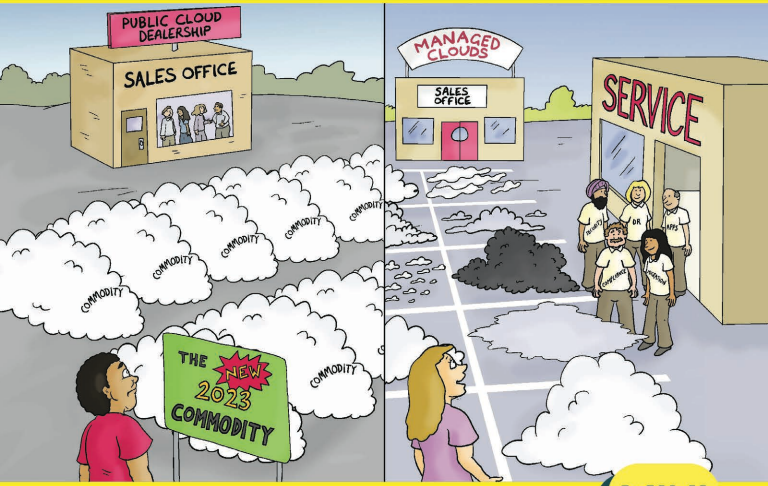
ConversationalGeek

Conversational
Managed Cloud Services

Brien Posey (Microsoft MVP, Commercial Scientist Astronaut Candidate)



MINI Edition

Learn about:

- Why “Cloud First” doesn’t necessarily equate to being “Cloud Smart”
- When Managed Cloud is a better option than traditional public cloud offerings

Sponsored by

SANGFOR

Sponsored by Sangfor Technologies

Sangfor Technologies is a leading global vendor of IT infrastructure solutions, specializing in Cloud Computing and Cyber Security. Established in 2000, Sangfor currently has over 9,500 employees and more than 60 branch offices globally.

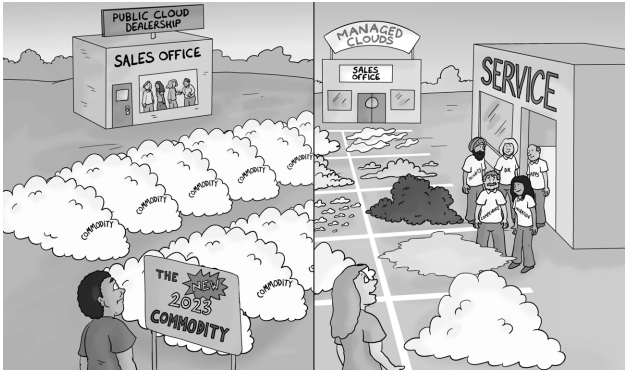
Sangfor offers a wide range of products and services, including Managed Cloud Services, Hyperconverged Infrastructure, Virtual Desktop Infrastructure, Next-Generation Firewall, Internet Access Management, Endpoint Protection, Managed Detection and Response, SD-WAN, and many other solutions. Sangfor takes customers' business needs and user experience seriously, placing them at the heart of corporate strategy. Constant innovation and commitment to creating value for customers help them achieve sustainable growth.

SANGFOR

To learn more visit
www.sangfor.com

Conversational Managed Cloud Services (Mini Edition)

by Brien Posey



ConversationalGeek®

Conversational Managed Cloud Services (Mini Edition)

Published by Conversational Geek® Inc.

www.ConversationalGeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at www.ConversationalGeek.com.

