



What is public cloud? Everything you need to know

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

A public cloud is a third-party managed platform that uses the standard cloud computing model to make resources and services available to remote users around the world.

TechTarget's all-inclusive guide covers everything from the public cloud's history, to its benefits and challenges, to the various public cloud services that are currently available.

Topics also include how it works, how it differs from private and hybrid clouds, how to reduce cloud expenses and cloud security best practices.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

What is public cloud? Everything you need to know

STEPHEN BIGELOW, SENIOR TECHNOLOGY EDITOR

A public cloud is a third-party managed platform that uses the standard [cloud computing](#) model to make resources and services available to remote users around the world. Public cloud resources typically include conventional IT infrastructure elements such as virtual machines, applications or storage.

Services can include an array of workloads including databases, firewalls, load balancers, management tools and other platform-as-a-service (PaaS) or software-as-a-service ([SaaS](#)) elements. Users then assemble resources and services to build an infrastructure capable of deploying and operating enterprise workloads. Public cloud services can be free or offered through a variety of subscription or on-demand pricing schemes, including pay-per-usage or pay-as-you-go ([PAYG](#)) models.

The main benefits of the public cloud are as follows:

- a reduced need for organizations to invest in and maintain their own on-premises IT resources;
- scalability to quickly meet workload and user demands; and
- fewer wasted resources, because customers only pay for what they use.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

HOW DOES THE PUBLIC CLOUD WORK?

Public cloud is an alternative deployment approach to traditional on-premises IT architectures. In the basic public cloud computing model, a third-party provider hosts scalable, on-demand IT resources and delivers them to users over a network connection, either over the public internet or a dedicated network. Public cloud computing is often viewed as *utility computing*, where computing capabilities are delivered to users on demand, just as any other utility, such as water, gas and telecommunications.

The public cloud model encompasses many different technologies, capabilities and features. At its core, however, a [public cloud consists of the following key characteristics](#):

- on-demand computing and self-service provisioning;
- resource pooling;
- scalability and rapid elasticity;
- pay-per-use pricing;
- measured service;
- resiliency and availability;
- security; and
- broad network access.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

Cloud computing 101

Cloud computing is a broad term that encompasses any technology that's involved in delivering hosted computing services across the internet. Cloud computing is made up of three different types of services: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Whether a public or private cloud is deployed, the purpose of cloud computing is to provide access to flexible and scalable computing resources and IT services, either over the web or through a private network.

What is the difference between IaaS, PaaS and SaaS?

■ USER'S RESPONSIBILITY ■ SERVICE PROVIDER'S RESPONSIBILITY

	EXAMPLES	APPLICATIONS	MIDDLEWARE	VIRTUALIZATION	DATA	OS	NETWORKING	RUNTIME	SERVERS	STORAGE
SaaS	Dropbox, Salesforce CRM, Zoom, Office 365, Google Apps	■	■	■	■	■	■	■	■	■
PaaS	Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine, Red Hat OpenShift	■	■	■	■	■	■	■	■	■
IaaS	Microsoft Azure, Amazon Web Services (AWS), Google Compute Engine (GCE)	■	■	■	■	■	■	■	■	■

SOURCE: <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-what-is-the-difference-and-how-to-choose/>

What is the difference between on-premises and public cloud computing?

	On-premises	Cloud
SECURITY	IT teams are responsible for the security of all data and workloads.	Providers manage technical administration of security and offer tools for vulnerability management.
RELIABILITY	Even the strongest data center will break at some point. Systems failures and natural disasters can take down entire facilities.	Outages affect availability, so apps that require high availability should stay on premises or be extended across regions for additional redundancy.
COST	Companies pay for the hardware—plus excess capacity if needed—as well as facility operations.	Only pay for what is used. But companies can overpay if a workload isn't properly optimized.
EXPERTISE	Those who have studied and worked with these technologies know the ins and outs of the infrastructure, tape library management, required programming languages and so on.	Takes away the more complex and challenging parts of computing, which allows IT teams to home in on business objectives. It also requires learning skills to adapt to the new environment.

What are the characteristics of a cloud architecture?

- Self-service provisioning
- Elasticity
- Pay-per-use
- Workload resilience
- Migration flexibility
- Broad network access
- Resource pooling

Worldwide public cloud market share for Q1 2022

Provider	Market Share (%)
AWS	33%
Microsoft Azure	21%
Google Cloud	8%
Others	38%

SOURCE: STRATISTA

The public cloud provider supplies the infrastructure needed to host and deploy workloads in the cloud. It also offers tools and services to help customers manage cloud applications, such as data storage, security and various monitoring and reporting capabilities.

