Purposeful Clouds

We simplify your journey to the Cloud

White Paper

Security and the Cloud?

You want to move to the Cloud, but have heard horror stories about how the Cloud is not secure. How do you determine if the Cloud is right for your workloads?

Walter Lapinsky, CCSK
Vice President, Cloud Security
Purposeful Clouds
Walt@PurposefulClouds.com

Introduction

When we talk to people about the Cloud we consistently hear three reasons why they want to move to the Cloud:

1. They have to improve the bottom line, "do more with less," or change capital expense to operating expense. I call this the "**cost**" reason.
2. They want to take advantage of new business opportunities, competitive actions, or periodic IT requirement swings much more quickly. I call this the "**agility**" reason.
3. Especially in organizations where IT is critical to their operation, but not part of their core competency, they are alarmed at the manpower cost of running IT. They are concerned that they really are not giving it the attention it deserves to protect their business from interruptions. I call this the "**aggravation**" reason.

The priorities change from organization to organization, but almost everyone is trying to fix one or more of their cost, agility or aggravation woes. Fortunately, the Cloud has the power to resolve all three of these business issues.

Unfortunately, there are also many concerns. The three major concerns that most people have when they contemplate moving to the Cloud:

1. **Security**. This is almost always the number one concern. In fact, if it does not get mentioned I try to ascertain whether it really should be an issue.
2. **Performance**. Will the Cloud allow the company to adhere to its formal or informal Service Level Agreements (SLAs) to its employees, partners and customers?
3. **Availability**. Dare I trust my business to the Cloud? Will it be there when I need it?

Like the issues, the priorities change between organizations and over time. Again, the Cloud has the potential to solve all three of these concerns. It is fairly clear how to resolve the performance and availability issues in the Cloud, usually at significantly reduced cost, appreciably reduced aggravation and with considerably enhanced agility. Security, on the other hand, is not that clear.

Data breeches will have a serious impact to your business. The Ponemon Institute estimates that the actual cost to a company for the loss of data protected by regulations or laws is US$200 *per lost record*. This is in addition to the cost of your tarnished reputation and potential criminal penalties.

The Complexity of the Cloud

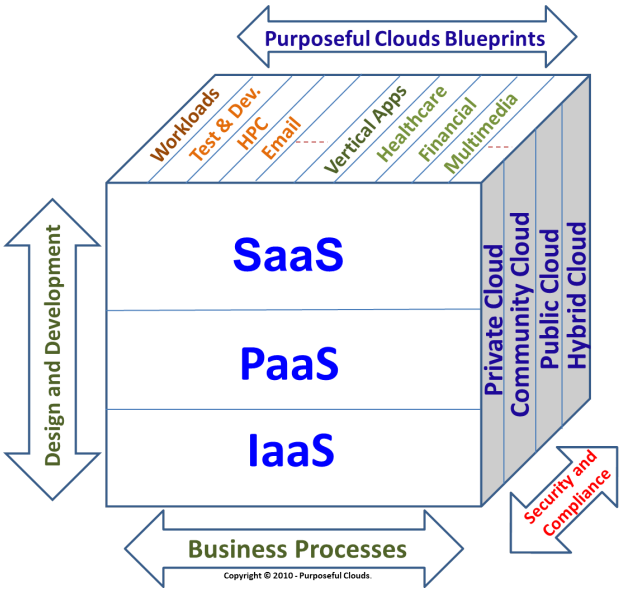
You most likely have a good understanding of the Cloud, but let us take just a minute to review it. The Cloud is more a concept than a product. If someone is selling a digital camera, you have a pretty good idea of what it is, although there may be a zillion different features and cost points. At least, fundamentally, you have an idea what it looks like and what it does.

Not so with the Cloud. The National Institute of Standards and Technology (NIST) defines the Cloud as:

> Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- On-demand self-service
- Ubiquitous network access
- Location-independent resource pooling
- Rapid elasticity
- Pay-per-use

In actuality it is the natural extension of virtualization to the Internet. This virtualization goes beyond just servers, to also encompass networks and storage. It also extends to more than just the hardware to include virtual platforms, software, and actual business solutions. It can turn your IT into a utility that you pay for as you need and use it.