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Brien Posey
Project Editor:	Hope Crocker
Content Editor:	Nick Cavalancia
Content Reviewer(s):	Libby Li
	Glay Wang
	Nicholas Tay Chee Seng
	Francis Tsang

The “Conversational” Method

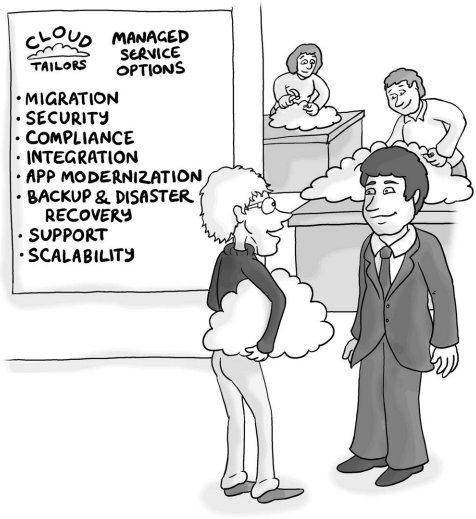
We have two objectives when we create a “Conversational” book. First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

“Geek in the Mirror” Boxes

We infuse humor and insight into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

Getting Smart with Your Choice of Cloud



Can I get "the works"?

If you were to make a list of the biggest IT trends of the last ten years, the transition to the cloud would surely be at the top of the list. In fact, countless organizations have adopted a "Cloud First" approach to the way that they do business. The problem with

this, however, is that in their rush to be cloud first, at least some organizations have failed to be "Cloud Smart".

When I say that organizations fail to be cloud smart, what I am suggesting is that while there is nothing wrong with running workloads in the cloud, the public cloud isn't automatically the best fit for every workload. Sometimes it's going to be less expensive or perhaps more practical to run a workload on-premises.

I once saw an organization abandon all of its brand-new backup hardware, not because there was anything wrong with it, but because they wanted to be "cloud first". In other words, they moved their backup to the cloud simply for the sake of moving to the cloud, even though there was no business benefit to doing so. That's a perfect example of a company *not* being cloud smart.

Of course, part of being cloud smart means knowing which workloads should run in the cloud and which workloads would be better suited to running in your own datacenter. For example, there are some sensitive datastores that might be best suited to the cloud. The same might also be said for backups for external, cloud-based services. Conversely, you might have workloads with high performance, low latency requirements that might be a better suited to running on-premises on in a local Managed Private Cloud.

Of course. there is more to being cloud smart than just deciding whether to run a workload in the cloud or to run it on-premises. Being cloud smart also means choosing the right cloud for your cloud-based workloads. Organizations often place workloads in hyperscalers such as Amazon AWS, Microsoft Azure, or Google Cloud simply because “that’s what everybody uses”. Sometimes though, using a “managed cloud” might be a better choice.

What is a Managed Cloud?

If you look up the phrase “managed cloud” on the Internet, you will likely end up with all kinds of different and sometimes contradictory definitions. Even if you put aside the fact that a lot of these definitions were created by companies who are trying to sell you something, many of the definitions amount to little more than a bunch of IT buzzwords strung together. That being the case, let’s take a moment and explore the definition of what a managed cloud actually is.

First, let’s put aside special purpose clouds such as Software as a Service (SaaS) clouds or system development environments (Platform as a Service or PaaS clouds) – the two main types of clouds that people are generally aware of. So, we’re left with public clouds, such as AWS and Azure, and there are private clouds. Private clouds use hardware and software running in your own datacenter to provide cloud like services for your organization’s own private use.

A managed cloud might best be described as an alternative cloud offering that avoids some of the problems that are inherent to public and private clouds. A managed cloud is like a private cloud, except that the cloud infrastructure is managed and maintained by a Cloud Provider or Cloud Service Provider. While this definition might sound like a public cloud, there are key differences between the two. Unlike a public cloud, a managed cloud is your cloud and it gives you far more control than what you might get in a public cloud environment, while typically also giving you a better ROI.

The Problem with Public Cloud

At the very beginning of this book, I talked about why it is so important to be "Cloud Smart" and to choose the best location for your workloads. That being said, why not just run all of your cloud-based workloads in the public cloud? After all, countless organizations are already doing that.

While the public cloud definitely has its own practicalities, it is not perfect. Public cloud providers have done a really good job of selling to the IT

industry all of the benefits of running workloads in the public cloud, but public cloud shortcomings seem to be discussed far less often.

Hidden Costs

One of the primary disadvantages of running workloads in the public cloud is the cost of doing so. When the major public cloud providers first came on the scene, they worked really hard to convince potential customers that operating in the cloud was the cheapest way of doing things. Their message was that you could run your workloads in their clouds, on enterprise grade hardware, at a fraction of the cost of running that same workload on-premises.

Increasing Rates

Of course, the reality has been something altogether different. While the public clouds might have initially been the inexpensive alternative to on-premises operations, costs have steadily increased over time and it can now be just as expensive (if not more so) to run a workload in the public clouds rather than to run that same workload on-premises. Obviously, the

less expensive option is going to vary by workload. Even so, it would be a fallacy to say that the public cloud is always going to be the least expensive option.

Unforeseen Usage

While on the subject of cost, it's also worth noting that one of the things that tends to frustrate organizations about public cloud costs is that it can be difficult to predict the true cost of operating a workload in the cloud. Yes, unanticipated usage spikes can unexpectedly drive up cloud costs, but there are other areas of concerns as well.

Billing Complexities

The bigger issue is that most of the public cloud providers use complex billing models that make it tough to predict what it is going to cost to run a workload in the cloud. A Cloud Provider might for example, offer a flat hourly rate for running a particular virtual machine instance, but that rate may not include services like storage I/O, storage consumption, or network bandwidth consumption.

Expensive Egrees Fees

Public cloud providers may also try to lock in their customers through the use of data egress fees or other hidden charges. A data egress fee is an extra charge for moving your data out of the public clouds. If for example, you were to discover that it is going to be less expensive to run your workload on a competing cloud, you may find that the cost of migrating your data (due to data egress fees) may offset any savings, thereby forcing you to keep your workload where it is instead of migrating out

Inflexible Options

Another issue with using the public cloud is that public cloud operations are somewhat inflexible. Let's take a look at some of examples of inflexibility you may encounter.

Limited Instance Sizing

Suppose for example, that you want to create a virtual machine instance in the public cloud. Typically, your public cloud provider would give you a few different instance types to choose from. These

instance types will determine the hardware resources that are going to be available to your virtual machine instance. Things like CPU resources, memory, and storage type tends to vary from one instance type to the next. The instance type that you choose also directly determines the per hour cost associated with running that virtual machine instance.

The problem with this particular model is that while public cloud providers do generally offer quite a few different instance types, you may have a tough time finding one that exactly fits your needs. That being the case, you may have to decide between choosing an instance type that is a little too small (which can mean sluggish performance) or an instance type that is bigger than what you need (which means paying for resources that you don't need).

Supported Operating Systems

Additionally, public cloud providers will generally offer a few of the more popular operating system choices for use on virtual machine instances. If however, you need to run an older or a less well-known operating system (or perhaps even a brand-

new operating system that has only recently been released), then the cloud provider may not offer that option.

Even though I am using virtual machine instances as an example, the idea that cloud resources are somewhat rigid and inflexible applies to nearly any public cloud service offering.

Required Refactoring

One important thing to bear in mind is that the inflexibility associated with public cloud service offerings may impact more than just your overall cost. For example, if you want to move an on-premises workload to the public cloud, you are probably going to have to re-factor that workload. That's because public cloud providers tend to be inflexible and therefore require you to alter your workload to fit into their requirements as opposed to being able to give you what you really need.

It isn't just public cloud services that are inflexible, most public cloud providers require their customers to choose from a few predefined support options These support options can be costly, and few if any providers offer an option for on-site support.

Partial Security

Another potential issue with public clouds is that of security. This may seem to be an odd thing to talk about being that public clouds are often presented as being more secure than on-premises environments, but there is a reason to be concerned about public cloud security.

The problem isn't the cloud services themselves. Those services are secure. The problem is the separation of responsibilities with regard to security.

Unclear Responsibilities

Public cloud providers operate under a shared responsibility model in which the provider is responsible for keeping the underlying infrastructure secure, while the customer is responsible for securing their data and any other resources that they deploy in the cloud. This often means that the customer, not the provider, bears the greatest burden with regard to keeping cloud resources secure.