When selecting a [cloud service provider](#), organizations can opt for a large, general-use provider -- such as [AWS](#), [Microsoft Azure](#) or [Google Cloud](#) -- or a smaller provider. General cloud providers offer broad availability and integration options and are desirable for multipurpose cloud needs. Niche providers offer more customization or a focus on specific cloud capabilities.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

MIGRATION TO THE PUBLIC CLOUD

Myriad factors drive businesses to [migrate from on-premises facilities to the public cloud](#).

For example, some organizations require support for more diverse workload types that data centers can't provide. Cost considerations, less overhead, lower direct maintenance and readily available redundancy options are other common reasons.

After choosing a provider, the IT team must select a cloud migration method to move data and workloads into the provider's cloud. Offline migration requires IT teams to copy local data onto a portable device and physically transport that hardware to the cloud provider. Online data migration occurs via network connection over the public internet or a [cloud provider's networking service](#).

When the amount of data to transfer is significant, offline migration is typically faster and less expensive. Online migration is a good fit for organizations that won't move high volumes of data.

Organizations also onboard existing on-premises applications into the cloud, and there are a few approaches to consider. A lift-and-shift method moves the application to the cloud as is, without any redesign. This approach is fast but prone to complications -- the application might not perform properly within cloud architecture and might cost more than if it remained on premises. Alternatively, IT teams can refactor on-premises applications ahead

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

of the migration. Refactoring takes more time and planning, but this method ensures that the application will function effectively in the cloud. Another option is to rebuild entirely as a cloud-native application.

Whichever strategy you choose, there are a range of cloud-native and third-party migration tools to help you manage the move to the public cloud.

PUBLIC CLOUD ARCHITECTURE

A public cloud is a fully virtualized environment that relies on high-bandwidth network connectivity to access and exchange data. Providers have a [multi-tenant](#) architecture that enables users -- or *tenants* -- to run workloads on shared infrastructure and use the same computing resources. Each tenant's data and workloads in the public cloud are logically separated and remain isolated from the data of other tenants.

Providers operate cloud services in logically isolated locations within public cloud regions. These locations, called *availability zones*, typically consist of two or more connected, highly available physical data centers. The links below describe the dozens of regions and availability zones worldwide for AWS, Azure and Google Cloud:

- [AWS regions and availability zones](#)

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

- [Azure regions and availability zones](#)
- [GCP regions and availability zones](#)

Organizations select availability zones based on compliance and proximity to end users. Cloud resources can be replicated across multiple availability zones for redundancy and protection against outages.

Public cloud architecture can be further categorized by service model. These are the three most common service models:

- **IaaS.** A third-party provider hosts infrastructure components, such as servers and storage, as well as a virtualization layer. The [IaaS](#) provider offers virtualized computing resources, such as VMs, over the internet or through dedicated connections.
- **PaaS.** A third-party provider delivers hardware and software tools -- usually those needed for application development, including OSes -- to its users as a service.
- **SaaS.** A third-party provider hosts applications and makes them available to customers over the internet.

The service model determines how much control the user has over certain aspects of the cloud. For example, in IaaS deployments, cloud customers create VMs, install OSes and manage cloud networking configurations. But in PaaS and SaaS models, the cloud networking architecture is fully managed by the provider.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

