

Choosing the right cloud tool for the job

A multi-cloud environment gives agencies a wide selection of options for achieving their mission goals



Jason Payne
Microsoft

A **POPULAR ADAGE** says that when you're holding a hammer, everything looks like a nail. However, when you have a complete toolset, you can pick the best tool for the job. Multi-cloud environments enable agencies to expand their technology options and choose the best cloud for their needs.

Successful multi-cloud adoption starts with a strategy that focuses on what is important to an agency's mission. Most strategies seek resiliency, better security and the ability to innovate. When agencies have a goal of capitalizing on multi-cloud and migrating applications or workloads seamlessly from cloud to cloud, they end up embracing modern tools and practices such as DevSecOps, infrastructure as code, interoperable container-based application architectures, and cloud-native tools that drive security and decrease the time needed for accreditation.

Furthermore, the government is somewhat unique compared to the commercial market in its approach to multi-award cloud contracts that have agency-specific requirements and goals. That approach drives contractors to collaborate on common

requirements while still differentiating themselves from other companies. Competition among vendors benefits agencies in terms of pricing and the pace of adopting commercial innovation.

MEETING EVER-EVOLVING SECURITY REQUIREMENTS

Adding multi-cloud environments into an agency's IT portfolio does come with challenges. In particular, it can create complexity for security teams that must protect the agency's identities, devices, data, applications and infrastructure.

“Agencies can improve governance by leveraging cloud platforms' built-in security tools and then deciding where they need to govern horizontally across multiple cloud platforms.”

Traditional cybersecurity tools weren't designed for multi-cloud environments, and it can be difficult to transition from existing tools to platform-specific and cloud-native ones, but doing so is essential for taking full advantage of cloud's market-leading security capabilities.

Agencies can improve governance by leveraging cloud platforms' built-in security tools and then deciding where they need to govern horizontally

across multiple cloud platforms. Some clouds provide state-of-the-art tools for achieving a single pane of glass for security. For example, Azure Arc, Microsoft Defender, the Microsoft Graph Security API and Sentinel were built to manage and monitor not only Microsoft's cloud, but also a customer's common infrastructure whether it's deployed on other cloud platforms or even on premises.

UNDERSTANDING COMMON CLOUD PRINCIPLES

At Microsoft, we're often asked whether developers, technologists and systems administrators need to be experts on all the clouds that agencies use. The reality is that commercial cloud platforms are too broad and complex for IT teams to master all of them. Microsoft Azure alone has hundreds of services that we provide to government agencies.

My advice is to focus on training employees to understand the common principles of cloud technology: compute, network and storage and how they are implemented across various platforms. Within that base of knowledge, team members can then develop specialized skills on individual cloud platforms based on agency and mission needs.

Source: Gremlin

We also hear from agencies about interrelated demands for compatibility, interoperability and preventing vendor lock-in. Agencies can achieve interoperability between cloud platforms, but then they might not be able to maximize the benefits of an individual platform.

There are times when an agency will want to fully utilize a cloud platform. For example, enabling a broader pool of developers and increasing development velocity through low-code technologies such as the Microsoft Power Platform provide agencies with agility, data access and ultimately a clear mission value.

The key to multi-cloud success lies in building a solid set of principles that form the foundation of agencies' cloud choices as they move toward the platforms of the future. ■

Jason Payne is CTO at Microsoft Federal.



The choice for classified missions.
A classified cloud that works well with others.

aka.ms/ClassifiedMissionCloud