

Accelerate Time to Value and Mission with Secure, Compliant Multicloud as a Service

How to Overcome Common Hurdles to Fully Realize the Benefits of the Cloud

Federal government spending on cloud computing jumped about 8 percent in fiscal year 2020, to \$6.6 billion, and will reach \$8.5 billion by FY2023, according to Bloomberg Government. The sheer dollar figure and expected growth demonstrate agencies' willingness to embrace the spirit and letter of the Fed's Cloud Smart strategy and the Modernizing Government Technology Act.

Looking beyond the numbers, however, agency cloud progress runs the gamut from nascent to deeply experienced. The Department of Veterans Affairs, for example, has migrated more than 100 applications to the cloud, while the National Oceanic and Atmospheric Administration published its inaugural cloud strategy in July 2020.

Secure multicloud as a service can rewrite the cloud trajectory for agencies, no matter where they are in the cloud journey. It frees agencies to focus squarely on their mission, while entrusting cloud operations and security to the experts.

Keeping Eyes on the Prize

The advantages of the cloud are well known – especially its ability to accelerate IT modernization. In a 2020 survey of government decision makers by analyst firm IDC, respondents said business agility and innovation, improved customer service, and improved security were the top benefits they expected to achieve from cloud adoption.

Further, the shift from a CapEx to OpEx model gives agencies flexibility in budgeting, and cloud services enable agencies to cost effectively right-size their technology ecosystems. Cloud-based infrastructure enables IT organizations to rapidly create development environments and sandboxes where they can develop, test, and fail or succeed with minimal risk and cost. Agencies can take advantage of this rapid development capability to leverage and operationalize emerging technologies, such as artificial intelligence and edge computing.

For agencies to fully realize the benefits of the cloud, they must overcome myriad challenges and misperceptions, and undertake extensive preparation before moving forward.

Understanding Cloud Options

Early moves to the cloud often involved purchase of a software as a service (SaaS) application to quickly bring a new capability to an agency team. Often categorized as shadow IT, these early cloud uses acclimated employees to IT as a service. Frequently, movement of email or collaboration platforms was the next step in cloud adoption. As migration continues and agencies embrace enterprise-wide cloud on a larger scale, however, complexity increases exponentially. Hybrid versus multicloud is a common point of confusion as agencies consider their options.

A hybrid cloud includes private cloud infrastructure such as an agency's data center, as well as one or more public cloud services, usually working together to achieve mission goals. A multicloud environment employs public cloud services from multiple cloud providers. For example, an agency might host its call center application on Amazon Web Services and its Windows applications on Microsoft Azure. Multiclouds may include a private cloud component; when they do, they are both multicloud and hybrid cloud.

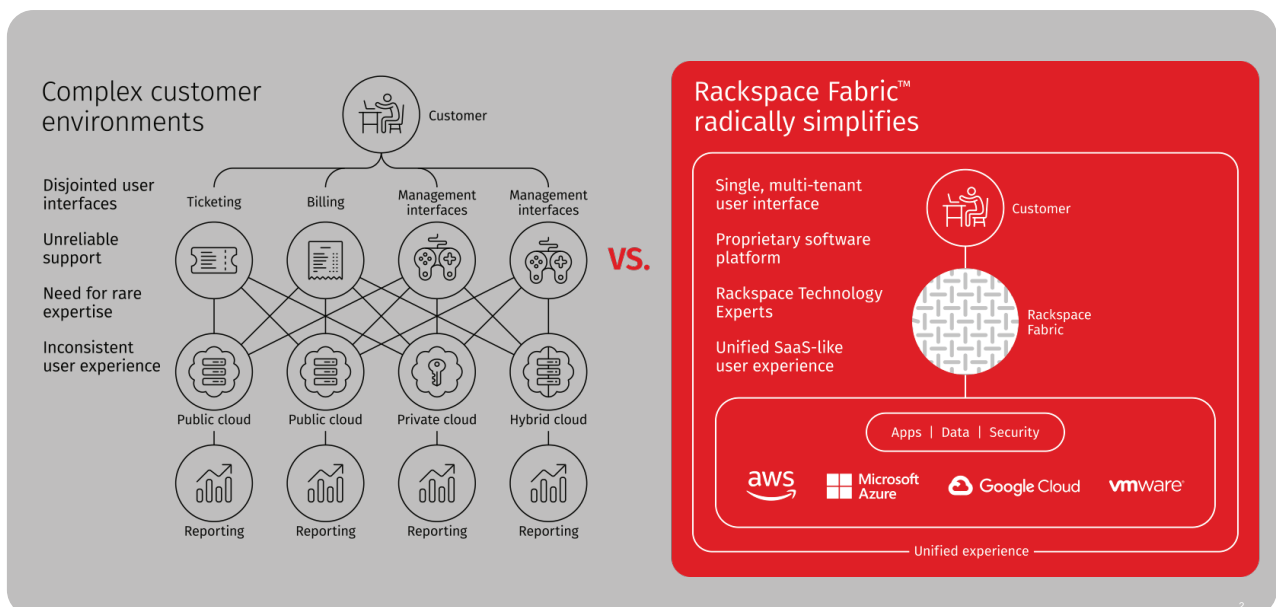
Agencies adopting a multicloud strategy are able to leverage the strengths of multiple cloud providers to acquire capabilities that best meet their mission requirements. A multicloud strategy also prevents lock-in to a single cloud provider, helps agencies hedge against potential security threats and service outages, and enables agencies to optimize IT budgets by comparing pricing and negotiating with multiple providers to fully realize the cost savings that cloud can bring.


