HYTRUST

# HyTrust government cloud adoption survey

## Security a top concern with hesitancy to relinquish control of data

White Paper

HYTRUST

White Paper

# HyTrust government cloud adoption survey

## Security a top concern with hesitancy to relinquish control of data

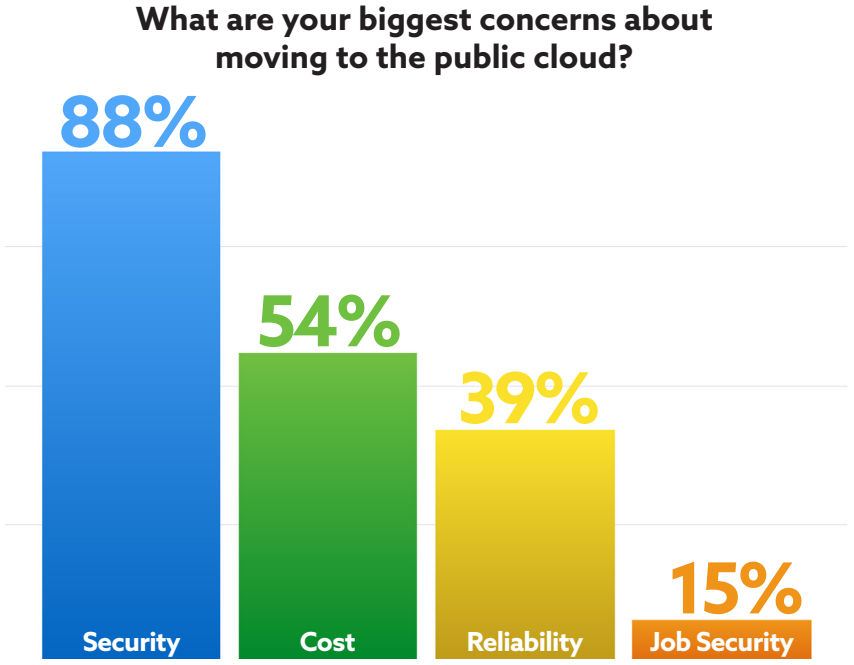
### Introduction

With the Cloud First initiative and the push to drive down data center costs in Government, cloud is becoming a component of government agencies' IT strategy, yet many are wrestling with how fast and how far to go. These agencies 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 agencies' current cloud initiatives and where they are headed with their cloud ambitions, HyTrust surveyed government attendees at VMworld 2016 in Las Vegas. This provided an excellent opportunity to gain insights into 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. Agencies find the speed, agility and convenience of the public cloud

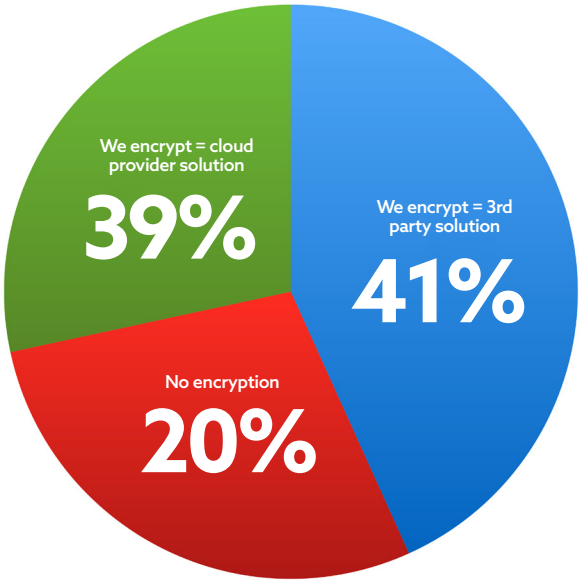


very appealing but despite all of those advantages, the uncertainty that the use of public cloud creates drives many to rate security as a top concern (88%). There are deep-seated psychological reasons for this. Understandably the realization of "putting your data in someone else's data center" can raise security concerns. It is worth noting that all of that agility, speed and convenience comes at a cost, with cost being a top concern (54%) 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 among government organizations, but what is a surprise is that despite security being the top concern (88% rated security the top concern) roughly 20% of agencies using public cloud are not encrypting data stored there. The good news is that a majority of agencies using public cloud have some form of data encryption in place (80%). Encryption is table stakes for anyone who even pretends to be serious about security or compliance. With data

**How are you handling encryption in the public cloud?**




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 breach occurs and sensitive information is encrypted, there is no requirement to provide customer notification like what would be required if the information was not encrypted.

