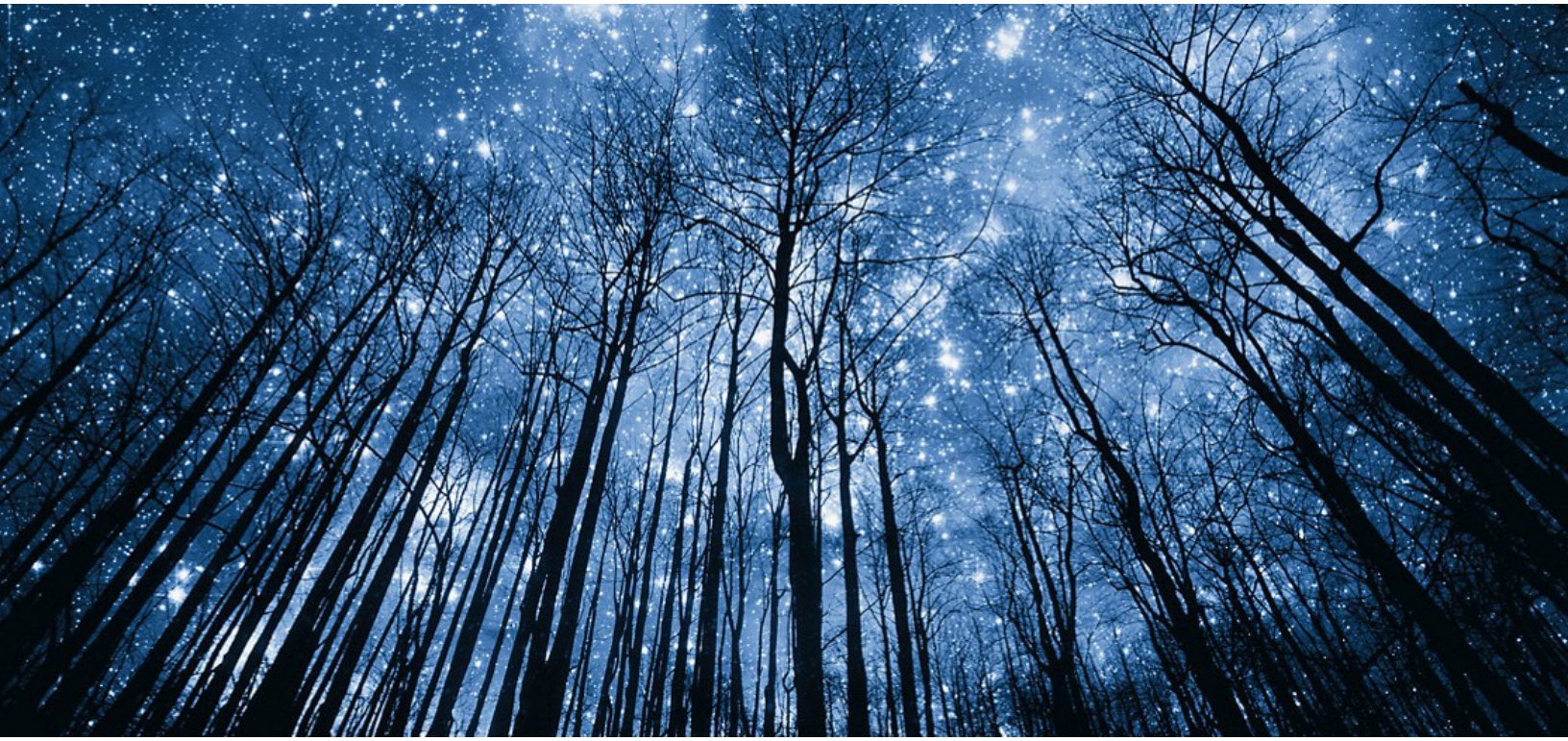
DELL Technologies

LET YOUR WORKLOAD DICTATE THE ARCHITECTURE



Vinay Joel Dmonte
Supervisor, Inside Sales Management
Dell Technologies

Amal D. Nair
Inside Sales Engineer
Commvault

Akshay A G

DELL Technologies
Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged and Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Contents

Abstract

We all are aware and educated about the fact that the business that happens today is not just limited to a city, a state, or even a country, business today is something that is conducted across a highly interconnected environment where geographic borders and time zones seem to blur out of the picture and business transactions flow almost all day and night for the complete year. The needle unanimously points towards the relevance of cloud adoptions and its various models to support different kinds of business use cases and needs. With that in place and consideration to extract the most value from every investment that they make it is important to maximize the utilization of resources while holding down the cost to its minimum, but the most critical subset being choosing of workload that best fit in what kind of resources.

