Market Connections®
Research you can act on.

SEPTEMBER 2018

The Rise of the Multi-Cloud Environment In Federal Agencies

Two years into the post-Cloud First era, it's clear U.S. federal agencies have adopted cloud with varying degrees of sophistication and success. The data from our most recent study shows that nearly half of agencies are relying on hybrid or multi-cloud models. Different factors necessitated this — diverse missions, varying security requirements for different uses, and diverse sources of funding were the easiest to identify. Does this mean we traded legacy silos for virtual ones? Not quite, as it would be next to impossible to justify a one-size-fits-all approach for a federal agency due to those factors stated.

PRESENTED BY

NUTANIX
Your Enterprise Cloud Platform

PREPARED BY

Market Connections, Inc.
11350 Random Hills Road, Suite 800
Fairfax, VA 22030
TEL 703.378.2025
www.marketconnectionsinc.com

SHARE THIS STUDY

The questions we need to answer in the post-Cloud First era are:

- When and where does renting or owning compute resources make the most sense?
- How can we better manage/secure/optimize IT infrastructure resources?
- How do we prioritize the more strategic, mission-critical elements of IT — the applications — to deliver greater value to users and the mission?

The commercial sector has been using hybrid and multi-cloud models to best meet organization demands for years — and using management plans to ensure that security, cost and asset management is in their control.

Are federal agencies moving toward the same conclusions? And if not, why?

For three years, Nutanix has worked with market research firm Market Connections to explore how federal agencies are adopting, implementing, managing, and optimizing hyper converged infrastructure and hybrid cloud. This year's research, compared to that of 2016 and 2017, revealed some interesting trends. The use of IT in federal agencies is at a critical juncture, and the opportunity to make critical decisions that free agencies from the unsustainable tech refresh cycles is at hand.

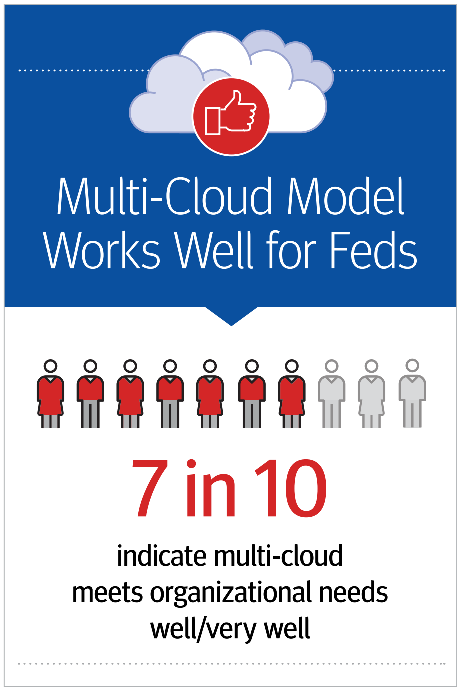
Three Years, Three Trends

This year's study dives into the current realities of working in a post-Cloud First, multi-cloud environment. Over three years of collecting this data, three key trends emerged:

- Security remains the top concern for IT professionals when evolving from legacy architectures to new formats such as cloud computing.
- Cost control is always important to federal agencies, and more than one-third say managing costs is more difficult or the same as over the last three years.
- IT professionals find managing and optimizing assets a challenge, one that the use of cloud computing complicates.

The 2018 study data shows that 95% of respondents are using some form or combination of cloud in their agency environment, with 48% reporting the use of hybrid or multiple clouds, with 71% of those respondents indicating that this approach works well/very well.

Because the primary concerns are similar across studies, the data suggests that while technology capabilities are progressing, the processes surrounding the acquisition and deployment of technology may be preventing real transformation. More than one-third (39%) cite the procurement process as the biggest barrier to change. The technology is evolving, but the processes to evaluate and procure it have not. But is the answer one agency, one cloud? The following discussion of the trends uncovered in our research indicate a definite no.


Multi-Cloud Model Works Well for Feds

7 in 10

indicate multi-cloud meets organizational needs well/very well

Security: A Case for the Multi-Cloud Approach

In the first year of the study, 2016, more than half of respondents (55%) noted security concerns most often as the greatest challenge faced when managing their agency's virtual environment, the predecessor to the cloud. In 2017, security was still the top concern, with 71% noting security risk as one reason agencies do not use a public cloud.

Security remained the top concern in 2018, with respondents noting compliance and different security requirements between programs most often as the reason organizations are using more than one cloud platform (44%). Aside from the wisdom of spreading security risks across an environment, rather than concentrating them into a single environment, the multi-cloud approach is enabling the diverse security requirements of different users and departments to be met.