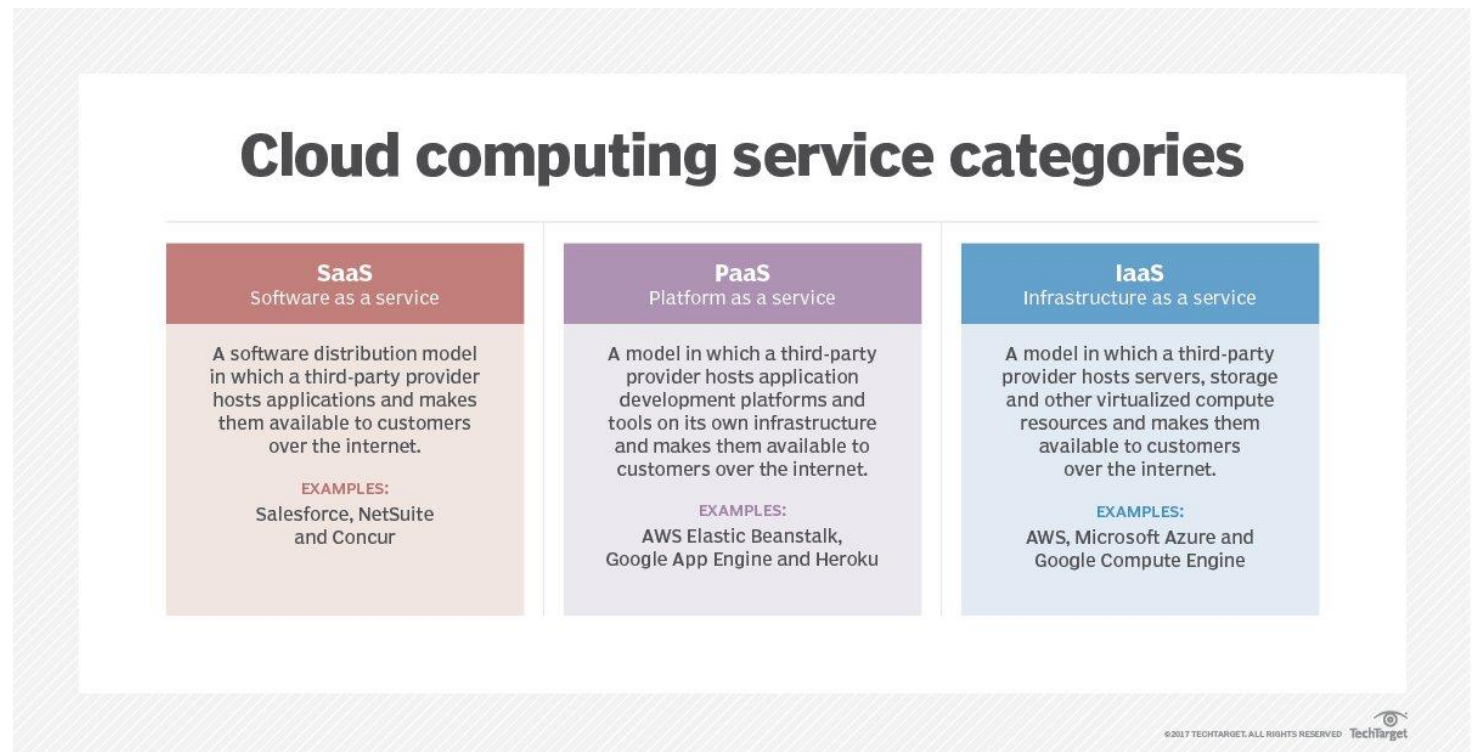
[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)



In addition to the three main service models, a function-as-a-service ([FaaS](#)) model further abstracts cloud infrastructure and resources. This is particularly useful for customers that create microservices. It is based on [serverless computing](#), a mechanism that breaks workloads into small, event-driven resource components and runs the code without the need to deliberately create and manage VMs. This enables organizations to execute code-based tasks on demand when triggered; the components exist only for as long as the assigned task runs. As with all other cloud models, the provider handles the underlying [cloud server](#) maintenance.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

Organizations can also opt for a storage-as-a-service provider in the public cloud. The provider delivers a storage platform with offerings such as bare-metal storage capacity, object storage, file storage, block storage and storage applications like backup and archiving.

BENEFITS AND CHALLENGES OF PUBLIC CLOUD COMPUTING

Enterprises must weigh the [advantages and drawbacks of public cloud adoption](#) to determine whether it's the right fit.

BENEFITS

[The cloud has many advantages](#) over on-premises IT:

- **Access to new technologies.** Organizations that use large cloud providers get early and instant access to the IT industry's latest technologies, ranging from automatically updated applications to machine learning and AI. Many cloud customers lack the resources to obtain such access on their own, typically because the business might not have enough money or expertise to implement such capabilities in-house.
- **Virtually unlimited scalability.** Cloud capacity and resources rapidly expand to meet user demands and traffic spikes. Public cloud users also achieve greater redundancy and high availability due to the providers' various, logically separated cloud locations. In addition to redundancy and availability, public cloud users receive faster connectivity between cloud services and end users through their provider's network interfaces -- though bandwidth and latency issues are still common.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

- **Flexibility.** The flexible and scalable nature of public cloud resources enables users to store high volumes of data and access them easily for computing or retrieval. Many organizations rely on the cloud for disaster recovery -- to back up data and applications in case of emergency or outage. It's tempting to store all data indefinitely, but users should set up a data retention policy that regularly deletes old data from storage to avoid long-term storage costs and to maintain privacy.
- **Analytics.** Organizations should gather useful metrics on the data they store and resources they use. Doing so presents another benefit: cloud data analytics. Public cloud services can perform analytics on resource and service usage to determine utilization and cost trends for better business insights.

