CLOUD SERVICE PROVIDERS (CSPS) EXPLAINED

The cloud was initially looked at with scepticism over the risk of handing over control to another party. Today's digital age, however, is firmly anchored in a cloud-first approach.

In particular, startups are innovatively disrupting incumbents due to their ability to quickly set up on public clouds *without* the upfront capital required to set up the IT infrastructure by themselves. And with the global pandemic heightening the need for remote working, being cloud native is fast becoming a key differentiator for corporate success.

Gartner forecasts that worldwide end-user spending on public cloud services will grow by 23.1% in 2021 to total $332.3 billion. Cloud capabilities are extremely useful for leveraging new technologies—artificial intelligence, containerization, and IoT—while providing the flexibility that agile and DevOps approaches prefer.

Who are cloud service providers?

For your company to access public cloud services, you need to engage a cloud service provider (CSP). In simple terms, the CSP makes cloud services available to consumers.

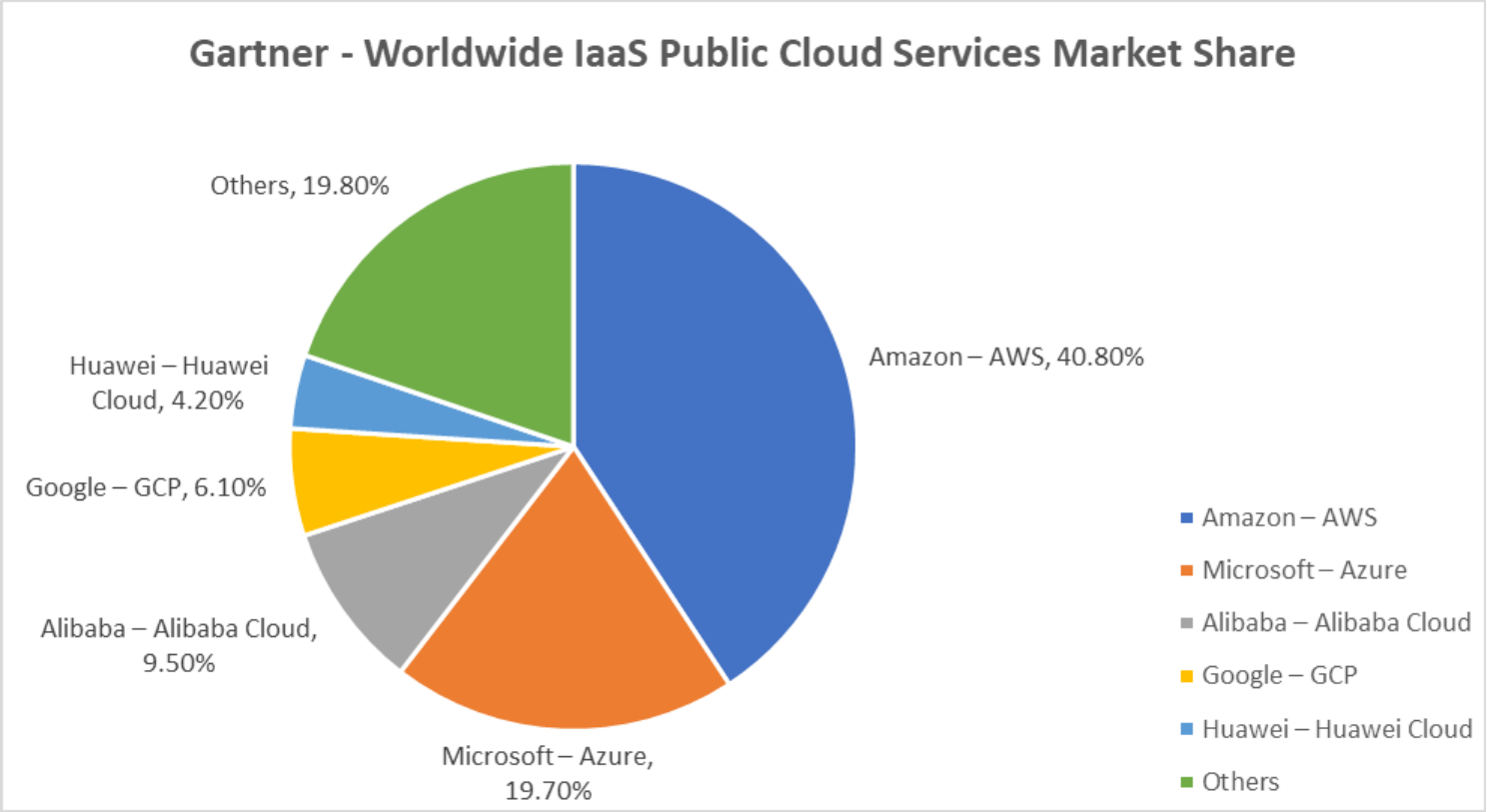
According to the NIST Cloud Computing Reference Architecture, NIST SP 500-292, a CSP:

- 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

The main advantages that CSPs 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.