YEAR OVER YEAR

SECURITY Top Concern

2018

44%

Noted **security issues as the #1 reason** organizations are using more than one cloud platform

More than two-thirds (69%) say the organization would change cloud providers because the current provider is not meeting security needs and requirements, but 41% believe it would be extremely hard or impossible to change, which further highlights the wisdom of using a multi-cloud environment.

Cost Controls: Avoiding The Sprawl

In 2016, 51% of respondents noted that the cost to implement/maintain, and the cost to procure (50%) made it difficult to incorporate new technology/architecture models into their organization's existing environment. In 2017, despite 39% of respondents noting that public cloud computing benefited their organization greatly in terms of cost savings, IT decision makers noted that the main reasons the public cloud didn't realize a greater cost savings is because it is challenging to control/manage costs (50%) and it is too easy for costs to escalate (45%).

Cost Controls Are Growing Concern

2016	2017	2018
at least **50%** *noted* **cost is a barrier to incorporate new technology**	**50%** **find it challenging to control/manage costs** *and* **45%** **find it too easy for costs to escalate in public cloud**	**72%** **have completed or are in process of managing/ optimizing costs**

BOTTOM LINE: Cost controls were harder than expected. Agencies are evolving their cloud use to increase their control.

2016 Study: Hyperconverged Infrastructure: An Effective And Efficient Path To Federal IT Modernization
2017 Study: The Enterprise Cloud Balancing Act: Emerging Trends in the U.S. Federal Government

As agencies gain more experience in the cloud, they find that the cost has been as expected (49%), although more than a quarter still say costs are more than expected.

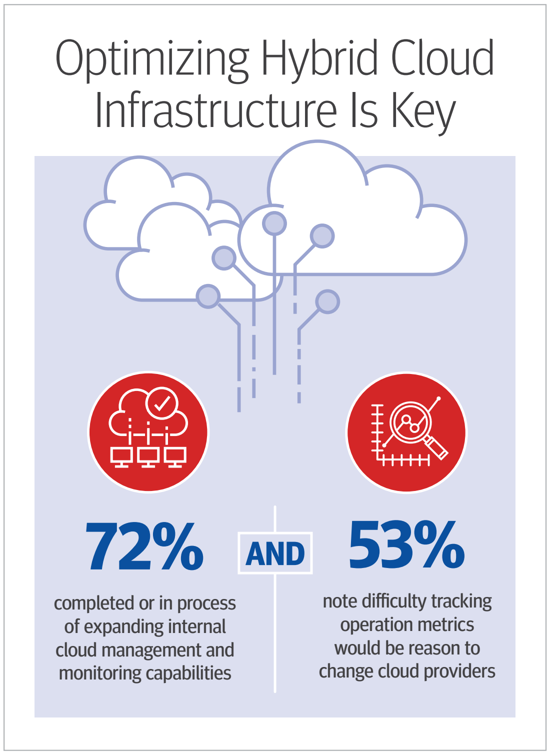
"We hear people say that once you're in the cloud, you can't turn it off or reverse it overnight, and there's an ongoing cost that they didn't expect. Part of the problem is that lifting and shifting without any back-out plan or any way to migrate workloads back and forth makes managing costs difficult," said Dan Fallon, Nutanix Director of U.S. Federal Systems Engineering.

In 2018, nearly three-quarters (72%) of respondents indicated they have completed or are in the process of managing/optimizing cost for the existing clouds used.

While there are technology initiatives like the Data Center Optimization Initiative (DCOI) and the Modernizing Government Technology Act that have provisions to manage cost, the complexity of accomplishing the cost, power, and space savings — while maintaining and upleveling services and service levels — is where agencies face the greatest challenge.

Managing and Optimizing Infrastructure: Assuming Control

Three years ago, managing both physical and virtual platforms efficiently was the second greatest challenge (behind security) when managing an organization’s virtual environment (33%). By the following year, federal IT professionals were beginning to believe that “you have to get used to giving up control over infrastructure management in a public cloud” (29%).



Optimizing Hybrid Cloud Infrastructure Is Key

72% completed or in process of expanding internal cloud management and monitoring capabilities

AND

53% note difficulty tracking operation metrics would be reason to change cloud providers

The problem with that, says Fallon, is that when you don’t know exactly what you have, exactly where it is, or have the ability to command it when you need to, the security risk, the possibility of making redundant purchases, spending more than necessary, and so on, increases.

Agencies realize this, and as of 2018 nearly three-quarters (72%) have completed or are in the process of expanding their internal cloud management and monitoring capabilities. In addition, over half (53%) say that difficulty tracking operational metrics with a current provider would be a reason to change cloud providers.

