Successfully Adopting a Multicloud Operating Model in Public Sector

ATARC Multicloud Working Group

December 2022

ATARC

Advanced Technology Academic Research Center

Acknowledgements

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of the 2022 Report titled **"Successfully Adopting a Multicloud Operating Model in Public Sector"**, authored by the members of the **ATARC Multicloud Working Group**.

I would like to take this opportunity to recognize the following individuals for their contributions:

Kapil Bareja, MIT; Working Group Advisor Chair

Jessica Davis, Microsoft

Robert Ficcaglia, CNCF

Erik Johnson, Cloud Security Alliance

Geoffrey Mershon, UnifyPoint

Jeremiah Sanders, VMWare; Working Group Industry Chair

Manjit Singh, Agilious; Working Group Industry Vice Chair

Sid Sripada, Working Group Government Chair

Steve Vincent, TIAG

Sincerely,

Tom Suder, Founder, Advanced Technology Academic Research Center (ATARC)

Disclaimer: *This report was prepared by the ATARC Multicloud Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated.*

Table of Contents

Preface

The collective experiences of the authors of this document, both former and current government and industry counterparts, discerned there is a noted gap in current definitions and understanding around the concept of multicloud and multicloud operating models across industry, government, and analyst organizations. Consequently, many public sector organizations are struggling with multicloud complexity as they adopt cloud-based technologies at enterprise scale. Organizations are growing their way into multiple commercial service provider (CSP) clouds, on-premises clouds, and edge cloud instantiations. They are adopting multiple app development and deployment models in the cloud (traditional waterfall delivery, agile/continuous delivery/DevSecOps, etc.). All of this is happening, often without understanding the ensuing Day 2 multicloud ops and security complexities that hamper enterprise digital transformation.

This document intends to add to the conversation and close the gap in understanding multicloud and multicloud operating models. As such, the authors set forth the following problem statement to guide the contents of the document:

> *How do we enable public sector organizations to understand and contend with the Day 2 operational complexities of the multi cloud operating model they will encounter as they adopt and establish various app operations models in multicloud context?*

1 What is Multicloud and What are the Potential Operational Pitfalls?

The evolution of commercially managed cloud services has blended across traditional definitions that categorized operating environments (e.g. on premises, off-premises, edge) and commercial providers of Infrastructure as a Services (IaaS), Platform as a Service (PaaS), and Software asa a Services (SaaS). Today's cloud marketplace does not prescriptively delineate among providers of these architectural layers or operating environments. Rather, the 'you manage' vs. 'aaS' decision-space now spans cloud operating environments from off-premises, to on-premises to Edge. Further, many Cloud Service Providers (CSPs) do not cleanly fit into the 'IaaS' box anymore, as expanded managed service offerings include many facets of IaaS, PaaS and SaaS across on-prem, off-prem and edge environments.

Similarly, commonly used definitions of multicloud, hybrid cloud, and edge cloud fall short of informing enterprise-wide implementations that enable a truly consistent and seamless cloud operating model requisite of modern software delivery across these various cloud environments. The result is fractured cloud operations akin to 'multiple siloed clouds' that inhibit the agility requisite of modern digital enterprises.

The key enabler of a modern digital enterprise is a consistent enterprise cloud operating model. Digital IT operations must deliver software-enabled mission and business outcomes with seamless virtual consistency across multiple networks, infrastructures, application platforms and software services from multiple providers. In addition, that consistency must extend to on-premises operations/data centers and exponentially prevalent distributed edge devices. Collectively, these cloud environments must be consistently deployed, managed, and secured to complete the rich end-to-end, cyber-secure multicloud operations environment enterprises require.