There are 5 major players in the public cloud infrastructure space who command over 80% market revenue share, per Gartner in 2020:



The rest of the pie is shared among some international and local-based players. While some were dedicated cloud service providers from the start, others originated from internet service providers who simply saw the gap in providing data centre services which evolved into cloud services. Others who exploited the same gap evolved from web hosting providers and computing hardware providers.

(View availability regions & zones for major CSPs.)

What do CSPs provide?

CSP service offerings are broadly grouped into three main categories:

- **Infrastructure as a Service (IaaS).** This includes the physical computing resources underlying the service, 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.)

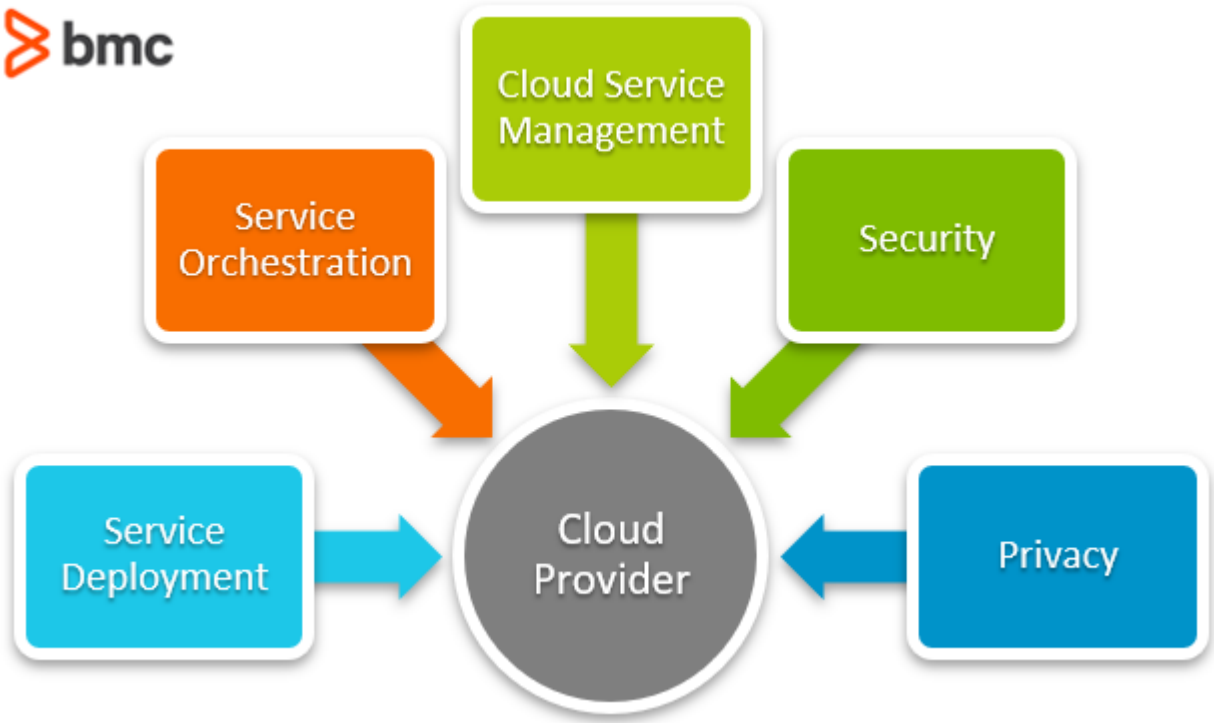
However, these groupings do not adequately capture many of the capabilities that CSPs are currently providing, including containers (CaaS), serverless computing (FaaS), storage, edge computing, private cloud, and AI/ML platforms.

The table below outlines a sample of the many offerings from some of the major 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

NIST 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.

What are CSPs biggest challenges?

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 CSPs 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.)

What does the future hold for CSPs?

The cloud is here to stay, and most leading technology-centric organizations are going with a cloud-first strategy. The Flexera 2021 State of the Cloud Report reported that:

- 92% of enterprises surveyed had a multi-cloud strategy.
- 90% expected cloud usage to exceed prior plans due to COVID-19.

The benefits of the cloud heavily outweigh the drawbacks, so CSPs will continue to see demand for their services continue to rise in the foreseeable future.

However, the major CSPs will most likely experience increased scrutiny from the government and civilians due to their level of dominance and control of information. CSPs will continue to be the target of cyberattacks due to the perceived economic value of the data they hold for organizations globally.

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