HYTRUST

HyTrust cloud adoption survey

Despite security concerns, multi-cloud adoption on the rise

White Paper

HYTRUST

White Paper

HyTrust cloud adoption survey

Despite security concerns, multi-cloud adoption on the rise

Security was the biggest concern about moving to the public cloud.

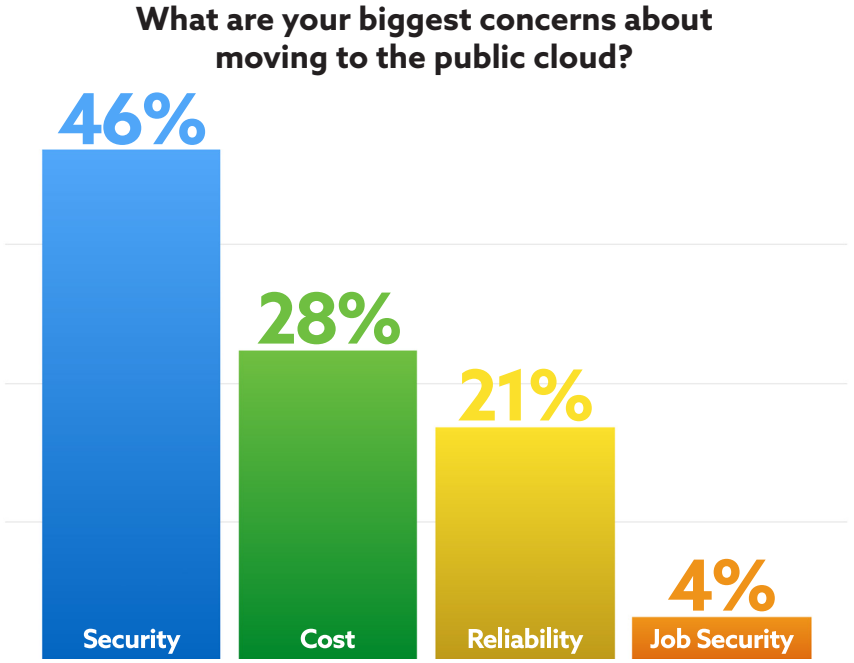
Introduction

For almost every organization cloud is a component of their IT strategy, yet many are wrestling with how fast and how far to go. These organizations and their IT departments are faced with many challenges and demands as they adopt and deploy cloud technologies. While business leaders find the speed and agility of the cloud to be irresistible, IT is faced with the challenge of dealing with the many implementation details required to make this cloud vision a reality.

In order to get a better understanding of organizations' current cloud initiatives and where they are headed with their cloud ambitions, HyTrust surveyed over 400 attendees at VMworld 2016 in Las Vegas. This provided an excellent opportunity to survey IT leaders across a variety of industries and gain insights into their cloud provider choices, top challenges and intentions for the future.

Security remains a top concern

Not really a surprise but the security concerns about cloud and in particular public cloud remain. Organizations find the speed, agility and convenience of the public cloud very appealing but despite all of those advantages, the uncertainty that the



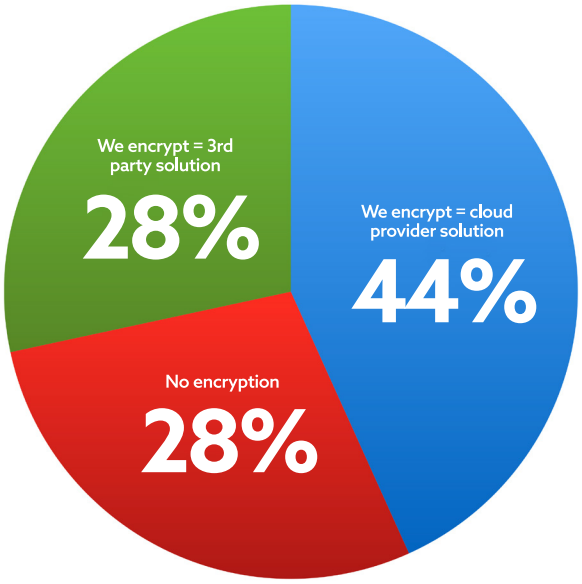
Surprisingly, 28% of organizations polled reported they were not using encryption in the public cloud.

use of public cloud creates drives many to rate security as a top concern (46%). There are deep-seated psychological reasons for this, with the thought of "putting your data in someone else's data center" making many uneasy. It is worth noting that all of that agility, speed and convenience literally comes at a cost, with cost being a top concern (28%) for moving to a public cloud, but well behind security.