The IT admins or the Architects need to leave no page unturned and double tap on every parameter and decision factor that is responsible for this critical decision to be made. It plays a key role because any flaw in the decision of the same can mean inefficient deployment, degraded performance, or nonfulfillment of the expectations, and added onto all this increase in investments to move the data again from the cloud to on-prem or any other deployment models not to mention the complexity that accompanies with the same.

But for effective planning and implementation with all the parameters considered it is first important for the deployment and planning team to be aware of the consideration and have a blueprint with regards to planning mapped before any of the actions. This paper serves as a quick reference guide and knowledge article for anyone looking to have the parameters handy when dealing with one such situation.

The paper summarizes various inputs and pointers that can be adopted even as best practices such as strategic considerations for workload placement, deployment suggestions concerning business velocity, and requirements and considerations to segregate them into specific groups.

The following can be some of the subsets that can be expected from this paper:

1. Overview of Cloud Implementation Models & Services.
2. Categorizing the Workloads and its Placements.
    a. Business Considerations
    b. Technical Considerations
    c. Ecosystem Considerations
3. The Decision Criteria.
4. Embracing for future developments.

1. Introduction

Building an IT solution for your workload is a complex process that requires careful planning and execution. The solution should be designed to meet the specific needs of your organization, while also providing the necessary flexibility and scalability to adapt to changing requirements.

The first step in building an IT solution for your workloads is to understand the requirements of the organization and the workloads themselves. This includes understanding the specific needs of the workloads in terms of compute resources, storage, and networking capabilities, as well as any regulatory or compliance requirements.

Once the requirements are understood, the next step is to evaluate different options for the IT solution. This includes evaluating different cloud platforms, such as public clouds, private clouds, or hybrid clouds, as well as evaluating on-premises solutions. The choice of platform will depend on the specific requirements of the organization and the workloads themselves.

After the platform has been chosen, the next step is to design and implement the IT solution. This includes designing the architecture of the solution, selecting the necessary hardware and software, and configuring the solution to meet the specific needs of the organization and the workloads.

Once the IT solution has been built, the next step is to test and deploy it. This includes testing the solution to ensure that it meets the specific needs of the organization and the workloads, as well as deploying the solution in a production environment.

After deployment, it's important to monitor and maintain the IT solution to ensure that it continues to meet the needs of the organization and the workload. This includes monitoring the performance of the solution, troubleshooting, and debugging any issues, and making any necessary updates or changes to the solution.

2. Cloud Service Models

It is important to understand the different Cloud Service models that would best fit the requirements. Choosing the right cloud service model depends on the specific requirements of your workloads and your overall business goals. Here are some key factors to consider when choosing among the different cloud service models:

1. Infrastructure as a Service (IaaS): IaaS provides virtualized computing resources, such as servers, storage, and networking, over the internet. It is a good option for organizations that need to have control over their infrastructure and the ability to customize it to their specific needs. It's also a good option for organizations that want to move existing on-premises workloads to the cloud.
2. Platform as a Service (PaaS): PaaS provides a platform for developing, running, and managing applications, without the need to manage the underlying infrastructure. It's a good option for organizations that want to focus on developing and running applications, without the need to manage the underlying infrastructure.
3. Software as a Service (SaaS): SaaS provides access to software applications over the internet. It's a good option for organizations that want to use software applications without the need to install, configure, and manage them.
4. Function as a Service (FaaS): FaaS allows developers to write and deploy small units of code, called functions, that can be executed in response to an event, like a user request, a message

from a queue, or a timer. This service model is cost-effective, as you only pay for the resources consumed by the function when it runs. It's a good option for organizations that want to build and run event-driven, serverless applications.

