How to Reap the Rewards of a Multi-Cloud Environment

MARKET TRENDS REPORT

govloop

FOUR POINTS TECHNOLOGY

aws

Introduction

Government agencies' decade-long transition into the cloud is steadily — and rapidly — evolving toward adoption of multi-cloud strategies.

A year ago, 70% of federal agencies were using two or more cloud providers, and in April 2024, the Senate Homeland Security and Governmental Affairs Committee approved the bipartisan Multi-Cloud Innovation and Advancement Act, which would help streamline multi-cloud adoption.In August 2024, the Biden administration moved away from defining different tiers of authorizations (previously JAB and Agency) and toward one designation of FedRAMP Authorized. Going forward, all authorized cloud service providers or CSPs will be considered FedRAMP Authorized, regardless of path, which will further enable cloud adoption.

Moving to a multi-cloud environment offers agencies the flexibility to manage their distributed infrastructures while optimizing resources, maximizing efficiencies, and enhancing security and compliance. Agencies can also optimize costs by taking advantage of pricing models from different vendors.

But none of this happens automatically. Implementing a multi-cloud environment, which combines on-prem, private and public clouds, numerous Software as a Service (SaaS) applications, orchestrated container environments, and other elements, is a complex task requiring careful planning and execution.

Agencies have at times struggled with cloud implementations, reflected in some agencies' low marks on the Federal IT Acquisition Reform Act scorecard and admonishments about cloud security from the Government Accountability Office. Many agencies would benefit from effective guidance.

This Market Trends report is a step toward providing that direction. To learn how to best reap the rewards of multi-cloud, GovLoop partnered with Four Points Technology LLC and Amazon Web Services (AWS). We'll examine the challenges agencies face and how to overcome them, best practices, and the essential capabilities of a true multi-cloud environment.

By the Numbers

What Exactly Is Multi-Cloud?

The term multi-cloud can be confusing. It doesn't mean multiple clouds, and multi-cloud isn't hybrid clouds or hyperscalers such as AWS and other CSPs — at least, not on their own.

A multi-cloud environment involves all the above and more: hyperscalers, on-prem cloud, edge solutions, SaaS and even colocation (shared space within a data center). It allows an organization to acquire capabilities according to their specific workload needs while avoiding vendor lock-in.

Agencies Turn Increasingly to Multi-Cloud Environments

Federal agencies are adopting diverse multi-cloud environments, a June 2024 report from Nutanix found. Although more than 80% of respondents said their agencies would benefit most from a hybrid environment encompassing public and private clouds, they are moving toward reducing the presence of on-premises private clouds in favor of public clouds. Here are some highlights:

Exclusive use of a non-premises data center/private cloud:

- **Today:** 27%
- **Within 1-3 Years:** 5%

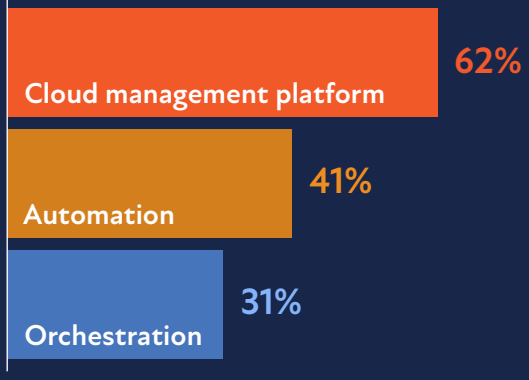
Reliance on a hybrid model combining private infrastructure with a single cloud:

- **Today:** 60%
- **Within 1-3 Years:** 35%

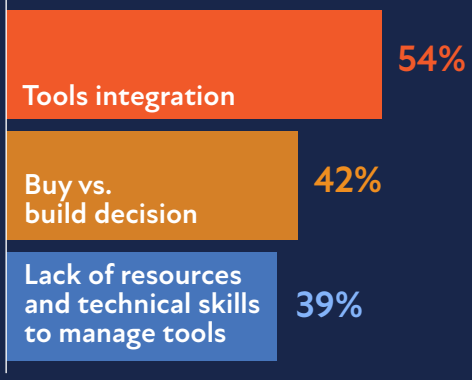
Agencies Identify Hurdles to Managing the Cloud

A survey by SAIC in June 2023 found that 70% of federal agencies were using two or more cloud providers.

What agencies use to manage cloud services and infrastructure:



Agencies identified several challenges in the cloud:



Agencies Are Pushing Forward, Despite Challenges

83%

identified application management as a moderate to significant challenge.

70%

have moved at least one application to a different environment in the past year.

84%

of federal organizations have containerized at least some applications, enabling cloud portability.