Other public cloud benefits include access to the provider's reliable infrastructure and the abstraction of overhead management tasks. These enable IT staff to focus on tasks that are more important to the business, such as writing code for applications.

CHALLENGES

While the public cloud presents many advantages, organizations must separate cloud computing myths from realities and also face a range of challenges:

- **Runaway costs.** Increasingly complex cloud costs and pricing models make it difficult for organizations to keep track of IT spending. The cloud is often cheaper than on-premises options, but organizations sometimes end up paying more for cloud. Pricy data egress fees make staying on a cloud budget even more challenging.
- **Scarce cloud expertise.** Another challenge is the skills gap among IT professionals in the cloud computing industry. Companies struggle to hire and retain staff with

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

expertise in building and managing modern cloud applications. Without this expertise, organizations are ill-equipped to handle the complexities of modern IT demands. IT professionals that hope to fill these roles can better prepare for [career opportunities](#) by [fine-tuning their cloud skills](#) in areas such as architecture/engineering, operations and coding.

- **Limited transparency and controls.** Public cloud users also face the tradeoff of limited control over their IT stack since the provider can decide when and how to manage configurations. Other public cloud challenges include [data separation](#) problems due to multi-tenancy, latency issues for remote end users and adherence to industry- and country-specific regulations.
- **Vendor lock-in.** Although each public cloud can offer similar resources and services, the controls and delivery of those assets can vary between providers, making it difficult for one data set or application to migrate easily between providers. This poses the risk of vendor dependency, which can raise costs and limit capabilities for business users.

Cloud management tools and strategies can help organizations address some of these public cloud challenges and optimize their use of cloud resources and costs. As a start, even a general understanding of cloud basics is helpful. Test your cloud knowledge to see what gaps you might need to fill.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

Pros and cons of cloud computing

Pros

- Lower operations costs
- Massive scalability
- Rapid access to the latest hardware and software
- Faster connections between cloud-based services and to end users
- Secure underlying infrastructure
- More reliable and redundant than most enterprise data centers

Cons

- Complex pricing structures
- Potentially prohibitive egress fees
- Can require specialized skills and experience, as well as knowledge of data residency requirements and cloud security models
- Restrictions on instance configuration options
- Limited customer support



ILLUSTRATION: APINAN/ADOBE STOCK

© 2020 TECHTARGET. ALL RIGHTS RESERVED 

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

DIFFERENCES BETWEEN PUBLIC CLOUDS, PRIVATE CLOUDS AND HYBRID CLOUDS

The term *public cloud* arose to [differentiate between the standard cloud computing model and private cloud](#), which is a proprietary cloud computing architecture dedicated to a single organization. A standard [private cloud](#) extends a company's existing data center resources and is accessible only by that company.

Public and private clouds offer similar services -- such as compute, storage and networking -- and capabilities such as scalability. However, the two models have significant differences in how they operate and provide those services.

Public cloud resources run on multi-tenant, shared infrastructure and are available globally to users over the internet. Conversely, private cloud consists of single-tenant architecture that runs on privately owned infrastructure. Essentially, a private cloud builds on an organization's traditional local data center infrastructure by adding layers of virtualization, cloud-type services -- such as resource pooling and on-demand provisioning -- and management.

Beyond architectural differences, public and private cloud models differ in price, performance, security, compliance and more. Private cloud requires large upfront investment for cloud infrastructure, as opposed to the public cloud's PAYG model. In terms of performance, public cloud can be subject to network bandwidth and connectivity issues,

