PUBLIC CLOUD DEPLOYMENT MODELS AND THEIR CASES

Public cloud adoption

Public cloud adoption has soared since the launch of the first commercial cloud two decades ago. Most of us take for granted the countless ways public cloud-related services—social media sites (Instagram), video streaming services (Netflix), web-based email applications (Gmail), and more—permeate our lives.

In the business sphere, both large enterprises and small startups depend on public cloud computing models to provide the flexibility, cost-effectiveness and scalability needed to fuel business growth. According to an International Data Corporation (IDC) report (link resides outside ibm.com), worldwide spending on public cloud provider services will reach $1.35 trillion in 2027.

Here, we explore 10 top business use cases that reveal how a public cloud helps form the foundation for modern business and fuels ongoing digital transformation.

Public Cloud models typically involved third-party providers that host the infrastructure, software, and applications in shared data centers. These providers own, operate, and manage the hardware, reducing the on-premises equipment required.

What is a public cloud?

A public cloud is a type of cloud computing in which a third-party service provider (e.g., Amazon Web Services (AWS), Google Cloud Platform, IBM Cloud or Microsoft Azure) makes computing resources (e.g., ready-to-use software applications, virtual machines (VMs), enterprise-grade infrastructures and development platforms) available to users over the public internet on a pay-per-usage basis. Moreover, a public cloud model enables companies to automatically scale compute and storage resources up or down (along with data security measures and services) to meet their individual needs.

The public cloud is the most widely used model. It allows users to access a vast range of cloud-based services.

How does public cloud computing work?

In a public cloud computing model, a cloud service provider (CSP) owns and operates vast physical data centers that run client workloads. Public cloud environments are multi-tenant, where users share a pool of virtual resources automatically provisioned for and allocated to individual tenants through a self-service API interface. Multi-tenant hosting allows cloud service providers to maximize utilization of their data centers and infrastructure resources to offer services at much lower costs than a company-owned, on-premises data center.

Cloud service providers are also responsible for all hardware maintenance and for providing high-bandwidth network connectivity to ensure rapid access and exchange of applications and data. They also manage the underlying virtualization of servers, operating system software networking and other infrastructure that power a public cloud data center and maximize data center resources. For instance, with virtualization, one physical server can be split into multiple, distinct virtual servers that serve different clients.

All major public cloud providers continuously update and maintain their infrastructure and leverage the highest data protection and security requirements to prevent data breaches.

Additionally, they offer numerous cloud security tools and solutions like identity and access management (IAM), data loss prevention (DLP), and security information and event management (SIEM).

Finally, a service level agreement (SLA) defines the relationship between a CSP and a client and covers the performance, availability and manageability of cloud services.

Public cloud service models

Today's cloud providers offer hundreds of managed services and tools across four main categories. These services are not mutually exclusive; most large organizations use all four to create a modern IT cloud computing environment.

Software-as-a-Service (SaaS) is on-demand access to ready-to-use, cloud-hosted application software.

Platform-as-a-Service (PaaS) is a complete cloud platform—hardware, software and infrastructure—for developing, running and managing applications.

Infrastructure-as-a-Service (IaaS) is a cloud computing model that delivers fundamental compute, network and storage resources.

Serverless computing (serverless) is a cloud computing model that offloads all the back-end infrastructure management tasks—including provisioning, scaling, scheduling and patching—to the cloud provider.

Benefits of a public cloud

The following are some of the benefits that organizations can enjoy if they employ a public cloud solution:

I. **Cost-effectiveness:** Reduce spending on hardware and on-premises infrastructures with pay-per-usage or subscription pricing models.
II. **Efficiency:** Eliminate wasted resources by paying only for what you use.
III. **Elasticity:** Automatically add capacity in response to unexpected surges in traffic (e.g., e-commerce flash sales).
IV. **Scalability:** Effectively increase workloads by upgrading the capabilities of existing resources (scaling up) or incorporating additional resources to share the load (scaling out).
V. **Innovation:** Access cutting-edge technologies (e.g., artificial intelligence (AI), edge computing, the Internet of Things (IoT)).
VI. **Spending predictability:** Experience more predictable ongoing operating expenses to achieve lower costs for overall IT spending.
VII. **Team collaboration:** Access public cloud resources from anywhere and allow teams to communicate with each other across distributed locations in real time for faster outcomes.
VIII. **High availability and reliability:** Achieve less downtime and ensure data resilience with automatic backup and disaster recovery.
IX. **Sustainability:** Enhance energy efficiency through pooled CSP resources to reduce your carbon footprint.

The top public cloud use cases

Here are 10 ways businesses leverage public cloud computing services to achieve cost savings, innovation and overall business growth.

1. Storage

Public cloud storage consists of storage capacity and technology as-a-service, which helps organizations reduce or eliminate the capital costs of building and maintaining in-house storage capabilities. By storing the same company data on multiple machines, cloud storage offers the redundancy needed to support business continuity in the face of a natural disaster, an outage or other emergencies.

2. Dynamic resource allocation

A public cloud gives companies the elasticity to scale resources up or down depending on business needs. For instance, an e-commerce site with highly seasonal sales can quickly expand its online services with a public cloud. They only pay for added capacity during peak periods and then can scale back down during regular sales.

3. Development and testing

A public cloud setting offers an ideal environment for developing and testing new applications compared to the traditional waterfall method, which can be far costlier and more time-consuming. For instance, in just minutes, developers can provision testing environments on public cloud-based virtual machines (VMs). When developers finish using a testing environment, they can easily take it down.

4. Cloud-native applications and DevOps

A public cloud setting supports cloud-native applications—software programs that consist of multiple small, interdependent services called microservices, a crucial part of DevOps practices. Developers use DevOp tools to automate cloud-native development and rapid delivery of high-quality software, building containerized applications once and deploying them anywhere.

5. Low code

Low code is a visual approach to software featuring a graphical user interface with drag-and-drop features that support the automation of the development process. Low-code platforms democratize app development for “citizen” developers—users with little formal coding experience. Low code helps businesses streamline workflows and accelerate the development of websites and mobile apps, the integration of external plugins, and cloud-based next-gen technologies, like artificial intelligence (AI) and machine learning (ML).

6. Analytics

With the rise of data collected from mobile phones, the Internet of Things (IoT), and other smart devices, companies need to analyze data more quickly than ever before. Big data analytics—the use of advanced analytic techniques against very large, diverse big data sets—has become crucial to business success. A public cloud environment provides the computing and networking infrastructure needed to support big data so companies can make faster data-driven decisions and deliver better customer experiences in real-time and at scale.

7. Hybrid multi cloud strategy

A public cloud is pivotal to a hybrid multi cloud strategy. By integrating public cloud services with private cloud or on-premises infrastructure, organizations can choose where to run workloads and select the best services from different CSPs. For instance, a financial institution may want to use the public cloud to test and develop new applications while deploying workloads sensitive to fraud and subject to regulation on a private cloud hosted by a dedicated CSP.

8. Generative AI

With its massive need for compute, storage and networking capabilities, generative AI needs the cloud to process data in real-time and at scale. Public cloud providers offer companies the capability to access data and harness processing power from multiple distributed data centers that can support generative AI workloads.

9. Edge computing

Edge computing brings enterprise applications closer to data sources (e.g., mobile phones, sensors, IoT, devices or local edge servers) for faster insights, improved response times and better bandwidth. For instance, edge devices help monitor power grid operations to reduce energy waste in the energy sector. A public cloud works synergistically with edge services by connecting them to a centralized public cloud or other edge data centers. Most often, only the most relevant data is processed at the edge. In contrast, less critical data is sent to a primary public cloud data center for processing, freeing up computing resources to ensure low latency.

10. Quantum computing

Quantum computing uses computer hardware, algorithms and other quantum mechanics technology to solve complex problems. While quantum computing for business is still in its early stages, organizations in industries that require vast computing capabilities (e.g., chemistry, biology, healthcare, finance) are beginning to tap into quantum's potential to transform the way they do business. Today's public cloud service providers have started to offer services involving renting quantum machines, platforms for developing utility-scale quantum algorithms and applications and more.

PRIVATE CLOUD DEPLOYMENT MODELS AND THEIR CASES

Instead of owning and maintaining physical servers, cloud technology has given us the opportunity of leveraging computing resources over the internet with flexibility in payment modes, scalability, adaptability, and easier deployment on a secure worldwide server. Public, Private, and Hybrid Clouds are the different cloud deployment models in cloud computing. Consider industry-recognized cloud certifications to boost career prospects. Research AWS Solutions Architect certification costs based on desired level. Private Cloud is better to use when: Sensitive data control and security are required. Customization is required in terms of compute, storage, or networking for the deployment of any business logic.

What is a Private Cloud?

Private Cloud definition: A private cloud deployment model can be defined as a model wherein the IT resources are dedicated to a single organization. It is a single-tenant infrastructure. It is like an internal server of a company, only users within that company can access the resources. They require allocations of space, hardware, and environmental controls. It is like a personal cloud for the organization.

1. Internal Private Cloud

An internal private cloud is present at the organization's local data center. All the resources are owned by the organization itself. This allows more control over the resources of the organization. The capital expenditure in this model is high. It is difficult to scale and offers higher latencies as servers are deployed on-premises.

2. External Private Cloud

An external private cloud is hosted by a third-party cloud provider for the organization. They dedicate resources on behalf of the organization. This gives lesser control to the organization. The capital expenditure in this model is low and expenses are variable. It is easy to scale and offers lower latencies as servers can be deployed in different locations.

How Does a Private Cloud Work?

Private cloud computing follows a single tenancy, only one organization or customer has access to it. This also increases resource availability. Internal Private Cloud will not be connected to the internet as it is on-premises, and it can be connected through internal networks like data centers. Whereas External Private Cloud can establish connectivity over the public internet but over a VPN (Virtual Private Network), Fiber, or Ethernet. When considering a career in Cloud computing, it is important to keep in mind that obtaining a strong foundation in the fundamentals of Cloud Computing is crucial.

Private Cloud Architecture

A private cloud server is also based on technologies followed by other clouds such as public clouds which allow virtualizing IT resources to quickly scale and improve availability. Private cloud providers allow users to architect data centers using Virtual Machines, Containers, and Software Defined Networks instead of physical servers. They provide on-demand management of all the IT resources such as compute, storage, and network. To achieve this, a private cloud gets support from these technologies:

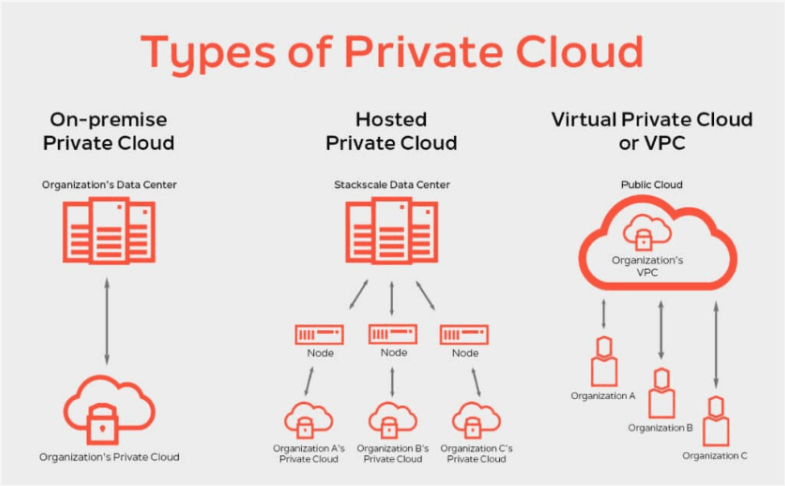
I. **Virtualization:** Virtualization is a means to create a virtual version of a device or resource, such as — Server, Storage, Network, or OS where the framework divides the resources into one or more execution environments. Devices, Applications, and Human Beings can interact with the virtual resource as if it were a single logical resource.

II. **Management software:** Management software provided by cloud server companies help the cloud administrator to monitor and manage the underlying infrastructure as well as the workloads above it having the business logic. It helps in scheduling tasks related to security, provisioning, scaling, etc.

III. **Automation:** If 10 identical complex servers need to be provisioned and there is no automated method available for it, it can become tedious. Automation reduces the need for it. The same process can be automated, and human resources can be useful for other tasks.

A private cloud can also leverage DevOps and cloud-native practices to maximize agility.

Private Cloud Services and Types



1. Virtual Private Cloud

It is simply a virtual network dedicated to one organization or user in a public cloud. It can be termed a Network-As-A-Service by the public cloud providers. Organizations can create logically isolated data centers and labs within them. Any computer resource deployed will be part of this customized private IP subnet or lab. The underlying infrastructure is maintained by the cloud provider itself. Organizations can access the resources within this subnet over a secured VPN connection. Examples of Virtual Private Cloud are – Amazon VPC, Google Cloud Platform (GCP) VPC, and IBM Cloud VPC.

2. Managed Private Cloud

In a managed private cloud, the hardware and software are owned by the organization. It can be on-premises or off-premises. However, the entire management, operation, and maintenance tasks of the cloud are outsourced to external private cloud providers.

3. Hosted Private Cloud

In a hosted private cloud, cloud providers provide isolated servers in their data centers. The cloud provider is responsible for the hardware, software, network, and security of the infrastructure. Labor and maintenance costs to the organization get reduced in this model.

4. On-Premises Private Cloud

On-premises private cloud allows users to host servers locally in data centers. It provides high security because the boundary of physical and logical accessibility is only within the organization.

Benefits of Private Cloud

I. It is easier to provide isolation and control into the infrastructure consisting of compute, storage, and network resources of a particular organization.
II. Since the resources are isolated, it provides greater data security and integrity. It offers private cloud storage.
III. Budgeting becomes easier for a company while using a private cloud, public clouds cannot be predicted.
IV. Since there is no resource or bandwidth sharing with any other organization or user, performance becomes better for a particular organization's workload.
V. It provides scope for customizing software and hardware requirements which is not provided at a high scale in a public cloud.
VI. Though the upfront capital expenditure is huge, there is a long-term pay-off benefit as subscription cost gets cut.
VII. Any industry and regulatory compliance are not forced upon private cloud users as in the case of a public cloud. Private clouds can decide this.
VIII. Organizations can easily adopt some of the public cloud functionalities in the future and shift to a hybrid cloud model.

Disadvantages of Private Cloud

- High upfront capital expenditure is required to set up physical data centers and servers.
- On-demand scaling is difficult and costly.
- Availability is very difficult to achieve. The area of operation is restricted.
- Since the entire infrastructure and workload management must be done by the organization itself, it can become cumbersome. A highly skilled IT team must be recruited to architect and manage it.
- The organization is accountable for any sort of inconsistency and not the cloud provider.

Reasons for Popularity of Private Cloud Environments

A private cloud is suitable to use when:

1. There is a requirement for high security for sensitive data as the resources in a private cloud can be accessed only by trusted people within an organization. It is not accessible over the public internet.
2. The organization requires high control and more isolation in the system and resources.
3. A high level of resource customization is required for any business logic. Since the infrastructure is dedicated, it becomes easier to customize.
4. Predictable costs are required. Public cloud costing can be unpredictable based on usage.

Major Private Cloud Vendors

Some of the major private cloud vendors are:

1. **Amazon Virtual Private Cloud (VPC):** It is a virtual network dedicated to one's AWS account. Private EC2 instances can be launched on this VPC. While there is no additional charge for creating and using an Amazon Virtual Private Cloud (VPC) itself, one can pay for optional VPC capabilities with usage-based charges.
2. **Hewlett Packard Enterprise (HPE):** HPE provides software-driven private cloud architecture solutions. Organizations can compose any workload, and any service, all while reducing infrastructure cost and complexity.
3. **VMware:** VMware's private cloud solution allows organizations to architect data centers using Virtual Machines and a Software Defined Network. ***There are three types of private cloud which VMware provides - Managed Private Cloud, Hosted Private Cloud, and Virtual Private Cloud.***
4. **IBM Cloud:** IBM's private cloud solutions include IBM Cloud Pak System, IBM Cloud Private, IBM Storage, and Cloud Orchestrator.

HYBRID CLOUD DEPLOYMENT MODELS AND THEIR CASES

What Is Hybrid Cloud?

A hybrid cloud is a computing environment that combines hardware and software running in a company's on-premises data center with computing capacity in a public cloud run by a third-party provider. Most organizations will establish governance, security, and privacy policies that apply across the IT systems they use, including on-premises and public cloud–based resources. The tools used to instantiate these high-level policies will vary; public cloud providers share the management burden of networks and compute and storage resources with their customers, whereas on-premises systems are managed by the organization's internal staff.

Hybrid cloud is a widely used description, but it isn't a term of art with a precise meaning—think of it as IT's catchall for "some stuff in the cloud and some stuff in my data center."

The hybrid cloud concept is a broad one that can include a variety of systems, configurations, and methods of control. More-specific terms are commonly used to describe variations that still qualify as hybrid cloud.

Distributed cloud, for example, is a model that distributes public cloud services across multiple geographic locations. This allows enterprises to take advantage of the distributed nature of public cloud infrastructure while still managing operations, governance, and updates centrally.

Multicloud is another important and growing facet of the hybrid cloud model. Companies with a multicloud strategy use two or more clouds, picking the best option for any given workload. This can mean choosing offerings from different cloud providers as well as leveraging systems in the company's own data centers.

These and other refinements show how a hybrid cloud approach, widely accepted as a viable strategy, is being implemented using many different architectures and deployment models.

Key Takeaways

- A hybrid cloud lets a company use both its on-premises data centers and multiple clouds, connecting the environments with shared management, security, and governance policies and simplified data integration.
- A hybrid cloud can let companies tap some of the best features of the public cloud, such as accessing the most up-to-date technology and responding quickly to new business needs, while keeping the control afforded by an on-premises data center.
- Companies choose hybrid clouds instead of a 100% cloud deployment for a variety of reasons, including data residency rules, an interest in a phased cloud migration, a need for low latency, and compliance with certain regulations.
- Hybrid clouds come in a wide range of deployment models.

Hybrid Cloud Explained

A hybrid cloud connects a company's on-premises hardware and software with computing capacity from cloud providers. Companies often engage multiple public cloud providers. These cloud and on-premises computing environments generally share some level of common management and security policies as well as the ability to integrate applications regardless of where they run.

Public cloud computing resources can include software-as-a-service applications, such as ERP or CRM apps, or infrastructure as a service and platform as a service, such as compute, storage, databases, and development environments. On-premises resources span the same gamut. For example, the on-premises data center might support legacy applications that still do their jobs but need to be integrated with a cloud application, such as a legacy billing system that needs to share data with a cloud-based CRM app. Or an on-premises ecommerce app might rely on a public cloud for bursts of extra capacity if customer demand spikes.

How Does Hybrid Cloud Work?

Cloud and on-premises computing environments work together in a hybrid cloud architecture. Hybrid cloud is a broad term, encompassing a range of cloud and on-premises software and infrastructure that are integrated in some way and exchange data.

Hybrid usually implies a shared management responsibility between the public cloud provider and in-house IT staff. For example, in a cloud setup where services are managed remotely by the provider but reside in a company's own data center, the in-house IT team manages the power, cooling, and operations of that data center, while the public cloud provider handles the maintenance and updates of certain hardware and software depending on the services being offered—SaaS, PaaS, IaaS or some combination of the three.

Management systems can provide a high-level view of a hybrid cloud environment, letting system managers monitor the interconnected nodes. Systems are also linked with shared security, networking, and data integration policies and approaches, which the company's IT architects must establish. System managers will still use the vendor's tools in each environment to configure and troubleshoot each element of the hybrid cloud.

Why Use Hybrid Cloud?

Organizations prefer hybrid clouds for a variety of reasons. Some intend for the mix of cloud and on-premises resources to be temporary as they incrementally move computing workloads to one or, more likely, multiple public cloud providers. The goal is to exit their on-premises data centers entirely, using a phased approach.

Other companies plan to keep a hybrid cloud setup indefinitely. Concerns about data residency requirements and control policies are one big reason. Some companies are comfortable letting many or even most applications and databases live in the public cloud, but certain customer data or product development information, for example, might need to stay on-premises, either by regulation or company policy.

Organizations may also have applications they feel are best kept on-premises. While they may decide to move many applications to SaaS—such as ERP, human resources, and CRM apps—there are often niche or custom legacy applications that they decide to leave on-premises and that must communicate with their cloud systems.

Bandwidth concerns are another reason companies choose hybrid clouds. If they have a certain application or workload that's particularly unforgiving of latency, and their operations aren't located close enough geographically to a cloud data center to remove that lag, keeping the system onsite makes sense.

Benefits of Hybrid Cloud

A hybrid cloud lets a company choose what elements they like about public cloud or on-premises operations and which tradeoffs they find acceptable. The growing range of hybrid deployment model options available lets companies align this mix of cloud and on-premises services even more closely with their needs. The following are some of the benefits of a hybrid cloud:

- Increased control. Some companies aren't comfortable ceding direct control for certain data or computing workloads to a third-party provider. Areas of concern include the physical control of storage and backup systems, decisions about infrastructure configurations, and the control of applications used to run a business process. The numerous hybrid cloud models now available mean companies can granularly address specific data and resource management needs to retain the desired control while getting many benefits of the cloud.
- Data residency. Data residency is a powerful reason for choosing a hybrid cloud. With a hybrid cloud, an organization can meet its data residency requirements by keeping data either on its premises or within a specific country's borders while still gaining some benefits of the public cloud.
- Regulatory compliance. Beyond data residency, using public cloud environments for select operations can help companies meet certain compliance attestations, such as the Payment Card Industry Data Security Standard (PCI DSS) for processing credit cards, Health Insurance Portability and Accountability Act (HIPAA) rules for patient privacy, the General Data Protection Regulation (GDPR), and even security standards such as the US's FedRAMP federal government standard.
- Improved security. Public cloud providers can devote far more money and specially trained people to security monitoring and updates than almost any individual company. While an organization's IT team shares the security responsibility for data in a public cloud, working with a hyperscale provider improves the odds that a system will be patched against the latest threats. A hybrid environment lets a company tap cloud-based security advantages for a swath of workloads, even if some of their computing environment needs to stay in an on-premises data center for control, latency, or other reasons.
- Cost optimization. A hybrid cloud gives a company an always-on test case that lets them constantly compare the cost of running applications in-house versus in a public cloud. On-premises systems are capital-intensive investments, and a hybrid setup allows organizations to convert some computing costs from capital expenses to more predictable operating expenses. The public cloud element also lets a company pay only for what they use, which is especially valuable for workloads with variable demand for resources.

- Responsiveness to business needs.Public clouds let IT teams quickly add capacity to meet a new or recurring business need. For example, using a public cloud can allow an organization to add elastic capacity—so-called "cloud bursting"—to let an on-premises system handle a spike in demand, or add new development environments in minutes or hours instead of the weeks it might take in-house, or get a SaaS application up and running much faster than a conventional on-premises application could be installed and configured.
- Access to the latest technologies, including AI. Connecting public cloud services to an on-premises data center can give a team access to technology innovations. For example, public cloud services can provide the kind of high performance computing needed to train an AI model on a massive data set, without the company having to buy hardware up front that it might not need on an ongoing basis.
- Multicloud options. A multicloud environment lets a company choose the right public cloud for any given workload based on that cloud's capabilities and cost. It gives IT leaders choice and leverage with third-party providers. A multicloud approach doesn't require a hybrid cloud setup—a company could run all its workloads on multiple public clouds—but companies often use a multicloud environment with an on-premises data center in hybrid strategies.
- Disaster recovery and risk reduction. Using at least two environments for computing—on-premises and a public cloud—creates a level of built-in risk reduction and can make disaster recovery planning simpler.

Hybrid Cloud Challenges

An on-premises data center comes with significant fixed costs—owning or leasing a building, acquiring and maintaining hardware, and employing skilled staff to run and maintain the infrastructure and applications. Public cloud services bring their own limitations, such as concerns about data residency and control. And while a hybrid strategy offers several benefits, it also brings unique challenges, including the following:

- **Data residency**. Data residency rules vary, and some require that select data remain in a country or region. That adds compliance complexity as companies must track where in the public cloud regulated data is stored. The answer is often to keep sensitive information on-premises to guarantee compliance. The key is to be thoughtful about where sensitive or regulated data will reside.
- **Costs:** Holding on to an on-premises data center means a company bears the building, maintenance, power, cooling, and personnel costs to keep the facility running. Having an on-premises data center plus multiple cloud providers can make total technology cost assessments complicated for a given process.
- **Management:** Each environment will tend to have its own management tools, nomenclature, and control points. IT staff tasked with monitoring and managing systems will need to be expert in managing both the on-premises and cloud environments.
- **Integration:** Companies can struggle to effectively connect their on-premises environments and public clouds for interoperability and to manage the related APIs needed to keep the integration working effectively. Release management becomes more challenging as API changes in the cloud or on-premises can break integrations.
- **Developer complexity:** Especially for companies using DevOps tactics such as continuous integration/continuous deployment, working in a complex hybrid cloud can create

complications for developers in areas such as making sure deployments go to the right cloud or on-premises environment, having sufficient capacity in the environment, and meeting testing and compliance requirements.

- **Data transport:** IT teams might talk about this as "data gravity," which refers to considering where the bulk of the existing data resides. It's often less expensive and simpler to put any applications or hardware related to data in the same location. Moving data among owned and cloud data centers takes time and may incur data egress charges.

Building a Hybrid Cloud

There are huge variations in how IT teams build their hybrid clouds. When it comes to connecting SaaS and on-premises applications, integration service providers offer a variety of connectors and integration platforms to allow for data sharing.

When it comes to connecting the networks that make up a hybrid cloud, including the on-premises data center, the IT team has two main options: a VPN, which goes over the public internet and is encrypted, or a dedicated connection, which comes with bandwidth guarantees.

Layered across these choices is the need to design with a clear understanding of what elements the in-house team controls and which are the responsibility of the cloud provider. Who's responsible for monitoring a given service, and what's the protocol if there's a problem? Many areas involve a shared responsibility. An example is security, where an in-house team might set certain standards and a cloud provider might be accountable for implementing and monitoring to those standards.

Hybrid Cloud Management

Hybrid cloud management approaches vary. Major cloud providers offer hybrid management systems that let IT teams look at the performance of both their public cloud environments and their on-premises systems within certain parameters. Some in-house IT teams use a software layer not from the public cloud provider, such as VMware, to manage compute, storage, and networking across locations and clouds. Others treat Kubernetes, an open source system for managing containerized applications, as this layer.

There are also cloud management platforms created specifically to manage some aspect of setting up, running, or monitoring multiple environments. With any of these approaches, it's critical to map workloads to specific clouds, set up service level agreements (SLAs) and security protocols for each workload, and develop a corresponding monitoring and incident response strategy.

There will be a security layer between internal and external systems, which must be factored into a management plan. Look for the ability to set up a central dashboard that offers visibility into all elements of the hybrid infrastructure—this is critical for effective management.

Hybrid Cloud Use Cases

Hybrid clouds can range from the very simple, such as an environment connecting a cloud ERP with an on-premises inventory system, to the complex—for example, a sophisticated multicloud environment running a wide range of computing workloads. Here's a sampling of hybrid cloud use cases.

- **Public cloud migration.** A hybrid cloud can offer a temporary configuration as a company steadily moves all its computing architecture to a public cloud, with the long-term goal of leaving its on-premises data center. A complete move like that can take years and requires a well-thought-out hybrid strategy in the interim.
- **Data residency.** When data needs to stay in a particular country or region, companies are sometimes most comfortable keeping it on-premises. To do that, one approach is to use public cloud resources inside a company's own data center.
- **Application development.** Companies often do app dev work and testing using on-premises environments, then move applications to a public cloud to run in production. The opposite is also common. For the transition from on-premises to the cloud to work, those environments need to be configured and behave the same for everything from APIs to operating systems. Packaging applications in containers typically addresses most environment dependencies.
- **Legacy applications.** While many legacy applications are being replaced by SaaS, other long-serving apps remain on-premises. A hybrid cloud lets those on-premises and cloud apps share data as needed.
- **Emerging technology.** A public cloud lets a company quickly benefit from the latest technology advances, such as using cloud resources for the computing power to train an AI algorithm. A hybrid environment provides access to those resources without a cost-prohibitive capital investment and lets those resources draw on training data from on-premises systems if needed.
- **Application integration.** Companies often need to integrate some on-premises applications—say, an inventory management or a point-of-sale system—with cloud-based ERP and financial systems.
- **Unified platform.** Some companies are very motivated to use a single platform, such as VMware, to run all IT infrastructure elements, and a hybrid cloud architecture lets them do this on-premises and in the cloud. Container systems such as Kubernetes can also be used to homogenize operations.
- **Disaster recovery.** With a hybrid cloud, on-premises and public cloud resources can be fine-tuned to meet an organization's unique disaster recovery and business continuity needs.
- **Shared service.** For services such as user identity, authentication, and access governance, companies might use a cloud service that applies to both cloud and on-premises applications alike.

Hybrid Cloud Examples

- A global bank might migrate databases from conventional on-premises data centers to servers that are managed by a cloud provider but reside inside the bank's own data centers.

This setup keeps certain data on-premises so the firm can continue complying with European data protection rules. The bank could then run some applications in its conventional on-premises data center, run some in the provider-managed environment in its data center, and shift some workloads to a second public cloud.

- In contrast, a technology company that's growing fast could run some applications on a public cloud and integrate those with on-premises instances of ERP, inventory management, and lifecycle management solutions while it takes steps into cloud native application development.
- Or consider a cyber-security company with thousands of customers globally that relies on on-premises colocation centers for computing infrastructure and plans to continue expanding into new market segments. It might choose to run select workloads on a public cloud to gain flexibility and the ability to handle bursts of demand.