Achieving Continuity With Multi-Cloud Capabilities

The Challenge: Identifying the Hurdles to Optimized Operations

When implementing a multi-cloud environment, organizations in all sectors face many of the same challenges, such as maintaining flexibility and finding cost-effective solutions with good security, including both identity and access management and key management. But there are some challenges for government agencies that may be particularly acute.

A Lack of Necessary Skills. "A key challenge that some agencies face is they don't have the skillsets internally to move to a modern architecture, which is the foundation of cloud from an infrastructure," said Mark D'Alessandro, Chief Technology Officer at Four Points Technology. They may lack experience with cloud-native applications — involving containers, Kubernetes or Docker orchestration, and microservices — as opposed to working in a monolithic or tightly coupled architecture, he said.

Understanding the Costs of Paying as You Go. Paying only for the services you use is not necessarily less expensive than an on-premises, capital expenditures model. A well-managed cloud environment like AWS offers significant cost and operational advantages, depending on how you use the cloud. For example, where an agency places workloads — on prem or in the cloud, including where in the cloud — can make a big difference in such a complex environment, D'Alessandro said. For example, costs can rise quickly because of poor operational rigor, resulting in paying for something like idle compute instances that should have been shut down. Hidden costs like higher storage from moving too much data around can happen even if in a private cloud because of poor programming.

Integration Problems. Agencies run many applications and ensuring seamless integration and interoperability across multiple clouds is a challenge. But without those capabilities, you get data silos, inefficiencies and difficulty in data sharing.

Ensuring Data Governance and Compliance. Agencies work with strict regulations and compliance requirements in terms of data storage, handling and security. Even in a public cloud, they share responsibility for security, with the hyperscaler providing security in the cloud and the customer providing security to the cloud. Agencies must implement a robust framework for monitoring to ensure compliance at all times.

The Solution: A Unified Approach Toward Continuity

Adopting a multi-cloud strategy while ensuring continuity of operations requires careful planning and management, focusing on achieving seamless integration and interoperability, and optimized workload placement and resource use. It's not easy, but with the right partnerships, agencies can implement a multi-cloud environment that improves performance while controlling costs.

At the user level, a multi-cloud environment should include an intuitive interface, support for accessibility standards, and ideally, a level of personalization that allows users to customize features. Security — including identity and access management, cryptographic key management and detection, response, and disaster recovery (DR) — is essential, of course. Cloud providers such as AWS include effective support.

A few other features of an efficient multi-cloud environment include:

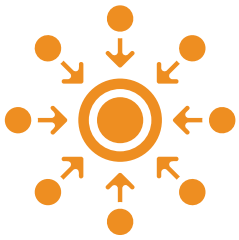
Optimized Workload Placement. Different cloud providers excel in different areas and may also offer cost advantages for specific types of workloads or geographic regions. "With a multi-cloud strategy, you can strategically place workloads where they are most cost-effective based on factors like data sovereignty, latency considerations, programming skills and even pricing structure," D'Alessandro said.

Improved Resource Utilization. An agency that matches specific workloads and applications with the most appropriate cloud service will use its resources more effectively while reducing overprovisioning. AWS CloudFormation allows you to provision the compute, storage and resources you need into a stack, execute operations and then release everything when you're finished, eliminating idle resources that can drive up costs.

Infrastructure as Code (IaC). A true multi-cloud environment will adopt IaC, which provides an automated means of provisioning and managing resources via code instead of hardware or manual processes. It enables the management of distributed systems, cloud-native applications and container environments, among other things, giving programmers a way to control public and on-prem workloads via a single interface that they are accustomed to using. AWS CloudFormation is just one example of how you could do it within the AWS cloud.

Best Practices in Managing Multi-Cloud

Here are four best practices that Four Points Technology says can help agencies effectively manage and optimize their multi-cloud environments.



1. Centralized Management and Governance

Establish a centralized management framework that provides visibility and control across all cloud resources and providers. A cloud management platform, or cloud services management tool, can monitor performance, track spending and enforce policies consistently throughout the environment.

Additionally, implement a unified governance model that addresses security, compliance and data management requirements, including those supporting standardized access control, encryption policy and audit trails.

2. Optimized Workload Placement and Resource Allocation

To make the most efficient use of cloud implementations, carefully analyze workload requirements. Before deciding which cloud provider or region to deploy a workload, consider factors such as performance and latency, data sovereignty, and cost.

Automated orchestration tools are effective at dynamically allocating resources based on workload demands, ensuring that you have efficient resource use and cost management. Regularly review workload placements and adjust them as necessary to make sure they continue to optimize performance and minimize cost.

3. Resilience, Backup and Disaster Recovery

Agencies need a comprehensive mission-resiliency strategy that includes redundancy and failover mechanisms across multiple cloud providers, ensuring high availability while minimizing the impact of outages.