Cloud Service Providers (CSPs) provide Cloud capabilities in a wide variety of forms, which we depict as the Purposeful Clouds Cube. To make it even more complex, different workloads in your IT environment will have sometimes vastly different security, performance and availability requirements. Each workload needs to be analyzed individually to determine its specific requirements. The trick is, for each workload, identify where in the cube it belongs, or if it belongs in the Cloud at all.

If the Cloud is suitable, the next step is to select one of the appropriate cloud models depending on your unique requirements followed by selecting a CSP that can meet those requirements.

Loss of Control

In most cases, an organization's data security is governed by a set of corporate policies, privacy laws, and potentially compliance regulations. All of these are manageable because the organization currently has control: control of its servers, networks, storage and personnel. Moving to the Cloud reduces the direct control that the organization will now have, and the degree of that loss of control varies by where you are in the cube. For example, as you move up the front face of the cube from Infrastructure as a Service (IaaS) through Platform as a Service (PaaS) to Software as a Service (SaaS) the less control you have. Similarly, you retain a lot more control with a Private Cloud model than with a Public Cloud model.

This loss of control has both negative and positive business considerations.

On the negative side, it means that your security policies are obsolete. It is someone else's servers, networks and storage that hold, process and pass your data. It is likely that there are multiple new partners involved as some CSPs may outsource functions like network and storage operations to other companies. It is possible that you may need more than one CSP in order to properly move all, or most of your workloads to the Cloud.

On the positive side, almost all CSPs are very vigilant at keeping all of their servers and other components updated with the latest malware detectors. They will probably do a better job than you can on intrusion detection and denial of service prevention, and can afford to have a more skilled security trained staff to deal quickly with any issues as they arise. They can take some of the responsibility for keeping your data safe, and take that aggravation away.

The Ten Security Questions

Before you move a workload into the Cloud, be certain that you have the answers to these ten questions about that workload.

1. Where is your data?

Just like real estate, location matters. Location has implications on how, or even whether, you can stay compliant with regulations and privacy laws.

Different governments have different rules, especially on privacy. Forty-six US states have privacy laws, and while they are similar they are not identical. Plus they are significant differences from privacy laws from other countries or regions like the EU, Canada, Japan, Australia, which also vary among themselves and, in some cases like the EU, their individual countries or smaller political entities. In all cases, however, they insist that their laws cover their citizens, no matter where their citizens are and no matter where the data is.

Location also has implications on cost, performance and availability, but those are beyond the scope of this paper.

2. Who owns your data?

Astonishingly, some CSP contracts specify that they own your data once you store it on their systems, and they can do anything they want with it. They are kind enough to let you continue to do anything you want with it also. Almost all CSPs reserve the right to put your data anywhere they want without notification.

3. Who has access to your data?

If you looked around your own IT facility, it would probably take a while to figure out who actually does have access to your data.

- Administrators (e.g., security, network, storage, virtualization)
- Help-desk personnel, both your own and your software or hardware vendor's
- Support personnel, including your vendor's support personnel, your building maintenance team, even your janitorial staff
- How much of this have you outsourced to another company? Where are they? What additional channels to your data have they created?
- What additional risks does virtualization of servers, storage and networks add? What if you don't know who else is also virtualized on those same servers, storage and networks?

4. How is your data secured?

Most, but of course not all, of the privacy laws do not require that you report the loss of covered data if that data was encrypted at the time of the loss.

- Should your data be encrypted?
- How strong should the encryption be?
- Who manages the encryption keys? Where are they stored? Who has access to them? How often are they changed?
- Even if you do use encryption, your data will be decrypted as various times in the Cloud. Where? Why? Who has access?

5. Who manages your software?

Depending on which "as a Service" you are using, it could be you, your CSP, or both. Your software includes the operating systems and associated components, your applications, and any other utility software that is part of your workload. Even if you are using standard software, often the configuration information for that application contains proprietary information that you would prefer your competition never gain access to. A key component to security is the assurance that your software is running exactly as it should without inappropriate modification, such as the introduction of malware.

