The growing power of multi-cloud

Creating a comprehensive cloud infrastructure from best-of-breed products is essential for innovation and modernization

MULTI-CLOUD environments are the natural evolution of the government's move to the cloud. As technologies become more targeted and sophisticated, it is clear that a single product cannot meet all of an agency's needs. Multi-cloud represents a highly individualized, fluid approach to capitalizing on everything cloud has to offer.

Cloud technology is integral to IT modernization, it is a natural fit for a hybrid workforce, and it facilitates the development of innovative digital services that exceed customer expectations. In recent years, a marketplace built on software, platform and infrastructure as a service has been expanding into anything as a service, with offerings as varied and game-changing as artificial intelligence, blockchain and database as a service.

The inherent flexibility of such options means agencies have a wealth of solutions at their fingertips for meeting any challenge.

"Cloud is no longer considered a location but rather an operating model for future innovation," said Dave McCarthy, research vice president for cloud and edge infrastructure services at IDC, in the firm's Worldwide Cloud 2023 Predictions. "The agility provided by cloud methodologies enables organizations to quickly deliver at scale on rapidly changing requirements from internal and external stakeholders."

THE BENEFITS OF A MULTI-CLOUD APPROACH

In a recent pulse survey of FCW readers, 49% of respondents said their agencies rely on hybrid cloud environments that combine public and private clouds with on-premises systems, and 39% said their cloud environments were based on private clouds. Only 8% identified themselves as multi-cloud.

Experts make a clear distinction between hybrid and multi-cloud environments. The General Services Administration's Multi-Cloud and Hybrid Cloud Guide notes that a multi-cloud architecture reflects the deliberate integration of services from multiple cloud service providers. "A collection of cloud services that serve an enterprise but were created on an ad-hoc or patchwork basis isn't considered a true multi-cloud architecture," the document states.

By contrast, a hybrid architecture integrates public cloud, private cloud and on-premises infrastructure. According to GSA, "Though [hybrid is] often mentioned as a form of multi-cloud, multi-cloud doesn't use on-premises IT infrastructure."

In a blog post announcing the release of the guide, GSA notes that "the decision to adopt a multi-cloud or hybrid cloud solution significantly impacts cost-effectiveness,

Multi-cloud by the numbers

Sources: FCW, Gartner, General Services Administration

$1.8T	93%	84%	290
Projected enterprise IT spending on cloud technologies by 2025	FCW survey respondents who cited flexibility as a key advantage of multi-cloud	FCW respondents who said applying security policies consistently across clouds was a major challenge	Number of FedRAMP-authorized cloud products as of January 2023

manageability, performance, reliability, security and privacy, and the IT workforce. Agencies should be aware of the relative benefits and trade-offs of each."

When asked about the greatest benefits of a multi-cloud approach, a whopping 93% of FCW survey respondents cited flexibility, followed by support for a hybrid workforce of on-site and remote employees at 65%. Other advantages include the ability to keep pace with industry innovations (53%), cost-effectiveness (44%) and ease of creating digital services (37%).

Those benefits underscore cloud technology's central role in IT modernization. However, integrating multiple cloud products and services — not to mention letting go of legacy on-premises systems — is not without its challenges. FCW survey participants overwhelmingly said applying security policies consistently across all clouds was a major hurdle at their agencies, with 84% of respondents citing it as a concern.

THE IMPACT OF FEDRAMP

Forrester's Planning Guide 2023: Security and Risk predicts that U.S. enterprises will have migrated 58% of their application portfolios to the cloud in the coming year and adds: "Security teams are spending a notable amount on cloud security, but given the percentage of workloads migrating to the cloud, they need to spend far more."

Many experts point out that cloud-based security tools are inherently more secure than their predecessors. Guy Cavallo, CIO at the Office of Personnel Management, told FCW: "I believe cloud is the most secure environment we have today." Industry leaders have cybersecurity teams that most agencies can't match in terms of resources and size, he added.

At OPM, "cloud tools have helped us automate many aspects of cybersecurity and helped us use artificial intelligence and machine learning to improve our cybersecurity posture," Cavallo said. He also emphasized that agencies have access to the latest security tools through FedRAMP, which GSA oversees.

He is far from alone in recognizing the power and impact of that program. Congress recently passed the FedRAMP Authorization Act as part of the fiscal 2023 National Defense Authorization Act. The law codifies the program, reduces duplication of security assessments and other obstacles to cloud adoption, facilitates agencies' reuse of cloud technologies that have already received an authority to operate, and requires GSA to work toward automating FedRAMP processes.

In a recent report, the Government Accountability Office said the Office of Management and Budget could help agencies improve cybersecurity by holding them accountable for authorizing cloud services through FedRAMP.

THE NEED FOR CENTRALIZED VISIBILITY AND CONTROLS

Concerns about complying with security policies reflect broader management challenges associated with complex cloud environments. FCW survey respondents also cited difficulties related to managing costs effectively (59%), gaining visibility into all cloud resources and activities (49%), hiring and/or training IT professionals with the necessary skills (45%) and instituting data retention policies across all clouds (44%).

Agencies must have continuity and visibility across their cloud-based activities to take full advantage of the technology's security, cost-effectiveness and operational efficiency. Strategies include choosing interoperable cloud products and/or investing in cross-cloud management solutions.

"To manage multi-cloud or hybrid cloud architecture efficiently and effectively, agencies are encouraged to use centralized visibility and controls as the foundation for their cloud operations," GSA's Multi-Cloud and Hybrid Cloud Guide states. That approach "requires a shift away from processes that are specific to on-premises infrastructure or different clouds (i.e., distributed management) and toward processes shared across IT environments."

Similarly, one of IDC's Worldwide Cloud 2023 Predictions is that "by 2025, 75% of organizations will favor technology partners that can provide a consistent application deployment experience across cloud, edge and dedicated environments."

In addition to addressing cloud security, GAO's report also recommends that agencies incorporate best practices for service-level agreements in their cloud contracts, including how data and networks will be managed, and update their strategic plans to tackle the workforce issues related to cloud computing. Finally, the report states that OMB should require agencies to "establish a repeatable mechanism to track cloud savings and avoidances" — another area where a comprehensive view of cloud resources is essential.

Government agencies have taken a mix of approaches to cloud adoption, with many creating hybrid environments as they grapple with modernizing on-premises systems and others choosing a single private cloud. For some agencies, multi-cloud is the goal or their current reality.

Regardless of where they are on their journeys, agencies continue to benefit from advances in cloud technology. That's because the same spirit of innovation that gave rise to the cloud is giving rise to new solutions for securing and managing cloud environments. ■