Creating that holistic, system-of-systems outcome and achieving true DevSecOps requires not just a one-time integration of all these clouds. Rather, they must be continuously aligned in the face of ever-evolving operational needs, cybersecurity threats and the IT rate of change. Hence, as we will further detail, we submit these expanded multicloud definitions:

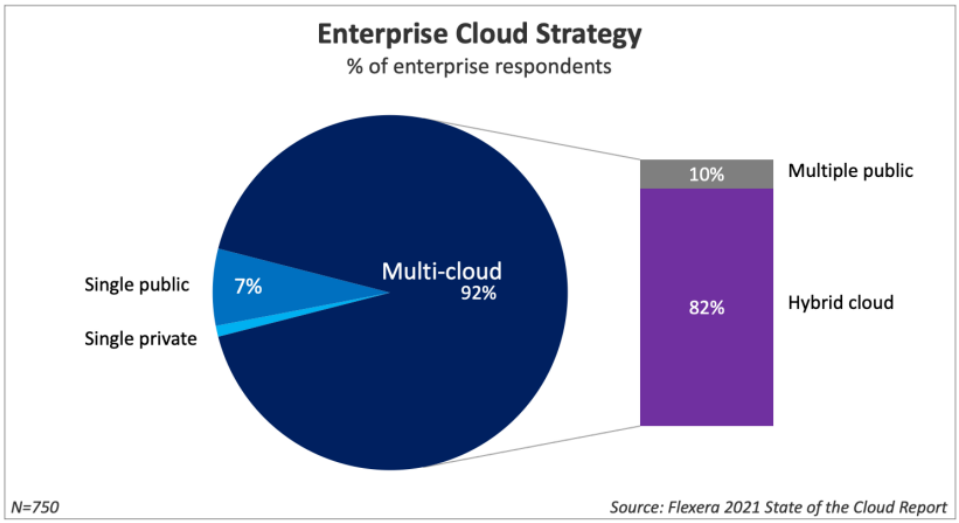
> **Multicloud: The infrastructure, application platform and software capabilities that enable enterprise cloud operations across one or multiple Commercial Service Provider (CSP) clouds, on premise clouds, and Edge clouds.**
>
> **Multicloud Operating Model: The infrastructure, application platform, and software capabilities required to continuously and consistently Build, Run, Manage, Connect and Protect IT and software at Day 2 scale across one or multiple CSP clouds, on premise clouds, and Edge clouds.**

It is not just Cloud Smart and Data Center Optimization Initiative mandates or Cybersecurity & Customer Experience Executive Orders driving Public Sector IT decisions. Globally, 80%[1] of IT executives have

[1] VMware Executive Pulse, June 2021

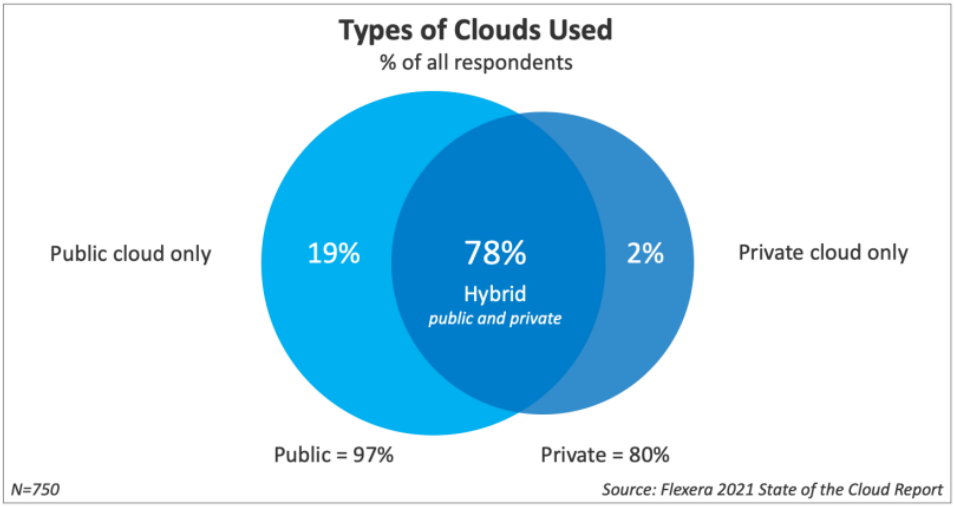
ongoing investment initiatives to digitally transform their enterprises across two dimensions - applications and infrastructure. Digital-age infrastructure entails cloud migration, and it's not just to one cloud! Business use-cases drive the need to transform how distributed workers and customers interact with workloads everywhere. Likewise, the speed and innovation of continuously delivered modern apps is a key differentiator that drives the need for boosting developer autonomy and adopting a DevSecOps model while reducing friction and improving developer experience (DEX) across the multicloud ecosystem. In response, 73%[2] of enterprises are deploying to a multicloud, which encompass multiple commercial cloud providers, on-premises operations and data centers, and the exponentially prevalent Edge.

