wavicle DATA SOLUTIONS

How to implement a multicloud strategy built for your business needs

Whether on purpose, or by accident, organizations are increasingly managing data across several types of cloud platforms, often from more than one provider.

This “multicloud” approach comes with several benefits that range from potential cost savings to workload flexibility. But it also presents a variety of challenges compared to single cloud.

When applications and data are dispersed among multiple cloud environments, it can be tougher to integrate, transform, access, and secure trusted data. You may have started out in the cloud to get a consolidated set of data from all sources. But with multicloud, an obstacle appears in the form of data silos that need to be connected.

If you’re like most organizations, your multicloud environment has grown out of a combination of deliberate action and circumstance, perhaps due to mergers and acquisitions or functional or geographic IT decisions.

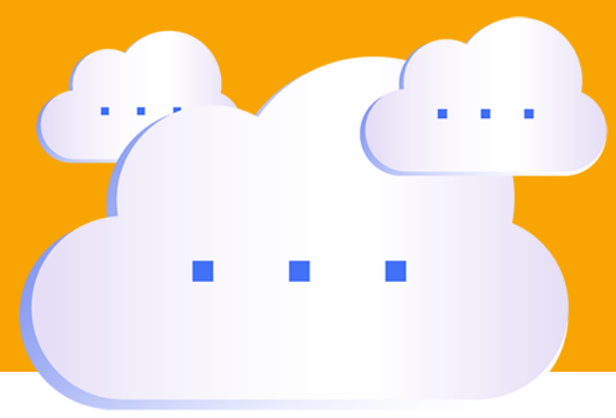
Whatever your situation is, it’s not too late to step back and take a more thoughtful approach to your multicloud situation. By aligning your cloud strategy with business needs and data strategy, you have a better chance of maximizing the value and minimizing the complexities of multicloud.

According to Gartner, “More than 80% of organizations use multiple cloud Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) providers, but many do not have a deliberate multicloud strategy.”[1]

Whether you are embarking on or expanding a multicloud approach, or just developing a long overdue strategy, this guide is for you.

Multicloud strategy

What is multicloud?



Multicloud is a situation in which data and applications are distributed across multiple cloud environments.

For example, an enterprise might use software-as-a-service (SaaS) offerings for applications such as email, customer relationship management (CRM), collaboration, finance, etc.; infrastructure-as-a-service (IaaS) to support its overall IT environment in combination with an on-premises data center; and platform-as-a-service (PaaS) to support its application development efforts.

Multicloud is not to be confused with hybrid cloud, which refers to the use of private and public cloud infrastructure in some combination with on-premises IT infrastructure resources such as data centers.

The services in a multicloud environment might be delivered by one or more of the major public cloud providers – Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) – or via industry-specific cloud vendors, or smaller niche vendors. With this type of strategy, an organization might be using different cloud vendors for storage, cloud computing, data analytics, cyber security, enterprise software, and other areas all at the same time.

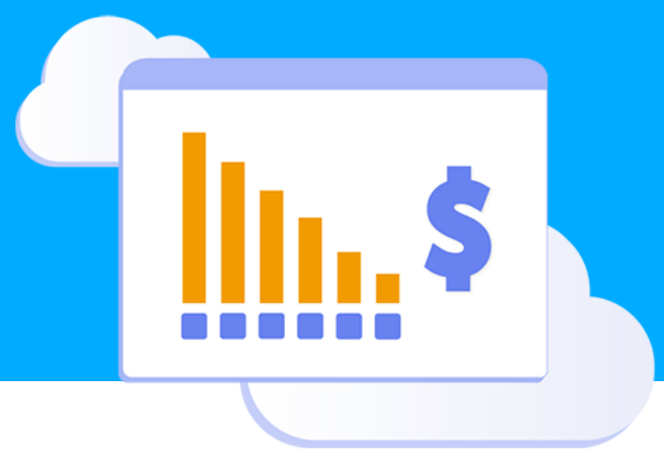
More than

90%

of companies now rely on multicloud environments, according to Flexera's State of the Cloud report. And on average, enterprises use 2.2 public and 2.2 private clouds.

– Source: CSO online article[2]

Benefits of multicloud



One of the biggest benefits of multicloud is flexibility. Using multiple providers eliminates the risk of vendor lock-in that comes from using a single service provider. This means less likelihood of outages and other services failures with easier disaster recovery, security breaches, compliance issues, etc. It also affords you the ability to move easily between providers because of changing strategies or service level agreements (SLAs). Other benefits include:

- **Best of breed solutions:** Use the best technologies and features from various providers to fit your specific needs. For example, you might pair Snowflake's Data Cloud solution with Event Hubs data ingestion from Azure.
- **Optimize cost and performance:** Controlling cloud costs is a concern for any cloud environment. With multicloud, you can leverage the ability to shift workloads from one environment to another. This shift allows users to take advantage of compute cost savings or to improve performance of the workload with minimal or no disruption.
- **Faster access to data:** Placing or federating data with different cloud providers based on geographic locations can reduce latency due to regional requirements for proximity to data.

Check out our infographic: Different cloud environments—which is best for you?
View now >

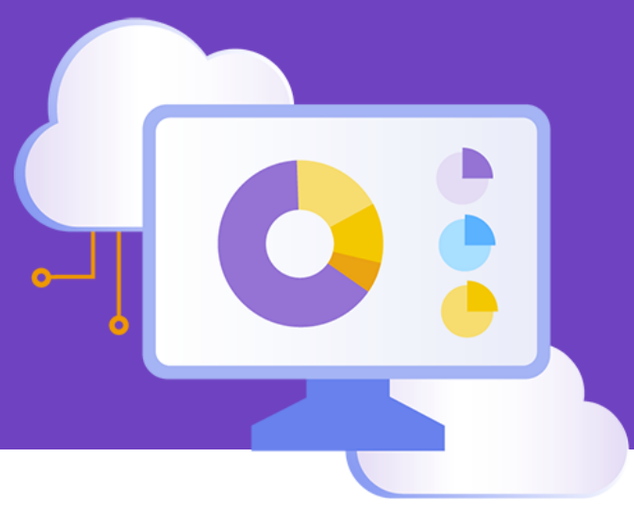
Challenges of multicloud

With the good comes the bad. Deploying a multicloud environment brings a host of potential challenges that, left unaddressed, can be significant barriers to success:

- **Greater complexity:** A multicloud environment means having a variety of service environments, SLAs, interfaces and integrations, architectures, data backup/ resiliency policies, cost structures, security, and privacy risks. Greater complexity requires more comprehensive cloud management.
- **Skills requirements:** With a multicloud environment, your team needs experience in the various cloud environments, architectures, types of services, security protocols, etc. to manage them. According to Gartner[3], "skills" is one of the top three areas of multicloud complexity, which can increase workforce costs because of training requirements, pay increases, or additional headcount.
- **Increased cost (potentially):** Yes, cloud can save you costs in terms of workload management, capital expenditures, and managed services, but the complexity and skill requirements mentioned above can quickly erode cost savings. Additionally, with multiple vendors in the mix and lower commitments per vendor, you may lose leverage when negotiating for pricing.
- **Reduced visibility and control:** With multiple cloud environments comes multiple monitoring tools or management dashboards. There is no easy way to get a unified view of application and database performance, cloud storage, network statistics, automation, etc. across all environments.

"A multicloud strategy increases the complexity and cost of IT and demands greater skills. While most organizations will eventually be multicloud, many adopt multiple providers without deliberate planning, creating unnecessary chaos."
– Source: Gartner[1]

Multicloud use cases tied to data and analytics



A multicloud environment supports various use cases for data and analytics, each of which have their own challenges and benefits. Two of these were analyzed in a recent Databricks webinar[4]:

- **Geographically diverse business units:** Growing companies often open new business units in different geographic regions to support those local markets, and those units might use different cloud services. Data scientists, data analysts, and others in the various regions are able to access data from the different cloud environments even though they use different tools and applications based on the cloud service of choice. They do this by adopting open interfaces and standards, as well as a common portfolio of tools.
- **Different organizational functions:** In this use case, the multicloud environment supports users in different functions across the organization. This might include marketing, advertising, and customer transactions. Each of these areas needs to use a platform that enables them to share data across separate cloud services.

Your multicloud strategy

Jumping into a multicloud environment for data and analytics without developing a cohesive data strategy is asking for trouble. Your multicloud strategy, or any cloud strategy for that matter, has to align with the overall business and data strategy of the organization.

As Gartner notes, multicloud strategies designed around business strategy produce the greatest business value, while multicloud strategies designed in isolation produce vastly less.

Business goals and priorities must be aligned and supported by cloud services. An organization needs a thorough understanding of what types of data will achieve their business objectives and how to leverage cloud platforms to manage and deliver that data.

When developing a multicloud strategy, include key stakeholders from a variety of disciplines in the effort. This might include the CIO, CTO, other C-level business leaders, top cyber security executives, governance committees, and executives from finance, legal, and risk management.

Strong collaboration among the teams is vital for ensuring successful multicloud strategy with a cohesive connection to data and analytics initiatives. Leaders in data science and analytics should also be leveraged for input. The organization should be actively establishing a holistic multicloud operating model.

For organizations utilizing multicloud, we unite business and technical strategies into a cohesive method around four key areas: managing people, managing data, managing technologies, and security.

People

Any new strategy requires an organization to empower its people for success. The management of personnel, a main component of data governance, increases in importance with multicloud. The additional complexity requires the development of new roles, policies for data accessibility, common policies, and retraining programs.

If the right users can’t easily access data across the multicloud environment, it ceases to be an effective approach for the organization. To regulate data access across multicloud, responsibility can be given to data stewards and employees focused on cross-cloud management.