While more than half of respondents are currently using a third-party tool for cloud management, they’re working in a siloed environment that may not provide the overall visibility into assets the agency needs. Agencies might have visibility into the specific assets that are in a particular cloud, but in a multi-cloud environment, you must refer to multiple sources to figure out where everything is. Ideally, agencies would leverage a management platform that provides a consolidated view of all assets, and diminish the security risks while creating much greater control and visibility within their organization.

How Can Agencies Regain Control of Their Cloud Environment?

The federal cloud environment need not fall into the same silos as legacy systems as long as agencies take advantage of the tools at their disposal to manage, control, and optimize a multi-cloud environment. The only way to do that is by establishing asset transparency and agency-wide governance over how they’re using the cloud. Unfortunately, the data shows that agencies are not doing this in a way that empowers them. Rather, they’re doing it in a way that gives the vendors all the power.

When users lack full visibility into all their assets, they can only manage, control, or optimize them in incremental degrees, not to any material degree. The answer to this challenge isn’t a single cloud: the perils of that play out daily in terms of outages, cost escalations, and lack of governance. Respondents have indicated that the multi-cloud environment is working for them. The key is taking those elements that work well, and isolating and eliminating those that don’t.

Fallon says there is a new approach where agencies can make multi-cloud work very well, an approach that seamlessly knits all the components together and empowers users to manage their environment from the application level — which is where infrastructure really matters. The old way of procuring technology meant focusing significant IT budget into the infrastructure, or, the plumbing. But we know today that the cloud is like any other infrastructure, and spending a majority of budget on infrastructure (cloud or hardware) reduces the investments that can be made in the area where real innovation happens — in the applications.

This approach includes creating a management to accompany a technical solution. Executing this plan via a proven technical platform enables agencies to manage all assets across public and private clouds, to migrate workloads with a few clicks, and have the control to run application workloads when and where they get the greatest advantage. The result is agencies aren't locked into a restrictive billing cycle that provides limited options for optimizing asset usage. If they go in with a plan up front, then they have the flexibility to optimize the multi-cloud environment for their best use case and their best financial benefit along the way.

Conclusion

As the commercial sector discovered, hybrid and multi-cloud environments are meeting federal agencies' needs, and is the choice more and more agencies are making. Despite how well this system works, agencies still face the same concerns as when adopting any new or innovative IT: security, cost controls, and managing and optimizing resources.

The good news is that addressing these concerns in a multi-cloud environment is ultimately the same as with any IT infrastructure — agencies realize the greatest promise with effective management and governance. A strong management plan will address the cloud lifecycle, leverage a proven platform to converge management of the multiple clouds, optimize how the agency uses the clouds, and provide full asset visibility/transparency that gives agencies the advantage in determining what they will use and how much to spend for the infrastructure "plumbing" within their IT environments. This winning combination will ensure federal agencies are truly able to maximize the promise of the cloud.

About the Study

The blind, online survey of 150 federal IT decision makers included 40% Department of Defense, military service or intelligence agency; and 60% federal civilian or independent government agency, including legislative and judicial agencies. Respondents all had responsibility for the agencies' IT: 53% evaluate and recommend solutions; 55% are on a team that makes decisions regarding solutions; 21% make the final decision regarding solutions; and 37% manage or implement solutions.

Respondents use of the cloud breaks down as: 29% have private cloud only (Is operated solely for a single organization; it may be managed by the organization or a third party and may exist on premise or off premise); 19% have limited use of public cloud (owned by a third-party organization that sells cloud services to the general public, available to the general public or a large industry group); 29% use a hybrid cloud (a cloud computing environment which uses a mix of on-premises, private cloud and third-party public cloud services with orchestration between the two platforms); 19% have a multi-cloud (use of multiple cloud services from different providers to meet specific workload needs but there is no orchestration or connection between them); and 5% are not using cloud — they have a data center environment.

ABOUT NUTANIX

Nutanix is on a mission to make datacenter infrastructure invisible, elevating IT to focus on applications and services that power the agency mission. The Nutanix enterprise cloud platform leverages web-scale engineering and consumer-grade design to natively converge compute, virtualization and storage into a resilient, software-defined solution with rich machine intelligence. The result is predictable performance, cloud-like infrastructure consumption, robust security, and seamless application mobility for a broad range of enterprise applications.

Learn more at www.nutanix.com/fedcloud, or follow them on Twitter @ NutanixFederal.

ABOUT MARKET CONNECTIONS, INC.

Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education.

For more information visit: www.marketconnectionsinc.com.

TO DOWNLOAD WHITE PAPER AND INFOGRAPHICS

Visit www.nutanix.com/fedstudy2018

SHARE THIS STUDY