- Who provides your software?
- Who controls updates?
- Who has access to your software?
- Who verifies that everything continues to work correctly as patches and updates are applied?
- Where have all the copies of your virtual image gone?

6. What about life cycle management?

You have policies on how long documents are to be kept, based on their type, purpose and content. When you move some of your data into the Cloud, how do you integrate that data into your life cycle management policy? What about the additional backup, archive and audit files that contain your data?

An even greater issue may be your ability to react to discovery orders. If a court orders discovery of data around specific topics, can you provide it quickly, inexpensively, completely yet restricted to only the required topics? Can you integrate and rationalize that response with the rest of your delivered data?

7. How do you get your data into the Cloud?

Transition to the Cloud can be tricky. Your CSP is usually very helpful and has a suite of tools to assist. However, you have to move to the Cloud without compromising your data's confidentiality, integrity or availability and without shutting your business down! Please, test before you actually go live. It will probably take longer than you think or your CSP predicts. Be patient. You can do this at your own schedule and you will almost always get lots of support from your CSP.

8. How do you get your data back?

Change will inevitably occur. Your selected CSP could go out of business, change their business model to something that doesn't serve your needs, or get bought-out by your competitor. You may find a better alternative elsewhere, or have changes in your own business goals that will force a change.

If you drive the change, you can take the time to plan and test before telling your CSP. If the CSP forces the change, you may have a very short and challenging time window, in some cases just a few days. You need to have an exit strategy and plan ready before you enter, and keep it up-to-date as your use of the Cloud changes over time.

How can you be sure you have not left any of your data behind? Be warned, it is still subject to discovery orders even if you don't know what is being kept on some old backup or archive media at your ex-CSP's disaster recovery site.

9. Can your business survive?

Many CSPs have very unusual contracts, including as mentioned above the ability to terminate your services for any reason on as little as ten days notice. In general, there is no financial penalty to the CSP for their early termination, but you may be liable for the full term of your contract if you terminate early. There is also the unlikely, but possible, event of the CSP just disappearing, either due to financial problems or a government shut down due to activity by another of their customers.

Your CSP or another of its customers may be the subject of an attack, such as a denial of service attack or malware attack. Such as attack may slow down or even deny access to your applications.

Government actions against another customer may result in confiscation of your data or unavailability of your data. Unlike a denial of service or malware attack, government action will not be quickly resolved.

10. Can you prove it?

Do you have the information and certifications you need to convince others that you are secure?

- Auditors
- Chief security officer
- Chief compliance officer
- Chief financial officer
- Compliance and regulatory organizations
- Customers
- Suppliers
- Stockholders
- Courts

What Workloads Are Suitable to Move to the Cloud, and Which Ones Are Not?

When you move to the Cloud, especially for the first time, you want a workload that can be moved with low risk and high reward. Depending on the importance of **cost**, **agility** and **aggravation** to your business, you should choose candidate workloads that have a lot of cost, a lot of variation in usage, or require a lot of manpower to manage. These are the workloads that will offer the best rewards.

Next, look at those workloads for the three concerns: **security**, **performance** and **availability**. While the Cloud can support most performance and availability requirements, I would not start with a business critical application that has thousands of transactions per second with sub-second response times, nor with an application that you can't afford to ever have go down for a couple of hours.

That leaves security. First make sure you really know the security requirements for the data involved in that workload. If that data has government defense-level security requirements or very strict compliance requirements like PCI-DSS (for processing credit or debit cards), then it is not a good primary candidate. Even lesser security requirements, like HIPAA which can be met in the Cloud, are not good candidates for your first project. If to be compliant, and there is a requirement that you must be able to physically audit your CSP's facility, you are unlikely to be able to do that.

How Do I Map My Security Requirements to a CSP?

Your CSP will become a very critical partner to your business. It has the ability to save you a lot of money, move capital expense to operating expense to more closely match costs to benefits, significantly increase the agility of your IT infrastructure, and eliminate or significantly reduce the aggravation of running an IT infrastructure. After all, that is exactly what their core business is.

