ZOHO

Maximizing efficiency and flexibility:

The power of multi-cloud for enterprise

AI series, Q1 2024

Multi-cloud architecture offers organizations tangible benefits but requires strategic guidance from IT leadership to address the complexities its adoption brings.

Cloud computing has fast overtaken on-premise as the standard across most enterprises, and taking a multi-cloud approach—using multiple public cloud computing and storage services within the same architecture—is becoming common practice. Almost 80% of respondents to Deloitte's Future of Cloud survey report that they use a multi-cloud approach[1], and the multi-cloud market is predicted to be worth almost $20 billion by 2031[2].

Whether multi-cloud is a deliberate strategy or grows up organically through the ad-hoc addition of new IaaS, PaaS, and SaaS platforms, it can offer enterprises a number of tangible benefits over on-premise solutions or a single private or public cloud infrastructure. These advantages include flexibility, scalability, and the opportunity to strengthen their bargaining position with vendors. But implementing multi-cloud can also present challenges, so a comprehensive multi-cloud strategy, careful planning, and robust governance are essential for seamless operation and data security.

[1] Deloitte, 2022 | [2] Allied Market Research, 2023

Most important benefits of multi-cloud:

(as cited by respondents to the Deloitte 2022 Future of Cloud survey)

- More choice in cloud services (85%)
- Application and data processing scalability (84%)
- Increased flexibility and negotiating leverage (83%)

Challenge: Data complexity

A survey by HBR found that even as organizations are eager to embrace multi-cloud, only 34% report having robust, multi-cloud-ready data governance policies in place[3]. As data analytics become ever more sophisticated, the benefits of best-in-breed at the department, operation, or even

[3] HBR, 2019

process level only become stronger. Multi-cloud enables enterprises to avoid vendor lock-in and leverage specialized BI and analytics tools, algorithms, and storage solutions from different cloud providers, while still preventing data silos and creating backups and redundancy where required. But with information increasingly created, collected, stored, and moved across cloud environments, maintaining confidentiality, integrity, and availability becomes challenging.

The value of an enterprise's data is highly dependent on its accuracy, which is more difficult to maintain when updates must be made across a distributed network of systems. Any latency in synchronization must be accounted for, as must any issues with interoperability between cloud services. Each cloud in the system must comply with all applicable data protection regulations, such as GDPR or HIPAA, even as the geographical locations of cloud data centers introduce additional compliance factors to consider.

Cloud providers approach identity and access control differently, so ensuring that data users have access to the data they need —and not to sensitive data that they don't— also takes careful consideration, especially if the aim is to give the end user a single sign-on experience.

The importance of robust data governance is only increased in a complex multi-cloud environment. Ideally, this will be driven by a dedicated data governance team, guided by the Chief Data Officer (CDO), or other senior executive responsible for data, who will identify data stakeholders in the organization and delegate responsibility for implementing governance on the ground. Best practice tools, like data catalogs, data tagging, and metadata management, and policies for establishing data ownership, single source of truth, cross-cloud access controls and data usage guidelines can go a long way towards taming the chaos. A well-designed, adaptive data governance framework can help rein in the multi-cloud complexity and establish cross-cloud control over who can access what data, while also improving the value extracted from data across the org. For example, the framework could leverage data centralization to earmark one cloud as a single source of truth for each data category

and then set the parameters to automatically push updates out to a connected network of resources.

> *As cloud computing has become more sophisticated, enterprises have come to expect, and demand, more unification across their tech stack. It is no longer sufficient for a cloud to offer good functionality; it must also offer interoperability.*

Saravanan Muthian,
Chief Information Officer at Zoho

Challenge: Security complexity

Security is a significant factor in multi-cloud adoption, with security considerations ranking as both the top benefit and the top challenge in the 2023 VMWare Multi-Cloud Maturity Matrix[4]. With security approaches differing between cloud providers, protecting multi-cloud architecture requires a comprehensive overarching strategy. Each cloud under consideration should be assessed not only for its individual security protections, but also for the difficulty, costs, and risks involved in linking it securely to the org's other clouds. Since transfer between clouds will always represent the weakest point for attack, it's also important to enforce robust encryption standards during data transfer as well as at rest in all cloud locations. However, with encryption methods differing between providers, this can be complex to achieve.

