THE NEXT ERA OF THE CLOUD

Following the "Cloud First" mandate, government agencies now consider cloud solutions an integral aspect of their operations.

BY ALL ACCOUNTS, the "Cloud First" era is coming to a close. Agencies are preparing to make cloud solutions an integral part of their operations going forward. The federal government's "Cloud First" policy, issued in Dec. 2010, went a long way toward helping agencies understand the potential benefits of cloud. Now the challenge is to build on that work and develop a more strategic approach that realizes the cloud's full potential.

The impetus for doing so is clear. Across the public sector, agencies are under pressure to modernize their IT infrastructure as a way to reduce costs, improve security, and deliver a higher caliber of IT services—and cloud computing is expected to be a vital element of these modernization efforts. According to a recent study by Forrester Research, cloud is set to become "the dominant technology model" in the private sector by 2020, with estimated revenues of $236 billion.

Government agencies might not adopt cloud at quite the same rate, but the trend is the same. Across the board, agencies are expected to expand their existing cloud solutions and make cloud the de facto platform for new applications. In fiscal 2016, 8.5 percent of all IT spending in the federal government involved the cloud, according to a report by industry researcher IDC.

Squeezing Savings From the Cloud

For many agencies, the potential for cost-savings continues to be the major driver for cloud adoption. The Department of Agriculture has been particularly efficient in extracting savings from the cloud, according to IDC, which points to a 30 percent savings in 2011 when the U.S. Forest Service migrated to a new cloud-based system.

How did the agency achieve such whopping results? Part of its technique is a new cloud-based management platform equipped with transparency—and a dashboard view into all network and telecommunications services and assets. The agency is now able to determine how its resources are being used in more than 6,000 locations through an automated process that helps to eliminate human error and cuts staff time spent on menial tasks, such as invoice processing.

"Soon all 29 agencies within the USDA migrated to this platform—and the real savings in employee time and money—continued to scale at that 30 percent rate, representing millions of taxpayer dollars annually," IDC reports.

In a similar vein, success of the Defense Department's milCloud project, an on-premises cloud solution managed by the Defense Information Systems Agency (DISA), has already prompted DOD to begin planning for milCloud 2.0 as a next generation cost-saver.

The 2.0 platform will offer both on-premises and off-premises capabilities to generate significant savings to the Pentagon, says DISA cloud portfolio chief John Hale.

Like its civilian counterparts in the Agriculture Department, milCloud 2.0's appeal will be based on its ability to lower costs, a significant factor in an era of sequestration, says Hale, speaking at an AFCEA meeting last summer. "By leveraging cloud capability—both commercial on-premises and off-premises—we can bring significant savings to the department," he says.

Even so, the platform has limitations. "There's always going to be the need for traditional hosting in a DOD data center," says Hale, who added that certain workloads, such as nuclear command and control, "just do not fit well in a virtualized or cloud model."

The bullish outlook for cloud suggests a similar expansion of cloud security activities. In the federal government, the focus is on building support for the Federal Risk and Authorization Management Program (FedRAMP). As part of that, the FedRAMP office began clearing cloud vendors to host high-impact systems, which expands the potential market for commercial cloud services considerably.

The program office also upgraded its marketplace dashboard to make it easier for agencies to connect with cloud service providers and third-party assessment organizations.

Prepping for Shared Cloud Services

The General Services Administration's new shared services framework—the "Federal Integrated Business Framework"—takes an innovative approach to shared services that could significantly expand the uses of cloud across the federal government.

The framework, announced in October 2016, is intended to document the functional business capabilities expected in each line of business across government and how those areas intersect, which sets the stage for buying SaaS solutions that could lower the cost of delivering administrative services.

In January, GSA's Unified Shared Services Management

Shutterstock.com

Office, which administers the federal shared service ecosystem, released a request for information asking for descriptions of any new or existing SaaS offerings applicable to key shared service areas, including financial management, human resources, acquisitions and IT.

The cloud is also is expected to get a push from continued efforts to consolidate and optimize data center operations. OMB's latest guidelines on data center optimization, released Aug. 1, called for increased use of both shared services and the cloud. The stage is set for a new era of cloud-based operations.

THE NEW ERA OF THE CLOUD DEMANDS A NEW TOOLKIT

The cloud is maturing as a platform—and prevailing cloud strategies are maturing as well. Agencies are taking a more thoughtful, considered approach. No longer a novelty or an experiment, cloud-based platforms are becoming an integral part of government agency strategy, whether public cloud, private cloud, or more often a hybrid model. This new face of the cloud requires a new toolkit to properly manage the increasing volumes of data and apps migrating to the cloud.

SOFTWARE-DEFINED EVERYTHING: The new era of the cloud is driven by software-based technologies. Software-defined computing, networking and storage are critical for properly and comprehensively centralizing and migrating existing services to the cloud. This software-defined infrastructure helps ensure the cloud's promise of performance, agility and security.

APPLICATION MANAGEMENT: It's not just data that is being migrated to the cloud, but also an agency's portfolio of applications. So agencies need a way to monitor and manage those applications. Some applications may reside in the public cloud, others in a private cloud, but being able to manage them all through a single dashboard is essential.

REPORTING TOOLS: Moving to cloud technology can greatly reduce the burden of IT maintenance and operations. Nevertheless, there still must be cloud-based reporting tools and workflows to ensure smooth operations and help guarantee that agencies are making the right mission-critical decisions.

DATA MANAGEMENT: The new face of the cloud requires a new class of tools for data management. Tools for archiving, classifying and analyzing data are now standard when considering the cloud as a massive source of both structured and unstructured data.

CLOUD SERVICES: Selecting the right cloud services provider with the right portfolio of services can make or break a cloud migration effort. A true enterprise-grade provider can help agencies ensure that they will accelerate and streamline their migration to the cloud, while taking better steps to ensure success. A cloud service provider must be able to scale to meet variable needs for storage, security, and data and application management.

SECURITY AND COMPLIANCE: Moving application and data workloads to the cloud helps reduce cost and increase flexibility and scalability, but security and compliance concerns must be addressed. Security remains a constant concern for the cloud, and all government agencies are subject to varying levels of compliance. Toolsets to ensure security, encryption and compliance must be part of the picture.