UNIT III CLOUD ARCHITECTURE, SERVICES AND STORAGE (8)

Layered Cloud Architecture Design – NIST Cloud Computing Reference Architecture – Public, Private and Hybrid Clouds - laaS – PaaS – SaaS – Architectural Design Challenges – Cloud Storage – Storage-as-a-Service – Advantages of Cloud Storage – Cloud Storage Providers – S3.

Virtualization and dynamic provisioning of resources are the principles on which cloud computing works. In terms of architecture, the cloud hosting can be sliced into four different layers.

The Physical Layer:

This layer comprises of physical servers, network and other aspects that can be physically managed and controlled.

The Infrastructure Layer:

This includes storage facilities, virtualized servers, and networking. Infrastructure as a Service or IaaS points to delivery of services in hosted format. They include hardware, network and servers, delivered to end users. Consumers can enjoy access to scalable storage and compute power as and when needed.

Platform Layer:

This layer includes services such as OS and Apps. It serves as a platform for development and deployment. The Platform layer provides the right platform for development and deployment of applications vital for the cloud to run smoothly.

Application Layer:

The Application Layer is the one that end users interact with in a direct manner. It mainly comprises of software systems delivered as service. Examples are Gmail and Dropbox. SaaS or Software as a Service ensures delivery of software in hosted form which can be accessed by users through the internet. Configurability and scalability are the two key features of this layer. Customers can easily customize their software system using Meta data. These layers allow users to use cloud computing services optimally and achieve the kind of results they are looking for from the system.

NIST Cloud Computing Reference Architecture

The National Institute of Standards and Technology (NIST), along with other agencies, was tasked by the U.S. Chief Information Officer with specific activities aimed at accelerating the adoption of cloud computing. These include the delivery of a US Government Cloud Computing Technology Roadmap and the creation of other NIST Special Publications (NIST SPs) that address the definitions, security aspects, and reference architecture of Cloud Computing.

This document was developed as part of a collective effort by the NIST Cloud Computing Public Security Working Group in response to the priority action plans for the early USG cloud computing adoption identified in NIST SP 500-293: US Government Cloud Computing Technology Roadmap Volume 1, High-Priority Requirements to Further USG Agency Cloud Computing Adoption. NIST SP 500-293 highlights concerns around the protection and control of cloud Consumer data.This document introduces the NIST Cloud Computing Security Reference Architecture (NCC- SRA or, for the sake of brevity, SRA), providing a comprehensive formal model to serve as security overlay to the architecture described in NIST SP 500-292: NIST Cloud Computing Reference Architecture.

This document also describes a methodology for applying a Cloud-adapted Risk Management Framework (CRMF) using the formal model and an associated set of Security Components (derived from the capabilities identified in the Cloud Security Alliance's Trusted Cloud Initiative Reference Architecture [TCI-RA]) to orchestrate a secure cloud Ecosystem by applying the Risk Management Framework described in NIST SP 800-37 (Rev. 1): Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. The study upon which the NCC-SRA is based collected, aggregated, and validated data for a Public cloud, considering all three cloud service models – Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) – and all cloud Actors (i.e., Consumer, Provider, Broker, Carrier, and Auditor). While this document focuses on a Public cloud deployment model because it best supports illustrative examples of all of the NCC-SRA Security Components and security considerations, the NCC-SRA (the formal model, the set of Security Components and the methodology for applying the CRMF) is agnostic with respect to cloud deployment model, and its methodology can easily be applied to Private, Community, or Hybrid clouds.

The NCC-SRA introduces a risk-based approach to determine each cloud Actor's responsibility for implementing specific controls throughout the life cycle of the cloud Ecosystem. Specifically, for each instance of the cloud Ecosystem, the security components are analyzed to identify the level of involvement of each cloud Actor in implementing those components. The ultimate objective of this document is to demystify the process of describing, identifying, categorizing, analyzing, and selecting cloud-based services for the cloud Consumer seeking to determine which cloud service offering most effectively addresses their cloud computing requirement(s) and supports their business and mission-critical processes and services in the most secure and efficient manner.