IP tunnels are secure communication channels established between different cloud environments to facilitate data transfer while maintaining confidentiality, integrity, and privacy. Configuring tunnels is an essential part of any comprehensive multi-cloud security approach to ensure security, reliability, and optimal performance of data transfer across the interconnected cloud environments.

While hybrid cloud architecture (a computing network that includes at least one private cloud or on-premises system alongside public clouds) shares the same security risks as

[4] VMWare, 2023

multi- cloud, it can also offer security benefits by allowing organizations that handle particularly sensitive data to store it only in private systems, reducing its exposure to risk. This is likely to increase cost and potentially data latency, so each organization should assess these trade-offs against their security needs.

Challenge: Operational complexity

A successful multi-cloud solution can facilitate scaling resources up or down as requirements evolve or fluctuate, and the option to switch services between vendors can offer resilience against service disruptions. However, effective operational management over a multi-cloud architecture is a major challenge for many organizations. While getting the best price for each cloud function is an attractive prospect, it takes careful consideration to ensure that savings are actually realized. Cloud investments can include on-demand self-servicing, broad network access, rapid elasticity, resource pooling, and measured service, and costs can easily spiral if workloads aren't deployed strategically.

Maintaining the required level of oversight and visibility into each part of a multi-cloud system without losing sight of the overall picture is no mean feat. Built-in monitoring tools offered by cloud vendors don't monitor other clouds, and inconsistent metrics and between vendors make it challenging to source third-party tools that offer off-the-shelf compatibility with all of an organization's cloud resources. This leaves IT teams without a holistic overview, risking blind spots.

A relatively new strategy that is gaining ground involves building a compatibility layer, known as a "metacloud" or "super cloud", to sit logically above an organization's various cloud platforms to provide users access to common services

79% of IT decision makers say they've experienced at least one significant downside to their multi-cloud migration, with increased complexity being the most common complaint (48%). Larger companies, and companies with larger cloud budgets, are more likely to experience greater downsides.

[Foundry, 2022]

while maintaining consistency and giving administrators centralized control and a "single pane of glass" for monitoring across all clouds. This not only streamlines operational procedures, but can also offer increased security by allowing developers to set a single security configuration to apply to all cloud environments. Building and maintaining a metacloud requires significant internal technical resources, but can offer a sophisticated holistic solution for organizations that can support it.

Incorporating enterprise SaaS solutions like Zoho CRM into your multi-cloud environment can reduce the burden on IT and security teams through effective data privacy and backup and robust integrations and API connectivity with other vendors and cloud solutions.

With the right multi-cloud strategy, the sky's the limit

While cloud usage and requirements vary significantly across enterprises, it is by now clear that multi-cloud is here to stay, and the complexity it brings with it appears to be growing, not shrinking. As multi-cloud matures, enterprises that could previously get away with an ad-hoc approach will start to need a more comprehensive multi-cloud strategy to protect against breaches, system failures, and unexpected cost increases. A successful strategy will use a range of tools to cover both technical aspects (such as architecture, interoperability, and automation and orchestration) and process-oriented policies for cost and resource optimization, data management and security, and practical considerations (like skill development and training). Collaboration among IT security teams, cloud architects, and stakeholders will be essential to align each tool and approach with overarching business processes and goals.

Why Zoho for Enterprise?

Proven software, customer commitment, tremendous value.

Scalability & Reliability

Zoho for Enterprise reduces the cost of infrastructure, unifies existing apps, and solves complex business problems for increased enterprise fitness, resilience, and scalability.

Customization & Extensibility

Through granular customizations and powerful in-house developer platforms, Zoho lets you orchestrate workflows, streamline data management, and deploy world-class solutions at scale.

Security & Privacy

From owning our own data centers to GDPR compliance features, Zoho enables enterprise organizations to focus on core business priorities, rather than data management.

Enterprise Services

From data migration to consultation and implementation, our team is armed with the in-depth product knowledge and industry expertise to meet your unique technical requirements.

Are you ready to transform your organization?

We’re here to help. Have a 15-minute, no-obligation call with one of our **Business Architects** to get all your questions answered.

Find us at **zoho.com/enterprise** |