Getting Beyond a Pilot Project

A small cloud project typically serves as a pivot point for modernization across the agency, noted Adam Grandt, managing director at GSA's Cloud Adoption and Infrastructure Optimization Center of Excellence (CoE), at a January 2021 training event.

Sometimes, migration to the cloud stalls after the pilot project because upfront preparation didn't fully assess the costs of their legacy operations or set clear goals for the initial implementation. If agencies don't fully understand the total cost of operation of their current, on-premises implementation across the full lifecycle, the transparent

Rackspace Government Solutions has held FedRAMP Joint Authorization Board (JAB) certification since 2015, as well as Department of Defense Impact Level 4 and DFARS/Cybersecurity Maturity Model Certification authorization.





pricing of a cloud implementation can look more expensive than the status quo. Agencies must also take into account their role in operating and securing public and hybrid cloud implementations, even if they are using a hyperscaler. And absent a specific definition of success, leaders may not have the justification they need to move to the next stage of deployment.

Staffing is another sticking point. To ensure success, agencies must identify leaders who are able to lead cloud initiatives and ensure they have skilled staff to support the implementation – in house, contracted, or both. In agencies laden with legacy systems, headcounts for cloud staff are already slim, while competition in the broader marketplace is fierce. Without enough skilled staff members, successful pilot initiatives often wither as their scope expands.

Overcoming the Challenges of Rationalization and FedRAMP

Agencies are also challenged by the very mandates that are designed to enable modern operations. The Cloud Smart strategy, for example, directs agencies to rationalize their application portfolios to drive Federal cloud adoption. Lift and shift is the simplest approach, but it ensures agencies won't get the best value from the cloud. That's because 84 percent of on-premises workloads are overprovisioned, according to a study by Bain & Company and TSO Logic (now AWS Migration Evaluator). If those workloads are simply shifted to the cloud, the agency is still paying for more computing than it is using – and is likely to pay 10 to 15 percent more than on premises, according to Bain and TSO's analysis of more than 60,000 workloads. In contrast, organizations that conduct a thorough analysis and right size workloads before moving to the cloud can save 30 to 60 percent, Bain and TSO found.

A substantial application rationalization is critical to cloud success. Moving to cloud, when done properly, can save money and improve security, but requires careful planning. On a case-by-case basis, agencies must decide whether to:

- **Rehost** – lift and shift
- **Replatform** – use cloud-native functionality such as a managed service to run the app
- **Refactor** – modify the app to make sure it works well in the cloud
- **Rearchitect** – replace the entire application
- **Retire** – eliminate the application

FedRAMP authorization also poses a substantial hurdle in the cloud journey and is rife with misunderstanding. The FedRAMP program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services and products. Agencies are directed to use cloud solutions that have gained FedRAMP authorization, whether those solutions are procured or developed in house. Often, agencies believe that hosting an application on a FedRAMP-authorized public cloud means that the application is FedRAMP authorized. But that's not the case. By hosting an application on a FedRAMP-authorized public cloud, agencies inherit 10 to 15 percent of the security controls they need for FedRAMP authorization of the application. They must undertake the other 80 to 85 percent – or they can leverage a FedRAMP authorized platform as a service, which can get them up to 80 percent of the way to FedRAMP compliance.