Lack of Expertise

And now understanding that there are parts of a cloud environment that the customer organization is responsible for, there's the question as to whether an internal resource even exists that has experience and expertise in securing the cloud; it's more likely than not that this person (let alone a team) exists.

How Managed Cloud Can Help

Public clouds simply cannot replace managed clouds. The entire public cloud business model is tied to economies of scale. In other words, public cloud providers depend on large numbers of

customers running workloads on their clouds. Those customers share the cost associated with the underlying infrastructure, thereby enabling the provider to offer those resources at a reasonable or discounted price.

The problem with this business model is that it only works at scale. This means that the provider's services must be somewhat generic – a "one size fits all" solution that can offered to everyone.

I tend to think of public cloud services as being like new cars. If you want to buy a custom car, you don't go to the dealership. Car manufacturers create a few base models that they hope will have mass appeal. The same basic concept applies to public cloud providers. They offer very specific services and offer little in the way of customization.

Offering custom solutions to customers would undermine a public cloud provider's business model. That's why you will generally see public cloud providers offering a choice of predefined instance types rather than letting customers pick and choose exactly the resources that they want to allocate to their instances. In other words, when you run a workload on a public cloud, you are using a somewhat generic, inflexible service that may or may not align well with your needs.

Conversely, a managed cloud with its tailored services can give you the flexibility that the typical public cloud is unable to provide. Remember, a managed cloud is essentially like a hosted private cloud. This means that you can allocate and right fit the exact resources to your workloads based on their needs, rather than basing resource allocation on the predefined plans that a public cloud provider has carved out for its customers.

The added flexibility that you get with a managed cloud service may also make it easier to migrate workloads to the cloud. Because you are in control of the managed cloud and the resources that are

running on it, you may find that you are able to migrate workloads to the cloud without having to refactor them.

It's always best to avoid refactoring a workload if possible. Refactoring a workload is expensive and the need for refactoring also means that your cloud migration will take much longer than it would if a lift and shift migration were possible. It's also possible to introduce bugs during the refactoring process.

Be Cloud Smart

In many cases, using a managed cloud service is a better option than using a one size fits all public cloud. Even so, it's important to be cloud smart and to carefully consider what it is that you really need from a cloud provider. While not an all-inclusive list, here are some important things to consider:

Lowered Cost

Costs are always a prime consideration with regard to cloud workloads. When considering costs, be sure to look out for any hidden costs and to also consider the cost benefit analysis for the long term.

Increased Flexibility

Are you OK with running your workloads on a one size fits all cloud platform, or would you be better suited for tailor-made cloud services?

Comprehensive Security

What are the security implications of using a particular cloud platform? If a security incident were to occur, what does the incident response process look like? Is the provider ready and willing to provide support and the forensic resources that you need?

Intelligent Workload Migrations

Will you need to refactor a workload before moving to the cloud, or can that workload be migrated as-is? And if you do migrate a workload to the cloud

and then later decide to bring that workload back in house, what will that process involve? Will the workload have to be refactored once again? Will you incur massive data egress fees?

Within Compliance

If your organization is subject regulation, how well can each cloud provider meet your compliance and governance obligations? Although the hyperscale cloud providers will allow you to place workloads in a region of your choice, the underlying infrastructure causes all of the regions to be connected to one another. This means that even if you place a workload in a local region, behind the scenes connectivity exists to overseas regions, potentially impacting data sovereignty.

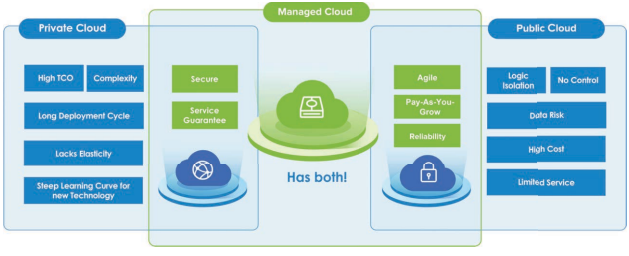
The Big Takeaways

Although “Cloud First” is a catchy marketing slogan, it is far more important for an organization to be “Cloud Smart” than to be Cloud First. A big part of being Cloud Smart is considering the various options that are available and choosing the platform that is best suited to meet the organization’s needs, rather than automatically choosing one of the hyperscaler clouds just because “that’s what everybody else uses”.