Customers should adopt different cloud service models depending on their specific business needs and goals. Each model offers different levels of flexibility, scalability, and control over the infrastructure and services.

- **IaaS (Infrastructure as a Service):**
  - Have more control over their infrastructure: IaaS provides customers with more control over their infrastructure, as they can configure and manage their own virtual machines, storage and networking resources.
  - Scale their infrastructure quickly: IaaS allows customers to scale their infrastructure quickly and easily, as they can provision new resources as needed, without the need for significant upfront investment.
  - Reduce capital expenses: IaaS eliminates the need for customers to invest in and maintain their own physical servers, which can result in significant cost savings.
  - Achieve greater flexibility: IaaS provides customers with greater flexibility, as they can choose from a variety of operating systems, programming languages, and other software.
  - Meet specific technical requirements: IaaS allows customers to meet specific technical requirements, as they can choose the operating system, programming language, and other software that best meets their needs.
  - Run legacy applications: IaaS allows customers to run legacy applications, as they can create virtual machines with the same configurations as their existing physical servers.
  - Create disaster recovery and business continuity plans: IaaS allows customers to create disaster recovery and business continuity plans by replicating their infrastructure in multiple locations.
  - Meet compliance and regulatory requirements: IaaS allows customers to meet compliance and regulatory requirements by allowing them to control the configuration of their infrastructure and data.

- **PaaS (Platform as a Service)**
  - Develop, deploy and manage applications quickly and easily: PaaS provides customers with a pre-configured environment for developing, deploying and managing applications, which can help to speed up the development process and reduce the complexity of managing infrastructure.
  - Focus on application development: PaaS allows customers to focus on application development, as they do not need to worry about managing the underlying infrastructure.
  - Scale their applications quickly: PaaS allows customers to scale their applications quickly, as they can provision new resources as needed, without the need for significant upfront investment.
  - Meet specific technical requirements: PaaS allows customers to meet specific technical requirements, as they can choose the programming languages, frameworks, and other software that best meets their needs.
  - Build and deploy microservices: PaaS allows customers to build and deploy microservices, which can help to break down monolithic applications into smaller, more manageable services.
  - Build and run serverless applications: PaaS is a key building block for serverless applications, which allow customers to build and run applications and services without having to manage any servers.

- Utilize pre-built templates, libraries and services: PaaS providers often come with pre-built templates, libraries and services that customers can use to quickly build and deploy their applications.
- Accelerate time-to-market: PaaS accelerates time-to-market by providing customers with pre-configured environments for developing, deploying, and managing applications, which can help to speed up the development process and reduce the complexity of managing infrastructure.

- **SaaS (Software as a Service)**
  - Access software and applications on-demand: SaaS provides customers with on-demand access to software and applications over the internet.
  - Reduce IT costs: SaaS eliminates the need for customers to install, maintain, and update software and applications on their own systems, which can result in significant cost savings.
  - Improve collaboration and communication: SaaS provides customers with tools for collaboration and communication, such as email, document management, and project management software.
  - Increase accessibility: SaaS allows customers to access software and applications from any location with an internet connection, which can improve accessibility and productivity.
  - Meet compliance and regulatory requirements: SaaS providers often have compliance and security certifications that can help customers meet regulatory requirements.
  - Get regular updates and upgrades: SaaS providers often handle software updates and upgrades, which means customers will always have access to the latest version of the software.
  - Get technical support: SaaS providers often offer technical support, which can help customers troubleshoot and resolve issues.
  - Improve scalability: SaaS allows customers to easily scale their usage up or down as needed, which can help to improve scalability and reduce costs.

The difference in each type of service model is the levels of control the user intends to have over the hardware. The following Figure 1 showcases the side-by-side difference between all the service models.