Results from Flexera's 2021 State of the Cloud report[3] show that enterprises have almost entirely embraced multicloud. 92% of respondents reported having a multicloud strategy. 82% are taking a hybrid approach, combining the use of both public and private clouds.



99% of respondents are using at least one public or private cloud. 97% percent of respondents utilize at least one public cloud, while 80% have at least one private cloud. 78% of respondents are using hybrid cloud.

[2] VMware July 2021 Digital Momentum Study
[3] 2021 State of the Cloud Report, Flexera



The GovLoop 2022 Market Trends Report: Bring Choice, Control and Speed to Your Cloud Environment, indicates 93% of Federal agencies have a hybrid cloud strategy, 81% are already using multiple commercial cloud platforms, and 89%, as you might expect given the mission use-cases among government agencies, expect to maintain an on-premise cloud footprint in three years.[4]

These digital transformations are paying off for enterprises who implement them successfully. Successful multicloud adopters are seeing 35% revenue increases from faster delivery of modern apps delivered 42% faster, 41% fewer costs and hours spent on IT infrastructure and security incidents, and 35% productivity savings across a distributed workforce.[5] These enterprises go fast, spend less and freely and flexibly leverage the best of breed capabilities of any cloud. Yet, those successes do not come easy, and are, unfortunately, often the exception due to complexities that are not addressed in the IT planning and procurement cycle.

For many public sector agencies, multicloud initiatives have been driven through the lens of expanding the vendor pool and business opportunities across hyperscalers. Yet, beyond the simplicity of an expanded vendor pool, the reality of multicloud adoption involves myriad complexities to consider; both in initial cloud migration and in Day 2 operations. Public Sector multicloud IT operators need consistent, easy-to-use tools to manage thousands of diverse objects, services, containers, apps, data sources, and user profiles. In addition, they will grapple with varying degrees of cloud-readiness among heritage systems required to support government mission users and the constituency for the foreseeable future.

Multicloud operating challenges compound during the 'adoption cost period' of digital transformation, where legacy tech stacks often operate in parallel to modern cloud-based instantiations for several years. During this period, "IT pros must contend with the complexities of parallel infrastructure stacks, hybrid and/or multicloud architectures, disparate IT operations models, and untenable cyberattack surface proliferation."[6]

---

[4] Market Trends Report: Bring Choice, Control and Speed to Your Cloud Environment, GovLoop
[5] VMware July 2021 Digital Momentum Study
[6] Why Digital Transformation Demands a Culture Shift Alongside the Tech, Sanders, Feb 2021

These IT operational complexities demand diligent focus in the early stages of agency cloud adoption efforts, to ensure scalable success that meets the mission. For initial cloud migration, these include:

- A recent ESG study shows it takes an average of 27 days for enterprises to refactor and migrate an application to the cloud[7], and 90% of enterprises report skills shortages in cloud-related disciplines[8].
- Many organizations who were early adopters of native cloud offerings are finding they have lost the portability they need to maintain multicloud relevance and operational resiliency. Dependence on native cloud services stands in the way of true multicloud portability, and Gartner predicts, "applications deployed on a hyperscaler's platform using native tooling will take over a year (on average) to migrate to another platform.[9] In effect, agencies adopting cloud via native tooling become vendor locked!