A real surprise: Despite security concerns, many don't encrypt data in the public cloud

It is no surprise that security is a top concern, but what is a surprise is that despite security being the top concern roughly 28% of those using public cloud are not encrypting data stored there. The good news is that a majority of organizations using public cloud have some form of data encryption in place (72%). Encryption is table stakes for anyone who even pretends to be serious about security or compliance. With data encryption, even if a breach occurs, the data is protected, and while it may be downloaded it will be meaningless without the encryption key. If a

How are you handling encryption in the public cloud?



breach occurs and regulated data like private health information (PHI) is encrypted, there is no requirement to provide customer notification, which would be required if the PHI were not encrypted.

Of those with public cloud encryption in place, 44% indicated that they are using a cloud provider solution for encryption. It is good that data is being encrypted but some organizations may not be as protected as they think. A cloud provider encryption service can sometimes be problematic, particularly when the cloud provider holds the encryption keys. In these situations, if there were a breach at the provider this could result in a breach of the data. Additionally, if law enforcement or other government entities request (or demand) access to data, the provider may be compelled to hand over the data, in some cases without customer notification.

From the survey it appears that 28% of the respondents may have already considered this. They have chosen to pursue encryption and retain control of the encryption keys outside the cloud provider. This ensures that the only people who are entitled see one's data are the only people that are actually able to see it. An advantage of this approach is that when it comes time to securely retire a workload,

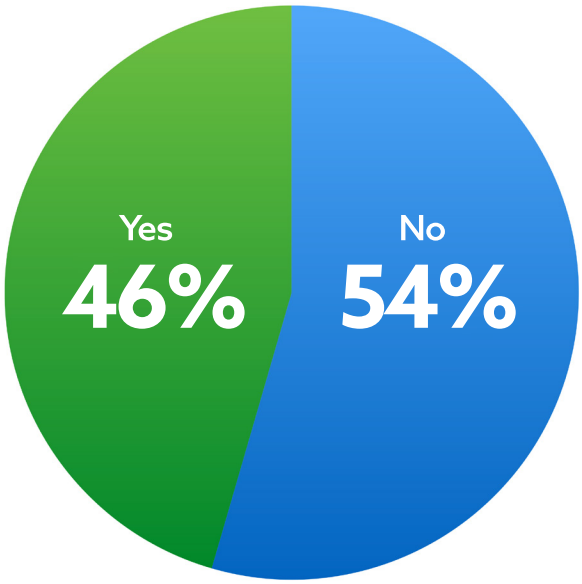
A majority felt that existing security approaches would not work in the cloud.

it can be done by destroying the encryption key, rendering that workload (or backups and other copies of that workload) unreadable and decommissioned without worry that backups or other copies remain somewhere in the public cloud.

Cloud security: Something new or more of the same?

When moving to the public cloud, a lot of things change. Things happen more quickly, staff does more work on business facing applications and less on building and configuring on premises IT resources. How do security approaches change for cloud deployments? The survey revealed that just over half (54%) think that the current security approaches will not work for cloud deployments, yet 46% thought existing approaches would work.