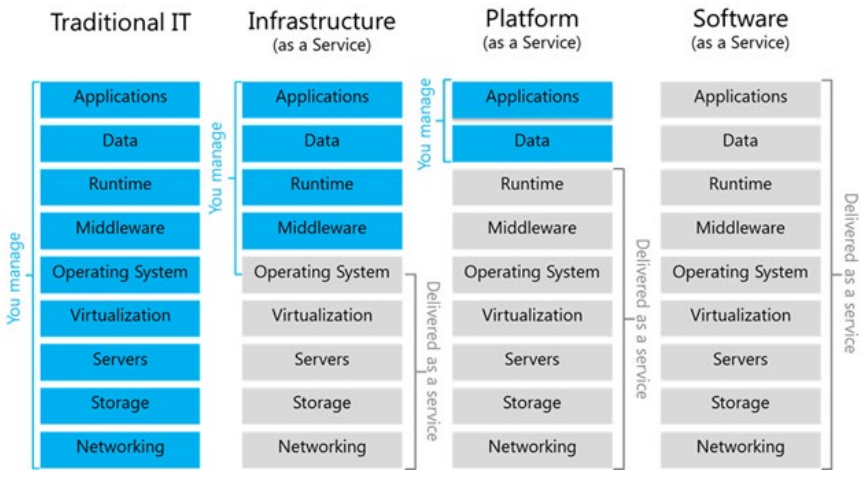


Figure 1: Cloud Service Models

(Source: https://dachou.github.io/2018/09/28/cloud-service-models.html)

3. Cloud Deployment Models

There are three main cloud deployment models:

1. **Public Cloud:** Public cloud deployment is when the cloud infrastructure is owned and operated by a third-party service provider and made available to the general public over the internet. Public clouds are typically operated by large providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Public clouds are known for their scalability, flexibility, and cost-effectiveness.
2. **Private Cloud:** Private cloud deployment is when the cloud infrastructure is owned and operated by a single organization and not made available to the general public. Private clouds can be hosted either on-premises or by a third-party provider and offer more control and customization for organizations with specific security and compliance requirements.
3. **Hybrid Cloud:** Hybrid cloud deployment is when an organization uses a combination of public and private clouds to meet the specific requirements of their workloads. This allows organizations to take advantage of the scalability and cost-effectiveness of public clouds while still maintaining control and security of their private clouds.

Additionally, there are also other models like:

4. **Community Cloud:** Community Cloud is when the cloud infrastructure is shared by a group of organizations with similar requirements, such as those in the same industry or region.
5. **Multi-cloud:** Multi-cloud deployment is when an organization uses multiple cloud providers to host their workloads. This allows organizations to take advantage of the strengths of different cloud providers and avoid vendor lock-in.

Figure 2 showcases the primary models of deployments of the cloud and best summarizes all the different types of Cloud deployment and their differences.

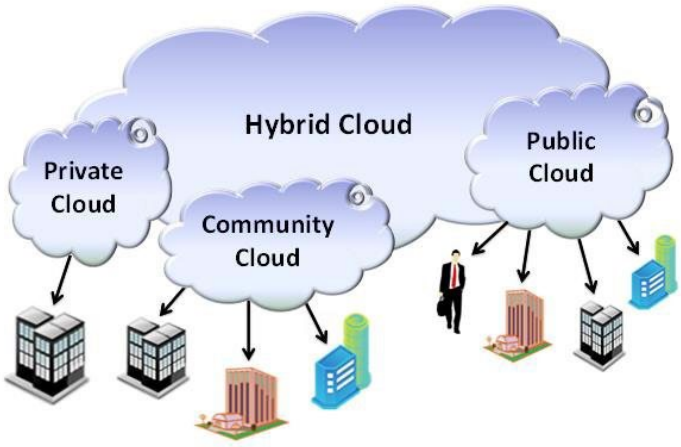


Figure 2: Cloud Deployment Models

(Source: https://www.researchgate.net/figure/Cloud-Computing-Deployment-Models-Mell-and-Grance-2011_fig2_275036700)

The choice of cloud deployment model depends on the specific needs of the organization, including security, compliance, scalability, and cost. Organizations can choose one or more of these models to meet the needs of their workloads and achieve their business goals.

Choosing the right cloud platform for your workloads is a crucial decision for organizations looking to leverage the benefits of cloud computing. With the increasing adoption of cloud computing, organizations now have a wide range of options to choose from when it comes to cloud providers. Each provider offers different services, features, and pricing models, which can make it challenging to determine the best fit for your workload.

When choosing a cloud platform, it's important to consider factors such as security, performance, cost, compliance, and ease of use. Security is a vital consideration, as you want to ensure that your data and workloads are protected against cyber threats and breaches. The cloud provider should have robust security measures in place, such as encryption and secure access, to protect your data and workloads.

Performance, as you want to ensure that your workloads are running optimally and meeting the necessary SLAs. The cloud provider should have the necessary infrastructure and resources to support your workloads and provide the necessary performance and scalability.

Cost, as you want to ensure that the cloud platform is cost-effective, both in terms of the initial deployment and ongoing costs. Cloud providers typically offer different pricing models, such as pay-as-you-go or reserved instances, which can affect the overall cost.

Compliance, as you want to ensure that your workloads are in compliance with relevant regulatory requirements and industry standards. The cloud provider should have the necessary certifications, such as SOC 2, PCI-DSS, and ISO 27001, to support the compliance of your workloads.

Ease of use, as you want to ensure that the cloud platform is easy to use and manage, with the necessary tooling and automation capabilities to manage and maintain your workloads.

When evaluating cloud providers, it's also important to consider their ecosystem, including partners, community support, and third-party services. A robust ecosystem can provide additional services and support for your workloads, as well as the ability to integrate with other services and technologies.

It's important to keep in mind that choosing one cloud platform may not always be the best answer, as many organizations are looking at multi-cloud and hybrid cloud solutions as well, to get the best of all worlds. Multi-cloud allows organizations to use different cloud providers for different workloads, based on their specific requirements, while hybrid cloud allows organizations to use a combination of on-premises and cloud resources.

Multi-cloud and hybrid cloud solutions are becoming more popular for a variety of reasons.

One of the main reasons is the ability to take advantage of the unique features and capabilities of different cloud providers. Each cloud provider has its own strengths and weaknesses, and by using multiple providers, organizations can select the best provider for each workload, based on the specific requirements of the workload. This allows organizations to optimize their IT solutions for cost, performance, and security.

Another reason is the ability to achieve greater availability and redundancy by using multiple cloud providers. By spreading workloads across multiple providers, organizations can reduce the risk of service disruptions and outages and ensure that their workloads are always available to users.

Hybrid cloud solutions, which combine on-premises and cloud resources, also offer several benefits. One of the most important is the ability to keep sensitive data and workloads on-premises while still taking

advantage of the scalability and flexibility of the cloud. This allows organizations to maintain control over their infrastructure while still leveraging the benefits of the cloud.

Additionally, the use of multi-cloud and hybrid cloud solutions also provides more flexibility for organizations in terms of vendor lock-in and geographic location of data. With the use of multiple providers, organizations can avoid vendor lock-in and choose the provider that best fits their needs. Also, with the use of multiple providers, organizations can place their data in the geographic location that best fits their needs, whether it be for regulatory compliance or data sovereignty.

4. Understanding of the Workload

For an appropriate placement of workloads in the cloud one can choose to have 2 approaches, one being the general statistical approach where the user can have a high-level overview of the data and recommend a placement, and the next is the technical consideration.

On a high level let's take a look at what types of workloads are well suited for various types of cloud.

4.1 Workloads in Public Cloud

Characteristics of Workloads that are well suited for the public cloud include those that demonstrate the following features:

- Have low to moderate security requirements.
- Don't handle sensitive data that is regulated.
- Have peak usage or sudden increase in demand.
- Have a need for on-demand, pay-as-you-go resources.
- Have a need for global access to resources.
- Can benefit from the cloud provider's expertise and managed services.
- Have a need for fast deployment and minimal IT overhead.
- Can take advantage of the cloud provider's economy of scale. Examples of such workloads include:
- **Examples:** Web and mobile applications, development and testing, backup and disaster recovery, big data analytics, Media and entertainment, IoT and edge computing, software as a service (SaaS)

4.2 Workloads in Private Cloud

Similarly, taking a look at the Private cloud, characteristics of Workloads that are well suited for the private cloud include those that demonstrate the following features:

Workloads that are well suited for private cloud include those that:

- Have strict security and compliance requirements.
- Handle sensitive data that is regulated (e.g. HIPAA, PCI-DSS).
- Have steady and predictable resource requirements.
- Have a need for dedicated and isolated resources.
- Have a need for full control and customization of the infrastructure.

- Have a need for maintaining legacy applications.
- Have a need for integrating with on-premises infrastructure.
- Have a need for a high degree of availability and disaster recovery Examples of such workloads include:
- **Examples:** Financial services and healthcare, government and defense, Manufacturing and retail, energy and utilities, Business-critical applications, database and storage, Enterprise resource planning (ERP), and customer relationship management (CRM), etc.0

4.3 Workloads in Hybrid Cloud

Finally, Workloads that are well suited for hybrid cloud include those that portray the following characteristics:

- Have a mix of sensitive and non-sensitive data and workloads.
- Have a need for a combination of public and private cloud resources.
- Have a need for integrating with on-premises infrastructure.
- Have a need for a high degree of availability and disaster recovery.
- Have a need for using specific services that are only available in a public cloud while maintaining control over sensitive data on a private cloud.
- Have a need for burst computing capabilities or temporary workloads
- **Examples :** Business-critical applications with sensitive data, backup and disaster recovery, Big data analytics and machine learning, Internet of Things (IoT) and edge computing, virtual desktop infrastructure (VDI).

5. Workload & Placement - Choosing where to deploy a workload:

When deciding on where to place your workloads, the most important thing to consider is your organization's business needs and challenges. Identify the concerns that keep organizational leaders awake at night, such as growth, data control, cost, and IT scale. Use these priorities as a guide in making your decision.

5.1 Business Considerations while Planning

When determining a cloud strategy, it's crucial to take into account the business needs rather than just the technical aspects. Before delving into specific workloads, it's a good idea to review general guidelines that can save you from unnecessary workload analysis. Also, different industries will have different priorities when it comes to business considerations. For instance, in one of the studies carried out by Intel, in the academic sector, it was found that the three main business considerations for workload placement and the right questions to ask are:

- **Compliance:** Are there any laws or regulations that mandate educational institutions to keep data on-premises?
- **Tolerance for compromise:** What is an acceptable level of trade-offs such as a slight decline in performance or listed customization in exchange for a smaller data canter?
- **Risk management:** What level of risk is the organization willing to take? Is the solution able to go offline? Who is responsible for the data in the cloud?

The following are some of the first-hand considerations that are needed to be taken while planning to deploy a workload in the cloud. But added to all these considerations it is also important to consider the technical requirements of the user to accurately performance size the solution.

5.2 Technical Considerations while Planning

The technical consideration can be broadly classified and used as a basic mode of identification of the cloud model as follows:

- **Performance:** High-performance workloads include solutions that prioritize speed and latency for users in specific locations and transactions that require a lot of resources with guaranteed service level agreements.

- **Security:** Some workloads handle sensitive data that could be harmful to the organization if compromised. This rating also takes into account if security solutions are readily available for that specific workload. For example, security solutions for email workloads are well-developed.

- **Integration:** Integration challenges both traditional and cloud migrations. The number and complexity of connections to other systems impact the cost and placement of workloads. Each integration must be evaluated, modified, and refactored to meet the operational level agreement (OLA).

- **Data Volume:** Data size and location are the main factors to consider when moving data. Large datasets can be difficult to transfer over long distances. For example, it would be too expensive and time-consuming to transmit and store network log data for analytics externally.

The technical consideration stated above helps the planning team immensely in paving a direction to understand the thought process required to decide. Based on the studies by Intel, the following Figure 3 showcases how a team can look into nature of the system and take data-driven decisions on choosing the appropriate cloud.