Further, subsequent Day 2 ops complexities of multicloud are stifling efforts to scale digital transformation. These include:

- Inconsistent infrastructure constructs, application SLAs and incompatible machine formats
- Disparate operations, management and security tools and policies which drive an increasing training burden and oftentimes duplicative IT operations teams with specialized skills
- IT operations and Security teams get stretched too thin and are forced to be jacks of all trades and tools. Gartner found that customer administrator misconfigurations account for 70% of mobile device breaches and 80% of cloud breaches.

An April 2022 Forrester survey of 501 Government IT leaders[10] found the most challenging technical aspects of multicloud operations are:

- Maintaining Integration (72%)
- Managing network performance/latency between clouds and to/from cloud platforms (68%)
- Security of data in transit (63%)
- Difficulty identifying security risks or exposures (61%)
- Difficulty managing complexity of the multicloud environment (61%)

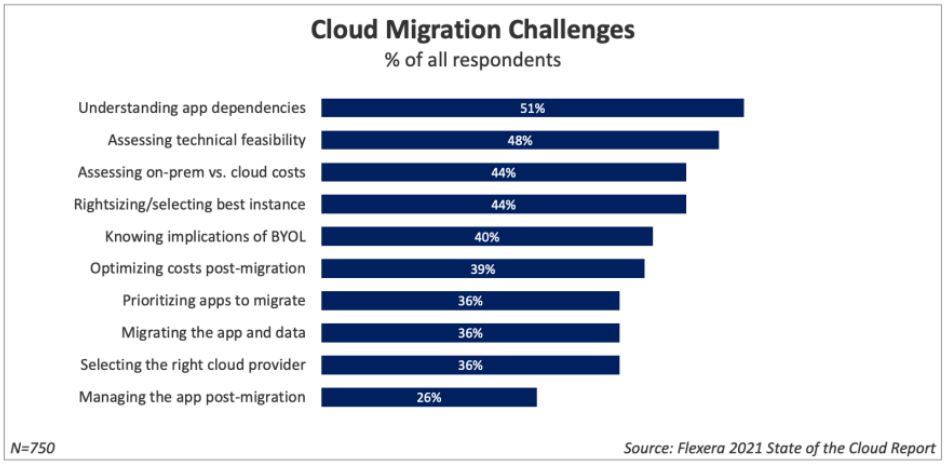
Further, this Forrester study enumerated resultant organizational implications of contending with those multicloud technical challenges:

---

[7] Hybrid Cloud Trends Survey, The Enterprise Study Group, March 2019
[8] 451 Research, (Nov 2018), 2019 Trends in Cloud Transformation
[9] Gartner: The Future of Cloud in 2025: From Technology to Innovation, by Lerner, Chandrasekaran, Smith, MacDonald and Mitchell-Smith, 2020
[10] Forrester Research Report: Multicloud Is The New Frontier Of Government IT - Where Agencies Are Today And The Roadmap To The Future, April 2022

- Culture of the IT organization (65%)
- Increased training requirements for operations and security teams using disparate native tooling (62%)
- Misalignment between IT and the Line of Business (61%)
- Increased operations and security staffing requirements to effectively manage multiple siloed cloud environments (61%)
- Cost of data migration to cloud (60%)
- Regulatory/compliance issues (58%)
- Lack of skilled employees to manage multiple cloud platforms (58%)

In addition to dealing with these complexities, siloed multicloud implementations may bring possible service disruptions (potential connectivity issues, service-level agreements, breaches), failover/failback capabilities, regulatory compliance, and a lack of skills. Without a consistent cross-cloud abstraction It is challenging to move a workload with dependencies on CSP-specific native services from one cloud platform to another, and the lack of interface standards make it difficult to maintain visibility into disparate cloud environments to manage application and data environments, security, and costs.



