concerto
cloud services

SOME CLOUDS ARE MEANT TO BE KEPT PRIVATE

Addressing the Application Needs of Business for Sensitive Data & Customized Applications

WHITE PAPER

Contents

1. EXECUTIVE SUMMARY

2. INTRODUCTION

3. THE RIGHT CLOUD FOR THE APPLICATION

   Public Cloud vs. Private Cloud

   How do breaches happen in multi-tenant environment?

4. PROTECT ENTERPRISE DATA

5. PRIVATE CLOUD – A CRITICAL COMPONENT OF YOUR IT STRATEGY

6. DON'T JUMP RIGHT IN: SELECT THE RIGHT PRIVATE CLOUD PROVIDER

7. CONCLUSION

8. RESOURCES

Executive Summary

Cloud adoption is increasing at a rapid pace and as more businesses are looking to deploy some type of cloud technology, it is worth taking a step back to understand how it works with an organization's goals and objectives. The numbers speak for themselves. IDC predicts a 25 percent surge in cloud spending (software, services and infrastructure) this year, reaching more than $100 billion.

Cloud adoption has introduced unique and complex security considerations for users. Organizations must look at how adopting a certain cloud model could affect their risk profile to data security, privacy and availability. With the number of cloud solutions on the market today and the various analyst reports touting which direction to take, there's no wonder why businesses are questioning what approach is best.

Ready or not, cloud computing is here to stay and businesses need to make sure they are well educated on the benefits of each model and know how to select an experienced cloud provider. A well-managed private cloud can address concerns for applications with sensitive data or availability for customized solutions, while public clouds offer lower cost options for more generalized applications and storage. The key is to understand which applications are best for each cloud model, and why some applications are meant solely for private cloud.

Introduction

Today's digital economy requires reliable and secure connectivity. In order to handle daily operations and respond to customers, employees need access to their data at all times, from any location, using any device. Organizations are also storing more data electronically in lieu of hard copies. Whether they are storing large multi-media images or sensitive compliance and regulatory documents, there is no question that the files are getting bigger and there are more of them.

In a traditional setting, IT departments have several on-premise servers, a backup system, hardware supporting the company's processes and software that were likely implemented several years prior. This leads to a demand for new capital expenditures – and most importantly, the ongoing requirements for additional server space to accommodate new solutions and growing amounts of data. Internal IT teams are not only saddled with managing the company's infrastructure, but its phones, printers and even the security of the employees' personal devices – all requiring different levels of expertise.

The advances in cloud computing allow IT departments unprecedented speed to delivering new and updated solutions compared with traditional on-premise models. Designing the right cloud platform to meet the unique needs of a business requires time and a highly specialized team, which is why many organizations decide to employ a third party for implementation and cloud management.

The advancements in private cloud technologies offer specific advantages for enterprise-level applications housing sensitive data, including a wide range of opportunities to save time and streamline resources and costs, all while keeping confidential information more secure and allowing greater flexibility for customization and integration with other applications.

The Right Cloud For The Application

Cloud computing technologies have enabled many business benefits without a significant increase in IT budget. However, the debate over public versus private clouds continues to be a source of confusion for many IT managers and C-level executives.

PUBLIC CLOUD

A public cloud service is provided "as-a-service" over the Internet and the organization's infrastructure or applications are hosted off-premise by a cloud service provider. In a public cloud, the business application software, hardware, data center and operating system is shared with all of the other users. As a result, it is a very low cost option. Businesses can take advantage of the provider's infrastructure and a best-of-breed process, which lowers capital spend and alleviates the pressure on IT departments.

Advantages:

- Simplicity and efficiency: Public cloud services are offered as a service, usually over an Internet connection.
- Low cost: No need to purchase physical hardware or software. A shared model delivers a high efficiency of scale and lower price point.
- Reduced time: Internal IT resources are not responsible for configuration or maintenance of the solution (hardware or software).
- Pay as you go: Users can scale the solution up and down as needed.

Disadvantages:

- Data Security Concerns: Most public cloud providers have security measures in place. However, the nature of a shared model means that data resides in the same servers and instances and therefore can be breached. For businesses with sensitive data, i.e. financial, medical and regulated information, the security is not enough to meet those standards.
- Lack of control: Third-party providers are in charge and upgrades are done automatically. Customizations and integrations with other solutions may be lost as a result of a forced upgrade.
- Slow Performance: Public cloud services share resources with other organizations and during peak times, your solution's performance can be affected.
- Less Flexibility: Because the application runs on shared servers and instances, your ability to change your solution (i.e. customize or integrate) in a public cloud is limited to a standardized set of options.

