Issue Brief

Multicloud Enabled IT Modernization in Government

Simplified and secure multicloud solutions are helping agencies increase agility, accelerate innovation, and achieve faster time to mission and IT value.

Rising to the Challenge of COVID with the Cloud

Government IT departments responded quickly and effectively to the unparalleled disruption resulting from the global COVID-19 pandemic. Much of this successful shift was underpinned by an unprecedented move to leverage the flexibility of cloud infrastructure and solutions.

At the time of the pandemic's outbreak, many public sector IT departments held concerns regarding remote work and the security of sensitive data stored in the cloud. But according to Lorenzo Winfrey, Senior Product Manager at Rackspace Technology and a 13-year veteran of the Defense Intelligence Agency (DIA), COVID-19 demonstrated that "there is no bogeyman in the closet" when it comes to cloud computing. As a result, the past 12 months have witnessed a dramatic uptick in public sector cloud deployments in order to accommodate a newly remote workforce and address constituent and mission needs with minimal disruption. According to Federal Times, "the federal cloud computing market is poised for strong growth in response to both ongoing IT modernization initiatives and new demands caused by the COVID-19 public health crisis."

Accelerating IT Modernization with Multicloud

Becoming multicloud enabled is foundational for government agencies to accelerate modernization and time to mission value through IT. It is also fundamental to drive the digital innovation necessary to address technology readiness and ensure operational efficiency – to deliver on mission needs.

"There was a vision for all the ways cloud technologies and solutions could modernize government operations," says Winfrey "but it never fully materialized and now the shift with programs like FedRAMP and policies like cloud-first and cloud SMART are helping to push agencies forward to make the vision a reality."

Every agency has various types of data they use that require different levels of security and compliance – hence the need for a strong multicloud strategy with technologies and solutions that can evolve with the data it handles and changing requirements.

A strong multicloud enablement strategy delivers three key advantages to government IT departments:

1. **Shifting CAPEX Costs to Industry:** Leveraging cloud infrastructure obviates the need for public sector IT departments to negotiate and secure funding for massive hardware contracts. Industry becomes responsible for purchasing expensive servers.
2. **Freedom to Focus on Mission Objectives:** As cloud infrastructure becomes the responsibility of cloud service providers, public sector IT departments are freed from the time-consuming process of patching and maintaining physical hardware. They can use this time instead to focus on their organization's mission objectives.
3. **Increased Agility:** In his time at the DIA, Lorenzo Winfery found that testing the viability of a new piece of technology could take "months" due to the need to secure licensing and funding for equipment. This same evaluation work can now be done in weeks, or even days, thanks to scalable and readily available cloud-delivered compute resources.

Federal government estimates:

$2,250,000 to achieve a FedRAMP authorization

$1,000,000 a year to maintain

The Challenge of Changing Security and Compliance Requirements

Despite the opportunity offered by cloud computing in general and distributed cloud in particular, agency IT departments and the Cloud Service Providers (CSPs) that seek to serve them are often overwhelmed by the complexity and frequency of changes to the security and compliance requirements set forth by FedRAMP and other governmental programs. There are of course good reasons for these requirements – federal authorities have a responsibility to ensure that agencies are secure. But CSPs also have to make a business decision about what to invest in and there is a high cost associated with federal certification programs.

To illustrate, according to the federal government's own estimates "the total median cost for a mid-range CSP was $2,250,000 to achieve a FedRAMP authorization," a number which can balloon higher depending on the unique characteristics and complexity of the CSP's offering and which does not account for "about $1,000,000 a year" to maintain "an acceptable risk posture through Continuous Monitoring." As a result, only a small minority of CSPs bring their offerings to market, resulting in less choice for agency IT departments.

Navigating FedRAMP Levels: FedRAMP High or FedRAMP Moderate?

The passage of H.R. 3941, the Federal Risk and Authorization Management Program Authorization Act of 2019, in the House of Representatives and its referral to the Senate Homeland Security and Governmental Affairs Committee has only increased agency and CSP interest in the FedRAMP program. Unfortunately, a number of misconceptions abound, many of which concern the levels of impact risk within FedRAMP. Specifically, many CSPs mistakenly assume that they must meet the requirements of FedRAMP High, intended for only the most sensitive government data, in order to be competitive.

Winfrey notes that "the overwhelming majority of FedRAMP authorizations occur at the moderate level, with only around eight percent of authorizations occurring at the high level. While the additional controls at the high level may be helpful, the vast majority of requirements are at the moderate level."

The Role of Distributed Cloud: The Path to Edge Compute

Not all clouds are created equal and while multicloud technologies and solutions deliver benefits like reduced CAPEX costs, improved agility, and increased mission focus, many applications utilized in the public sector require low levels of latency that cannot be adequately addressed by a single centralized data center. Instead, many government IT departments have begun to leverage a distributed cloud model that allows for the centralized management of geographically dispersed data centers and edge devices.

Phil Fuster, Senior Director of Public Sector Sales at Rackspace Technology, notes that "crunching data at the edge and aggregating it at the center is the way of the future, opening the way for faster data analysis and better decision-making." Lorenzo Winfrey adds that "as mission objectives become more dynamic so too must the approaches IT leverages to accomplish them. Distributed cloud offers a path to address new use cases as agencies are able to leverage compute resources that are closer to where they're needed in the field."

Charting a Path Forward

CSPs looking to serve the public sector want to focus on their core competency: solving government pain points by delivering great solutions; not worrying about underlying infrastructure. Likewise, federal IT departments want to leverage the same leading technologies used by their counterparts in the private sector to meet their mission objectives in a secure manner.

Rackspace Government Cloud (RGC) on VMware was designed from the ground up to deliver on the promise of a secure and compliant cloud and bring together CSPs and agency IT departments. RGC on VMware is authorized for secure government use via the FedRAMP Joint Authorization Board, enabling CSPs to inherit up to 80% of the solution's over 325 security controls. Doing so dramatically cuts down the time needed to obtain FedRAMP authorization from years to as little as four months. As Lorenzo Winfrey points out, "RGC on VMware customers never have to start from scratch, they're able to build on our existing investments to get to market faster and at lower cost." Additionally, RGC on VMware provides continuous monitoring and management of those security controls to ensure CSP solutions are always in compliance with changing requirements.

How to Get Started

Drawing on his experience at the DIA, Lorenzo Winfrey, Senior Product Manager at Rackspace Technology, recommends the following steps for government IT departments looking to leverage the cloud:

Understand your requirements. Have a clear understanding across the organization of what you're looking to achieve and the difference between a CAPEX and OPEX financing structure.

Set up a good governance structure from the beginning. Make sure you know how data is going to be managed and what various parties are accountable for.

Don't take your existing methodology and blindly apply it to the cloud. The cloud requires a different way of thinking than traditional on-premises installations to get the most value.

Understand your legacy IT investments. Taking the time to do a cloud readiness assessment across your application portfolio is invaluable in generating quick wins and building the momentum necessary to tackle more complex tasks.

Underwritten by: rackspace technology vmware carahsoft