In aggregate, these multicloud challenges drive lacking enterprise visibility and cybersecurity postures, higher costs, decreased mission agility, and higher risks. Many agencies are in the throes of dealing with these challenges the hard way because they were unaware to plan for them up-front in procurement and architecture planning efforts. Indeed, 74% of Federal multicloud customers cite complexity as their biggest challenge.[11]

We assert this lack of awareness and upfront planning is due, in large part, to definitions and understanding of 'multicloud' falling short of accounting for the scope of capabilities needed to successfully implement a true multicloud operating model. This is confirmed by a recent Forrester

[11] Market Trends Report: Bring Choice, Control and Speed to Your Cloud Environment, GovLoop

survey with over 500 government agency IT leader respondents. It found that while 65% of organizations are increasing investment in professional development for developers, only 35% of these organizations have an outstanding training program in place for cloud technologies.[12]

[12] Multicloud Is The New Frontier of Government IT, Forrester Consulting, April 2022

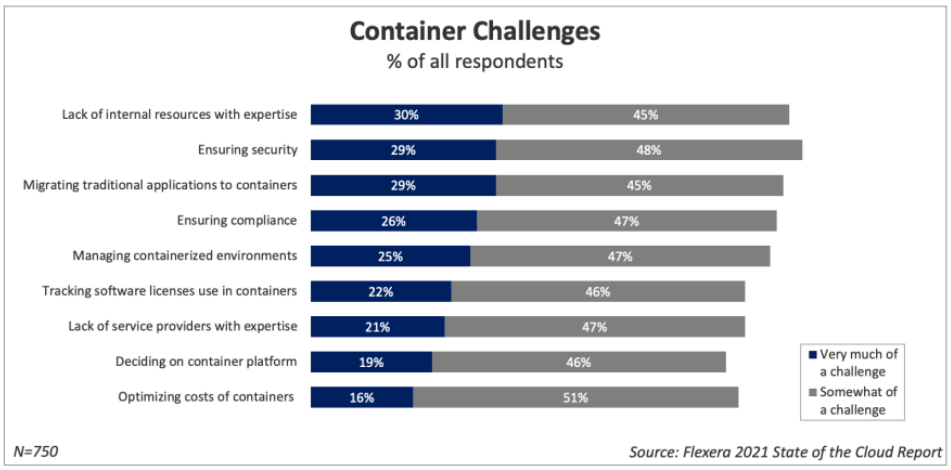
2 Multicloud Workload Migration Considerations

Cloud rationalization is the process of evaluating assets to determine the best way to migrate or modernize each asset in the cloud. Since every application is unique, there's no single set of steps to follow for modernization when moving to the cloud. Some applications are ready to modernize; some may require minor changes in code, others may require a complete redesign to make them cloud-ready; and some may need to be completely replaced. Choosing the right migration approach for different applications is key to a successful implementation. One must consider the five R's of Rationalization:

1. Rehost - Rehosting can be considered a first step toward cloud adoption and is the fastest way to migrate because it doesn't require any code changes to your app. Often referred to as a "lift-and-shift" migration; each app is migrated as is to reap the benefits of the cloud without the risk, cost and time associated with code changes.
2. Refactor - Often referred to as "repackaging", refactoring your legacy application by modernizing your application deployment architecture lets you retain your existing application code and business logic. With this approach, you can add cloud-enabled and innovation capabilities to your application with minimal code changes.
3. Rearchitect - Rearchitecting is to modify or extend the existing application's code base to optimize it for cloud platform and better scalability. Rearchitecting for migration is about modifying and extending app functionality and code base to optimize app architecture for the cloud. This is common with legacy applications.
4. Rebuild - If a legacy application requires too much work in order to modernize, it may make sense to leverage cloud native technologies in order to build a new application.
5. Replace – Sometimes it makes sense to replace an application entirely and move to a software as a service (SaaS) application.