Attribute	Public Cloud Indicators	Private/Hybrid Cloud Indicators
Organization Size and Maturity	• Small or startup organization • Little or no IT infrastructure • Limited in-house IT investment	• Large or mature organization • 500+ physical servers running at 50%+ capacity • Large in-house IT investment
IT Engineering Team	• Little or no in-house IT support • Limited cloud expertise available	• Large in-house IT support • Deep cloud technical bench
Financial Strategy	• OPEX or subscription/payments preferred • No funding for initial data center deployment • Lighter data volumes • Mainstream business processes	• CAPEX and depreciation preferred • Large IT/capital budget • Large data volumes • Many customized business processes
End-User Location	• Global customer base – requires global entry point for applications and operations • End-user latency concerns – customers in remote locations • Funding multiple data centers is not cost effective	• Country restrictions on Internet – private WAN connection to private data center required • End-user locations do not contribute to latency concerns • Large corporation with global but consolidated end-user locations – multiple private data centers are cost effective • Data sovereignty restrictions
Compliance and Control Regulations	• No or low regulations or compliance requirements	• Major regulations or compliance requirements • Data sovereignty restrictions (PII or controlled technology)
Service Level Agreement (SLA) Flexibility	• Flexible SLAs • Risk-accepting of Internet/service provider failures • Contract can be placed to penalize providers for latency/downtime or to ensure redundancy	• Restrictive SLAs or 100% availability required at all times • Risk-adverse to SLA failures – trust private infrastructure over the Internet/service providers
Business Asset Control (Risk) Tolerance	• Organization trusts third parties to manage data • Business policies permit data residing outside the firewall	• Requires absolute control of business data and intellectual property (IP) • Failing to maintain IP and data control may result in the loss of critical business assets

Figure 3: Business Considerations stated by Intel

(Source https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/optimal-workload-placement-for-public-hybrid-and-private-clouds-white-paper.pdf)

Apart from both the type of considerations, it is also recommended to have an ecosystem consideration approach that would increase the level of accuracy of the solution being proposed for the user.

5.3 Technical Considerations while Planning

The ecosystem considerations that need to be considered are below mentions the questions that one should encounter in the process of planning while considering a cloud solution for their business use case. The following are some of the questions a user can have as a checklist to visit:

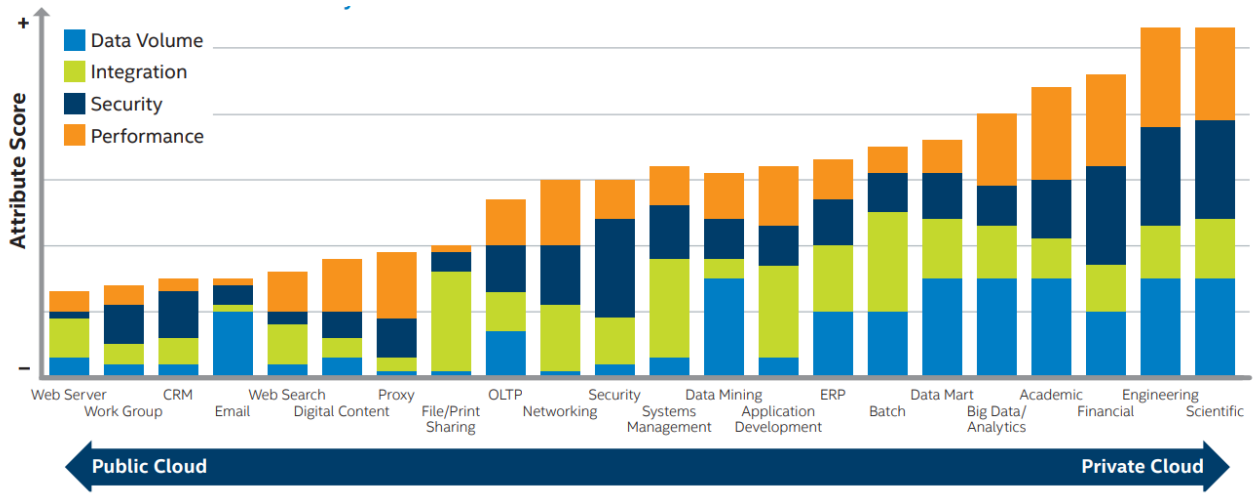
1. **Provider ecosystem:** Does the chosen deployment location have a robust ecosystem of partners, such as ISVs, system integrators, and managed service providers, that can provide additional services and support for the workload?
2. **Community support:** Is there a strong community of developers and users that can provide support and assistance for the workload?
3. **Tooling and automation:** Does the chosen deployment location provide the necessary tooling and automation capabilities to manage and maintain the workload?
4. **Integration with other services:** Does the chosen deployment location have the ability to integrate with other services such as CDN, DNS, and Identity and Access Management (IAM) to support the workload?