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

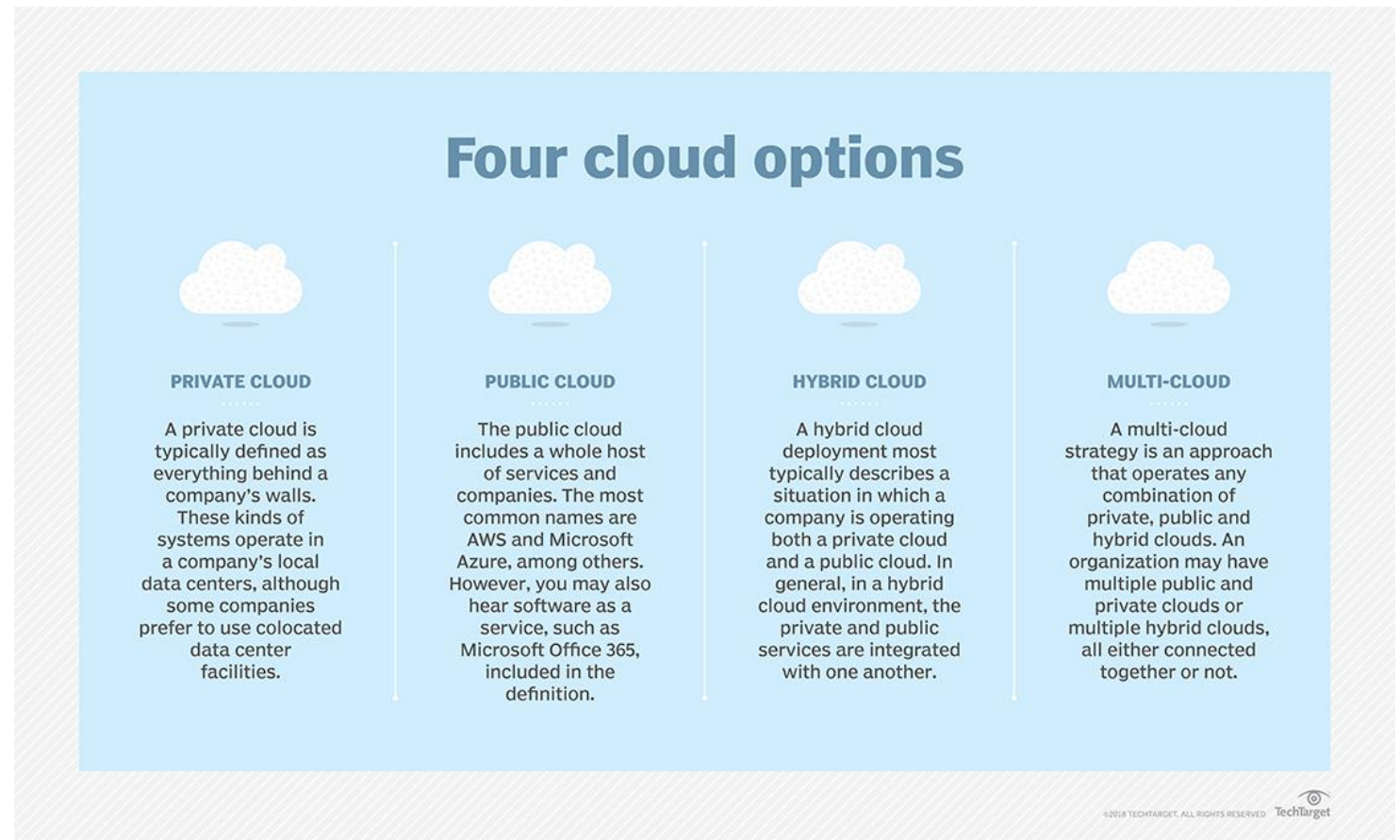
[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

since it largely relies on the public internet. Private cloud can offer more consistent performance and reliability, since it is a localized site.



In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

Both public and private cloud models provide extensive security offerings. However, the private cloud offers more fine-grained control over configurations and physical isolation. Private cloud also poses fewer compliance issues, since data does not leave the on-premises facility. Organizations with strict compliance needs and cloud aspirations often choose private cloud.

These differences apply to the standard on-premises private cloud. However, alternative private cloud models blur the lines between public and private computing. Cloud providers now offer on-premises versions of their public cloud services. Examples include AWS Outposts, Azure Stack and Google Anthos, which bring physical hardware or bundled software services into an enterprise's internal data center. These distributed deployments act as isolated private clouds, but they are tied to the provider's cloud and form a type of hybrid cloud implementation.

HYBRID AND MULTI-CLOUD SERVICES

A third model, *hybrid cloud*, is a combination of public and private cloud services, maintained by both internal and external providers and with orchestration between the two. This model enables organizations to tap into the benefits of the public cloud for certain workloads, such as to accommodate demand spikes, but also maintain their own private cloud for sensitive, critical or highly regulated data and applications. There are a number of hybrid cloud

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

benefits, including flexible deployment options, greater cost control and the ability to move between environments.

A related option is a multi-cloud architecture, in which an enterprise uses more than one cloud. Most often it refers to the use of multiple public clouds. Depending on its needs, a business might choose to use both the hybrid and multi-cloud models.

