The Challenge of Migrating Government Applications to the Cloud

vmware® | aws

Today's world is now a digital-first world. The private services we consume, whether it's finding a new book to read on our Kindle or streaming the latest movie on Netflix is normally underpinned by technology. It is because of this ease of service and consumers settling into a routine of using them, that we now expect a similar service from our public sector and government agencies. Government leaders are turning to IT modernisation to keep citizens engaged, improve employee productivity, drive value and cost efficiencies and meet citizen expectations for modern, efficient, personalised and cost-effective services. If they haven't already started having these conversations, they'll find themselves playing catch up.

But government agencies still need to resolve many challenges: reducing data siloes, improving agency efficiency, and boosting IT performance to name just a few. Hybrid cloud has played an important role in resolving these challenges by providing the speed, agility, scale and accelerated innovation needed for IT modernization. However, when government agencies consider adopting a hybrid cloud path, they can face the risk of unexpected costs, risks and delays incurred by their IT modernisation project.

Here, we explore the challenges government agencies face when it comes to migrating applications to the cloud, how they can be overcome, and the benefits digital transformation can offer the public sector to meet citizen demands for modern and effective public services.

Why migrate to the cloud?

To talk about why cloud, we must first talk about innovation. As citizens see technological innovation in their personal and work lives, they expect to see the same level of innovation from the government agencies that serve them. There is a greater recognition and appreciation of how technology can help transform local, regional and national governments and those operating within it to deliver better, more personalised experiences and serve citizens faster and more effectively.

Migrating to the cloud will give government agencies the ability to facilitate greater consistency for public sector staff working across centralised and field-based locations. , This can be achieved with equal accessibility remotely or on-premises, with a consistent, reliable and highly-available hybrid cloud environment. What's more, the flexibility of cloud infrastructure gives IT teams within governments more power and license to innovate with the ability to develop, deploy, test and evaluate new tools to deliver highly engaging digital experiences to citizens, akin to those they will be used to from the private sector.

Cloud migration requirements in the public sector

As government agencies hold a wealth of sensitive data – personal identifiers, financial data, demographic data – the security of data storage options is a pertinent concern. The cloud provides essential security through content filtering and firewall parameters, which keep staff and citizens from falling victim to ransomware or other cybersecurity attacks.

Swathes of sensitive data also presents government institutions with scalability challenges. Digital transformation inevitably creates more demand on central IT to deploy and manage new digital services. Hybrid cloud provides an infrastructure provisioning model which allows government offices to scale IT to where they need it, without the significant upfront costs of a physical IT upgrade or investments in new data centers.

Cloud infrastructure also gives government agencies greater interoperability, through a consistent set of tools, workflows, configurations, and policies to operate infrastructure and applications across a multitude of devices. As a result, staff can benefit from productivity boosters such as specialised applications which run on BYO devices and can be easily accessed through a unified application catalogue with conditional access policies to maintain compliance.

The agile nature of cloud infrastructure enables government organisations to facilitate the delivery of new mission capabilities, as well as increasing the speed of mission cycles. What's more, cloud migration can open up new service delivery models for government, creating new digital experiences for both employees and citizens that are faster and more innovative than old models. This in turn reduces capital and operating expenditures by reducing the data center footprint, hardware, licensing, and operating costs, all while improving organisational performance and agility.

Finally, with the future of work now squarely rooted in enabling distributed workforces, government agencies must take the necessary steps to facilitate out-of-office IT users while maintaining strict levels of data privacy and security. By migrating to the cloud, governments can tackle both these issues simultaneously, through intelligent device management to keep employees productive and engaged wherever they are working, along with context-aware, zero trust access security paradigms. Crucially, the cloud allows organisations to be ready for any challenges or disruptions by leveraging an infrastructure that can scale to support all apps and data, providing flexibility for remote workers with desktop and application virtualization solutions.

What is holding government back?

But before reaping the benefits of public cloud, government agencies need to successfully move there. This is easier said than done. The first step – deciding whether to move to the cloud at all - is often the hardest. If and when the decision is made to migrate, complexity abounds as agencies struggle to adapt and/or refactor applications to run in their selected cloud environment.