Cloud Deployment Models

The cloud deployment models summarised below are the following:

- **Private Cloud:** the cloud services used by a single organization, which are not exposed to the public. A private cloud resides inside the organization and must be behind a firewall, so only the organization has access to it and can manage it.
- **Public Cloud:** the cloud services are exposed to the public and can be used by anyone. Virtualization is typically used to build the cloud services that are offered to the public. An example of a public cloud is Amazon Web Services (AWS).
- **Hybrid Cloud:** the cloud services can be distributed among public and private clouds, where sensitive applications are kept inside the organization's network (by using a private cloud), whereas other services can be hosted outside the organization's network (by using a public cloud). Users can them interchangeably use private as well as public cloud services in every day operations.

The biggest differences between public, private and hybrid cloud are described in the table below.

Difference	Private	Public	Hybrid
Tenancy	Single tenancy: there's only the data of a single organization stored in the cloud.	Multi-tenancy: the data of multiple organizations in stored in a shared environment.	The data stored in the public cloud is usually multi-tenant, which means the data from multiple organizations is stored in a shared environment. The data stored in private cloud is kept private by the organization.
Exposed to the Public	No: only the organization itself can use the private cloud services.	Yes: anyone can use the public cloud services.	The services running on a private cloud can be accessed only the organization's users, while the services running on public cloud can be accessed by anyone.
Data Center Location	Inside the organization's network.	Anywhere on the Internet where the cloud service provider's services are located.	Inside the organization's network for private cloud services as well as anywhere on the Internet for public cloud services.
Cloud Service Management	The organization must have their own administrators managing their private cloud services.	The cloud service provider manages the services, where the organization merely uses them.	The organization itself must manage the private cloud, while the public cloud is managed by the CSP.

Hardware Components	Must be provided by the organization itself, which has to buy physical servers to build the private cloud on.	The CSP provides all the hardware and ensures it's working at all times.	The organization must provide hardware for the private cloud, while the hardware of CSP is used for public cloud services.
Expenses	Can be quite expensive, since the hardware, applications and network have to be provided and managed by the organization itself.	The CSP has to provide the hardware, set-up the application and provide the network accessibility according to the SLA.	The private cloud services must be provided by the organization, including the hardware, applications and network, while the CSP manages the public cloud services.

Common Examples of SaaS, PaaS, & IaaS

Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

SaaS: Software as a Service

Software as a Service, also known as cloud application services, represents the most commonly utilized option for businesses in the cloud market. SaaS utilizes the internet to deliver applications, which are managed by a third-party vendor, to its users. A majority of SaaS applications run directly through your web browser, which means they do not require any downloads or installations on the client side.

SaaS Delivery

Due to its web delivery model, SaaS eliminates the need to have IT staff download and install applications on each individual computer. With SaaS, vendors manage all potential technical issues, such as data, middleware, servers, and storage, resulting in streamlined maintenance and support for the business.

SaaS Advantages

SaaS provides numerous advantages to employees and companies by greatly reducing the time and money spent on tedious tasks such as installing, managing, and upgrading software. This frees up plenty of time for technical staff to spend on more pressing matters and issues within the organization.

SaaS Characteristics

There are a few ways to help you determine when SaaS is being utilized: Managed from a central location Hosted on a remote server Accessible over the internet Users not responsible for hardware or software updates

When to Use SaaS

SaaS may be the most beneficial option in several situations, including:

Startups or small companies that need to launch ecommerce quickly and don’t have time for server issues or software Short-term projects that require quick, easy, and affordable collaboration Applications that aren’t needed too often, such as tax software Applications that need both web and mobile access

SaaS Limitations and Concerns

- **Interoperability.** Integration with existing apps and services can be a major concern if the SaaS app is not designed to follow open standards for integration. In this case, organizations may need to design their own integration systems or reduce dependencies with SaaS services, which may not always be possible.
- **Vendor lock-in.** Vendors may make it easy to join a service and difficult to get out of it. For instance, the data may not be portable–technically or cost-effectively–across SaaS apps from other vendors without incurring significant cost or inhouse engineering rework. Not every vendor follows standard APIs, protocols, and tools, yet the features could be necessary for certain business tasks.
- **Lack of integration support.** Many organizations require deep integrations with on- premise apps, data, and services. The SaaS vendor may offer limited support in this regard, forcing organizations to invest internal resources in designing and managing integrations. The complexity of integrations can further limit how the SaaS app or other dependent services can be used.
- **Data security.** Large volumes of data may have to be exchanged to the backend data centers of SaaS apps in order to perform the necessary software functionality. Transferring sensitive business information to public-cloud based SaaS service may result in compromised security and compliance in addition to significant cost for migrating large data workloads.
- **Customization.** SaaS apps offer minimal customization capabilities. Since a one-size- fits-all solution does not exist, users may be limited to specific functionality, performance, and integrations as offered by the vendor. In contrast, on-premise solutions that come with several software development kits (SDKs) offer a high degree of customization options.
- **Lack of control.** SaaS solutions involves handing control over to the third-party service provider. These controls are not limited to the software–in terms of the version, updates, or appearance–but also the data and governance. Customers may therefore need to redefine their data security and governance models to fit the features and functionality of the SaaS service.
- **Feature limitations.** Since SaaS apps often come in a standardized form, the choice of features may be a compromising tradeoff against security, cost, performance, or other organizational policies. Furthermore, vendor lock-in, cost, or security concerns may mean it’s

not viable to switch vendors or services to serve new feature requirements in the future.

- **Performance and downtime.** Because the vendor controls and manages the SaaS service, your customers now depend on vendors to maintain the service's security and performance. Planned and unplanned maintenance, cyber-attacks, or network issues may impact the performance of the SaaS app despite adequate service level agreement (SLA) protections in place.

Examples of SaaS

These are several popular examples of SaaS, including: Google GSuite (Apps), Dropbox, Salesforce, Cisco WebEx, SAP Concur, and GoToMeeting.

PaaS: Platform as a Service

Cloud platform services, also known as Platform as a Service (PaaS), provide cloud components to certain software while being used mainly for applications. PaaS delivers a framework for developers that they can build upon and use to create customized applications. All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers can maintain management of the applications.

PaaS Delivery

The delivery model of PaaS is similar to SaaS, except instead of delivering the software over the internet, PaaS provides a platform for software creation. This platform is delivered via the web, giving developers the freedom to concentrate on building the software without having to worry about operating systems, software updates, storage, or infrastructure.

PaaS allows businesses to design and create applications that are built into the PaaS with special software components. These applications, sometimes called middleware, are scalable and highly available as they take on certain cloud characteristics.

PaaS Advantages

No matter the size of your company, using PaaS offers numerous advantages, including:

- Simple, cost-effective development and deployment of apps
- Scalable
- Highly available
- Developers can customize apps without the headache of maintaining the software

- Significant reduction in the amount of coding needed
- Automation of business policy
- Easy migration to the hybrid model

PaaS Characteristics

- Builds on virtualization technology, so resources can easily be scaled up or down as your business changes
- Provides a variety of services to assist with the development, testing, and deployment of apps
- Accessible to numerous users via the same development application
- Integrates web services and databases

When to Use PaaS

Utilizing PaaS is beneficial, sometimes even necessary, in several situations. For example, PaaS can streamline workflows when multiple developers are working on the same development project. If other vendors must be included, PaaS can provide great speed and flexibility to the entire process. PaaS is particularly beneficial if you need to create customized applications. This cloud service also can greatly reduce costs and it can simplify some challenges that come up if you are rapidly developing or deploying an app.

PaaS Limitations and Concerns

- **Data security.** Organizations can run their own apps and services using PaaS solutions, but the data residing in third-party, vendor-controlled cloud servers poses security risks and concerns. Your security options may be limited as customers may not be able to deploy services with specific hosting policies.
- **Integrations.** The complexity of connecting the data stored within an onsite data center or off-premise cloud is increased, which may affect which apps and services can be adopted with the PaaS offering. Particularly when not every component of a legacy IT system is built for the cloud, integration with existing services and infrastructure may be a challenge.
- **Vendor lock-in.** Business and technical requirements that drive decisions for a specific PaaS solution may not apply in the future. If the vendor has not provisioned convenient migration policies, switching to alternative PaaS options may not be possible without affecting the business.

- **Customization of legacy systems.** PaaS may not be a plug-and-play solution for existing legacy apps and services. Instead, several customizations and configuration changes may be necessary for legacy systems to work with the PaaS service. The resulting customization can result in a complex IT system that may limit the value of the PaaS investment altogether.
- **Runtime issues.** In addition to limitations associated with specific apps and services, PaaS solutions may not be optimized for the language and frameworks of your choice. Specific framework versions may not be available or perform optimally with the PaaS service. Customers may not be able to develop custom dependencies with the platform.
- **Operational limitation.** Customized cloud operations with management automation workflows may not apply to PaaS solutions, as the platform tends to limit operational capabilities for end users. Although this is intended to reduce the operational burden on end users, the loss of operational control may affect how PaaS solutions are managed, provisioned, and operated.

Examples of PaaS

Popular examples of PaaS include AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, and OpenShift.

IaaS: Infrastructure as a Service

Cloud infrastructure services, known as Infrastructure as a Service (IaaS), are made of highly scalable and automated compute resources. IaaS is fully self-service for accessing and monitoring computers, networking, storage, and other services. IaaS allows businesses to purchase resources on-demand and as-needed instead of having to buy hardware outright.

IaaS Delivery

IaaS delivers cloud computing infrastructure, including servers, network, operating systems, and storage, through virtualization technology. These cloud servers are typically provided to the organization through a dashboard or an API, giving IaaS clients complete control over the entire infrastructure. IaaS provides the same technologies and capabilities as a traditional data center without having to physically maintain or manage all of it. IaaS clients can still access their servers and storage directly, but it is all outsourced through a “virtual data center” in the cloud.

As opposed to SaaS or PaaS, IaaS clients are responsible for managing aspects such as applications, runtime, OSes, middleware, and data. However, providers of the IaaS manage the servers, hard drives, networking, virtualization, and storage. Some providers even offer more services beyond the virtualization layer, such as databases or message queuing.

IaaS Advantages

IaaS offers many advantages, including:

- The most flexible cloud computing model
- Easy to automate deployment of storage, networking, servers, and processing power
- Hardware purchases can be based on consumption
- Clients retain complete control of their infrastructure
- Resources can be purchased as-needed
- Highly scalable

IaaS Characteristics

Characteristics that define IaaS include:

- Resources are available as a service
- Cost varies depending on consumption
- Services are highly scalable
- Multiple users on a single piece of hardware
- Organization retain complete control of the infrastructure
- Dynamic and flexible

When to Use IaaS

Just as with SaaS and PaaS, there are specific situations when IaaS is most advantageous.

Startups and small companies may prefer IaaS to avoid spending time and money on purchasing and creating hardware and software. Larger companies may prefer to retain complete control over their applications and infrastructure, but they want to purchase only what they actually consume or need. Companies experiencing rapid growth like the scalability of IaaS, and they can change out specific hardware and software easily as their needs evolve. Anytime you are unsure of a new application's demands, IaaS offers plenty of flexibility and scalability.

IaaS Limitations and Concerns

Many limitations associated with SaaS and PaaS models – such as data security, cost overruns, vendor lock-in and customization issues – also apply to the IaaS model. Particular limitations to IaaS include:

- **Security.** While the customer is in control of the apps, data, middleware, and the OS platform, security threats can still be sourced from the host or other virtual machines (VMs). Insider threat or system vulnerabilities may expose data communication between the host infrastructure and VMs to unauthorized entities.
- **Legacy systems operating in the cloud.** While customers can run legacy apps in the cloud, the infrastructure may not be designed to deliver specific controls to secure the legacy apps. Minor enhancement to legacy apps may be required before migrating them to the cloud, possibly leading to new security issues unless adequately tested for security and performance in the IaaS systems.
- **Internal resources and training.** Additional resources and training may be required for the workforce to learn how to effectively manage the infrastructure. Customers will be responsible for data security, backup, and business continuity. Due to inadequate control into the infrastructure however, monitoring and management of the resources may be difficult without adequate training and resources available inhouse.
- **Multi-tenant security.** Since the hardware resources are dynamically allocated across users as made available, the vendor is required to ensure that other customers cannot access data deposited to storage assets by previous customers. Similarly, customers must rely on the vendor to ensure that VMs are adequately isolated within the multitenant cloud architecture.