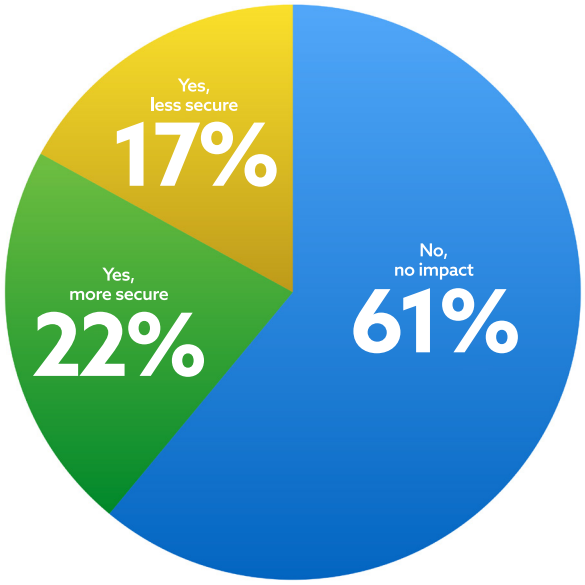
Will existing security approaches work with present or future cloud deployments?



Speaking of cloud and security, while the cloud may change many things, the IT professionals surveyed were not worried about job security, with 83% saying that there would either be no change or an increase in job security with a move to the cloud.

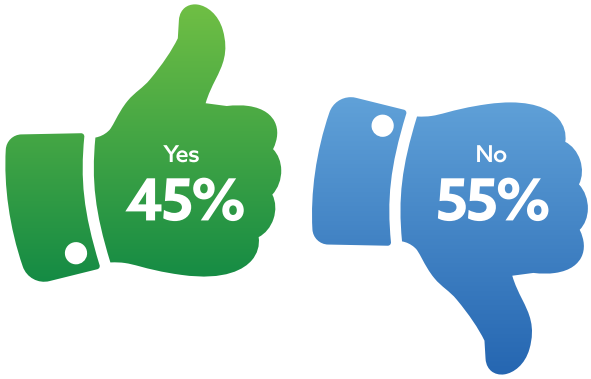
Job Security: 83% thought the cloud would either make their jobs more secure or have no impact on job security.

If you move to the cloud, will that impact your job security?



Another security debate that is taking place in the market is the question of whether an organization's security is better with a cloud provider than if its own staff did it, in-house. When you ponder the relative asymmetry in scale, resources and expertise when comparing any of the cloud service providers with any normal enterprise, it would seem reasonable to expect better security from the cloud than in the enterprise data center. That said, trusting a vendor is for many a big ask as 55% said they do not expect security in the cloud to be better than it is in their in-house data centers.

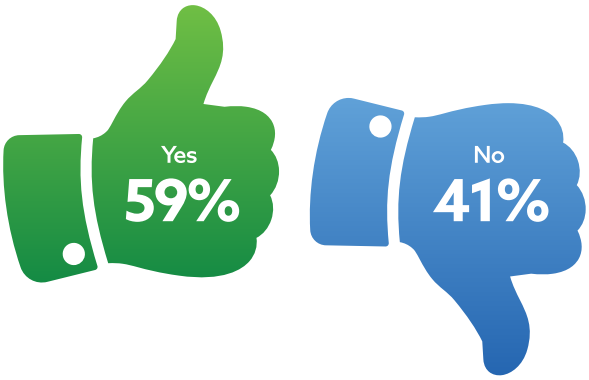
Will security be better in the cloud than in-house?



Best of both worlds: The hybrid cloud

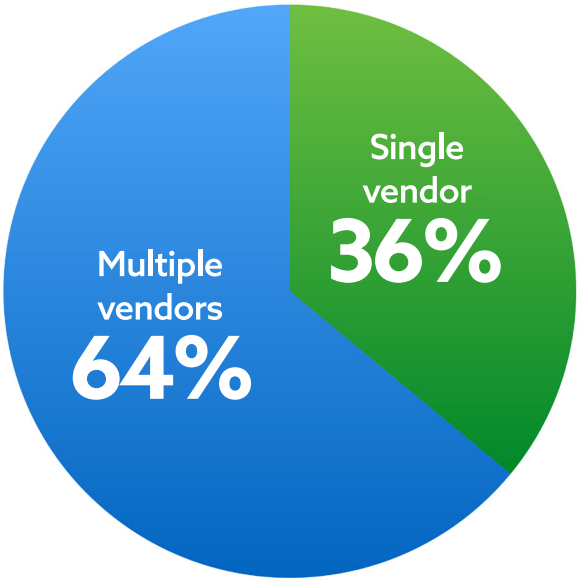
One way that organizations are seeking to get the benefits of public cloud while maintaining the advantages of on premises deployments is the use of hybrid clouds – combining public and private cloud. This strategy is being planned by

Are you planning any sort of hybrid cloud deployment?



