PARADIGM™ technology

THE MULTI-CLOUD JOURNEY

Cloud computing continues to be more prevalent than ever. All industries – Financial Services, Manufacturing, CPG, Healthcare, etc. – are moving to the cloud. Why are 76% of companies adopting a multi-cloud strategy? The top reason is to have access to vendor-specific capabilities. These might include best-of-breed services on one platform that simply outshines competing offerings, or it may mean integration with on-premises software running mission-critical workloads.

No matter the reason, the multi-cloud journey (and overall cloud strategy) needs to be planned diligently to future-proof your organization.

Join us on a trek through challenges and trends, cloud optimization best practices, and holistic approaches - including migration framework recommendations - that can influence your adoption journey.

Avoid Vendor Lock-In

Gartner forecasts worldwide end-user spending on public cloud services will grow to almost $400B in 2023.[1] As seen with AI-language programs like ChatGPT or Google's Bard, cloud providers create new competitive offerings daily. The ability to use multiple clouds or migrate from one cloud to another delivers competitive edge - so how can organizations find flexibility and avoid vendor lock-in to a single provider?

Vendor lock-in is a challenge in cloud computing, occurring when organizations become dependent on a single provider. This can happen when they choose to use proprietary tools and services or sign long-term contracts. Vendor lock-in can be a problem because it limits options and makes switching providers difficult. If an organization becomes locked into a particular CSP (cloud service provider), they may be forced to pay higher prices or stuck with a tool and service that doesn't meet their needs.

Tips to avoid cloud vendor lock-in include:

- Use open-source tools and services which are not tied to any cloud provider.
- Sign shorter-term contracts for flexibility to switch if you become dissatisfied.
- Be aware of lock-in risks before signing a contract - consider things like data retrieval limits.
- Have a plan for migrating data and applications to another cloud provider in the event you decide to switch.

Being aware and proactive allows you to protect your organization from potential challenges vendor lock-in can cause.

Cloud Service Providers are Unique

One of the biggest challenges posed by CSPs is the sheer number of options available. Cloud services are unique in that they offer a variety of benefits to businesses including scalability, flexibility, and cost-effectiveness. This can make it difficult to choose the right provider for your needs. Additionally, these services are constantly evolving; new services are developed while existing ones are updated and improved, making it difficult to keep up with the latest trends and technologies.

Applying a Well-Architected Framework to your multi-cloud strategy will enable you to take advantage of various providers' unique capabilities while maintaining order across environments. A key multi-cloud best practice is to choose the best provider for a specific workload or application.

Operational Excellence
Run and monitor systems, continually improving processes and procedures - automating changes, responding to events, and defining standards to manage daily operations.

Security
Protect information and systems - confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

Reliability
Intended function performance and failure recovery - distributed system design, recovery planning, and adapting to changing requirements.

Performance
Structured and streamlined allocation of IT and computing resources - selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve.

Cost Optimization
Avoid unnecessary costs - understanding spend over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending.

Sustainability
Minimize environmental impacts of running cloud workloads - shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize resources and reduce downstream impacts.

What does this look like in action? A company may choose Amazon Web Services (AWS) for its data warehousing needs, Microsoft Azure for its enterprise resource planning (ERP) system, and Google Cloud Platform (GCP) for its artificial intelligence (AI) and machine learning (ML) workloads. By utilizing the strengths of multiple providers, you can optimize IT infrastructure and gain competitive edge in the market supporting your customers.

Consistent & Holistic Approach

Juggling multiple providers, tools, and services to manage multiple cloud environments can be complex and costly (which can create a barrier to entry). And achieving success often requires a team of skilled cloud professionals who are prepped to tackle potential risks as well (think data breaches or outage risks).

A holistic approach not only alleviates the challenges of complexity, cost, skill, and risk, it also:

- Improves security via a single view of cloud environments;
- Increases agility via easier app and service deployments; and
- Enhances compliance via clear regulation and standard compliance.

An effective and efficient holistic approach to managing multi-cloud environments requires organizations follow a handful of best practices. How have you incorporated these into your business strategy?

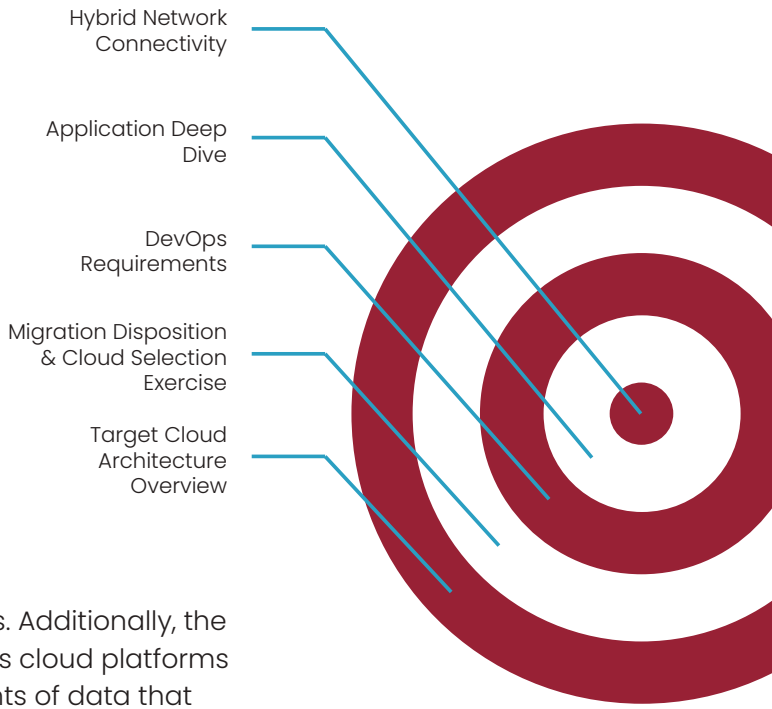
Cloud Migration for #1 Global Distributor of Security Products