Of those agencies with public cloud encryption in place, 39% indicated that they are using a cloud provider solution for encryption. It is good that data is being encrypting but this can also be troubling for some agencies as they 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 stored at the provider. If access to data is requested by an entity, the provider holds the encryption keys and may be required to hand over the data without its customers knowing.

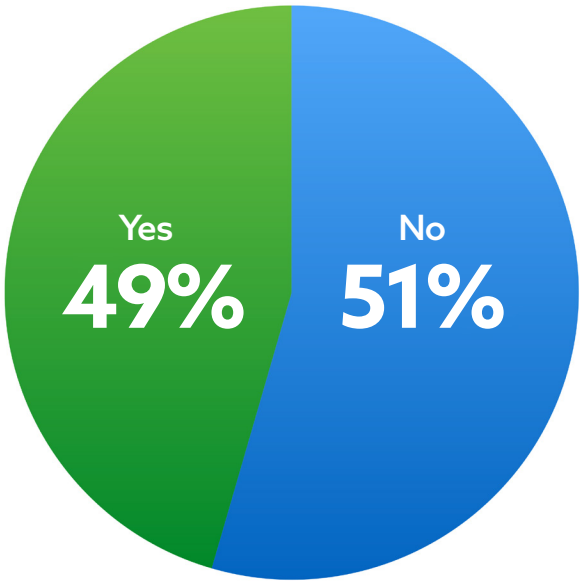
From the survey it appears that 41% of the respondents may have already considered this. They have chosen to pursue encryption and retain control of the encryption keys outside the cloud provider. This ensures that the only people who

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, 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 the provider still has copies accessible 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 enabling business workloads versus building and configuring on premises IT resources, and security can be left largely in the hands of someone else. How will security approaches change for cloud deployments? The survey revealed that just over half (51%) think that the current security approaches will not work for cloud deployments, yet 49% thought existing approaches would work.

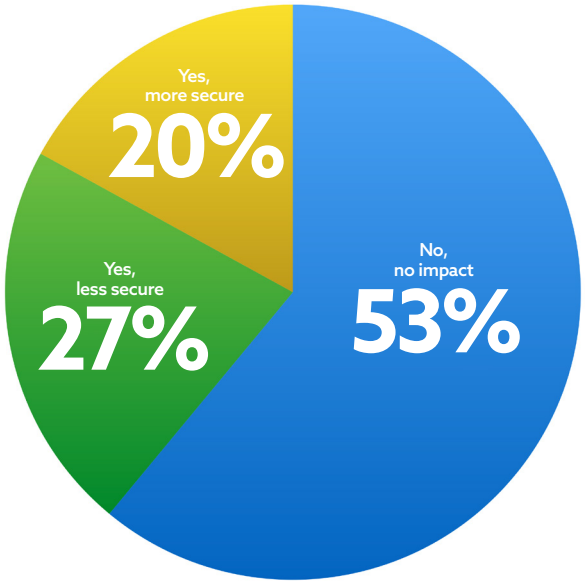
**Will existing security approaches work with present or future cloud deployments?**




Speaking of cloud changes and security, while the cloud may change many things, the IT professionals at agencies that were surveyed are not worried about job security, with 73% saying that there would either be no change or an increase in job security with a move to the cloud.

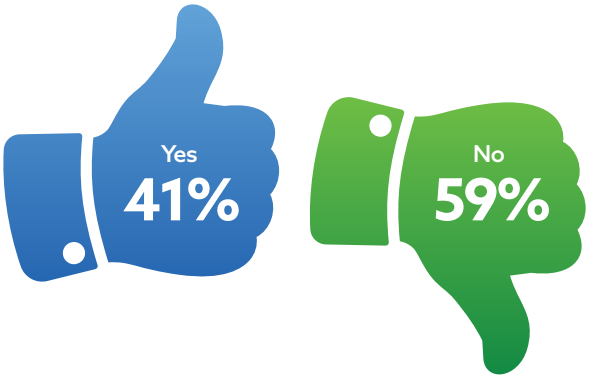
Another security debate that is taking place in the market is the question of whether an agency's security is better with a cloud provider than if its own staff did it, in-house. When you ponder the relative asymmetry in scale, resources and

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




expertise when comparing any of the cloud service providers with any normal agency, it would seem reasonable to expect better security from the cloud than in the agency's data center. That said, trusting a vendor, is for many, a big ask as 59% said they do not expect security in the cloud to be better than it is in their in-house data centers.