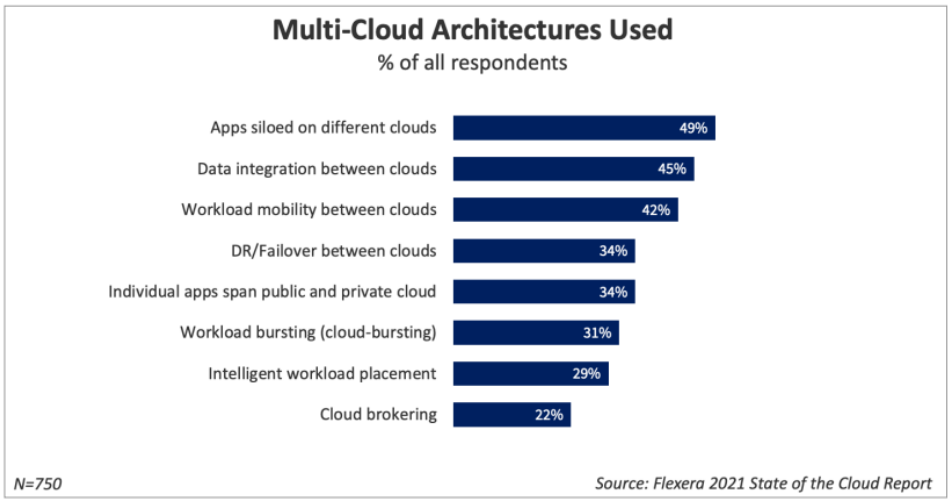
Many people use containers to refactor, update and extend existing applications or build new ones. Containers are a way to wrap up an application into its own isolated package. In its container, the application is not affected by applications or processes that exist outside of the container. You can deploy containers on IaaS or PaaS while using additional cloud managed services.

Containers can bring challenges as well. The top container challenges are the lack of internal resources with expertise, ensuring security and migrating traditional applications to containers. Since traditional apps are not optimized for microservices, these apps should be evaluated before taking a containerized approach. At best, rather than refactoring to a modern microservice architecture, organizations may just move legacy applications into 'fat containers', lumping the entire legacy app and its associated dependencies in a container, for several years as they remain in a modernization backlog awaiting developer resources.



Oftentimes, replacing outdated legacy applications with COTs is the simplest course of action. According to the Report to the President on Federal IT Modernization, agencies must leverage shared services and embrace commercial technologies such as Software as a Service (SaaS) where possible, building new capabilities only when shared services and commercial technologies cannot meet mission need. SaaS is a great option when these solutions meet requirements without having to build something new.

Another important aspect of multicloud workload migration planning is understanding the intended interaction of the workloads in the multicloud operating model. As referenced in the multicloud architecture survey below, there are myriad strategies and use-cases that guide multicloud adoption and enterprise operations. Understanding app dependencies, interactions and data flows can better inform a Cloud Smart multicloud strategy. Many organizations take a 'move everything we can to the hyperscaler' approach, only to realize unintended cloud cost overruns due to ingress/egress charges and app performance degradation due to latency as dependent workloads sprawl across multiple CSPs, on-premises and edge clouds. Understanding workload dependencies, mission/business use-cases, and opportunities for cost, performance, development and time to market optimization via a holistic utilization of CSP, on-premises and edge-hosting options is an important aspect of implementing a successful multicloud operating model.



3 Cost Management Considerations

One benefit of moving to the cloud is that it shifts how you pay for capacity, from CAPEX to OPEX. Your overall budget allocation moves from a CAPEX investment to OPEX pricing models that can fluctuate based on capacity or utilization of the cloud environment. Your organization can realize meaningful improvements in financial statements, with improved cash flow timing and a reduced need to acquire assets that result in a fixed cost structure.