PRIVATE CLOUD

A private cloud is also provided "as-a-service" or on demand, but the infrastructure is based on dedicated hardware under the control of a provider organization, or sometimes outsourced by internal IT departments. Virtualization is the key technology that helps a company realize similar cost savings to a public cloud solution, while giving them a separate application instance and virtual "pod" for their infrastructure.

In a private cloud, the only shared component is the provider's infrastructure. The virtual layer is software that allows the application to use shared hardware and still remain protected. A company's business applications and database are stored on its own virtual layer, creating a protective bubble around the application set and data.

Advantages:

- More control / higher security for sensitive data: Cloud services are dedicated to a single company and the infrastructure is designed to ensure the highest levels of security. Some providers offer customized security based on regulatory requirements.
- Flexibility for customizations and integrations: Allows companies to tailor its applications, control upgrades and integrate with other solutions.
- Reduced maintenance / upgrade costs: The cloud provider maintains the cloud platform and infrastructure, and keeps the overall infrastructure up to date.
- Redundancy: A private cloud provides greater control over redundancy and disaster recovery because the business is in control and can choose an environment with the redundancy required.
- Lower Risk: Private cloud providers offer usage reports, security and reporting compliance to alleviate risk.
- Stronger Performance: Private clouds deliver stronger system performance because the application is not subject to peaks from other organizations.

Disadvantages:

- Higher cost: Private cloud is generally more expensive than public cloud options, but less expensive than implementing the same solutions in-house.
- On-site maintenance: Some organizations deploy private clouds in-house rather than outsourcing to a provider. With a private cloud hosted on-premise, the company will need to provide adequate power, cooling, general maintenance and security over the data center.
- Capacity ceiling: Depending on the provider and environment, there will be a capacity ceiling.

HOW DO BREACHES HAPPEN IN MULTI–TENANT ENVIRONMENT?

Deploying sensitive or high business impact data in a public cloud service, or multi-tenant environment, could expose your organization in the event of a data breach.

How? In a multi-tenant environment, cloud providers collocate your data with other customers on the same servers. Sometimes they will assign customers their own application server, but they will still have an instance of the server application (example: Microsoft SQL Server) on a shared database server.

In this model, if one customer exposes a server to vulnerability, that server can then be leveraged to distribute malware to others in the provider's environment. The malware hops from machine to machine, leveraging the hashed passwords that are stored on the originally infected machine. Eventually it will find a cached domain administrative credential where it will then infect the domain controller, effectively owning the entire environment.

If you are in a multi-tenant model this is of obvious concern. While your company may have in-depth training for your users on how to protect themselves against phishing attacks, other "tenants" may not, and the mistake of one user outside of your organization could put your company's name in the headlines. Most cloud providers would argue that this couldn't happen on their watch, but so would the thousands of businesses that have already been compromised using these techniques. In a single-tenant (private) cloud, an attack can still occur, however the negligence of one customer can't affect the other environments.

Protect Enterprise Data

CYBER ATTACKS – ONE OF TODAY'S BIGGEST IT CONCERNS

Data security is a major concern for any company that has valuable information to protect. High-profile cyber security attacks make news headlines just about every week, but there are even more events of this nature that fly under the radar. The majority of organizations don't have the bandwidth and tools to protect themselves, and often a company won't even know its data has been breached until it is too late. Therefore, cyber security should be a big factor when selecting the right cloud provider and solution.

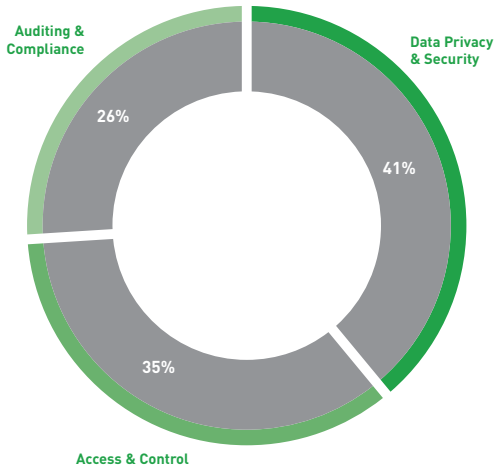
For critical enterprise applications, a private cloud is a better model. Although private clouds can cost more, increasing numbers of organizations are selecting them to host and manage their critical workloads and sensitive information such as financials, regulated data and intellectual property that would wreak havoc on a business if breached.

Amazon, Google and other public cloud providers are not designed to protect sensitive data – they deliver economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual user an attractive low overall cost, but offer limited security protections. Those models are best suited for other applications such as online retail catalogs, email, training servers and company websites.

There are numerous news outlets covering the NSA, Microsoft, Amazon, Google, Facebook and others accused of collecting information without consent. These events are happening because companies pay public cloud providers to give them access to personal data.

Mark Herschberg, CTO at Madison Logic, a New York-based company that provides data for advertisers, stated in The Dallas Morning News that, "There are thousands of companies out there today collecting information on customers, and together they are aggregating quite a bit of data." Google is reading users' emails, and Amazon is tracking not only what a consumer buys, but what they shop for.

TOP CLOUD COMPUTING SECURITY PROBLEMS



Think about the highly sensitive information stored in a company's accounting and ERP system, as well as employee data and customer buying patterns. It's a goldmine for those in possession of valuable data, and regulations on data collection and consent are murky at best. The price of the security of a private cloud far outweighs the exposure and lower costs of a public cloud offering.

Take Target for example. ABC News reported the retail giant said it ignored early signs of a data breach. Staff failed to respond to the security alert and 70 million users were affected, equating to 20 percent of the U.S. population. The cost is a staggering $61 million in direct expenses so far.

The reality is that companies of this size are bombarded with alerts often with little information on logs. The risk is everywhere, accountability is uncertain and liability is not well defined.

Private Cloud – A Critical Component of Your IT Strategy

CYBER ATTACKS – ONE OF TODAY'S BIGGEST IT CONCERNS

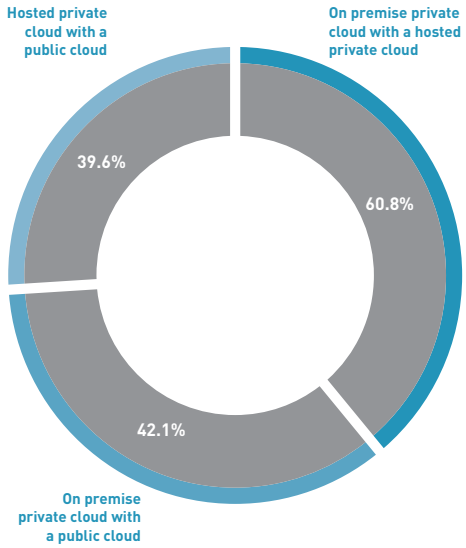
With a greater awareness of security issues, as well as additional security concerns of businesses in highly regulated industries, private cloud conversations are a critical component of an IT business strategy.

The current satisfaction with private clouds seems to come at the expense of public models according to InformationWeek. The survey reported a five-point increase in the percentage of respondents saying they're phasing out their public cloud use.

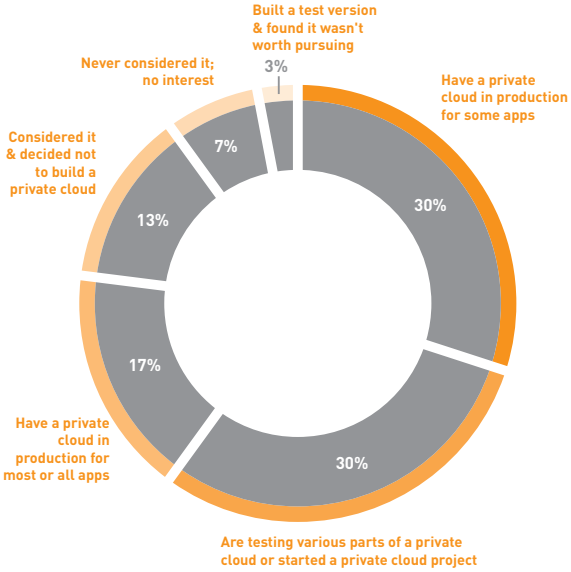
In 2012, the biggest reasons for not pursuing a private cloud were: other projects took priority; a cloud model didn't support their applications; lack of budget; or no need. Today, the percentage of companies saying they haven't considered private cloud integration fell from 20 percent in 2012 to just 7 percent according to the survey.

Reported by Healthcare Informatics, "The Private Cloud Gets Some Respect," Mac McMillian, national chair of the HIMSS Privacy and Security Task Force, notes that the private cloud, whether hosted or on-site, offers a much greater degree of control for the provider organization that is using it, compared to the public cloud. "They know where their data is, they know who has access to it, and they have better control over the resources around it and the rules around it," he says. In his view, the public cloud is not designed to support a heavily regulated or heavy security related environment such as healthcare, and it is not suited for storage of clinical information.

HAS YOUR ORGANIZATION CONFIGURED THE FOLLOWING CLOUDS FOR INTEROPERABILITY?



WHAT'S THE STATE OF YOUR PRIVATE CLOUD ADOPTION?



Don't Jump Right In: Select the Right Private Cloud Provider

In a global mobile environment, companies want a solution that does more than just integrate with its existing legacy systems. And with so many cloud providers and solutions on the market today, how do you make the right choice for your business?

Many companies jump right in and start evaluating providers based on vendor offerings. But to really be successful with a cloud implementation, businesses first need to identify, research and analyze their internal requirements. When you are ready to engage a cloud solutions provider, make sure you conduct a thorough evaluation of the provider as well as its offerings. Privacy, financial health, data center security measures and concerns must be carefully vetted to ensure your information will be safeguarded.

The following list is a guideline to help you cut through the hype and be better equipped to choose an experienced cloud provider.

- How long has the provider been in business and do they know your industry?
- Compare solutions. Each may not satisfy a business' needs 100 percent, but should provide the maximum number of required functionalities and offer an expected return on investment.
- Take the time to learn which vendors are staying on top of trends and investing in new technologies.
- What are the provider's security credentials and policies? The provider must be able to show a solid track record – this includes support for regulations such as Sarbanes-Oxley, HIPAA and others.
- Make sure the cloud provider is up-to-date on data center and industry certifications. Have they met the security and availability criteria for SOC2 and SOC3?
- Understand how each provider charges for traffic – do they offer pre-sales design resources, rather than just quoting? Will you be given visibility into usage numbers, costs and chargebacks?

One in four cloud services providers won't be around by 2015, according to a recent Gartner report. With the possibility of a major consolidation on the horizon, businesses need to make sure they are doing their homework before selecting a preferred provider.

- Private cloud providers that get involved in the initial design tend to understand business goals better and find more efficient ways of deploying the cloud. Make sure your provider sees you as a partner in the process.
- Understand the process to update and make maintenance changes to your solution. Does your provider follow ITIL (Information Technology Infrastructure Library) best practices or have a review board for changes?
- Can the provider provide usage, compliance, and related reports on the accessibility and health of your solution?

As with any other critical business move, selecting a cloud provider should not be taken lightly. It is important to employ a vendor with the flexibility to offer solutions that fit different application needs and stages of the development lifecycle. Be sure to discuss your goals and objectives early and often with the cloud provider. The strength of their expertise, not just the quality of the solution, will be a key factor in the success as the company's goals will evolve and grow over time.

Conclusion

Cloud computing is quickly becoming the technology of choice for enabling businesses to be more focused on providing strategic value rather than spending time on IT resources and infrastructure needs. With applications that contain sensitive information, such as financial or regulated data, moving to the cloud will require special considerations. Companies in the financial, healthcare, or other regulated industries are also aware that they must satisfy regulations and regulators, and they must meet these standards in an environment that is often subject to government surveillance and data center hijackers.

These concerns can make the private cloud a more realistic option for companies that want data sovereignty, in which they can secure critical data internally, without exposing it through widely available public interfaces that characterize the public cloud environment.

A private cloud offers the most secure way to more quickly deliver agile and updated applications. Coupled with the right provider that invests in security and utilizes the most recent technology advances, businesses can realize significant opportunities to save time, resources and money – all while reducing risk.

Resources

1: 451 Research; Hosting and Cloud Go Mainstream 2014

2: IDC; Forecasts Worldwide Spending on Hosted Private Cloud Services

3: Inc.; Michael Dell on Why Data Security Is the Most Important Issue You Face

4: CNNMoney; Microsoft Defends its right to read your email

5: InformationWeek; Private Cloud Adoptions On A Roll

6: InformationWeek; Report: Private Clouds Step Up

7: Healthcare Informatics; The Private Cloud Gets Some Respect

8: ABC News; Target Nearly Doubles Estimate of Customers Affected by Data Breach 9: The Dallas Morning News; The NSA is watching, but so are Amazon and Google 10: Computerworld; One in four cloud providers will be gone by 2015

The Cloud That's Up to Your Challenge

If the cloud you choose isn't ready to manage your most complex mission-critical demands, it's not ready for your business. Concerto Cloud Services combines application expertise with superior service and technical support to offer you a private cloud developed for the highest levels of performance, security and speed. Our team specializes in the rapid deployment of enterprise applications with seamless integrations across on-premise, third party and public cloud solutions to deliver a customizable, hybrid cloud platform.

We built Concerto Cloud for your toughest challenges and your most complicated applications. Concerto transcends public clouds designed for the masses by helping you leverage a platform that can tackle your unique business needs. We take a holistic approach to ensure your infrastructure supports your strategic objectives, from streamlining daily operations to scaling global growth.

concerto cloud services

CONCERTO CLOUD | 208 South Hoover Blvd. Suite 200 | 844.760.1842 | WWW.CONCERTOCLOUD.COM