After roles and accessibility are adjusted for a multicloud environment, an organization will need to retrain employees based on the changes to architecture and technologies. For continued learning and success, review boards and centers of excellence can be established.

Data

The increasing volume of raw data spread across a multicloud environment presents problems like multiple formats and siloed data. Therefore, a multicloud environment needs master data for a consistent and uniform way of classifying data across domains like customer, product, partner, employee, and supplier.

Master data management (MDM), is the tools, technologies, governance, and overall philosophy enacted by an organization for all data to be available in a single reference point. It's designed to ensure the uniformity and accuracy of master data sets shared across disciplines.

The creation of a single management portal for access to cloud-based data, services, and applications is often a solution. Even with a single portal, access still needs to be regulated.

For Vyaire Medical, with 20,000 products, 370,000 customers, and numerous vendors, creating a single source of master data was difficult. Wavicle created a unified portal for a single "golden record".

Learn more about the master data management solution >

Technology

The various technologies organizations use to supplement their cloud and data and analytics overall, need to be assessed with the introduction of a multicloud environment. After the elimination of platforms that aren't optimal for a multicloud environment, an organization needs to consider new vendors designed for multiple clouds.

Open-source software (OSS) have advantages in cloud development like speed, flexibility, integrated management, greater control, and wider compatibility. According to an IBM survey, OSS was rated equal to or better than proprietary software by 94% of respondents.[5]

The current models of storage and backup should be evaluated to make way for more efficient replication and virtualization.

Security

A multicloud environment creates security challenges because it involves many different components, architectures, platforms, and applications. There are variables to consider, such as the fact that each of the major providers offers different cloud-native solutions for cyber security.

The growing sophistication of threats and the existence of vulnerabilities put organizations at risk of cloud-based attacks that can result in significant losses. Here are some considerations to keep in mind:

- Security policies differ among providers, so companies need to implement a security program that covers all the various environments.
- The responsibility for security must always be shared between a cloud provider and the customer. But that relationship is not always clear, so it must be covered in SLAs and thoroughly understood by the company using the cloud services.
- IT and security leaders need to understand that multicloud adoption adds extra layers of management complexity, particularly when entities within an organization add cloud services in an ad hoc manner. Policies should address the overarching security requirements of the organization and make it clear that this applies to any "shadow IT" endeavors.
- Data is virtually in constant motion with multicloud. This creates more opportunities for data breach.

98%

of cloud security professionals say that a multicloud environment creates additional security challenges.

– Source: Techradar[6]

Prepare for change

As you develop your multicloud strategy, keep in mind the dynamic nature of data, technology, and business. As organizational needs change, be prepared for the strategy to evolve as well. Expect to revisit the strategy often to make sure it's serving the needs of the business and digital transformation initiatives as they move forward.

Does your organization need multicloud?

The push to the cloud has been relentless, especially over the past few years. This isn't surprising, given the potential benefits of the cloud model like reduced capital expenses, greater agility, and easier scalability.

Many organizations have found the cloud to be so appealing that they've created multicloud environments—sometimes as a deliberate corporate strategy and others because of a spontaneous need for particular cloud services. The fact is, many organizations' data is most likely already in a multicloud environment, because of applications and services that are built in the cloud.

Here are some key questions to ask when considering deploying or expanding a multicloud environment with the goal of improving data analytics:

- What benefits will multiple cloud services deliver for data analytics efforts, and are these benefits worth the costs of a transition?
- Will having more than one cloud service provide increased flexibility, agility, and efficiency for analytics workloads?
- Will multicloud effectively support existing components such as data discovery, integration, mining, and security, as well as efforts in artificial intelligence/machine learning?
- How much of a competitive edge will a multicloud environment deliver, and how can this best be measured?

Some cloud solutions, workloads, and applications work best in particular cloud environments, so it's important to align data and analytics needs with the cloud tools and technologies that are the best fit.

Multicloud can be a game-changing strategy for many types of organizations. It's imperative that CIOs and other top decision makers consider all the options.

Need more information on cloud strategy, optimization, and migration?

guide

Cloud migration: Taking your data and analytics to the cloud >

read

infographic

Different cloud environments: Which is best for you? >

read

case study

Cloud migration brings agility and innovation to Cars.com, strengthening brand experience >

read

blog

Cloud data architecture from right to left: start with the business needs >

read

Sources:

[1] **Gartner:** "A Multicloud Strategy Is Complex and Costly, but Improves Flexibility." (PDF)
[2] **CSO online:** A New Approach to Multi-cloud Security
[3] **Gartner:** "IT Leaders' Strategy Deck: Multicloud and Hybrid Cloud" (Slides)
[4] **Databricks:** Managing a multicloud data and analytics platform (webinar)
[5] **IBM:** In the era of open hybrid cloud, open source skills matter more than proprietary software skills (blog).
[6] **Techradar:** Almost all experts say multi-cloud needs a serious security upgrade