

REMOVE THE MULTI-CLOUD BARRIERS TO YOUR AGENCY'S DIGITAL TRANSFORMATION

How federal agencies can operate across multiple clouds more efficiently by leveraging the power of an enterprise-wide application delivery controller.

96

cloud service platforms have been certified to do business with the government

The federal government's transition to the cloud, which began with the Obama administration's "Cloud First" policy in 2011, is poised to reach new levels of growth this year. Federal agencies of all sizes have embraced cloud computing to provide IT services and reduce the need for large-scale, traditional IT infrastructure investments.

As of last count, 96 cloud service platforms have been certified to do business with the government and another 81 are working toward achieving that certification, according to the government's Federal Risk and Authorization Management Program (*FedRAMP*).

Many view the accelerating pace of cloud adoption in the government as a positive sign that IT modernization efforts and digital transformation are gaining real traction. But as data and applications operate across a growing array of cloud services, agency IT officials find themselves facing a new set of challenges, that if left unaddressed, could lead to the same kinds of inefficiencies they were hoping to overcome by moving to the cloud in the first place.

One of the fundamental pitfalls in moving to the cloud that government IT managers and senior decision makers need to avoid is the relative inability for users to move smoothly and securely from one cloud-based solution to another.

The prevalence of multiple cloud services from different vendors throughout an agency can be a nightmare for users. From the user perspective, it's hard to navigate and aggregate all of the different services they may need to access. For example, users may need to access Workday, Salesforce, ServiceNow, Office 365, Google Docs or Adobe, to name but a few, to get their jobs done. That's not to mention the data they need could be warehoused at a variety of additional cloud locations.

Agency CIOs and network administrators are quickly realizing the need to take greater control over how their applications are delivered and interoperate across these cloud service platforms.

They're not alone: According to an IDC *survey* released in 2017, 82 percent of organizations globally said their ability to migrate apps to the cloud is hindered by the increased complexity of their networks infrastructure. And 79 percent of them said they plan to address application disruption via a unified application delivery strategy.

82%

of organizations globally said their ability to migrate apps to the cloud is hindered by the increased complexity of their networks infrastructure

LEVERAGING AN APPLICATION DELIVERY CONTROLLER

One way to overcome those challenges and actually accelerate cloud adoption is through the use of a centrally managed application delivery platform. An ADC can quickly and easily

deploy applications, and the policies that need to go with them, wherever they need to reside – whether it's in a physical data center, in the cloud or in a containerized environment.

That in turn can create a more secure and productive virtual work environment for employees, regardless of whether they're accessing data and applications internally or remotely.

A centrally-managed application delivery platform also ensures greater security assurance and compliance across an agency's network, as well as to solutions operating in the cloud. That can help agencies navigate the challenges associated with cloud-based productivity solutions, such as Office 365.

IT managers are likely familiar with **NetScaler** – the application delivery controller from Citrix Systems Inc. that handles 75 percent of all internet traffic. Many of the largest private enterprises and government agency websites are optimized and controlled by NetScaler.

Citrix's experience with NetScaler puts it in a unique position to help agencies on their digital and cloud transformation journey.

"We can help by giving our customers a secure digital cloud-based workspace that will allow the users one point of access to log on in a secure manner," said Jose Padin, Citrix's public sector chief technology officer.

"Inside that digital workspace, we can aggregate multiple different cloud solutions and still connect you to the traditional on-premises apps that you may have. There's still going to be big and important Windows applications and Linux applications that we can connect into one workspace, relieving users from worrying about which cloud they have to access to get their job done," he said.

Those **provisioning tools** can also allow an agency's IT department to set up an entire cloud implementation of virtual machines on Microsoft's Azure Government Cloud. Some customers may be able to by point and click from a central console and deploy to the cloud, according to Padin.

“

We can help by giving our customers a secure digital cloud-based workspace that will allow the users one point of access to log on in a secure manner.



STANDARDS PLUS SECURITY

There have been many examples where agencies have deployed specific cloud solutions only to discover that the vendor at the other end could not support key public-sector security standards, such as smart card authentication, encryption or data isolation.

"We have agencies that want to use an office solution, but they want to limit access from people from certain locations, [such as] accessing the cloud from outside the network. So, we give them one secure point to do that," Padin said. "Because we have the network to do that, we can increase the encryption level from end to end. We can function as an IDP to give them one place to log on, and on the back end authenticate the user to the cloud solution they want to use. Not everyone can do that."

Citrix also provides virtualized applications for the government user. This is a unique capability that allows visibility on what's going happening on the client side, the networking side, the back end and the cloud.

All that visibility also gives access to a lot of analytics that can help drive intelligent, autonomous decisions, Padin said. For example, if a user is coming in from an untrusted network, the agency may want to limit their access to only certain applications.

"Being able to sit in front and optimize and secure government websites and provide the analytics to detect and respond to threats is a big part of the NetScaler story," he said.

THE BENEFITS OF END-TO-END VISIBILITY

The key to Citrix's analytics capabilities is the fact that NetScaler is deployed in the network and is controlling the website at the application layer.

"We're getting access to a lot of information that other traditional networking equipment is not going to see," said Padin. "We are at a higher level of the OSI model that lets us see what's actually going on at the application-specific layer, and so we can do a lot of things that are different."

For example, because most attacks often use public-facing websites, Citrix can gather data on what a safe and secure transaction looks like — and from that agencies can automate responses based on the deviation.

Citrix's analytics platform can also automate configurations and ensure they stay in compliance with current government security standards. This is a big benefit for agencies, according to Padin. "As agencies go through implementation processes and go through different ATOs, it's a big effort and configurations keep changing."

MAKING DIGITAL WORKSPACES MORE SECURE

Agencies have been chasing the "work from any device and any location" paradigm for years. But Citrix takes this to a new level with the secure digital workspace — an end-to-end capability that gives users IT managers one central location to manage everything.

"They're struggling with a lot of challenges to lock down the devices and do a lot of configuration that doesn't focus on helping users to do what they need to do, which is actually at the application layer," Padin said.

Citrix Workspace features XenApp and XenDesktop — two leading solutions for application and desktop delivery, with more than 100 million users worldwide. Citrix Workspace enables secure, remote access to Windows applications and desktops as well as Linux, web and SaaS applications from any device, over any network.

"We can take a device, like an iPad, that's never been in the network and we can show them how they could get access to all agency applications through one login," Padin said. "We can show customers how easy it is to move to the cloud right from our console."

[Find out more](#) about how a software-based ADC can help your agency run your applications securely on premises and in the cloud, provide end-to-end control and ultimately improve employee and mission productivity.

“

We are at a higher level of the OSI model that lets us see what's actually going on at the application-specific layer, and so we can do a lot of things that are different.

“

We can show customers how easy it is to move to the cloud right from our console.