Shutterstock/FCW Staff

Building best-of-breed CLOUD ENVIRONMENTS

To make the most of the technology, agencies must become more strategic about developing, monitoring and evolving their multi-cloud ecosystems

THE GOVERNMENT'S APPROACH TO CLOUD TECHNOLOGY has changed dramatically in the years between the 2010 Federal Cloud Computing Strategy, known as Cloud First, and the 2019 Cloud Smart Strategy. The first policy pushed agencies to consider cloud technologies before others, while the second offers actionable advice on how to deploy the technology.

Today, 81% of federal agencies use more than one cloud platform, according to a MeriTalk survey. In addition to mixing on-premises systems with private and public clouds, agencies also use products and services from a variety of vendors to create multi-cloud environments. Such environments were born of necessity because there is no single, one-size-fits-all cloud solution. Instead, agencies can choose best-of-breed products in each area to meet their specific needs.

Because of its inherent flexibility and scalability, cloud technology played a key role in agencies' response to the pandemic and their ability to shift employees to remote work. Now government leaders recognize that multi-cloud environments are crucial for ensuring resiliency during a crisis.

The Cloud Smart Strategy explicitly references hybrid and multi-cloud environments as essential tools for improving mission outcomes and service delivery. "Cloud Smart operates on the principle that agencies should be equipped to evaluate their options based on their service and mission needs, technical requirements, and existing policy limitations," the strategy states.

Agencies across government are heeding the call. Last year, the CIA awarded its Commercial Cloud Enterprise contract to five cloud service providers that will compete for task orders from across the intelligence community. In addition, the Defense Department recently announced that it was canceling the $10 billion Joint Enterprise Defense Infrastructure contract, which would have been awarded to a single cloud provider, and replacing it with the Joint Warfighter Cloud Capability, a multi-vendor indefinite-delivery, indefinite-quantity contract.

Acting DOD CIO John Sherman cited a variety of reasons for the change in direction, including the evolution of DOD's cloud ecosystem and the need for DOD to leverage multiple cloud environments to execute its mission.

Tackling the challenges of multi-cloud

Despite the benefits of multi-cloud environments, they can present management challenges for many agencies. For instance, it can be difficult to migrate mission-critical legacy apps to the cloud, ensure the interoperability of products and services from multiple vendors, enforce security policies across systems, or even have visibility into all aspects of a multi-cloud ecosystem.

In a recent survey of FCW readers, 55% of respondents said their agencies have comprehensive strategies for multi-cloud

MULTI-CLOUD by the numbers

90%

Global enterprises that will rely on a mix of legacy platforms, private clouds and multiple public clouds by 2022

$6.6 billion

Amount federal agencies spent on cloud computing in fiscal 2020, up from $6.1 billion in fiscal 2019

55%

FCW survey respondents who said their agencies have comprehensive strategies for managing multi-cloud ecosystems

29%

FCW survey respondents who said their agencies use only one cloud provider

Sources: Bloomberg Government, FCW, IDC

management while 45% have no such strategies. In addition, security was the biggest challenge to managing a cloud ecosystem, with 74% of respondents citing it. Integrating different products and services came in second at 61%, and a lack of skilled employees rounded out the top three at 50% of respondents.

Efforts are under way to ease these pain points. For example, the Federal Risk and Authorization Management Program continues to look for ways to accelerate the process for cloud providers to obtain authorities to operate and make it easier for agencies to reuse ATOs granted by other agencies. In addition, the Cloud Smart Strategy seeks a larger role for FedRAMP in helping agencies make informed decisions about the cloud solutions they deploy.

The strategy acknowledges that cloud adoption is about more than the technology, stating: “Agencies are also encouraged to take a multidisciplinary approach to hiring and training their workforce, as well as provide community spaces where digital services experts, information security professionals, procurement specialists, and others with a mutual interest in effective, secure cloud adoption can collaborate on current challenges and opportunities in the cloud computing space.”

A foundation for innovation

President Joe Biden’s Executive Order on Improving the Nation’s Cybersecurity, released in May, includes an emphasis on bolstering cloud security. “The federal government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises or hybrid,” it states. The executive order encourages cloud service providers to share their unique insights into the risks facing federal information systems and calls on agencies to adopt zero trust security architectures and accelerate the move to secure cloud services.

The day after the executive order was issued, the General Services Administration released a request for information seeking industry feedback on the development of a governmentwide blanket purchase agreement for commercial software-as-a-service, platform-as-a-service and infrastructure-as-a-service solutions. According to GSA’s announcement, “The pandemic has pushed agencies to innovate and expand their digital and virtual environments. More specifically, GSA observes agencies moving toward more cloud-based solutions to make their [agencies] more agile and telework-friendly, reduce their reliance on on-premise/legacy systems, and scale their operational capacity.”

Cloud changes are also happening at the state and local level. In a recent MeriTalk survey, 83% of state and local IT managers said the pandemic amplified the importance of migrating to a hybrid cloud environment, with 66% saying the pandemic accelerated adoption by a year or more. However, only 29% said their agencies’ hybrid cloud strategies have kept pace with accelerated adoption.

As the options for cloud platforms and services expand, it’s crucial for agencies to take a more strategic approach to building and managing their multi-cloud environments. A successful strategy enables agencies to improve how they manage workloads, data and apps. It also gives them the necessary visibility to institute a risk-based approach to security that incorporates zero trust, automation and policy enforcement across cloud environments. With the right cloud ecosystem, agencies can achieve mission success in other key areas, including employee engagement, customer experience and IT modernization.

Cloud technology has become indispensable for government IT operations and a foundation for innovation. “To realize the full benefit of cloud technology, agencies must cultivate an organizational mindset of constant improvement and learning,” the Cloud Smart Strategy states. “Modernization is not a commitment that is sustained solely by interventions once every decade. Rather, modernization is a constant state of change and part of the day-to-day business of technology at every agency.” ■