MOVING TO THE CLOUD: 5 ESSENTIALS FOR ANY AGENCY

For feds, hybrid IT and managed services can help achieve security and mission

INTRODUCTION

When the federal government chose to implementa "Cloud First" policy in 2010, there were three main drivers: cost savings, increased computing power and improved flexibility. At its core, the program's goal was to help agencies optimize their performance through the use of top-quality tech.

When the federal government chose to implement a "Cloud First" policy in 2010, there were three main drivers: cost savings, increased computing power and improved flexibility. At its core, the program's goal was to help agencies optimize their performance through the use of top-quality tech.

Cloud—the on-demand acquisition of IT services—has been recognized as the best way for agencies to achieve this, because of its cost-savings, agility and opportunities for innovation. Unlike traditional IT models, in which agencies would purchase and own all hardware needed for peak loads or risk outages in times of high usage, the scalability of the cloud allows for agencies to dial up or down computing power as necessary. This allows for agencies to harness unprecedented computing power while simultaneously saving money—something that is especially critical given today's federal budget constraints.

But some agencies are experiencing growing pains as- sociated with cloud migration. Government owned data tends to be highly sensitive—including everything from personally identifiable information to defense tactics— making security the foremost concern. Agencies worry about security, workload migration and integration, compliance and information governance in a cloud environment. They struggle to access the powers of the cloud while still maintaining enough control over their data to ensure complete data security.

When it comes to the cloud, the federal government has unique and rigorous requirements. They need to know their infrastructure is high performing, compli- ant and secure. Keeping this in mind, we've compiled an essential list of five key ways for feds to get the most out of their cloud environments.

1. Explore your hybrid options.

Increasingly, agencies are choosing to opt for a hybrid model—one that links together multiple cloud infrastructures using proprietary technology that enables portability. Given the security requirements of government, choosing to build out a hybrid infrastructure often makes the most sense for several key reasons.

First, with hybrid cloud, agencies can own their assets, but still have the infrastructure to interact with workloads that live on the public cloud where computing resources are shared. Because the public and private infrastructures are linked, moving workloads from one environment to the other is easy and quick. Sensitive data can be stored privately and ported out to the cloud for use in a complicated analytics program before being brought back to the private environment for storage.

In addition to the security benefits, hybrid opens up government to increased flexibility, elasticity and cost savings. Agencies can manage their workloads while still retaining the ability to spin up applications in the cloud in times of high activity. This allows agencies to meet peak demand without having to spend an inordinate amount on hardware up front that will, most times of year, remain underutilized.

Essentially, going hybrid allows agencies to access the benefits of computing in a cloud environment while improving their security posture by allowing for improved data governance.

Going hybrid allows agencies to access the benefits of computing in a cloud environment while improving their security posture by allowing for improved data governance.

2. Develop a comprehensive and integrated approach to security and compliance.

Physical and logical security are critically important for agencies seeking to use the cloud. Agencies need to be confident that their data is protected from cyber attacks by rigorous technical controls, such as end-to- end encryption, restricted user access and real-time security monitoring. They also need assurance that the building in which the data is stored has environmental controls in place to make it physically difficult to penetrate or damage.

Given the dire consequences of a data breach, the Federal Risk and Authorization Management Program (FedRAMP) was developed to help develop trusted relationships between cloud service providers and federal agencies. Any cloud provider seeking to work with government must first achieve FedRAMP compliance, which requires proving various security measures are in place. The goal is to provide government with insurance that any provider they're using is providing the required levels of security necessary for government.

At QTS' FedRAMP compliant data centers for the federal government, extra security procedures have been put in place to enable data protection. In addition to rigorous logical security controls, these measures include concentric rings of security, K-12 rated fences around the facility, a 500-foot setback to all buildings, armed security guards and/or the use of biometric information systems.

3. Understand the value of data center consolidation.

There's no getting around it: Data centers are massive consumers of power. But that doesn't mean they have to be energy inefficient. Data center consolidation refers to the implementation of strategies that allow for more efficient usage of IT infrastructure. This can mean literally reducing the number of data centers being operated, or simply introducing new technologies that make an existing data center run more efficiently.

Under traditional IT models—in which each agency stands up their own infrastructure—agencies are forced to operate under the assumption that many of the servers they deploy are, most of the time, underutilized. This is a tremendously inefficient use of power, because the servers are powered but not used optimally.

By contrast, agencies operating in a cloud environment can drastically reduce their energy usage by improving the energy efficiency of their infrastructure. With the cloud, multiple agencies or divisions can utilize the same physical infrastructure and, because the cloud is virtualized, each agency's workloads are completely separated from other organizations'. This enables agencies to share resources, leading to enormous improvements in energy efficiency and a drastic reduction of energy usage.

4. Consider the benefits of managed services.

Despite a desire to migrate to the cloud, many agencies worry that they don't have the in-house expertise and resources to transition to a cloud environment. It's important for agencies to know that their clouds are supported by professionals, trained in the specifics of cloud and dedicated to ensuring smooth operations.

Managed services provide agencies with additional technical support, where and when needed. Choosing a cloud provider that offers a large array of managed services lets agencies pick and choose which operations they want to manage themselves, and which they'd like to outsource. They can use managed services from the beginning—during project scoping, build-out and migration—or they can bring managed services in later for help with day-to-day operations.

By pairing a hybrid environment with managed services, agencies can customize their cloud environments. They can pick or choose to operate as many or as few applications in the cloud as they need, and have the ability to bring in technical support as needed. These capabilities are especially important for government, where reducing risks and gaining efficiencies are critical to successful long-term operations.

In order for agencies to get the most out of their clouds, they need to train their personnel on how to properly work in a cloud environment.

5. Remember that smooth operations are as much about the people as the specs.

When it comes to the cloud, a common pitfall is reducing conversation to just talk of technical controls. In reality, the people behind the systems are equally important to operation success.

In order for agencies to get the most out of their clouds, they need to train their personnel on how to properly work in a cloud environment. Employees trained in the specifics of cloud are more likely to take advantage of cloud's improved capabilities and to develop innovative applications suited to a cloud environment. They're also less likely to accidentally compromise data through improper use of procedure. To make sure everyone is on the same page, it's often a good idea for agencies to ask their cloud provider if there is any onboarding support or training that it can provide.

A secure, compliant, high-performance environment is one that is powered by people. As agencies go about developing and building out their cloud operations, keeping this piece in mind will be critical to success.

ABOUT QTS | 877.QTS.DATA | QTSDATACENTERS.COM

QTS Realty Trust, Inc. (NYSE: QTS) is a leading provider of secure, compliant data center, hybrid cloud and managed services. QTS features the nation's only fully integrated technology services platform providing flexible, scalable solutions for the federal government, financial services, healthcare and high tech industries. QTS owns, operates or manages more than 5 million square feet of data center space and supports more than 1,100 customers in North America, Europe and Asia Pacific. In addition, QTS' Critical Facilities Management (CFM) provides increased efficiency and greater performance for third-party data center owners and operators. For more information, please visit www.qtsdatacenters.com, call toll-free 877.QTS.DATA or follow us on Twitter @DataCenters_QTS.