Public Clouds

Krishnan Subramanian
Analyst & Researcher
Krishworld.com

A whitepaper sponsored by Trend Micro Inc.

Introduction

Public clouds are the latest evolution of computing, offering tremendous value to businesses in terms of better economics, agility, rapid elasticity, etc. The public cloud infrastructure is operated by a cloud service provider and the services are offered over the internet. This very nature of public clouds offers various advantages such as better ROI and faster time to market, while also raising concerns about lack of visibility, security, reliability, etc. Public clouds are well suited to meet the collaborative needs of today's global workforce distributed across different geographies and time zones.

What is a Public Cloud?

Simply put, a public cloud is the availability of IT resources, like compute, storage, development platforms, applications, etc., as service over the internet and which can be provisioned on demand using a self-service portal. Public clouds offer rapid elasticity and seemingly infinite scalability with an ability to consume resources on a pay-per-use basis.

Typically public clouds are operated and managed at datacenters belonging to service providers and shared by multiple customers (multi-tenancy). Such a shared model helps reduce vendor costs, which manifests itself in better cloud economics. However, there is also less visibility and control in a public cloud than a private cloud because the underlying infrastructure is owned by the service provider. The degree of visibility and control depends on the specific public cloud delivery model.

Delivery Models

The most common framework for cloud delivery models is the SPI model (Software, Platform, Infrastructure) in which cloud services are classified into three different delivery types:

- **IaaS** (Infrastructure as a Service) - Shared infrastructure such as servers, storage and network are delivered as a service over the internet. Some examples include Amazon Web Services, Rackspace Cloud, etc. IaaS offers the most control to the users and generally the least security from the service provider. The users are expected to be responsible for ensuring the security of their cloud infrastructure as well as the applications built on top of them.
- **PaaS** (Platform as a Service) - Application development framework offered as a service to developers for quick deployment of their code. Some examples for PaaS include Google App Engine, Heroku, Cloud Foundry, etc. PaaS offers no control over the underlying infrastructure while offering some control over the applications and its configuration. While the provider takes care of the security of the underlying infrastructure, the developer is responsible for application security.

- **SaaS** (Software as a Service) - Application software offered as a service using a multi-tenant model which can be consumed using web browsers. Some examples are Gmail, Salesforce, etc. With SaaS solutions, service providers are responsible for security because they control the infrastructure and applications. However, because service providers retain control, SaaS offers the customer very little visibility and customizability over the infrastructure underneath or even application configuration.

Trend Micro Survey Results

A recent survey conducted by Trend Micro, a cloud security company, offers some insights into the expectations and concerns businesses have about cloud technologies. The survey was conducted in six different countries with 1200 respondents from companies with at least 500 employees. Some of the key results are:

- 43% of the respondents using a cloud service reported that they have experienced a data security lapse/issue in the last 12 months.
- 55% expressed concerns that shared storage is vulnerable without encryption.
- 49% of them said a guaranteed SLA will help them adopt public clouds.
- 93% of the respondents indicated that their organization is using at least one cloud service when they were presented with a list of cloud providers. However, 7% of these same respondents had previously indicated in the survey that their company had no plans to deploy cloud services—showing that this 7% did not realize that their company had already deployed cloud computing.
- 85% of those using a public cloud in production said they are encrypting the data stored in the cloud and keep a local copy synched to the cloud.

In general, these results clearly highlight the need for these companies to have better awareness on how they can use cloud services. Also, these concerns indicate the need for these companies to control the security of their data in public cloud services.

Benefits

The very fact that public cloud services are offered by third-party providers with an ability to scale big offers some unique advantages that are otherwise not available in private clouds. The use of public cloud services shifts the responsibility of managing complex IT, which is not the core business of many companies, to a third-party provider, thereby, offering some benefits that cannot be realized either in traditional infrastructure or private clouds. Some of the benefits offered by public clouds to business organizations are:

Cost Savings

- Eliminates capex and offers reduced opex because the maintenance and labor costs associated with managing the infrastructure is offloaded to a third-party provider.
- Ensures cost efficiency because of the pay-per-use models. Typically, service providers charge by the hour and this comes in handy when a company's resource needs are for a temporary project or to meet a sudden spike in usage, avoiding the need to build out internal infrastructure to cover these projects.
- Offers self-service provisioning, leading to lower costs and better agility because human intervention in resource provisioning is minimized.

Business Agility

- Provides massive scalability and an ability to elastically re-size compute resources based on the organization's IT needs.
- Gives programmatic access to compute resources through API, helping applications scale automatically without any human intervention.
- Supplies robust infrastructure with better support staff, offering cost and talent advantages in an increasingly shrinking pool of expertise.

Security Considerations

Even though the public cloud offers tremendous benefits, businesses cannot embrace public cloud services without taking some security considerations into account. The use of public clouds requires trust on the side of businesses using these services and transparency on the side of cloud providers. In this section, we will highlight some of the security considerations that are important for any business planning to move to public clouds.

- **Multi-tenancy risks:** The shared multi-tenant nature of public clouds adds security risks such as unauthorized access of data by other tenants using the same hardware. Also, a multi-tenant environment exposes resource contention issues whenever one of the tenants using the hardware consumes a disproportionate amount of resources either due to need or due to hack attacks.
- **Control and visibility:** Businesses have limited control and visibility because the vendor is responsible for completely managing the infrastructure. This adds some additional security concerns associated with lack of transparency. Business organizations need a mental shift as they cede the control of IT to a third party while using public cloud services.
- **Security responsibility:** Security is a shared responsibility between the vendor and the user, with the degree of responsibility of each varying by type of cloud model.

- **Data and encryption:** Data privacy is at risk if data in the cloud is unencrypted. There is the potential for unauthorized access either by a rogue employee on the cloud service provider side or an intruder gaining access to the infrastructure.
- **Data retention:** When the data is moved or deleted by a service provider or customer, there may be remaining data remnants, potentially exposing sensitive data to unauthorized sources.
- **Compliance requirements:** Different countries have different regulatory requirements on data privacy. Since some public cloud providers offer no information on the location of the data, it is important to consider the regulatory requirements on where data can reside.

Security Best Practices

This section focuses on the security best practices for the IaaS cloud model. IaaS provides customers with the most flexibility and responsibility to provide their own security. As mentioned above, the service provider is responsible for most, if not all, of the security for the SaaS and PaaS cloud models.

Public cloud services require businesses to rethink traditional security practices. In this section, we will highlight some of the best practices that can greatly reduce the risks associated with public clouds. With less risk, businesses can move more data safely into the public cloud, allowing them to realize IaaS cloud benefits, such as service agility and cost savings.

- **VM-level security:** Unlike the traditional computing model or private clouds, the idea of perimeter completely vanishes in a public cloud environment. A defense should be built at the Virtual Machine (VM) level so that it travels with the VM into the cloud infrastructure.
- **Multi-layered defense:** Using tools like firewall, IDS/IPS, log inspection, etc. geared towards virtual machines is important. More importantly, the traffic between the virtual machines should be continuously monitored by setting up policies appropriately. It is also equally important to take advantage of the security features offered by the public cloud providers themselves.
- **Data and encryption:** Data in the cloud should be encrypted. An encryption solution should have well-designed encryption key management policies to ensure data integrity. Also, businesses should maintain encryption key ownership. In fact, encryption and efficient key management can offset any lack of transparency on the cloud provider side.
- **Patch management:** Having the right set of policies around patching is important. Patching in the cloud environment is much more difficult than in the physical environment, because VMs can be moved around and switched on and off at will.

- **Identity and access:** Businesses should consider using third-party tools for single sign-on and for implementing better access control than what is available in the management console of the cloud provider.
- **Regulatory compliance:** Businesses should understand the impact of regulations and assess which policies and procedures change with respect to the public cloud deployment. Companies should realize the nature of this change and associated impact; develop processes to collect evidence, such as audit logs; and store this evidence securely. It is absolutely critical to collect the necessary evidence from the public cloud provider and store it outside the cloud environment. Also, businesses will benefit from selecting an auditor who understands the changed dynamics and challenges of using public cloud services.

Recommendations for Public Cloud Adoption

Public Cloud Implementation

In the Trend Micro survey, 13% of respondents had a public cloud in production and another 43% were implementing or were in the midst of piloting a public cloud.

Public Cloud Use Cases

Businesses can take advantage of the cost benefits and elasticity of public clouds to their advantage. A video production company can use public clouds for video rendering and pay for only the time they used the resources. A business can tap into public clouds when they expect unpredictable demand during a marketing promotion. A pharmaceutical company can run their drug design processes on public cloud, thereby, accelerating the time to market. With proper security procedures, more and more workloads can be moved to the public clouds. In fact, public clouds easily match the private clouds with respect to availability and business continuity.

Conclusion

Public clouds offer tremendous value for businesses of all sizes across many different verticals. Even with stringent compliance requirement, businesses can take advantage of public cloud services to enjoy benefits such as better cost structure, business agility, etc. Public cloud services require a different set of security considerations to mitigate any potential risks, but by following security best practices such as self-defending virtual machines and encryption in cloud environments, data can be safely deployed into the public cloud. Hybrid and private clouds are considered in two other whitepapers where security considerations and solutions on these environments are discussed.