early days of cloud, security was an afterthought, and the corporate datacentre was the place to be for anything sensitive or mission-critical.

That was then. Now cloud providers realize that good security is good business. The shared security model has been adopted by hyperscalers like AWS and Microsoft to describe who does what. Simply stated, the provider is responsible for the security of the cloud — the infrastructure that runs the services — and the customer or MSP/CSP handles security in the cloud — everything else.

However, that doesn’t mean the cloud is immune to security risks. All three pillars — people, process and technology — must receive equal attention to keep any system, anywhere, secure. If the people are inadequately or improperly trained, if the operating processes don’t focus on the right things, the most secure technology can quickly turn into a trainwreck. A painful example: the oft-compromised AWS S3 buckets. AWS secures S3 buckets by default, but untutored or careless users deliberately turn off that security or make other configuration errors. Result: headlines you don’t want your company featured in.

“Security in the cloud is just as important as ever, and keeping track of various deployments across a hybrid cloud environment can be overwhelming. Taking stock of your footprint first and applying general security frameworks to cloud to cover all your bases methodically with tools and centralized security management will ensure a strong security posture.

Peter Kelly, CISO, Carbon60

Customers still need to think through their requirements. What level of encryption is required? What industry-specific compliances must be adhered to (PIPEDA, PHIPA, PCI, something else)? Do they need to manage their own keys, or do they want the provider to do so? Are there regulatory requirements around data residency or how data may be routed while in transit? What are disaster recovery and business continuity needs, and can the provider you’re looking at accommodate them?

MYTH #5

You can move anything you like to the cloud

Definitely not. Some workloads will not migrate, some may need work before they can shift. Cloud migration needs careful planning to be successful. And that means having knowledgeable staff or a partner who understands the requirements and can provide good advice.

Consider, for example, applications that need extreme responsiveness. While having a brief delay in a point-of-sale application might be acceptable, it would be deadly if latency delayed, say, a command to an automated vehicle.

> **“A balanced approach to cloud migration, especially for legacy systems, helps organizations prioritize their cloud transformation. It’s a process more than a race, especially if your resources are constrained. Starting your team on easier workloads will build confidence for the tougher migrations to come.**
>
> Troy MacVay, CTO, Carbon60

For stable legacy applications that depend on other workloads and are running well on existing infrastructure, it could make economic sense to leave them alone or shift them to a private cloud. Applications that do a lot of data transfers could be extremely expensive to run in the cloud; a thorough cost/benefit analysis should be conducted before deciding to move them. Industry consensus is that for the foreseeable future it will be a hybrid world, with some workloads moved to the cloud when appropriate, others remaining on-prem, and yet others spanning the two models.

One more thing

Myth: You move to the cloud and you don’t need to be concerned about where your data is.

This was an early selling point for cloud, and it may have been fine when consumers were the target market, but in today’s regulatory environment you’d better know where the data is, and be able to control its destinations. Most major cloud providers offer the choice of data storage locations.

Conclusion

Moving to the cloud simply because it's the "done thing" could be an expensive mistake. However, with the proper people, processes, and technology in place, and the help of an experienced partner, any organization can leverage the power of the cloud in ways that will leave IT and the business side leaders smiling.

> **"Cloud economics are multi-faceted so it's important to look at the big picture on the savings beyond just the bill. Early on in your cloud journey, the hard savings may not be clearly visible. But, as more apps are modernized using DevOps approaches and optimization tactics like reserved instances and savings plans are in place, the financials start to make more sense."**

Bik Dutta, VP Product & Marketing, Carbon60

About Carbon60

Carbon60 is a managed cloud services provider for mid-market and enterprise customers with business-critical workloads. We deliver secure and scalable cloud solutions using AWS and Azure public cloud and our own cloud hosting platforms in Canada, UK, and US. Our 24x7 SOC2 compliant managed services include server management, optimization, backups and disaster recovery, and a robust security portfolio to protect your IT environment.

Contact Details

1-888-227-2666

sales@carbon60.com

www.carbon60.com

CARBON60®
THE MANAGED CLOUD COMPANY

About CanadianCIO

CanadianCIO is an integral source of strategic insight for CIOs and senior executives. It focuses on issues related to the strategic use and management of information technology within the enterprise. It takes a hands-on, real world approach to exploring issues such as: the creation of business value through the use of IT; the evolving role of the CIO; IT-driven business transformation; innovation; information privacy and security.

www.canadiancio.com

CanadianCIO