The choice of local computing, a public cloud, a hybrid cloud and even multi-cloud implementations are not mutually exclusive. Such infrastructure choices simply offer tools that enable a business to host and operate various workloads. It's possible to adopt any mix of infrastructure to meet workload needs and business goals. However, some alternatives -- including hybrid and multi-cloud options -- can be extremely complex and demand high levels of engineering and management expertise on the part of the business.

PUBLIC CLOUD PRICING

Public cloud pricing is [typically billed on a pay-per-use or PAYG structure](#), in which cloud users pay only for the resources they consume. In many cases, this helps reduce IT expenses, since an organization no longer needs to purchase and maintain physical infrastructure for those parts of its business it deploys to a public cloud IaaS. Also, a company can account for public cloud expenditures as operational or variable costs rather than capital or fixed costs.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

This can provide more flexibility to the business, as these operational spending decisions typically require less-intensive reviews or budget planning.

However, it's easy to overspend in the cloud and erase those benefits because it can be difficult to accurately track cloud service usage in the self-service model. Common public cloud cost pitfalls include over-provisioning resources, failure to decommission idle workloads and unnecessary data egress fees. In addition to these cost challenges, public cloud providers have complex pricing models with rates that vary by region and service. Failure to understand a provider's pricing model can cause hidden costs to drive up the bill.

Organizations must factor in all the components that make up their cloud computing spend. This includes costs for application migration, data transfer, storage and resource consumption, along with the products to manage and maintain the environment.

Ironically, the principal challenge here is self-service. Since every cloud user is free to establish public cloud accounts, there is a natural lack of oversight and centralization to organize and track costs -- one department might not know what another department is doing in the cloud, for example. This leads to redundancy and waste. Recent initiatives such as FinOps are emerging to help organizations oversee and centralize public cloud use across the business to maximize its benefits.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

COST OPTIMIZATION STRATEGIES

[To rein in cloud costs](#), adopt tools and strategies that estimate costs and identify spending patterns. Cloud providers offer pricing calculators and cost monitoring tools, such as AWS Cost Explorer, Azure Pricing Calculator and Google Cloud Cost Management. Gain a solid understanding of your chosen cloud environment to help rightsize resources and pay only for what you need.

Also, explore providers' discount programs, such as cheaper alternatives to on-demand resources. For example, AWS and Azure offer reserved instances at a lower price, in exchange for commitment to use a certain amount of capacity within a specified time period.

Autoscaling is another way to keep costs down. Autoscaling features adjust application scale to meet demand, which avoids paying for unnecessary capacity. Proper visibility into the cloud environment also helps IT teams identify and shut down idle workloads to avoid paying for unused resources and prevent cloud sprawl.

Enterprises should consistently monitor their cloud bill and reevaluate deployment models to ensure the most cost-efficient approach. For example, an organization with high data egress fees can work on limiting data transfers. This requires close collaboration between cloud users, such as department managers, or a centralized FinOps group in the business.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

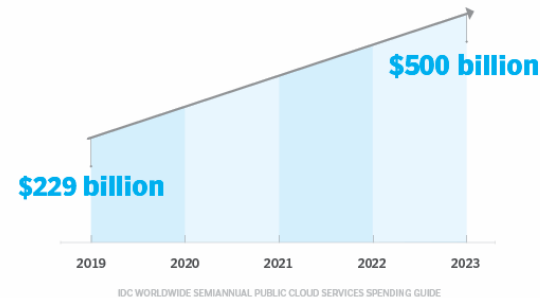
[Public cloud history](#)

The cost of cloud

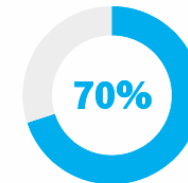
While the cloud can reduce IT expenses, it can also increase them if an organization lacks a cost management strategy. Optimization keeps budgets in check and prevents overspending.

Public cloud spending continues to grow

With a five-year compound annual growth rate (CAGR) of 22.3%, public cloud spending will more than double.



Overspending is a common problem



Organizations without a cloud cost optimization strategy overspend up to 70% on cloud services.

