Government Technology Insider

Optimizing and Securing Multi-Cloud Environments for Federal Agencies

By: Jenna Sindle, Managing Editor

As federal agencies embrace Cloud Smart they are frequently moving to a hybrid multi-cloud environment. According to a recent MeriTalk survey 77 percent of public sector IT leaders see hybrid cloud as the right choice. As smart as that strategy is it can still create some complications and introduce complexities for agency IT teams. But after listening to both industry and agency experts discuss the benefits and challenges of a multi-cloud environment, we've identified three strategies for optimizing a multi-cloud environment for federal agencies.

"The federal government has done an exceptional job of adopting the cloud in the mission," shared Cameron Chehreh, CTO and VP at Dell. "The cloud isn't just a tech tool it's an economic and business model, moreover it's the foundation of digital transformation." Federal IT leaders came to realize, though, that not all data belonged in the public cloud – or even the cloud at all – and that the public cloud wasn't a panacea to budget issues and that a multi-cloud strategy is preferable. "With a multi-cloud environment anything is possible," explained ViON's Department of Defense lead, Justin Ciaccio. "But it does come with its own challenges, such as security and compliance, architecture and connectivity, and end-user experience." So what's an agency to do to optimize their multi-cloud environment?

We distilled three strategies that agencies can take to optimize and secure a multi-cloud environment.

Step 1: Collaborate with a Partner to Architect Success

In a multi-cloud environment having options about where to store data or put applications creates a lot of complexity. Working with a technology partner that has architected many multi-cloud environments sets an agency up for success. “As agencies embrace AI and rely on the agility and nimbleness of DevOps getting the workload to the right place from the outset and architecting correctly is the best way to optimize a multi-cloud environment,” shared Chehreh.

Step 2: Build a Multi-Cloud Strategy That Embraces Infrastructure as-a-Service

Building a multi-cloud strategy that embraces Infrastructure as-a-Service the easiest way to manage budgets. “Buying as-a-Service means that you can buy what you need when you need it, rather than trying to estimate what you need at the beginning of a project,” explained Ciaccio. “There are other benefits too, including being able to tap into cloud experts when you need guidance, and being able to track usage and other important metrics on a single pane dashboard.”

Step 3: Bake Security and Compliance in From the Ground Up

There are several ways in which agencies can layer security and compliance into their multi-cloud environment. It starts with buying FedRAMP-approved solutions, but it also comes back to building the right architecture. But the ability to bake in security doesn’t just apply at the macro level of acquisition and pen testing; operating in a multi-cloud environment introduces the opportunity for more granular security controls. “Well-crafted multi-cloud solutions enable role-based access control and governance that denies and enforces access by user roles across the environment,” conclude Chehreh.

Leveraging industry expertise and combining it with agency-specific knowledge about goals, workloads, and data applications, empowers agency IT leaders to achieve their goals and deliver on the mission more quickly, more cost-effectively, and more securely. By embracing the cloud and the as-a-Service model agencies optimize not only their teams’ capabilities but also their budgets. Which, in the end, opens up more opportunities for investment in cloud, security, and many other mission-critical technologies.