

Hybrid Clouds

Krishnan Subramanian

Analyst & Researcher

Krishworld.com

A whitepaper sponsored by Trend Micro Inc.

Introduction

The economic benefits offered by public clouds are attractive enough for many organizations to push some of their non-critical workloads to such services while also using private clouds for their mission-critical needs. Such hybrid cloud deployments have proven to be advantageous not just in terms of better economics but also in terms of business agility. The best-of-both-worlds approach of hybrid cloud lets organizations take advantage of public clouds to reduce capex while still keeping their mission-critical workloads inside the organization. However, by combining private and public cloud models, hybrid clouds have the largest attack surface. Businesses must deploy security across both the private and public cloud elements. In this whitepaper, we will discuss the business benefits of hybrid clouds, the security considerations, and how one can mitigate the risks involved with the use of public clouds along with a private cloud.

What is a Hybrid Cloud?

In its simplistic definition, a hybrid cloud is a combination of both public and private clouds. If we apply the definition from the National Institute of Standards and Technology (NIST), “a hybrid cloud is a combination of public and private clouds bound together by either standardized or proprietary technology that enables data and application portability.” It could be a combination of a private cloud inside an organization with one or more public cloud providers or a private cloud hosted on third-party premises with one or more public cloud providers.

Trend Micro, a cloud security company, recently conducted a survey which indicated that public cloud services fail to meet IT and business requirements of some of the business organizations. A hybrid cloud environment can help meet their needs. In some ways, hybrid clouds can be considered an intermediate stage as enterprises prepare to move most of their workloads to public clouds.

Trend Micro Survey Results

A recent survey conducted by Trend Micro 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:

- 38% of the survey respondents say that their IT requirements are not being met by the cloud providers. Similarly, 38% claimed that their current cloud service providers are not meeting their business needs.
- For companies that have public cloud or hybrid applications currently in production, 45% of the existing applications are already deployed in the cloud and an average of 53% of new applications will be deployed in the cloud.

- 49% of the survey respondents indicated that if they knew how to secure their data in the cloud, it would increase their consideration for cloud adoption.

Increasingly, companies are realizing that the use of a hybrid cloud expands the number of applications they deploy into the cloud. However, almost half (49%) feel they need to improve their knowledge of cloud security to further increase cloud adoption. Using hybrid clouds will help them understand the security implications of the public clouds better before they move all their workloads there.

Benefits

Hybrid clouds offer the cost and scale benefits of public clouds while also offering the security and control of private clouds. In this section, we will highlight some of the business benefits of hybrid clouds.

Cost Savings

- Reduces capital expenses as part of the organization's infrastructure needs are outsourced to public cloud providers.
- Improves resource allocation for temporary projects at a vastly reduced cost because the use of public clouds removes the need for investments to carry out these projects.
- Helps optimize the infrastructure spending during different stages of the application lifecycle. Public clouds can be tapped for development and testing while private clouds can be used for production. More importantly, public clouds can be used to retire applications, which may be no longer needed because of the move to SaaS, at much lower costs than dedicated on-premise infrastructure.

Business Agility

- Offers both the controls available in a private cloud deployment along with the ability to rapidly scale using public clouds.
- Supplies support for cloudbursting, tapping the public clouds for an unexpected need for additional compute resources.
- Provides drastic improvements in the overall organizational agility, because of the ability to leverage public clouds, leading to increased opportunities hitherto unavailable in traditional infrastructure or pure private clouds.

Security Considerations

As organizations use hybrid clouds for their business needs, they must understand the new security requirements of a hybrid cloud environment. While hybrid clouds offer the security advantages of private clouds, there are some unique security challenges that arise as the

perimeter extends beyond the organization's boundaries. Along with the typical security considerations associated with private clouds, there are some additional factors one should consider in a hybrid environment.

