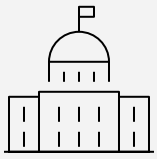

Digital transformation for government

How a hybrid multicloud platform delivers outcomes for government

Technology is often at the heart of the most significant innovations in government programs and services. Today, cloud redefines the technological landscape and underpins the capabilities that enable better outcomes for citizens and agencies alike. It's hard to understate the role that cloud technologies play in driving the digital transformation necessary for the modernization of government services. Innovations in cloud delivery models continue to accelerate the pace of change and set new standards for cloud adoption.

The rapid evolution of cloud technology

Since the early adoption of cloud technology around 2008, the focus was solely on public cloud and the public utility of compute. "Cloud First" policies at all levels of government catalyzed the rapid adoption of multi-tenant public clouds to save on hardware and data center costs, and the move from capital expenditure (CAPEX) to operating expenditure (OPEX). IT teams used public cloud to spin up development environments for rapidly prototyping new applications and functionality. Software as a service (SaaS) delivered over the cloud helped agencies meet line-of-business (LOB) needs, generate savings, and deliver elasticity, scale and connection to broader capabilities. Multiple clouds are now so common that agencies engage an average of three to five cloud vendors and some agencies report using more than 10.[1]

Throughout this time, questions about the security and privacy that cloud provided remained unanswered. Could administrators move data among environments and vendors and remain compliant with regulations? This concern led agencies to adopt private clouds, which offered the same service-based delivery system as public clouds but gave agencies more control as it was either hosted within the agency's environment or in a private enclave on a multi-tenant cloud. The resulting definition of the hybrid cloud model continues expanding so that workloads can span public and private clouds, edge computing, the Internet of Things (IoT) and traditional on-premises environments.

Despite the promise and projected ubiquity of public cloud technology, most mission-critical and data-sensitive applications don't run in the cloud. While relatively simple applications like email, websites and office productivity tools are most likely to be deployed by government agencies in cloud environments today[2], many mission-critical applications haven't had a business case to justify the migration to cloud. They use heritage technologies, have complex dependencies and multiple tiers tied to various transactional systems that are closely integrated with security and operational systems that are hosted in on-premise environments. Because no single public cloud works for every use case, governments of all levels look to **hybrid and multicloud environments to manage security, compliance and latency**.

Today's cloud technology: Open and hybrid

The challenges that hybrid and multiple clouds pose to IT leaders are inspiring the next generation of cloud capabilities. "Cloud Smart[3]" policies have replaced "Cloud First" in many national and regional governments, recognizing a new IT paradigm where leaders need flexibility and choice to deliver IT that serves unique government missions with speed, visibility, security and control across disparate environments. This paradigm, marked by a hybrid multicloud platform, is built on enterprise open source and open standards that can securely integrate, manage and govern workloads, applications and data across any cloud vendor and traditional IT infrastructure.

Hybrid multicloud enables agility through modernization of mission-critical heritage applications and with new cloud native development. The open stack based on the Kubernetes container platform and a set of common services such as monitoring, metering, logging and identity and access management, provide a high degree of multicloud manageability. Common services are essential for consistent management of applications and data that are distributed across environments, automation of compliance, and maintenance of an appropriate security posture.

Hybrid multicloud provides infrastructure independence allowing agencies to develop applications with high-value technologies from any vendor, providing freedom from the single-vendor approach that has been predominant. It also mitigates the risks associated with using one vendor, such as lock-in or a single point of failure.

Achieve agility with cloud-native architecture

Agencies in early phases of cloud adoption should first consider an open, cloud agnostic platform, such as Red Hat® OpenShift®, which enables management and orchestration of containers and microservices regardless of the underlying infrastructure. Containers and microservices, often referred to as cloud-native architectures, are fast-emerging industry standards that provide the speed, flexibility and portability needed to move and manage data and workloads securely across environments.

Definition:
Microservices *break applications down into their smallest components, which are then free to operate independently. Instead of a traditional, monolithic, approach to apps, where everything is built into a single piece, microservices are separate yet work together to accomplish the same tasks as the old monolith application. This software development approach provides nimble and lightweight granularity, so that multiple apps can share similar processes. Microservices run inside containers, which include everything needed to run, such as code, dependencies and libraries. Containers allow optimal portability among environments while retaining full functionality.*

Cloud-native architectures help development teams innovate faster without sacrificing security or quality. With microservices, teams update only what's needed using any programming language to deploy new value to citizens and stakeholders. Agencies can scale and replicate each microservice independently to enhance utilization and allocation of infrastructure resources.

The power of infrastructure independence

Modernizing mission critical applications and data is where the true value of an open hybrid multicloud approach comes to life. As applications are modernized with containerized microservices, they can live in a distributed state—independent of infrastructure and optimized for performance and security. For example, part of the application can reside on premises, close to sensitive data, and another part could be at the edge, for IoT use cases. Entire applications can be placed in a container and run in a cluster on premises or in the cloud to deliver new capabilities, such as high availability. Applications and workloads can mix and match cutting-edge technologies from different cloud vendors to build differentiating citizen and employee experiences or drive greater insights from data sources anywhere in the cloud or on premises.

The ability to modernize or write an application once and run it anywhere is not available from cloud vendors that promise hybrid cloud with proprietary private and public cloud technologies.

This form of hybrid computing promises what Gartner Analyst Daryl Plummer calls “like for like.” What’s offered on the vendor’s proprietary public and private clouds is essentially the same–the same services, same delivery of services and same control plane, whereby convenience and consistency are priorities. For government agencies that maintain heritage applications, the like-for-like hybrid model may prove difficult to integrate with different technologies and other control planes they may need, which leads to complications and potential corruption of data[4].

Alternatively, an open hybrid multicloud approach integrates different technologies with a container platform that can be deployed on any infrastructure, including multiple clouds[4]. Common services delivered through this platform provide consistent management of applications and data across multiple clouds and on-premises data centers.

Deliver the open hybrid multicloud promise

Seamless management across any infrastructure
As government modernizes applications from on-premises to hybrid and multicloud IT models, it must implement a management solution that delivers services across the entire ecosystem. A system of this caliber should enable application teams to use services from different vendors with the required availability and performance levels and enable operations teams to maintain the right level of governance and control.

Both development and operations need three unified capabilities to manage a hybrid multicloud environment.

Visibility 	Where is everything running? How is it running? What do I need to fix?
Governance 	Are applications running in the right environment? On the right infrastructure? At the right security levels of compliance?
Automation 	Are applications available? Are the applications performing? Are the applications being monitored?

Multicloud management tools that cross traditional virtual machines (VMs) and cloud-native clusters simplify governance and compliance requirements. To maintain compliance, role-based policy enforcement must be applied so that certain user privileges apply only to specific users. Moreover, specific controls, for example, the Health Insurance Portability and Accountability Act (HIPAA) or National Institute of Standards and Technology (NIST), can be applied to clusters and workloads across any infrastructure. When incidents occur, users and administrators can either be informed that they’re out of compliance or policies can automatically be enforced, providing continuous compliance.

Strengthen security for data and application
As agencies move to a cloud native approach and deploy workloads across infrastructures, the security focus moves away from a traditional hardened perimeter to a workload-centric, data-centric approach. Security teams must understand how applications work and where their sensitive data is located, then map the flow of data through on-premises environments, cloud networks and beyond.

Rather than build a fence around an entire IT estate, security in a hybrid multicloud world can build off the concept of "zero trust," where access to data by people, devices, networks and workloads must be verified at any point and any time[5].

Once security teams understand how their data flows, they can create micro-perimeters or secure zones across data centers and cloud environments that harden the perimeter of the data flows in any given transaction. Applying micro-segmentation then equips the appropriate users with access to data either along or at specific points of that transaction path. Agencies can use end-to-end encryption to avoid any data theft during transit.

Containers and container platforms offer unique new opportunities to achieve faster remediation and integrate protection across environments. Containers allow multiple levels of security at the container level and within applications. IBM® Secure Service Containers, for example, isolate workloads and provide full data encryption in multicloud environments. They also help protect encryption keys in a tamper-responsive, hardware security module, to help protect agencies from insider threats. When combined with DevSecOps methodologies, security aspects can be infused during testing and compliance phases, all the way to production and operations.

Create enterprise-grade open source

Open source is at the heart of hybrid multicloud environments. Today, Linux® is the #1 development platform[6] and is available on all public cloud platforms, which makes it easy to use consistent methods to build and deploy on any public cloud and on-premises infrastructure. The dominance of Linux opens a broad ecosystem of open source tools platforms that are fueling the hybrid and multicloud market.

Definition:
Kubernetes *is an open source container orchestration platform that automates the development, deployment and management of container-based applications. Kubernetes for government optimally supports all infrastructure platforms, including VMs, mainframes and bare metal servers.*

Understanding the difference between open source and enterprise open source is critical. Open source software is software with source code that anyone can inspect, modify and enhance[7]. In contrast, enterprise open source combines the advantages of the open source ecosystem development model with the stability, performance and support that's offered by traditional enterprise software.

Open source

- Source code anyone can inspect, modify or enhance

Enterprise open source

- Source code anyone can inspect, modify or enhance
- Tested
- Tuned for performance
- Proactively examined for security flaws
- Includes Service Level Agreements that detail what's supported, response and remediation times
- Documented lifecycle (necessary for mission-critical applications)

While anybody can download and install an open source project, enterprise open source products require testing and performance tuning, and proactive examination for security flaws. Moreover, as Joe Brockmeier of Red Hat writes, "it needs to have a security team that stands behind it, and processes for responding to new security vulnerabilities and notifying users about security issues and how to remediate them."[8]

Enterprise open source products have service level agreements (SLAs) that articulate what's supported and how quickly you should receive response and remediation. They have a predictable lifecycle, stated up front, to detail information about components that may move at different speeds and a lifespan that's suitable for governments to use when deploying mission-critical applications. An enterprise software vendor, such as Red Hat, may also take on the heavy lifting of supporting components well after the upstream project has moved on to newer versions. This support is necessary for software to be used within a timeframe that makes sense to government organizations.

With enterprise open source solutions, any agency can leverage the speed of innovation, expertise and diverse perspectives of the community... and advance a common set of enterprise goals.

Open source also provides a strategic opportunity for government agencies to address challenging skills gaps. In addition to open source tools and applications that mitigate vendor lock in, a community of skilled and dedicated developers and architects are available to build, patch and add to the code, and develop standards and definitions.

With enterprise open source solutions, any agency can leverage the speed of innovation, expertise and diverse perspectives of the community. Many of these agencies include researchers and academics who review vulnerabilities, harden deployment environments and advance a common set of enterprise goals. This best practice for implementing compliance enables advanced quality control for application performance and security.

Implement a hybrid multicloud environment

Government agencies that embark on a hybrid multicloud journey have the opportunity to unlock the benefit of cloud for mission-critical applications. New levels of data portability and interoperability offered by hybrid multicloud can help agencies realize the virtue of "write once, run anywhere." Here are four recommended steps:

Design the destination. Think open, multicloud, hybrid cloud. Your organization will live with the decisions you make today for years. Evaluate which of your workloads fit best in the public cloud, private cloud and traditional IT environments. Avoid environment lock-in and vendor lock-in and reassess approaches that might not survive as standards and technologies evolve.

Sequence the journey. Avoid "ready, fire, aim" approaches. Lay out a careful, clear roadmap of what you want to do and in what order. You may experience pressure to skip ahead without building a solid, open foundation. Resist it.

Mobilize the right skills and assets. Draw upon talent within and outside your enterprise. While it's important to develop and maintain in-house skills, engaging with trusted third-party services providers helps bridge short-term gaps while reducing fixed costs.

Manage to clear outcomes. Establish meaningful qualitative and quantitative measurements and commit to holding to them. Remain flexible and incorporate new technologies as they emerge. Always stay true to your mission, architectural, and technical principles.

Each government agency's journey to cloud is unique and tailored to specific applications, workloads, security and compliance requirements. To facilitate each unique cloud journey, IBM uses agile methods, such as the IBM Garage™ methodology to tailor roadmaps to individual journeys. IBM Garages are collaborative delivery models through which IBM co-creates with its clients to design, deliver and refine solutions on a continuous basis to accelerate the delivery of value to end users.

IBM's recent acquisition of Red Hat significantly enhances the company's hybrid cloud capabilities and firmly establishes IBM leadership within many open communities. The combined capabilities of IBM and Red Hat are based on open source and open standards to help governments accelerate their digital transformation.

Next steps

To learn more about the IBM Cloud, IBM Garage methodology and IBM's hybrid multicloud platform, watch the dynamic discussion between Red Hat and IBM public sector leaders.

Watch now:
www.ibm.com/cloudsummit-gov

Learn more about IBM Cloud solutions for government:
www.ibm.com/cloud/government

1 www.govtech.com/library/papers/Gaining-Steam-Cloud-Platform-Adoption-and-Emerging-Technologies-117139.html?promo_code=GOVTECH_web_library_list

2 www.fedscoop.com/federal-leaders-report-advances-cloud-adoption-critical-services

3 www.cloud.cio.gov/strategy

4 www.event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&partnerref=learnhybrid&eventid=2068971&sessionid=1&key=B3C57E41B385AC4FAE95D17FF36E1459&regTag=&sourcepage=register

5 www.resources.infosecinstitute.com/zero-trust-security-what-is-it

6 www.idc.com/getdoc.jsp?containerId=US43753318

7 www.opensource.com/resources/what-open-source

8 www.redhat.com/en/blog/what-enterprise-open-source