Building a Comprehensive Cloud Strategy for Government

Nick Michaelides
Senior Vice President, U.S. Public Sector Organization at Cisco
The Federal Government is actively moving toward cloud computing using a variety of public, private, and multi-cloud environments, underpinned by infrastructure that comes from countless different providers. It's a complex environment, which makes it a significant challenge when the government cannot decelerate the process of providing critical services to its citizens. These are services that people depend on – everything from benefit distribution to national defense, law enforcement to maintaining national parks, scientific research to mail service, and many more.

Unfortunately, more agencies than not struggle with an aging, inflexible computing infrastructure and limited IT budgets to support much-needed modernization programs. In fact, according to the President’s 2019 budget proposal, government agencies will spend 80 percent of their budget on operation and maintenance – leaving minimal funding for new deployments and innovation.

Agencies are discovering that cloud computing is the solution to many of their modernization problems. Several government mandates, such as the Federal Cloud Computing Strategy or the Modernizing Government Technology (MGT) Act of 2017, state that cloud computing should be used if at all possible for new technology deployments.

Nick Michaelides has been developing and working with cloud computing technologies since their onset, and currently serves as vice president of Cisco’s U.S. Federal Government Organization. In a recent interview, Michaelides explained why he believes that government agencies should move to the cloud. “Cloud is one of the best ways to accelerate modernization, because the cloud provides significant speed, flexibility and cost savings,” he noted. “It also enables agencies to deploy cloud-ready applications more quickly, allowing IT managers to migrate many services over to the cloud while they also maintain and modernize critical systems with sensitive data that they may not be ready to move.”

Cloud computing also allows agencies to offload standard programs such as collaboration tools, enterprise resource planning, email and other apps to cloud providers. This frees local IT staff from the burdens of routine maintenance so they can focus on other technologies that remain in-house.

Agencies can spin-up new development projects quickly in the cloud, creating a virtual sandbox where developers can innovate without dealing with legacy systems and controls. Even more, they can do it more cost effectively, efficiently, securely, and in a reusable environment.
Complexities of Government Computing Mandate A Multi-Cloud Environment

Government agencies have vastly different missions, and each one collects and handles data differently than the others. Their data also requires different levels of security, with some of it publicly available and some highly classified. Because of this, no single cloud solution is going to be the right fit for most agencies, much less across the entire federal government.

“In my opinion, it’s imperative for government to embrace a multi-cloud environment – building off a secure network as the foundation,” Michaelides emphasized. “This is a real opportunity to transform the way agencies serve both their employees and citizens.”

Based on their diverse needs, most government multi-cloud environments will consist of both public and private clouds, provided by multiple vendors. Agency IT staff will no longer have everything they manage located inside their buildings. Instead, it will be a mixture of on-premises equipment and cloud deployments, each containing multiple security levels. However, managing their data within that type of environment is much more challenging than the typical on-premises approach used in the past.

Managing and interconnecting multi-clouds is where the complexity lies. This can require a significant amount of time and rack up hidden costs. In extreme cases, inefficient management of multi-cloud environments can even cancel out many of the inherent advantages gained by moving to the cloud.

The key to successfully tapping into the innate advantages of cloud computing without losing the benefits to multi-cloud administration problems is to have a way to bring everything together into a single management domain. So agencies must seek ways to create an experience that makes the management of multi-clouds seem like working with a single on-premise technology deployment.

“Agencies will benefit from flexible tools that interoperate with multiple cloud providers, secure workloads between clouds, and most importantly, monitor billing among providers,” Michaelides continued. “At the same time, they should be careful to avoid lock-in, and insist on ownership of their content. It’s important that they understand how to modernize and control the network to securely access, transport and then leverage that data.”
Cisco is working to provide a unified management interface and strategy that can address all cloud computing deployments across the federal government’s many diverse missions, objectives and security requirements. This is being accomplished without restricting either an agency’s choice of cloud infrastructure provider, or the type of cloud instances that the government can install.

To accomplish this, Cisco begins by ensuring the government’s ability to use any public or managed cloud provider. The Cisco network is platform agnostic, meaning agencies can choose the best provider based on their offering, pricing, or any other factor, and Cisco's network services are equipped to support it.

Next, agencies are given the power to create their own private clouds in order to protect their most sensitive data. “We have been doing this for government data centers for decades,” Michaelides said. “It’s merely extending our offerings into private clouds for agencies that need them.”