- **Perimeter extension:** As a hybrid cloud extends the IT perimeter outside the organizational boundaries, it opens up a larger surface area for attacks with a section of the hybrid cloud infrastructure under the control of the service provider.
- **Identity and access management:** An easier approach to solving the identity needs of hybrid clouds is to extend the existing enterprise identity and access management to the public clouds. This opens up concerns about how this approach will affect the enterprise identity and its impact on the organization's security.
- **Management tools:** When organizations manage complex hybrid cloud environments using a management tool, either as a part of the cloud platform or as a third-party tool, organizations should consider the security implications of using such a tool. For example, the management tool should be able to handle the identity and enforce security uniformly across hybrid cloud environments.
- **Data migration:** A hybrid cloud makes the data flow from a private environment to a public cloud much easier. There are privacy and integrity concerns associated with such data movement because the privacy controls in the public cloud environment vary significantly from the private cloud's.
- **Security policies:** There are risks associated with the security policies spanning the hybrid cloud environment such as issues with how encryption keys are managed in a public cloud compared to a pure private cloud environment.

Security Best Practices

As the Trend Micro survey indicates, many organizations will consider moving to public clouds if they understand how they can secure their data in the cloud. Hybrid clouds can serve as a transitional approach and help businesses fine tune their strategies for future public cloud adoption. Hybrid clouds offer businesses a safe shell from which they can try out public cloud services, while still maintaining sensitive data in a more controlled private cloud. There are some best practices that will help mitigate the risks associated with hybrid cloud deployments. In this section, we will highlight some of them.

- **VM-level security:** The perimeter of the hybrid cloud environment is not only elastic but also spans multiple clouds including on-premise private clouds. This calls for self-defending security at the virtual machine level that travels through the on-premise data center, in the cloud and between multiple cloud providers.
- **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 policies appropriately.

- **Traffic control:** An on-premise gateway should be used to control incoming traffic to the public cloud rather than provide direct access.
- **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, the business should retain encryption-key ownership to maintain separation of duties between the business and the public cloud service provider. This also allows the business to apply their encryption across its private and public clouds and prevents vendor lock in, allowing the organization to move between cloud vendors.
- **Security control:** Cloud security should be controlled by the business and not the cloud vendor. Whether it is by using single sign-on or by using a third-party tool to securely extend the perimeter to the public cloud, the control over security should be with the business organization deploying the hybrid environment.
- **Regulatory compliance:** Businesses should understand the impact of regulations and assess which policies and procedures change with respect to the hybrid 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 cloud provider and store it outside the public cloud environment. Also, businesses will benefit from selecting an auditor who understands the changed dynamics and challenges of using public cloud services.

Recommendations for Hybrid Cloud Adoption

Hybrid Cloud Implementation

In the Trend Micro survey, 10% of respondents had a hybrid cloud in production and another 45% were implementing or were in the midst of piloting a hybrid cloud.

Hybrid Cloud Use Cases

There are many different scenarios for employing hybrid clouds but we will list out some of the most prominent ones:

- Using the private cloud for mission-critical applications and pushing the non-critical ones to public clouds. For example, a company might use a public cloud for test and development while using a private cloud inside the organization for production deployment. Another example would be using public clouds for external facing applications while using a private cloud for internal applications.
- Cloudbursting, a dynamic deployment of an application running on a private cloud into public clouds to meet an unexpected demand, such as a retail company's need to meet increasing traffic associated with holiday shopping.

- Another example is non-destructive Disaster Recovery (DR) testing. Organizations can test if their production environment is DR ready by tapping the public clouds and without any disruption.

Conclusion

Hybrid clouds offer a greater flexibility to businesses while offering choice in terms of keeping control and security. Hybrid clouds are usually deployed by organizations willing to push part of their workloads to public clouds either for cloudbursting purposes or for projects requiring faster implementation. Because hybrid clouds vary based on company needs and structure of implementation, there is no one-size-fits-all solution. Since hybrid environments involve both on-premise and public cloud providers, some additional infrastructure security considerations come into the picture, which are normally associated with public clouds. . Any businesses planning to deploy hybrid clouds should understand the different security needs and follow the industry best practices to mitigate any risks. Once secure, a hybrid cloud environment can help businesses transition more applications into public clouds, providing additional cost savings. Public and private clouds are considered in two other whitepapers where security considerations and solutions on these environments are discussed.