Often times a managed cloud will be a far better choice than using a public cloud, particularly when you need a greater degree of flexibility, cost control, or security.

Managed Cloud Services, Powered by Sangfor

Sangfor Managed Cloud Services (MCS) is a local distributed data center offering Infrastructure-as-a-Service (IaaS) with tailored services, where the end-user does not need to build their own data center. Think of it as a local public cloud with superior service and security.



Sangfor Managed Cloud Services is provided using their powerful Hyper-Converged Infrastructure (HCI), integrated with proprietary security technologies to ensure ultimate performance, reliability, and security.

The Sangfor MCS Service Catalog

No organization is simply looking for a cloud to use; they have specific business use cases – such as a *managed private cloud*, *application modernization*, *backup and disaster recovery*, and the *hosting of on-premises HCI-based infrastructure* – that the selection of cloud and its' included services must meet.

So, in addition to the powerful cloud services, customers can select from an extensive set of cloud services designed to meet the specific needs of the organization, including:

- Elastic Compute & Storage
- Dedicated Compute-as-a-Service
- Private Cloud & Container-as-a-Service (dedicated cluster)
- Managed Critical Applications & Data
- Managed Security Service (MDR)

- Disaster Recovery and Backup-as-a-Service
- Hosting Service for On-Premises HCI-Based Infrastructure

The Core Capabilities and Differentiators of Sangfor MCS

The key to Sangfor MCS isn't simply that it's a managed cloud; our focus is to develop and offer services that ensure the availability, durability, and security of your managed cloud.

Data Compliance

Sangfor takes the security of your data seriously. With locally-distributed data centers, your organization can be sure of 100% data localization. The use of dedicated compute and storage means you have full control over and isolation of your data, with complete visibility and traceability to audit access. Data is encrypted and backed up, ensuring an ability to recover easily, with an ability to migrate data offline free of charge.

Effective Security

Sangfor MCS's cloud-native security capabilities and managed security services provide your critical applications and data with the best possible protection. This significantly reduces a customers' investment in security skills and talent, saving at least 35% in security TCO.

As part of a Shared Security Responsibility Model, Sangfor takes on the bulk of the security responsibilities of your assets across data, endpoints, access, and applications. With a mix of cutting-edge technologies such as built-in ransomware protection, and professional security services that include Managed Detection and Response (MDR), Incident Response (IR), and Security Risk Assessments, Sangfor is dedicated to ensuring the security of your Managed Cloud.

Worry-Free Service

Sangfor MCS offers end-to-end cloud service support in collaboration with local certified service partners. Together, we provide customers with

effective response within 5 mins as well as 1-on-1 expert service, including application migration, business recovery, and troubleshooting. With Sangfor MCS, customers can be sure to receive the best and worry-free cloud experience.

NOTES

NOTES

SANGFOR

SANGFOR MANAGED CLOUD SERVICES

Your Exclusive Digital Infrastructure

Feeling the ***pressure*** of building and maintaining your own data center? Or looking for a **simpler**, more **reliable**, and **cost-effective** cloud solution to support your digital business?

Sangfor Managed Cloud Services (MCS) is Your Answer!

Get your FREE TRIAL 30 DAY

https://go.sangfor.com/mcs-free-trial-ebook

Learn More About Sangfor MCS

https://go.sangfor.com/mcs-website-intro-ebook

The advent of the public cloud has forever changed the way organizations operate. But commodity offerings, inflexible options, and a lack of customization have given rise to the Managed Cloud. In this eBook, you'll learn when what it is, why it's a viable cloud choice, and when it's the right option.

About Brien Posey

Brien Posey is a 21-time Microsoft MVP and an internationally published author and conference speaker with over two decades of IT experience. In addition to his technology work, Brien is also a Commercial Scientist Astronaut candidate.