Paradigm's cloud experts migrated from on-premise to the cloud and modernized integration architecture through an API integration center of excellence (COE).

- 40% of migration achieved through automation
- Improved performance by 32%
- Increased business satisfaction by 24%

Costs - People, Process & Technology

By 2025, 51% of IT spending on application and infrastructure software, business process services, and system infrastructure will have shifted from traditional solutions to the public cloud.[2] This shift will affect not just an organization's technology, but its people and processes. Costs are directly proportional to the teams supporting them, use of right technologies, and creation of efficient processes to navigate the complexity of managing and optimizing resources across multiple platforms.



One of the main cost implications of a multi-cloud strategy is the added complexity in managing and optimizing resources across multiple platforms. This leads to cost increases via personnel, tools, and processes required to manage and monitor environments. Additionally, the cost of data transfer and communication between various cloud platforms can add up, especially for organizations with large amounts of data that require regular movement.

Each cloud provider has its own unique services, pricing models, and terms of service, which can make it difficult to move workloads between different platforms. It can result in higher costs for certain services or being locked into a particular provider for a longer time.

So, how can you navigate process and technology for your multi-cloud solutions?

- **Define requirements:** Identify applications and data to move to the cloud as well as performance, security, and compliance requirements.
- **Choose the right providers:** Evaluate cloud providers and their offerings, security, and compliance records.
- **Design the architecture:** Identify applications and data to move to each cloud provider as well as networking and security requirements.
- **Migrate applications and data:** Plan, execute, test, and validate the cloud migration.
- **Manage the multi-cloud environment:** Monitor application performance and availability as well as manage data security and compliance.
- **Optimize the multi-cloud solution:** Evaluate the performance and cost of cloud providers, making changes to architecture to improve performance and reduce costs.

Regulatory & Compliance

A major concern for organizations moving to or expanding on the cloud is regulatory compliance. Choosing which cloud platforms to use hinges on security and compliance prerequisites that ensure the cloud computing workload meets regulatory requirements.

Data Encryption & Access Control

Convert data into a form that cannot be read by unauthorized individuals and restrict its access to protect from improper viewing and use.

Auditing & Incident Response

Track and record user activity to validate authorized or detect unauthorized access to sensitive data. Respond to and mitigate security incidents to protect sensitive data from being compromised.

Patch Management

Apply security updates to systems and software to protect from vulnerability.

Security Awareness Training & Third-Party Risk Management

Educate employees about security best practices to prevent mistakes that lead to security incidents. Assess and mitigate risks posed by third-party vendors.

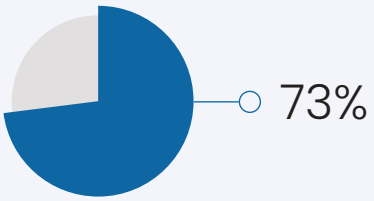
Regulatory Compliance

Ensure cloud workloads meet regulatory requirements - many regulations, such as GDPR, apply also to cloud computing.

Cloud & Modern Infrastructure for Large Credit Union

Paradigm's cloud and data management experts enabled regulatory compliance reporting via improved customer view and historical look-back for increased data confidence.

- Enabled data-driven decision-making
- $1.3M annual cost reduction
- 73% productivity improvement



Conclusion

Every cloud journey is different - not all organizations start in the same place at the same time with the same tools. Deciding whether to use a multi-cloud strategy depends on an organization's specific needs and requirements. You must carefully consider the costs and benefits addressed here. By taking into account vendor lock-in, added complexity, costs, and regulatory compliance implications, you and your organization can make an informed decision on whether a multi-cloud strategy is the right fit for your needs.

About the Authors

Josh Petla, Cloud Practice Leader - 16+ years' experience in the IT and services industry leading cloud transformations. He has led countless cloud migrations and cloud native development focused on software engineering and data analytics for organizations across both private and public sectors.

Chris Gately, Chief Revenue Officer - 20+ years' experience leading sales organizations across technologies focused on data analytics, storage, cloud, security, and mobile solutions.

The multi-cloud journey requires diligent planning to ensure future-proofed capabilities for your organization.

Contact us to **request a consultation** to be sure you are ready to take on these challenges.

REQUEST A CONSULTATION

[1]"Forecast: Public Cloud Services, Worldwide, 2020-2026, 3Q22 Update." Gartner. | [2]"Market Impact: Cloud Shift - 2022 Through 2025." Gartner.