To maximize efficiency, all software as a service (SaaS) offerings are fully supported. For example, Cisco’s cloud-based offerings, like the native cloud access security broker Cloudlock, are either FedRAMP-certified or are going through that process. In addition, Cisco is working to bundle many of their cloud-based services into a single platform that, once FedRAMP-authorized, can become a plug-and-play solution to support all aspects of an agency’s cloud deployment.

And finally, Cisco’s portfolio includes products and services to support a multi-cloud environment. The federal government’s programs, missions and goals are too diverse to be supported by a single type of cloud or a single cloud-providing vendor. As a result, the government’s openness and ability to embrace multi-cloud computing will be essential in successfully modernizing. Cisco can help provide the intelligence and the glue to keep those environments tied together, simplify their management and keep them running at peak efficiency.
In Today’s Threat Landscape, Security is Job One

Agency leaders know that any cloud-based initiative within the federal government, as with most federal programs, must consider data security above almost every other factor. This makes cloud deployments, where data is no longer stored within the physical walls of an agency, or even within a network that it owns, problematic. To help simplify and strengthen security, there is now a need to embed security directly into cloud networks and services. And Cisco has done just that with their Application Centric Infrastructure (ACI) cloud network and services.

“We know that the federal government maintains highly sensitive civilian and national security data and information, and protecting that data is a top priority,” Michaelides said. “As more applications, data and identities move to the cloud, government administrators will need to come to grips with the subsequent loosening of control over their network perimeter. Hackers are taking advantage of the increased attack vectors, and government is looking to technology experts to help mitigate those threats.”

Cisco takes a three-pronged approach to maintaining government security in cloud deployments. The first is providing security services designed specifically for the cloud, which they are doing through innovative programs like the aforementioned FedRAMP-authorized Cloudlock solution.

Cisco Cloudlock is a cloud-native Cloud Access Security Broker (CASB) that can secure federal identities, data and applications for cloud deployments of all types. It combats account compromises and data breaches as well as any cloud-based ecosystem risks. Plus, it operates from a simple, open and automated application programming interface (API) that can be made available from anywhere.

The second prong is providing security for cloud-based networks. Cisco is accomplishing this by reinforcing some of the same security and networking devices many agencies use today, such as next-generation firewalls or Cisco virtual routers, to extend security policies into the cloud. This way, federal IT managers can use the same toolsets and interfaces that have reliably protected physical networks to also defend an agency’s data throughout their cloud journey.

Last but not least, the third prong in Cisco’s cloud security strategy is enabling cloud applications to embed security principals into them as they are created. That also includes adding security forensics and deeper visibility to cloud microservices and components.

Michaelides also added that “security and global certification has been a priority for Cisco for decades, and we provide more hardware-certified products than many other vendors out there. Before a government agency buys a piece of hardware from Cisco, we have already done the work to ensure that it has all the certifications and protections needed for it to be placed within that government network. Now, as agencies move to cloud, we are doing the exact same thing with all of our SaaS offerings.”
The Need to Manage Government Multi-Cloud Environments with Maximum Efficiency

One of the best ways to tame multi-cloud complexity is to implement a network with all the tools needed to support and manage cloud environments, including multi-cloud deployments supported by various infrastructure providers. A perfect example of this capability is the Cisco Application Centric Infrastructure platform, which can help government agencies securely implement intent-based networking.

“Cisco’s network begins in the hybrid cloud with Application Centric Infrastructure (ACI),” Michaelides explained. “The heart of intent-based networking is that it contains the intelligence needed to secure and optimize the entire infrastructure. It comprises artificial intelligence, machine learning, and automation so that our federal customers can continue to do the things they must, and accomplish those tasks as simply as they can.”

The network is the lynchpin of any successful hybrid computing or multi-cloud environment. Each time an agency needs to use their hybrid environment, such as to move data from an on-premise server to an AWS or Azure cloud, it has to go through the network. If that network lacks the intelligence to manage any production flows, a multi-cloud environment can become overly complex and difficult to manage. In addition, features like artificial intelligence are built into the Cisco ACI, so when a cyberthreat or other problem is identified, the network not only stops and remedies the potential threat, it also learns how to prevent a similar event from happening in the future.

Michaelides closed by sharing that Cisco is not providing cloud infrastructure as a service. “Instead, what we are doing is taking the software we develop and making it FedRAMP-Authorized. Then the federal government can use it to simplify and support their cloud programs in all forms. Regardless of the agency, whenever they are ready to migrate, we will be there as a trusted partner – helping them to transform the way they serve their citizens.”

To learn how Cisco can help your agency implement a multi-cloud deployment with an application-centric network, visit:
cisco.com/go/federal