5. **Third-party services:** Does the chosen deployment location have a wide range of third-party services that can be easily integrated with the workload, such as databases or analytics services?
6. **Compliance and certifications:** Does the chosen deployment location have the necessary compliance and certifications, such as SOC 2, PCI-DSS, and ISO 27001, to support the workload?
7. **Interoperability:** Will the chosen deployment location be able to integrate with existing systems and technologies, and does it support the necessary APIs and standards?
8. **Marketplaces:** Does the chosen deployment location have a marketplace, where you can find and use other software and services, to support the workload?

6. Decision Criteria

Upon careful consideration and validation, the business use case, application, and the nature of the business against the above-mentioned various different consideration types help the user land on an appropriate solution that would help them get the best out of the cloud deployment choice they make.

One can compare their business consideration, technical consideration, and Ecosystem consideration against their application to take data drive decisions. As per the survey and studies done by intel, the following Graph 1 represents the broad classification of how the cloud should be adopted depending on its type and performance requirement.



Graph 1: Affinity Model for Public Versus Private Workload Placement

6.1 The future of data center solution design

The future of data center solution design is likely to be shaped by several trends and technologies, including:

1. Edge computing: With the rise of IoT and the need for low latency, data processing and analysis is moving closer to the edge devices, this will increase the demand for edge data centers.
2. Containerization and Kubernetes: Containerization and Kubernetes are becoming increasingly popular for deploying and managing applications in data centers, this will enable more efficient use of resources and improved scalability.
3. Artificial intelligence and machine learning: AI and machine learning will play an increasingly important role in data center management, providing insights into performance, security, and optimization.
4. Software-Defined Data Center (SDDC): Software-Defined Data Center (SDDC) solutions will provide more flexibility, scalability and automation capabilities, allowing companies to more easily adapt to changing workloads and business needs.
5. Power and Cooling optimization: New technologies in power and cooling, like liquid cooling, will lead to more energy efficient data centers that produce less heat.
6. Security: Security will be a critical aspect of data center design, with a focus on protecting against cyber threats, data breaches and compliance requirements.
7. Interconnectivity: Interconnectivity will be a key aspect of data center design as the increased use of cloud services and edge computing will require more efficient communication between data centers.
8. 5G integration: 5G networks will enable faster data transfer, low latency and high-density connections, this will open up new opportunities for data centers and network infrastructure.

Overall, the future of data center design is likely to focus on increasing efficiency, scalability, and security while reducing costs. The use of advanced technologies such as AI, containerization, and software-defined solutions will play a key role in achieving these goals.

7. Conclusion:

Multi-cloud and hybrid cloud solutions are becoming more popular as they allow organizations to take advantage of the unique features and capabilities of different cloud providers, achieve greater availability and redundancy, maintain control over sensitive data and workloads, and provide flexibility in terms of vendor lock-in and geographic location of data. Building an IT solution for your workload is a complex process that requires careful planning and execution.

The solution should be designed to meet the specific needs of your organization, while also providing the necessary flexibility and scalability to adapt to changing requirements. It's important to ensure that the IT solution is secure, and it is also important to keep in mind the compliance and regulatory requirements that might be imposed on the specific industry of the workload.

Ultimately, the best choice of where to deploy a workload will depend on the specific requirements of the workload and the resources available. A thorough evaluation and comparison of different deployment options should be done, considering the desired performance, scalability, security, and cost-efficiency of the system. Following the decision criteria as mentioned will help to ensure that the chosen deployment location is the best fit for the workload and the business, meeting both current and future requirements. This whitepaper intends to serve as a technical documentation or handbook that can act as a one-stop destination for having a checklist for discovery, analyze, and deciding of placing the workload appropriately in the Cloud.

8. Reference:

a. https://dachou.github.io/2018/09/28/cloud-service-models.html
b. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/optimal-workload-placement-for-public-hybrid-and-private-clouds-white-paper.pdf
c. https://www.researchgate.net/figure/Cloud-Computing-Deployment-Models-Mell-and-Grance-2011_fig2_275036700