Historical data can help manage costs when you analyze usage and costs over time to identify trends. Trends are then used to forecast future spending. Cost Management also includes useful projected cost reports. Cost allocation manages costs by analyzing your costs based on your tagging policy. And you use cost allocation for show-back/chargeback to show resource utilization and associated costs to influence consumption behaviors or charge tenant customers. Access control helps manage costs by ensuring that users and teams access only the cost management data that they need. Alerting helps manage costs by notifying you automatically when unusual spending or overspending occurs. Alerts can also notify other stakeholders automatically for spending anomalies and overspending risks. Various reports support alerts based on budget and cost thresholds.

4 Multicloud Workforce Considerations

Cloud adoption is a strategic change that requires involvement from both business decision makers and end users. Workforce upskilling/re-skilling strategies are one of the important aspects of cloud adoption. For the IT staff to function as change agents supporting current and emerging cloud technologies, their buy-in for the use and integration of these technologies is needed.

IT staff members may feel anxious about their roles and positions as they realize that a different set of skills is needed for the support of cloud solutions. But agile employees who explore and learn new cloud technologies don't need to have that fear. They can lead the adoption of cloud services and help the organization understand and embrace the associated changes.

During the transition from mainframes to the client/server model, the role of the computer operator largely disappeared, replaced by the system administrator. When the age of virtualization arrived, the requirement for individuals working with physical servers diminished, replaced with a need for virtualization specialists. Similarly, as institutions shift to cloud computing, roles and responsibilities will likely change to include Platform Operators, Site Reliability Engineers (SREs), Cloud Infrastructure Engineers, Cloud Services Engineers, CI/CD Engineers, etc.

5 Addressing Multicloud Complexity

Many organizations try to control multicloud infrastructure and operations inconsistencies by limiting choice and accessibility in ways that frustrate their developers, IT operators and customers alike. In essence, they abandon the freedom and flexibility of true multicloud agility and hamstring the efficiencies of multicloud we covered previously. However, seamless multicloud is possible with both freedom and control.

Forrester's 2022 Research Report: "Multicloud is The New Frontier of Government IT"[13] lays out a three-part strategy for successful multicloud adoption:

- Adopt third-party solutions that simplify multicloud management
- Use these solutions to remove complexity, make operations faster, and increase scalability and stability
- Select cloud platform providers with employee adoption in mind

This same Forrester report further details, "expanding a multicloud footprint requires centralized visibility and control across all environments. Most agencies expanding their multicloud footprint use third-party tooling for this purpose. Leveraging these tools allows agencies to support their current implementation along with the expanded services they plan on using."[14]

An emerging ecosystem of OEM-managed cross-cloud services enable a game-changing vision of multicloud operations at enterprise scale where applications and data have seamless portability among private and public clouds to create a resilient and unpredictable attack surface and unmatched business value. While on premise vendors and hyperscalers invest vertically to bring a rich and diverse set of capabilities to the multicloud marketplace, other companies are investing horizontally to automate and integrate all these diverse capabilities with cross-cloud consistency.

These cross-cloud capabilities extend much further than how Gartner frames 'Cloud Management Platforms', bringing truly ubiquitous software development and operations platform, cloud infrastructure and accompanying management, networking, security, and distributed workforce/end-user device management solutions for multicloud. These capabilities preserve speed and choice while streamlining management and control, delivering the power of multiple clouds with the simplicity of one.

These cross-cloud capabilities propel a 'migrate then modernize' cloud adoption and app portfolio modernization approach. Given the aforementioned untenable complexities of the 'adoption cost period' of digital transformation, where legacy tech stacks often operate in parallel to modern cloud-based instantiations for several years, for initial cloud migration, ***speed to cloud adoption*** is key. More specifically, avoiding up-front application refactoring by extending consistent cross-cloud infrastructure abstraction across all intended cloud operating environments allows moving workloads to the cloud

[13] Multicloud Is The New Frontier of Government IT, Forrester Consulting, April 2022
[14] Multicloud Is The New Frontier of Government IT, Forrester Consulting, April 2022

with speed. Once in the cloud, it is easier to modernize the applications (refactoring, rebuilding, replacing, etc.) all while providing a consistent and secure infrastructure and runtime environment where virtualized workloads, containers, Kubernetes, SaaS or cloud native apps can be managed seamlessly via a single pane of glass.

