Strategies to ensure a flexible & secure cloud future

By FedScoop Staff

Federal agencies are moving more of their IT operations to the cloud than ever before. While migrating applications and data to the cloud are getting easier, achieving a stable hybrid environment — that also works securely with your on-premises data centers — remains a pressing challenge for federal CIOs.

The need for federal agencies to get their hybrid-cloud roadmap in place has reached a tipping point over the past year as pressures mount to modernize the government's vast portfolio of aging legacy IT systems and make smarter use of available IT funding.

Agency IT leaders, however, face a deeper challenge: Deciding which applications to move to the cloud and which should be rebuilt or replaced to function securely in a hybrid cloud environment. And they must do so while planning for a rapidly changing cybersecurity landscape.

That's why rationalizing and rightsizing your applications deserves careful attention. It's also important to align with the right partners who can support your applications — regardless of whether they're in the cloud or on premises — which can mean the difference between successful IT modernization versus just lifting-and-shifting to the cloud.

Adapting to the new security paradigm

Citizens expect secure digital services delivered any time, at any place on any device. The same is true about the workforce. They need access to an increasingly complex hybrid IT environment in which connections and services are no longer fully managed by the agency.

Policies and tools developed for an IT environment managed solely behind a secure physical perimeter are no longer adequate. Data must be protected on any device and in transit over any type of connection within a virtual perimeter that spans both the agency data center and cloud providers in what could now be called an agency "digital virtual estate," according to Microsoft Federal CTO Susie Adams.

The evolution of these virtual estates requires CIOs and IT security teams to take a step back and reassess their plans to get the most out of their cloud migrations. It also requires adapting to a new security paradigm, says Adams, where:

- **Identity is the new firewall.** With hybrid environments and an increasing demand for cloud services, IT leaders need to focus on what entities must be kept out, what must be protected within, and how to manage that moving boundary. Because the movement of data to and from cloud weakens the perimeter security that organizations historically have relied upon, identity is now the new firewall — it's the foundation of your modern management and security platform. With a workplace that is increasingly mobile and cloud-centric, it's the user's identity that unlocks access to agency resources. Securing that identity is the critical first step to protect your data, and permissions must be granular and specific, while also ensuring compliance with data protection regulations.
- **Devices are the new perimeter.** Data is mobile in modern, collaborative work environments, and that means IT needs a way to secure data as it moves within a virtual agency environment. Most agencies still require employees to connect via VPN, which usually limits the ability to have granular control over the data. When agencies implement conditional policy-based access, you can look at the security state of the device the user is authenticating from, along with location data and credentials to determine what information should be accessible to that user.

- **A breach is assumed.** It's more important than ever to take a holistic end-to-end approach to security that focuses not just on protecting and responding, but also on detection capabilities. Incorporating tools that leverage hyperscale cloud capabilities, such as Microsoft Azure Government, that focus on threat detection using big data analytics and machine learning is critical. Azure's Intelligent Security Graph gives agencies the ability to see a consolidated picture of their security status.

Build in flexibility from the start

It's easy to underestimate the challenge CIOs face attempting to modernize their agency's IT. While moving to the cloud can sound straightforward, it involves a thorough understanding of the applications federal employees and citizens rely on and the expertise to reengineer them for a hybrid cloud environment without disrupting day-to-day operations.

That's one reason a growing number of agencies are taking a closer look at the flexibility and built-in security features of cloud, such as Microsoft Azure Government, which enables leaders to test out their theories, lower costs quickly and move that much closer to modernization in a matter of weeks to months.

Among agencies and departments already benefitting from Azure's flexible approach:

- **The U.S. Air Force**, along with the **Defense Logistics Agency**, leverage Microsoft secure cloud technology to provide the productivity and collaboration services that Service members need to fulfill their mission.
- **The State Department's** AirNow project places IoT sensors on embassies and consulates around the world to capture air quality monitoring data. That data is then analyzed using Power BI insights to foster diplomatic conversations about how the US can help other countries improve air quality and national health.
- **The U.S. Department of Veterans Affairs** uses Microsoft's Azure platform for its Access to Care web-based application which enables patients to more easily schedule VA hospital appointments and track likely wait times, creating a better patient experience.

Flexibility is a big plus for Azure customers. "We allow customers to port their data between devices, their data center, and the Azure Government cloud in a hybrid or multi-cloud infrastructure," said Karina Homme, Senior Director, Microsoft Azure Government. "From the security layer to layers up and down the stack, our ID management layer allows data to move from cloud to cloud. Portability is key."

It's also key for agencies to recognize that tomorrow's apps will be built in a fundamentally different way — requiring flexible tools and infrastructure, Homme said. It will be important to be able to spin up apps quickly on virtual machines or containers and blend multiple data types.

That flexibility allows developers to focus on development work and gives them the freedom to use any tool that they want to use.

Maximizing the value of the cloud

"CIOs can also benefit from Microsoft's own modernization journey to the cloud," Adams said.

"After all, like most agencies, we grew up in the on-premises world and had to transition to a hybrid cloud environment as well. We transitioned a significant portion of our internal IT systems to the cloud and regularly share with customers how we learned to manage our 'digital estate' so that they can hopefully benefit from our experiences," she said. "Our hope is that this knowledge will significantly increase the ability for agencies to serve their mission at high levels of security and at better price points."

Microsoft's own experience moving to the cloud, as well as working extensively with government agencies, offers several instructive lessons to CIOs and IT leaders for developing a successful roadmap to a multi-cloud and hybrid IT world, according to Adams.

Among the lessons Adams recommended agencies consider:

1. **Rationalize apps** – Agencies must rationalize their applications to ensure they are making the most efficient decisions. The inventory of apps in this rationalization is a six to nine-month process that will help agencies achieve their missions with security and cost-savings as top priority. The returns will be significant if they start now with those that must be kept on-premises and some that can be folded into the cloud.

2. **Set a solid cloud foundation** – As agencies inevitably transition to IaaS, SaaS and PaaS cloud platforms, it's critical for agencies to plan for a hybrid operating environment that creates a secure virtual digital estate. Fortunately, Azure provides a foundational layer that lets agencies create virtual environments that can work in their own data centers and in the cloud.

3. **Identify the right tools** – Agencies need to know they have the correct tools to go from on-prem to a multi-cloud environment. They need to know not only what provides a secure, core foundation for IT modernization, but also supports a comprehensive, integrated stack that can help agencies modernize faster.

4. **Establish a strong identity layer** – As data moves outside the agencies physical network and data center boundaries, identity becomes the key to unlock access for end users and system access to data regardless of where it lives. "The digital estate with the ID layer provides a stable hybrid-cloud solution so that CIOs can combat cyberthreats, save time and realize savings," said Adams. That layer needs to work fluidly with hybrid clouds, multiple partners and multiple devices, she stressed.

Microsoft's experience also suggests that agencies don't need to wait until they have the complete roadmap to the begin preparing for a hybrid cloud environment.

Rather, it's possible for CIOs and CISOs, with Azure Government, to adapt from existing roadmaps to rationalize their apps, set a solid foundation for the transition and get a better toolkit for moving to the cloud whether it's on the cloud or on-premises.

Find out more about how Microsoft Azure Government can help your agency lay the right foundation for a hybrid cloud future.

This article was produced by fedscoop for, and sponsored by, Microsoft Azure