Source: Gartner's "Realize Cost Savings After Migrating to the Cloud" April 2021



The price is right

Better estimate costs with pricing calculators, including:

[AWS Pricing Calculator](#)

[Microsoft Azure Pricing Calculator](#)

[Google Cloud Platform Pricing Calculator](#)

Resolve common cloud cost issues

ISSUES

RESOLUTIONS

Improper instance size	→	Right-size instances
Overprovisioning	→	Shut down unused resources
Traffic charges	→	Plot workloads to avoid ingress/egress fees
Storage	→	Consider lower-cost storage tiers and review retention policies

©2022 TECHTARGET. ALL RIGHTS RESERVED.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

PUBLIC CLOUD SECURITY

Security is a concern for many enterprises because of the multi-tenant nature of public cloud. Organizations host sensitive data and critical workloads in the cloud, so protecting the environment is a top priority. Public cloud providers offer various security services and technologies, but security in the cloud requires diligence from both provider and customer.

SHARED RESPONSIBILITY

Public cloud security duties are split between the provider and cloud user, outlined in a [shared responsibility model](#). This framework designates the particular aspects of security -- and accountability -- for the provider and the user. The specific tasks in a security agreement differ depending on the chosen provider and public cloud model. For example, the AWS shared responsibility model states that AWS is responsible for securing the infrastructure that supports the cloud environment, which includes hardware, software, network, storage and on-premises facilities used to run AWS cloud services. Meanwhile, the cloud user is responsible for securing anything that runs in the cloud -- namely, applications and customer data.

For example, a cloud provider is expected to secure the infrastructure, but it's up to the user to employ security tools, such as identity and access management (IAM) and firewalls, to establish and maintain proper security for data and workloads. In simpler terms, you might

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

rent a home and rely on the landlord to keep the property running properly, but it's up to you to lock the doors and close the windows.

PUBLIC CLOUD SECURITY CHALLENGES

Organizations must understand numerous challenges related to cloud security to protect cloud-hosted applications. Public cloud requires protection against external threats, such as malicious attacks and data breaches, as well as internal security risks, including misconfigured resources and access management policies.

Hybrid cloud security presents an additional set of challenges. Complexities such as securing data in transit over the public internet and networking components for disparate environments require additional protections, such as encryption.

SECURITY TOOLS AND PRACTICES

Cloud providers' security services and technologies include encryption and IAM tools. A comprehensive security strategy relies on a combination of these.

Cloud security monitoring is a crucial piece of the security strategy to provide threat detection. Security monitoring tools scan and observe the services and resources in your cloud environment and generate alerts when a potential security issue arises. Access control is also critical to public cloud security. Set up strong IAM policies that allot only the necessary level of permissions, such as zero-trust policies. Consistently update IAM policies and

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

remove access for users that no longer require certain permissions. Use multifactor authentication to bolster user verification.

In addition to security tools and policies, a well-trained IT staff is integral to ensure a safe cloud environment. Many vulnerabilities are the product of resource misconfigurations due to human error. Make sure your IT staff is up to date on security policies and proper configuration practices. Document established security policies and ensure that IT staff are capable of monitoring and maintaining local and cloud configurations against those policies.

PUBLIC CLOUD PROVIDERS AND ADOPTION

Estimates of public cloud usage vary widely across different countries, but most market research and analyst firms expect continued growth in worldwide adoption and cloud revenues. Data from Synergy Research Group [shows that](#) Q4 2021 enterprise spending on cloud infrastructure services exceeded \$50 billion, 36% above spending in the fourth quarter of 2020.

Today, there are three [main public cloud providers](#): AWS, Microsoft and Google. These providers deliver their services over the internet or through dedicated connections, and they use a fundamental pay-per-use approach. Each provider offers a range of products oriented toward different workloads and enterprise needs.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

- **AWS.** The leading public cloud vendor with the largest customer base, AWS was one of the earliest companies to provide scalable, PAYG cloud services. The company initially launched its cloud services platform to support the resource demands of Amazon's retail business. It has since expanded to provide cloud services to users worldwide. AWS offers more than 200 products for compute, databases and infrastructure management, as well as more advanced application development services for machine learning, AI and IoT.
- **Microsoft Azure.** The second largest public cloud provider, Azure offers the same types of computing services as its main competitor, AWS. Azure has a well-established PaaS portfolio that attracts many of its users. The platform's suite of PaaS offerings is grouped in the Azure App Service.
- **Google Cloud.** GCP has a less extensive list of cloud offerings than the two other industry leaders, but it has a growing user base and continues to add services.

Similar to the emergence of AWS from Amazon, Alibaba Cloud was created to support the Alibaba e-commerce parent company. Alibaba offers infrastructure, storage, networking and other application services. The company operates in international regions but is primarily focused on domestic Chinese and other Asian markets.