Implement an automated backup and DR solution that replicates not only the data, but the applications across cloud providers and geographic regions.

"A disaster recovery plan is absolutely critical, but it's equally important to regularly test your plan, validating its responsiveness and effectiveness," D'Alessandro said. "Waiting until an actual event occurs is the worst time to see if a plan works."

4. Vendor Management and Relationship Building

Providers are partners, so agencies must establish strong relationships through regular communications and collaboration on service-level agreements (SLAs), performance metrics and support requirements. Be aware of a provider's plans for new service offerings that leverage innovation and can help optimize your strategy.

Also, agencies should conduct periodic vendor evaluations to assess performance, reliability and cost effectiveness, so they can consider adjusting the mix of services if mission requirements or conditions change.

Case Study: How a Multi-Cloud Approach Unleashes New Capabilities

A federal agency that works with a lot of environmental data was relying on a single cloud provider for data storage and analysis. The agency ran into constraints during peak data collection periods because of limited scalability and had few options because it was locked into one vendor.

Four Points Technology recommended that the agency adopt a multi-cloud strategy including AWS and a second CSP, taking advantage of strengths from each provider to increase flexibility, scalability and capability. The agency selected AWS primarily for its robust data storage and compute capabilities.

"With this approach, the agency is now able to create new accounts and provision resources as needed in both AWS and the other CSP," D'Alessandro said. "During peak data collection periods, they can scale resources horizontally as well as vertically, based on workload demands, ensuring consistent performance without overprovisioning."

The agency uses different tools from each provider. For example, it uses Amazon Simple Storage Service for storing large volumes of sensor data and the other CSP's AI and ML tools for advanced data analysis. For identity management, security and compliance, it uses AWS's Key Management Service alongside Active Directory (AD) and the AD sensor for recording login information. The agency also replicates critical data between their two CSP's regions with automated failover to support DR and mission continuity.

The agency maintains a level of independence by avoiding vendor lock-in. That approach not only supports the agency's mission, but also establishes a model for using cloud technologies effectively within government agencies.

HOW FOUR POINTS TECHNOLOGY AND AWS HELP

Four Points Technology, LLC has worked with government agencies for more than a decade, simplifying the process of budgeting, procuring and managing cloud platforms while helping to speed adoption initiatives. By focusing on contract management, strong program management and operational details, the company has helped agencies implement cost-effective, innovative and secure cloud solutions.

It partners with major cloud providers such as AWS and other CSPs, plus a wide array of solutions partners, and it has worked with agencies such as the General Services Administration (GSA), Department of Homeland Security and NASA.

AWS GovCloud is an established, trusted provider of secure, scalable and resilient cloud services to government. When working with AWS, Four Points Technology can create new accounts, transfer accounts and integrate existing accounts for consolidated billing. Agencies get the flexibility to affordably add cloud capabilities. For example, Four Points Technology's SEWP/GSA/CIO-CS AWS $1 Bundle gives users access to all AWS future resources over the life of the contract.

Conclusion

Implementing a multi-cloud strategy requires a careful process that accounts for many moving parts. Agencies working within a budget and with employees who may have limited cloud skills need partners and providers that can help them cost effectively get the most from cloud's capabilities.

Managing contracts, billings and SLAs can be as important to a successful implementation as the technical capabilities. A partner such as Four Points Technology can manage the organizational and operational details that can make the difference.

The advantages are undeniable. Agencies can gain flexibility and scalability in managing services from the data center to the edge, while optimizing resource usage, maximizing efficiencies and minimizing costs. A multi-cloud implementation also can improve security and data protection while providing the resilience and DR capabilities agencies need.

Because agencies must ensure continuity of operations, multi-cloud environments are increasingly the right path for them.

Four Points Technology, LLC is a CVE-verified Service-Disabled Veteran Owned Small Business (SDVOSB) delivering technology solutions to our Government customers around the world. We partner with top manufacturers and software companies to provide our customers with leading edge information technology solutions. As a Federally- focused prime contractor, Four Points Technology offers a strong contract portfolio that includes Government- wide contracts such as GSA Schedule 70 and SEWP V as well as multiple agency-specific IDIQs and BPAs. Our disciplined approach to the management of product delivery and ancillary services provides access to the latest technology in an environment that supports rapid implementation, clear productivity gains, and short ROIs. www.4points.com

Since 2006, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud. AWS has been continually expanding its services to support virtually any workload, and it now has more than 240 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, media, and application development, deployment, and management from 105 Availability Zones within 33 geographic regions, with announced plans for 21 more Availability Zones and seven more AWS Regions in Malaysia, Mexico, New Zealand, the Kingdom of Saudi Arabia, Taiwan, Thailand, and the AWS European Sovereign Cloud. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop