WHAT IS A CLOUD SERVICE PROVIDER? CSPS EXPLAINED

The cloud has become the primary vehicle for IT infrastructure for many companies. Initial skepticism about handing over control to another party has largely melted away. Today's cloud-first approach is being driven by its many benefits, including the quick deployment of IT infrastructure without the need for a large upfront capital investment and the ability to support remote workers.

Spending on cloud services grew 20.4% in 2024, to total $675.4 billion, up from $561 billion in 2023, according to Gartner. The ability for companies to use new technologies like AI, new software engineering methods like containerization, and greater flexibility with DevOps approaches like Agile, are driving this growth.

What is a CSP in cloud computing?

In cloud computing, a CSP stands for cloud service provider. For your company to access public cloud services, you need to engage a CSP. In simple terms, cloud service providers make cloud services available to consumers.

According to the NIST Cloud Computing Reference Architecture, NIST SP 500-292, a CSP:

- Acquires and manages the cloud computing infrastructure
- Runs the cloud software that provides the services
- Makes arrangements to deliver the cloud services to consumers through network access

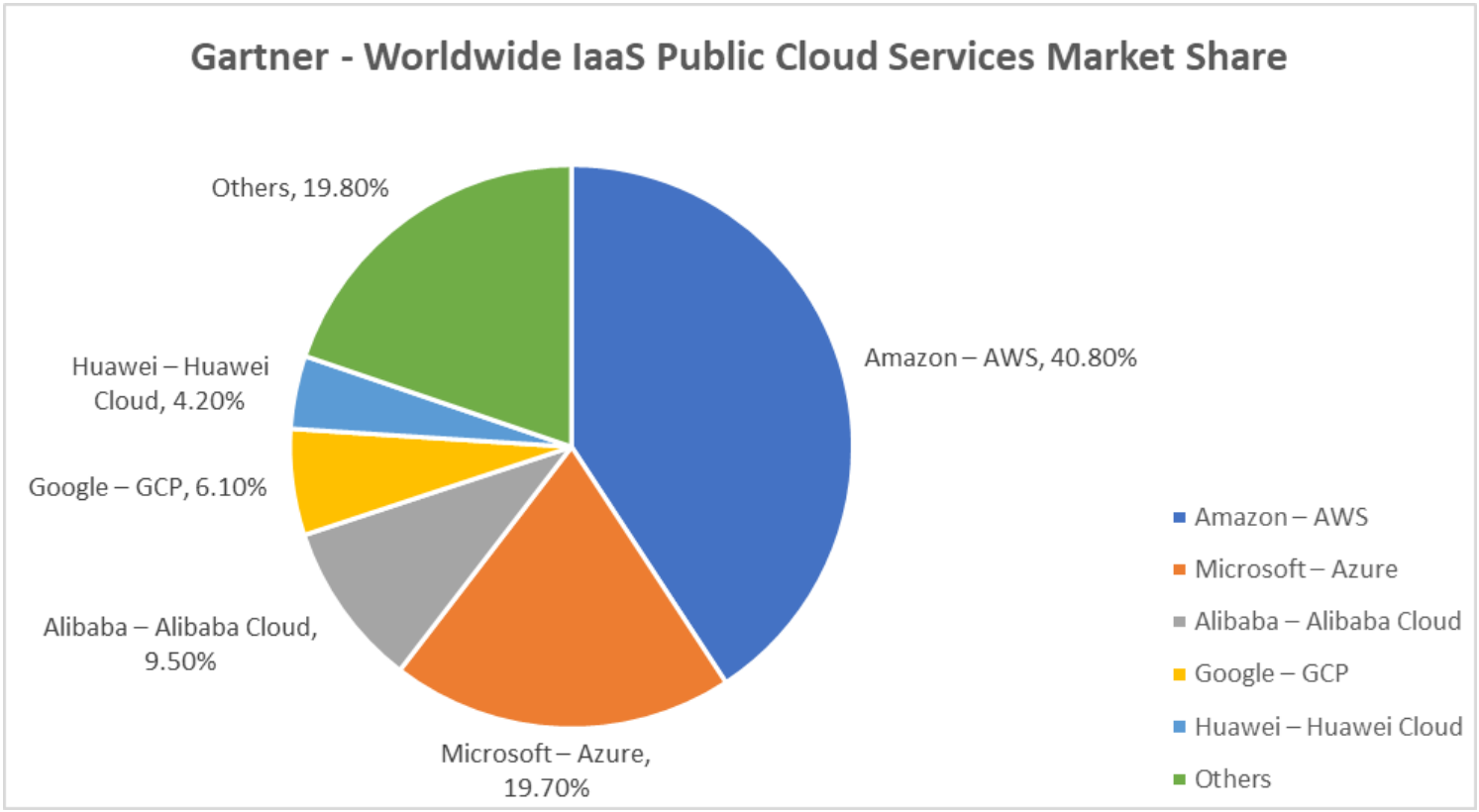
Click here if you're looking instead for CSPs as in communication service providers.

Benefits of CSPs

The main advantages that cloud-based services providers offer over traditional hosting services include:

- **Immediate access to more services**. A wide variety of capabilities and integrations.
- **Usage-based pricing**. Billing based on time use or capacity.
- **Global scale**. Coverage across most of the developed world.
- **Scalability**. It is quick and easy to right-size your IT resources, adding when business demands are higher or scaling down during slower times.
- **Flexibility**. Use the resources you need when you need them, adding and subtracting capabilities depending on demand.
- **Mobility**. Workers can access IT services any place they have a network connection—even when on the move.
- **Disaster recovery**. With failover redundancy, your services can move from a physical location suffering a power outage or other disruption to another location far from the problem, without missing a beat.
- **Security and compliance**. Large commercial cloud computing providers have security and compliance protections that are likely far beyond what a smaller company can acquire.
- **Automatic updates and maintenance**. With teams of experts on hand and direct access to the most innovative cloud networking service providers, you will have the latest tech, with the assurance that it is well-maintained.
- **Resource optimization**. You will be able make the most efficient use of right-sized resources, with access to powerful monitoring tools, to minimize waste and maximize application performance.

Five major players dominate the public cloud infrastructure market, with a near 82% market share, per Gartner in 2023:



(View availability regions and zones for major cloud computing providers.)

What do CSPs provide?

What are the cloud services that CSPs offer? CSP IT cloud solutions are broadly grouped into three main categories:

- **Infrastructure as a Service (IaaS).** This includes the physical computing resources underlying the cloud service solutions, including the servers, networks, storage, and hosting infrastructure, that are through a set of service interfaces and computing resource abstractions such as virtual machines. The customer makes selections based on desired computing resources such as processing, memory, capacity, and bandwidth, and manages the upper layers themselves.
- **Platform as a Service (PaaS).** This includes the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as the runtime software execution stack, databases, and other middleware components. The customer makes selections based on the requirements of the applications they intend to install and manage by themselves.
- **Software as a Service (SaaS).** Here, the CSP deploys, configures, maintains, and updates the operation of the software applications on a cloud infrastructure, and provides an interface for the customer to access the applications. The customer only has some limited administrative control and customization capabilities.

(Read our full IaaS, PaaS, SaaS explainer.)

However, these groupings do not adequately capture many of the capabilities that CSPs are currently providing, including containers (CaaS), serverless computing (FaaS), storage, edge computing, private cloud, and AI/ML platforms.

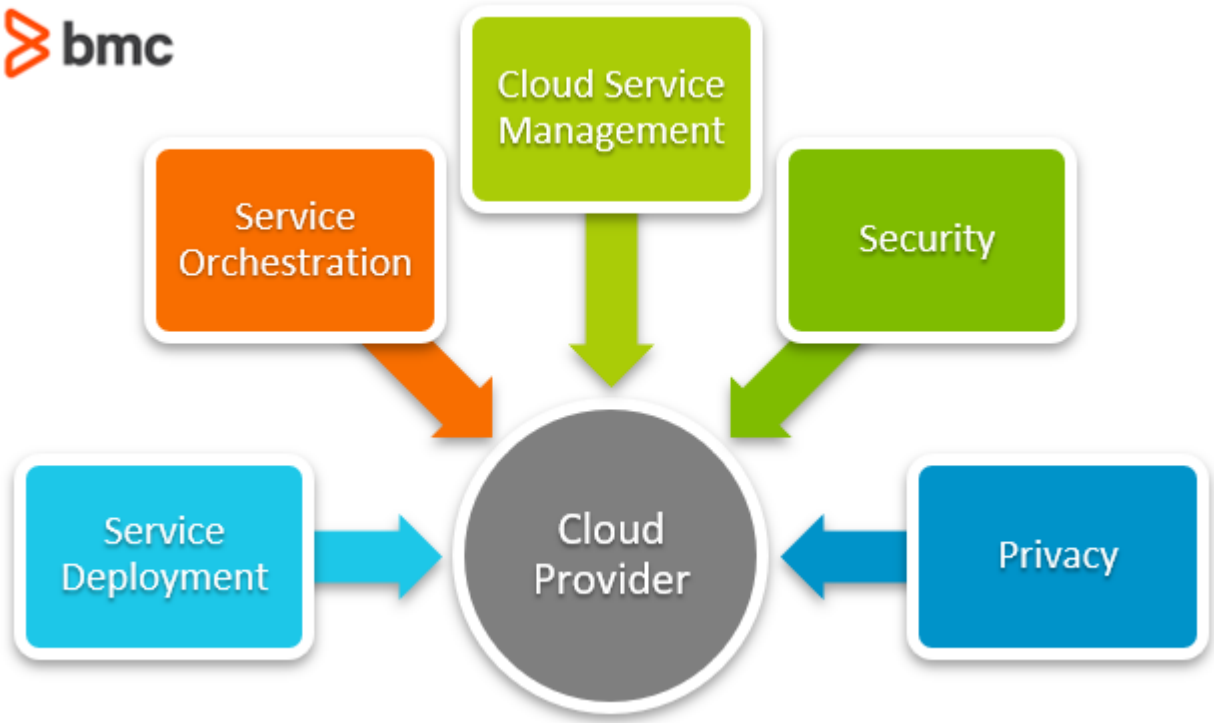
The table below outlines examples of the many cloud service solutions from some of the major cloud providers:

bmc

Service	AWS	Azure	GCP
IaaS	Elastic Compute Cloud (EC2)	Virtual machines	Compute Engine
PaaS	Elastic Beanstalk	App Service	App Engine
CaaS (Container as a Service)	Elastic Kubernetes Service (EKS)	Azure Kubernetes Service (AKS)	Kubernetes Engine
FaaS (Function as a Service)	Lambda	Function	Cloud Functions
Object Storage	Simple Storage Service (S3)	Blobs	Cloud Storage
Relational Storage	Relational Database Service	SQL Database	Cloud SQL
NoSQL Storage	DynamoDB	Cosmos DB	Cloud Bigtable

NI

ST SP 500-292 defines 5 major activities that CSPs perform:



- **Service deployment.** The operation of cloud infrastructure by the CSP on behalf of the consumer based on the following deployment models: public cloud, private cloud, hybrid cloud, or community cloud.
- **Service orchestration.** The activities involved in the arrangement, coordination, and management of computing resources through the composition of system components to provide cloud services to consumers.
- **Cloud service management.** The service-related functions that are necessary for the management and operation of those services required by or proposed for cloud consumers, including business support, provisioning and configuration, and facilitating data portability and interoperability.
- **Security.** Implementing security controls across the entire cloud service architecture and working with consumers and third parties to reduce attack surfaces, tackle vulnerabilities, and limit the impact of threats.
- **Privacy.** Protecting the assured, proper, and consistent collection, processing, communication, use, and disposition of consumer personal information (PI) and personally identifiable information (PII) stored in the cloud.

Challenges faced by cloud services providers

The last two activities, security and privacy, are intrinsically tied to the CSP's biggest challenge—governance.

Trust is invariably tied to security and privacy, as any organization that entrusts its data to a third party expects that measures have been put in place to ensure confidentiality, integrity, and availability are always guaranteed. The increasingly difficult legal and regulatory requirements on data privacy, especially concerning location and sharing, mean that cloud services providers must be on their toes to ensure compliance while at the same time dealing with new and evolving security threats.

CSPs must also grapple with the challenge of optimizing their capacity to meet customer demand

while maintaining service uptime to the highest degree possible. For the major players, any significant downtime comes with media scrutiny owing to the services that are consumed on a global scale.

Additionally, knowledge management is a significant issue, as CSPs require employees with technical competencies that are expensive and hard to replace.

(Explore cloud governance best practices.)

How to choose a cloud computing provider

Consider the following factors when evaluating your cloud computing options.

- **Cost**: To get the best deal, consider the details of the provider's cost model. Most use a per-use approach, but you may find variations that can materially affect the price you will pay.
- **Tools and features**: Make sure your provider offers the functionality you need today, including security and data management, along with the ability to support your future needs.
- **Ease of deployment and change management:** Consider each cloud provider's process for deploying, managing, and upgrading your applications and services. Access to APIs that make it easy to connect and build are invaluable.
- **Physical location of the servers**: Security and availability depend on where the cloud services are housed. Make sure the provider can meet regulations for secure data storage.
- **Reliability**: Typical SLAs specify service levels, such as percentage of uptime and compensation should they fail to deliver on that guarantee. Watch out for loopholes, such as excluding or discounting outages that are just a few minutes long. Depending on your industry, even short outages can severely affect your business.
- **Security**: Your business may require adherence to various security frameworks. Make sure your provider can meet those certifications and can support compliance in the long term. Pay special attention to their risk management processes and plans, and their data backup operations.
- **Strategic fit:** You will want to choose a cloud network provider with the tools and capabilities that support your immediate and longer-term goals.
- **Reporting**: Look for providers with controls and management tools that make it easy to monitor performance and usage.

What does the future hold for cloud-based service providers?

Cloud computing continues to grow and even accelerate. Many types of companies, not just technology firms, are using the cloud, with many taking a multi-cloud approach. The Flexera 2024 State of the Cloud Report confirmed that:

- 89% of enterprises surveyed had a multi-cloud strategy.
- 73% take a hybrid approach.
- 85% are experimenting with or using generative AI public cloud services.
- 59% prioritize cloud cost optimization.

The benefits of the cloud have been proven over time, with fewer organizations fearing the drawbacks. CSPs have increasingly drawn the attention of regulators seeking to balance benefits against risks. Given the growing importance of cloud services, as well as complex social, economic,

security, and service issues, it is important to consider the implications beyond the simple business arrangements between CSPs and their customers.

Related reading

- BMC Multi-Cloud Blog
- 10 Best Practices to Avoid Cloud Vendor Lock-In
- Common Roles in Cloud Computing
- Hybrid Cloud Security: Challenges and Best Practices
- The State of The Cloud Today
- Cloud Growth, Trends & Outlook