[IBM Cloud](#) is another vendor option with IaaS and PaaS offerings. IBM acquired open source software company Red Hat in 2019 to provide users with more flexible service options and extended hybrid cloud capabilities.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

Oracle is primarily known for its database offerings, but it also provides public cloud services. The company's IaaS offering, Oracle Cloud Infrastructure, is a good fit for organizations that require custom, high-performance computing and specialization.

CATEGORIES OF AVAILABLE PUBLIC CLOUD SERVICES

Each cloud provider offers a suite of tools and services across many service categories. A few of the core categories are compute, storage, container management and serverless. They generally work the same, but similar services are typically not interchangeable. As such, users should be mindful of any unique requirements or dependencies. Below are some of the product options from AWS, Azure and Google Cloud in each of these areas.

Compute. Amazon Elastic Compute Cloud (EC2) is a cloud IaaS service that provides compute capacity for AWS deployments on virtual servers, known as *EC2 instances*. There are various EC2 instance types and sizes designed for different user needs, including memory, storage and compute-optimized instances. Microsoft's primary compute service is Azure Virtual Machines, which similarly varies for compute, memory and general use. Google Cloud's IaaS compute service is called Google Compute Engine.

Storage. Each provider offers various storage types, such as block, object and file. The Amazon S3 object storage service is available in seven storage tiers -- S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access, S3 One Zone-Infrequent Access, S3 Glacier

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

Instant Retrieval, S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive -- that vary by access frequency. Other storage offerings on AWS include Amazon Elastic Block Store and Amazon Elastic File System. Microsoft storage offerings include Azure Blob Storage for object storage, Azure Files for file storage and Azure Managed Disks for block storage. Google Cloud offers Cloud Storage buckets for object storage; Filestore for file storage; and Zonal persistent disk, Regional persistent disk and Local SSD for block storage.

Containers. AWS offers four container management offerings: Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon Elastic Container Registry and AWS Fargate. Users can also deploy containers manually on EC2 instances. Microsoft's container management services include Azure Kubernetes Service, Azure Container Registry and Azure Container Instances. Google Cloud users can run containers on Google Kubernetes Engine, Google Cloud Run or Google Compute Engine.

Serverless. The primary serverless products from the big three providers are AWS Lambda, Azure Functions and Google Cloud Functions.

Public cloud providers also offer various tools and services for networking, monitoring, analytics, machine learning, IoT, big data support and human-machine interaction, such as text-to-speech.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

PUBLIC CLOUD HISTORY

While the concept of [cloud computing has been around since the 1960s](#), it didn't reach public popularity for enterprises until the 1990s. Salesforce, now a top SaaS provider, entered the market in 1999 by delivering applications through a website. Browser-based applications that could be accessed by numerous users, such as G Suite, soon followed.

In 2006, Amazon launched EC2, its IaaS platform, for public use. Under its cloud division, AWS, enterprises could "rent" virtual computers but use their own systems and apps. Soon after, Google released Google App Engine, its PaaS service, for application development, and Microsoft came out with Azure, also a PaaS offering. Over time, all three built IaaS, PaaS and SaaS offerings. Legacy hardware vendors such as IBM and Oracle also entered the market.

However, not all vendors that tried to compete succeeded. Verizon, Hewlett Packard Enterprise, Dell, VMware and others were forced to shut down their public clouds. Some have refocused on hybrid cloud and cloud management.

Public cloud adoption continues to rise as providers expand their portfolios of services and support. Technology developments -- including AI, machine learning, IoT and edge computing -- have all made their way into public cloud service portfolios. More diverse cloud application development approaches have also emerged as organizations embrace microservices, containers and serverless architectures.

In this guide:

[Introduction](#)

[How does the public cloud work?](#)

[Public cloud architecture](#)

[Benefits and challenges of public cloud computing](#)

[Differences between public clouds, private clouds and hybrid clouds](#)

[Public cloud pricing](#)

[Public cloud security](#)

[Public cloud providers and adoption](#)

[Public cloud history](#)

In general, cloud experts expect the next wave of public cloud computing will involve more automation and specialization. Providers will offer more granular and interconnected services to meet broader user needs. Emerging technologies and IT developments -- for example, quantum computing -- will shape the future of public cloud.

For a high-level overview, check out [FAQs about cloud computing](#). Think you know all there is to know about the cloud now? Take this [cloud computing basics quiz](#) to find out.



CONTINUED READING

[8 key characteristics of cloud computing](#)

[Top public cloud providers of 2023: A brief comparison](#)

[8 ways to reduce cloud costs](#)