Even after migrating to the cloud, when customers decide to modernise existing applications, they face many challenges that increase the cost, risk, and time of their modernisation project. When government agencies are considering migrating and modernising applications, they must first understand the challenges that come with migration in order to choose the right solution to fit their specific requirements.

1. Adapting people and process:

People and processes must change and adapt to develop new skillsets and tools for public cloud environments. Acquiring cloud skills disrupts current operational effectiveness due to the increased burden of hiring, training and retraining the appropriate talent. In a sector traditionally slower to digitally transform, employees can feel threatened by change, creating resistance which can limit the effectiveness of cloud adoption.

2. Re-architecting applications to run in public clouds:

Many existing applications running in on-premises data centers are not designed to run on public cloud infrastructure. Applications may need to be rearchitected, machine formats converted, and everything must be thoroughly revalidated. Networks need to be integrated and reconfigured, and storage must be migrated and conformed to capabilities available in the public cloud.

3. Resiliency of mission-critical applications:

Mission-critical applications must meet the same or better performance and availability requirements after migration as before. Applications that have relied on infrastructure to provide the desired level of resiliency need to be re-implemented to in order for it to be built-in. All mission-critical workloads need to be thoroughly re-tested in the public cloud environment to ensure that desired availability targets are met.

4. Cost, time and risk:

Migrating applications to the cloud is complex, and the rework required to make the leap can be costly and time-consuming. The effort required to migrate applications to cloud is often underestimated, resulting in projects that run over time and budget, or underdeliver in achieving the goals. Cloud-migration projects can drain resources and budgets from other critical IT activities, increasing the risk to support of ongoing business objectives.

5. Security and governance:

Government organisations face a need to give up a certain degree of control over their infrastructure in public cloud. Security policies and practices must be updated to conform with this new model. The differences between on-premises and public cloud infrastructure limits the reuse of established security and governance procedures and tools. Public cloud infrastructure has different consumption patterns. New governance models need to be established to control how cloud resources are acquired.

Addressing these challenges with VMware Cloud on AWS

A true hybrid cloud should deliver the ability to work consistently across on-premises and cloud environments, enabling public servants to deliver innovative applications and services, without compromising on cost efficiency or security.

VMware Cloud on AWS provides governments with an on-demand, scalable hybrid cloud service that enables them to seamlessly extend, migrate, and protect their infrastructure in the cloud. And once in the cloud, they can start their application modernisation journey with minimal disruption, with the same architecture and operational experience on-premises and in the cloud.

Crucially, government IT also benefits from hardened security and production-grade capabilities required to the run highly sensitive workloads common in the sector. This service helps governments to accelerate digital transformation and deliver exceptional experiences to public servants and citizens alike in a safe, secure and sustainable way.

A digitally transformed future

Fortunately for the public sector, these challenges are not insurmountable. Agencies within the sector are more than capable to adapt and commit to cloud migration, if they choose to make the leap.

One UK-based government organisation, for example, was facing with the challenge of its existing datacentre facility closing down. To continue managing its in-house disaster recovery (DR) functions, the team needed a solution that would eliminate the prospect of having to rack, stack and configure its hardware at another location. In addition, the IT team wanted to deploy a system that would empower developers to innovate, rather than lock them down in unfamiliar territory, as well as ensuring strong ROI on technology infrastructure projects, not only to deliver value back to citizens, but to re-invest money saved in further digital transformation projects.

To achieve this, the agency wanted to test whether DR could run in the cloud, selecting VMware Cloud on AWS as the technology provider. Thanks to the inherent efficiency and interoperability of the solution, the team had gone from the initial testing phase to successfully running a DR scenario within a timeframe of just three weeks.

In addition, replacement costs were reduced by 50 to 75 percent due to being able to rely less on physical hardware and reduce spend on replacements. As a result of the implementation, the organisation's DR operations are now faster than previous on-premises deployments, boosting the IT team's preparedness and agility to respond to surges in uses and improving uptime overall.

Whether it's in a distributed working environment or not, being able to manage changing needs, volumes and apps quickly and scale where needed, is critical. Adopting a cloud solution is the future of government and will give you the opportunity to transform the way in which you deliver best in class services to staff and citizens.

If you would like to learn more about how VMware Cloud on AWS can help you modernize your IT infrastructure, please check out the VMware Cloud on AWS website