The CSP also has the ability to inadvertently cause you a lot of grief or even put you out of business.

The most important first step is to know exactly what your requirements are. What performance and availability SLAs do you need? What are the security requirements for your data? What levels of metering, auto-scaling, and Cloud management do you require? What level of support do you need?

You will not get SLAs around security. So you have to ensure that the CSPs infrastructure, personnel, policies, and procedures will enable them to provide the appropriate level of security.

Investigate your potential CSPs at least as much as you investigate any critical partner. What is their reputation? Are they fiscally sound? Are they likely to be around, and in the Cloud business, for many years? Can they meet your SLAs and business requirements?

How much does your CSP outsource that could impact your data security? How does your CSP control physical access to their facility and your data?

Can you get copies of their security policies and procedures? Will they publish their vetting processes for employees, contractors and partners? Can you gain access to their security audit results?

There is a three-digit number of viable CSPs in the US today. In a couple of years there will be a four-digit number of them. In five years there will only be a two-digit number of them. You want to pick one which will either be one of the remaining batch, or who is doing well enough over the next two years that someone will buy or merge with them and be very interested in preserving their customer base.

Conclusion

There are two very important things to remember.

1. Compliance does not imply security.

The US Secret Service / Verizon RISK Team *2010 Data Breach Report* found that 21% of organizations that had breaches in their credit or debit card data had passed their most recent audit. In at least one case they had received their certification the same day as they were successfully attacked. Being compliant is necessary, and that show of good faith does help you if the case goes to court. However, there is more to being secure than just being compliant.

2. The security risk is all yours.

If your CSP allows inappropriate access to your or your customers' data:

- It is **your** fault.
- It is **your** problem to fix.
- It is **your** reputation that is harmed.
- **You** are the subject to the potential or financial and legal penalties.

Your CSP may help in the forensics, and they may do a much better, quicker and less intrusive job on the detection and correction of security flaws then you can. However, they will not share the risk nor will they share the penalties.

The Cloud is Evolving

Every year there are significant improvements in the capabilities of the Cloud. I expect to see significant advances in providing secure environments, probably as Community Clouds, to meet specific compliance requirements. Keep watching.

Don't Try This at Home

This is not easy, but it can be very rewarding to your business. If you don't have a staff with expertise in the ever-changing Cloud, get help from a recognized expert.

Author Biography

Mr. Lapinsky joined Purposeful Clouds with over 40 years of software development, marketing and partner relationship management experience. His prior assignment was as the marketing director for a new suite of security products at Unisys Corporation. These products represent strategic differentiation of their Cloud offerings. He has started multiple companies and is advising start-ups on how best to go to market. He co-owned and operated a custom software consulting company in San Diego, CA, for twelve years. He recently founded wrLapinsky Corporation to provide marketing, product management and development consulting to small software firms. He is advising Med-Communicator Inc. as their Vice President, Technology, and helping them take an innovative product to market. As Vice President, Cloud Security, for Purposeful Clouds he provides strategic and operational guidance on many fronts specifically leveraging his more than 15 years working in the DoD environment, concentrating on data security. Mr. Lapinsky has BS and MS degrees in Mathematics from the University of Delaware. He holds a Certificate of Cloud Security Knowledge (CCSK) from the Cloud Security Alliance.

About Purposeful Clouds

Purposeful Clouds (http://www.purposefulclouds.com) provides customized and standard consulting and training services to large and small organizations looking to improve agility, reduce aggravation and save significantly on IT costs by using Cloud Computing technology. These organizations rely on Purposeful Clouds experts to simplify their journey to the Cloud as they securely transition their business, processes, and applications to the Cloud or build and grow new Cloud business and related services. Because Purposeful Clouds is vendor neutral, they select the best-in-class combination of open or proprietary technologies, products, services and Cloud Service Providers. Purposeful Clouds services cover all phases of planning, implementation, on-going support, and reviews plus an all-encompassing training array to meet their client's specific short and long-term business and technology needs.

For more information, contact us at info@PurposefulClouds.com

February 2011