Answering Critical Cloud Questions

These are just some of the hurdles agencies face when migrating to the cloud. Along the way, agencies must address these questions and more:

- What is our multicloud strategy?
- What goes where – public, private, hybrid?
- Which public cloud is best for each use case?
- How do we manage a growing universe of integrations?
- How do we optimize operational efficiencies?
- How do we ensure appropriate security and compliance – and avoid the risk and expense of having to move data multiple times due to security and compliance risk?
- What tools do we need to manage our multicloud environment?

The multicloud environment enables agencies to leverage best-of-breed cloud capabilities for mission success. Managing the multi-cloud environment, however, can place a tremendous burden on in-house IT teams, because workloads are distributed across clouds and each cloud has its own interfaces, security requirements, SLAs, data flows, and more.

Turning to Secure Multicloud as a Service

Navigating the ever-evolving multicloud ecosystem is a complex, daunting task, and agencies increasingly seek a trusted guide that can provide unbiased insight and a clear path forward, while eliminating a mounting operational burden. Rackspace Government Solutions delivers multicloud as a service to solve this growing, and unnecessary, challenge.

Rackspace Government Cloud helps agencies and solution providers maximize the value of FedRAMP by accelerating the Authority to Operate (ATO) process and the rapid delivery of cloud-based solutions in support of agency missions. It offers automation, security, and multicloud adoption expertise on a secure FedRAMP-authorized platform as a service on public (AWS), private (VMware), or hybrid cloud infrastructure as a service. With Rackspace Government Cloud, agencies, system integrators (SIs), and independent software vendors (ISVs) inherit 80 percent of the controls required for FedRAMP ATO, which enables them to get to ATO in three to four months instead of 12 to 18 months, and at as much as 70 percent less cost.

Rackspace Government Cloud's embedded security controls and continuous automated security monitoring help ensure that agency SaaS solutions remain compliant with changing FedRAMP requirements. Rackspace helps customers prepare for their initial FedRAMP ATO process and provides ongoing support to ensure they remain authorized.

In addition, the Rackspace Government Solutions and managed services portfolio offers unparalleled multicloud, security and

Rackspace at a Glance

A leader in the 2020 Gartner Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide

A leader in The Forrester Wave: Multicloud Managed Services in North America, Q2 2020

Powers 15+ FedRAMP ATOs and numerous government cloud solutions

The largest AWS managed service provider; VMWare Premier Cloud Partner; Dell Titanium Partner

Delivers 80% of NIST 800-53 Inheritable Security Controls with Rackspace Government Cloud

Holds 6,000+ certifications across AWS, Microsoft, and VMware

compliance expertise and certifications, empowering agencies to confidently design, build, manage, and optimize the cloud. As a result, agencies can accelerate innovation and agility – and meet mission requirements faster. Rackspace Government Solutions enables agencies to focus on being mission experts, rather than cloud experts.

The Rackspace Fabric technology service platform unites all cloud platforms, enabling consistency in multicloud. With this service layer, Rackspace Government Solutions provides common governance, ticketing, billing, tagging, and more throughout agencies' multicloud estates. The solution does not replace native access to cloud technology; instead, it unifies the service layer between them. This enables a faster, more consistent approach to consuming cloud resources from multiple providers, enabling government organizations to realize the transformational capabilities of cloud much faster. Rackspace also delivers access to solution experts, engineers, data architects, and system administrators via solutions such as Rackspace Teams to help agencies ensure they have the skilled, experienced staff they need for a successful multicloud journey.

For more information about the Rackspace Government Cloud, visit <https://www.rackspace.com/cloud/rackspace-government-cloud>.