59% of the organizations surveyed. But just as organizations want choice and flexibility in the public and private cloud combination, they want the same with their cloud deployments. While the best possible world for IT would be one of simplicity with little to no overlap in vendors, the reality is that enterprises and other organizations often grow via acquisition and consolidation in ways that often leave the organization with some overlap and the cloud is no exception. There is also the reality that certain applications may be set up for certain environments which dictate the use of multiple cloud vendors. Additionally, an organization may want the ability to move workloads to the most cost effective cloud provider, maintaining relationships with multiple providers. Thus 64% of those considering a move to hybrid cloud expect to use multiple vendors. See figure below.

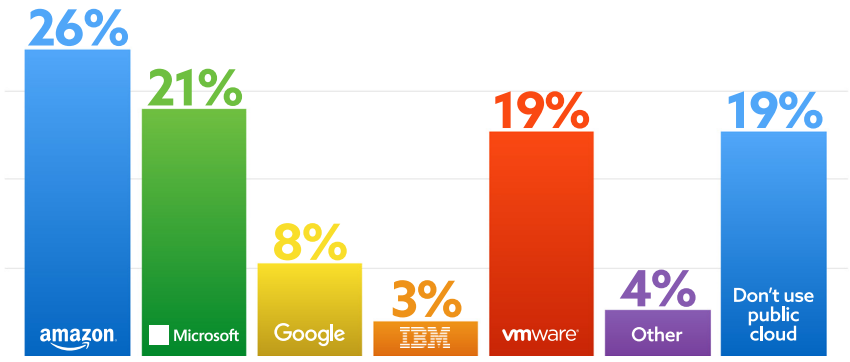
If/when you move to the hybrid cloud, will you work with a single or multiple vendors?



Pareto and the public cloud providers

It appears the 80/20 rule applies to public cloud adoption with 20% not using the public cloud. One might expect that number to be lower, but with the prevalence of shadow IT, it is easy to imagine relatively widespread use of public cloud services without the knowledge or participation of IT. The 80% who are using public cloud providers today are spread across a handful of platforms. Conventional wisdom has long held that Amazon is the dominant leader of the global public cloud market and it edged ahead of others in the survey with a 26% share. Microsoft gaining ground with Azure, cutting the gap between the two leaders with 21% indicating that they are currently using Microsoft for public cloud. In the survey, there was a stronger than usual showing of VMware (19%), perhaps due to the survey performed at the largest VMware gathering in the world. Similarly, while a modest 3% indicate that they currently use IBM for public cloud, the IBM Cloud offering is making aggressive moves in the market including an alliance with VMware to offer the VMware Cloud Foundation as a service, allowing customers to enjoy cloud versions of VMware offerings to build out an SDDC.

Which public cloud providers do you use?



Summary

The cloud is clearly here to stay. For many, it will not only be hybrid, but will be a multi-cloud, multi-vendor, hybrid deployment. Those who have not already started to look at workload-centric security and in particular multi-cloud workload security would be well advised to start such efforts soon. While many feel that they are well positioned with security relative to the cloud, there are obvious gaps including many who are not yet encrypting their cloud workloads as well as those who are running encryption solutions where they are not the only ones holding the encryption keys or prepared to support a multi-cloud encryption deployment.

For more information about the survey, please visit www.hytrust.com/cloud-adoption-survey/ For more information about how HyTrust workload security solutions address cloud security concerns visit www.hytrust.com or call +1 650 681 8100.

The survey was completed by 414 attendees of VMworld 2016 in Las Vegas, Nevada between August 28 and August 31. Participants were from diverse vertical industries; Gov./military 14%, financial 14%, healthcare/biotech 12%, insurance 5%, manufacturing 5%, transportation/shipping 3%, technology 29%, other 18%.

HyTrust
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100