This 'migrate with speed first' approach simplifies operations and security constructs, drives faster infrastructure consolidation, brings cost reduction, reduces migration manpower and training burdens, and supports applications throughout their modernization lifecycle. Powered by these types of cross-cloud services, analyst studies by IDC and Forrester[15] have shown enterprises migrate to cloud in roughly half the time, for half the cost, enjoy ongoing CAPEX and OPEX savings of roughly 60%, and a 3-yr ROI of over 350%.

Further, as organizations leverage a consistent cross-cloud infrastructure to free up resources for app portfolio modernization, implementing consistent multicloud Kubernetes to manage containers and microservices delivers additional benefits. This is key, given 70% of respondents to a recent ESG study indicate their container-based applications will deploy across a combination of public clouds and on-premises data centers. Enhancing developer and operator experience with managed, automated cross-cloud Kubernetes services reduces the administrative costs associated with K8s infrastructure planning, configuration, and deployment by 70-80%, helping enterprises adopt Kubernetes 300% faster than trying to configure and manage open-source Kubernetes.

At scale, these organizations see Day 2 multicloud K8s operational efficiencies of 94% and a 3-yr ROI of 201% for implementing consistent multicloud K8s capabilities. As these organizations get more valuable modern software into production, the other key benefit they see is maintaining workload portability across the multicloud operating environment, both back on-premises or across CSPs as the need arises. Ensuring portability is key to meeting future business or mission use-cases, as well as ensuring government maintains maximum competition and price control across cloud infrastructure providers.

For Public Sector to leverage these capabilities and successfully navigate multicloud complexity, procurements must account for them up-front by including requirements for the requisite cross-cloud services. To that end, agencies need to expand their definition of 'multicloud' and plan up-front for the eventuality of a multicloud operating model that encompasses the infrastructure, application platform, and software capabilities required to continuously and consistently Build, Run, Manage, Connect and Protect IT and software at Day 2 scale across one or multiple CSP clouds, on premise clouds, and Edge clouds.

[15] Business Value of Running Applications on VMware Cloud on AWS in VMware Hybrid Cloud Environment, IDC, 2020 and The Total Economic Impact of VMware Cloud on AWS, Forrester, 2019

6 Multicloud Procurement Considerations

For Federal agencies to avoid the pitfalls of multicloud complexity, procurements must account for the need to manage those complexities up-front. Armed with the information covered in this paper, this is as much of an educational opportunity across the Public Sector as it is an opportunity to appropriately structure government acquisitions contracts to ensure cross-cloud success. To that end, we offer the following draft multicloud procurement requirements:

a. **Common Compatibility Layer:** The CSP or Reseller shall provide a common cross-cloud compatibility layer to offer consistent, cross-provider virtualization and containerization infrastructure that will enable standardized security, hosting, management, operations and minimize downtime.

b. **Secure Workload Portability across CSPs.** The CSP or Reseller shall provide an instantaneous, continuous, and secure hybrid and multicloud workload portability solution that is compatible with all other CSPs. This solution shall enable seamless cloud migration and scaled operations of legacy virtualized, cloud-native and containerized workloads without refactoring.

c. **Leverage Private Cloud Investments:** The CSP or Reseller shall leverage existing Agency or DoD on-premises cloud solutions investments, and hyperconverged tactical edge technologies.

d. **Common Enterprise Infrastructure:** The CSP or Reseller shall provide a common enterprise infrastructure capable of hosting enterprise workloads across cloud providers, on premises and edge providers.