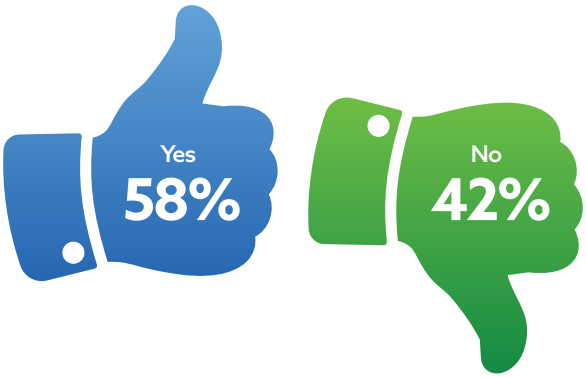
### Will security be better in the cloud than in-house?



### Best of Both: The Hybrid Cloud

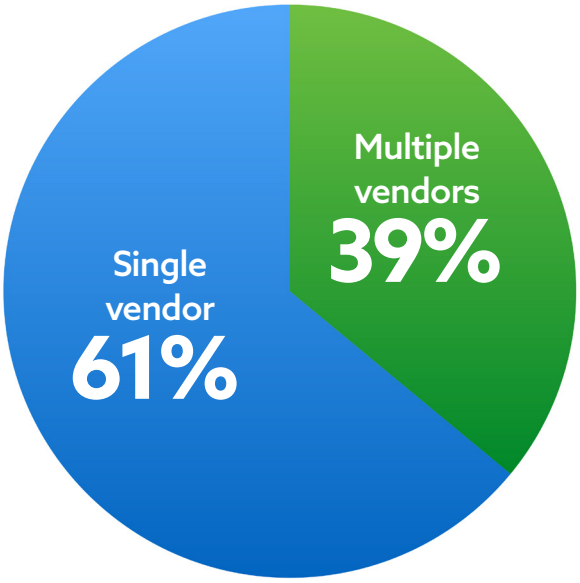
One way that government organizations are seeking to get all the benefits of public cloud while maintaining the advantages of on premises deployments is the use of hybrid clouds – combining public and private cloud. This strategy is being planned by

**Are you planning any sort of hybrid cloud deployment?**




58% of the organizations surveyed. But just as agencies 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 there is often 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 agency may want to ability to move workloads to the most cost effective cloud provider, maintaining relationships with multiple providers. Only 39% of those considering a move to hybrid cloud expect to use multiple vendors, perhaps highlighting the need for greater control and selectivity on where workloads are located. See figure below.

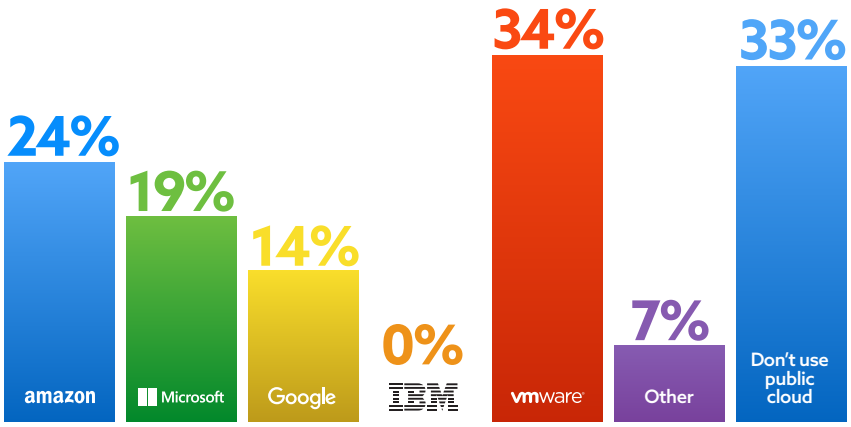
**If/when you move to the hybrid cloud, will you work with a single or multiple vendors?**



### Public Cloud Providers

33% of survey respondents indicated that they are 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. Those who are using public cloud providers today are spread across a handful of leading providers. 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 24% currently using Amazon. Microsoft gaining ground with Azure, cutting the gap between the two leaders with 19% indicating that they are currently using Microsoft for public cloud. In the survey, there was a stronger than usual showing of VMware (34%), perhaps due to the survey performed at the largest VMware gathering in the world. IBM Cloud adoption seemed to be non-existent among government agencies with none of the respondents indicating use of IBM Cloud.

**Which public cloud providers do you use?**




### Summary

The cloud is clearly here to stay and initiatives like Cloud First should drive greater adoption. For many, it will not only be hybrid, but will be a multi-cloud, 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 you may visit www.hytrust.com/STUDY. For more information about how HyTrust workload security solutions address cloud security concerns visit www.hytrust.com or call +1 650 681 8100.

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