Examples of IaaS

Popular examples of IaaS include DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metacloud, Microsoft Azure, and Google Compute Engine (GCE).

SaaS vs PaaS vs IaaS

Each cloud model offers specific features and functionalities, and it is crucial for your organization to understand the differences. Whether you need cloud-based software for storage options, a smooth platform that allows you to create customized applications, or complete control over your entire infrastructure without having to physically maintain it, there is a cloud service for you. No matter which option you choose, migrating to the cloud is the future of business and technology.

Architectural Design Challenges

Cloud computing is used for enabling global access to mutual pools of resources such as services, apps, data, servers, and computer networks. It is done on either a third-party server located in a data center or a privately owned cloud. This makes data-accessing contrivances more reliable and efficient, with nominal administration effort.

Because cloud technology depends on the allocation of resources to attain consistency and economy of scale, similar to a utility, it is also fairly cost-effective, making it the choice for many small businesses and firms.But there are also many challenges involved in cloud computing, and if you’re not prepared to deal with them, you won’t realize the benefits. Here are six common challenges you must consider before implementing cloud computing technology.

1. Cost

Cloud computing itself is affordable, but tuning the platform according to the company’s needs can be expensive. Furthermore, the expense of transferring the data to public clouds can prove to be a problem for short-lived and small-scale projects.

Companies can save some money on system maintenance, management, and acquisitions. But they also have to invest in additional bandwidth, and the absence of routine control in an infinitely scalable computing platform can increase costs.

2. Service Provider Reliability

The capacity and capability of a technical service provider are as important as price. The service provider must be available when you need them. The main concern should be the service provider’s sustainability and reputation. Make sure you comprehend the techniques via which a provider observes its services and defends dependability claims.

3. Downtime

Downtime is a significant shortcoming of cloud technology. No seller can promise a platform that is free of possible downtime. Cloud technology makes small companies reliant on their connectivity, so companies with an untrustworthy internet connection probably want to think twice before adopting cloud computing.

4. Password Security

Industrious password supervision plays a vital role in cloud security. However, the more people you have accessing your cloud account, the less secure it is. Anybody aware of your passwords will be able to access the information you store there.

Businesses should employ multi-factor authentication and make sure that passwords are protected and altered regularly, particularly when staff members leave. Access rights related to passwords and usernames should only be allocated to those who require them.

5. Data privacy

Sensitive and personal information that is kept in the cloud should be defined as being for internal use only, not to be shared with third parties. Businesses must have a plan to securely and efficiently manage the data they gather.

6. Vendor lock-in

Entering a cloud computing agreement is easier than leaving it. “Vendor lock-in” happens when altering providers is either excessively expensive or just not possible. It could be that the service is nonstandard or that there is no viable vendor substitute.

Cloud storage

Cloud storage is a model of computer data storage in which the digital data is stored in logical pools. The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

Cloud storage services may be accessed through a colocated cloud computing service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems. Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service (Amazon S3) or deployed on-premises (ViON Capacity Services). Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.

Object storage services like Amazon S3, Oracle Cloud Storage and Microsoft Azure Storage, object storage software like Openstack Swift, object storage systems like EMC Atmos, EMC ECS and Hitachi Content Platform, and distributed storage research projects like OceanStore and VISION Cloud are all examples of storage that can be hosted and deployed with cloud storage characteristics. Cloud storage is:

- Made up of many distributed resources, but still acts as one, either in a federated or acooperative storage cloud architecture
- Highly fault tolerant through redundancy and distribution of data
- Highly durable through the creation of versioned copies
- Typically eventually consistent with regard to data replicas

Advantages

- Companies need only pay for the storage they actually use, typically an average of consumption during a month. This does not mean that cloud storage is less expensive, only that it incurs operating expenses rather than capital expenses.
- Businesses using cloud storage can cut their energy consumption by up to 70% making them a more green business.
- Organizations can choose between off-premises and on-premises cloud storage options, or a mixture of the two options, depending on relevant decision criteria that is complementary to initial direct cost savings potential; for instance, continuity of operations (COOP), disaster recovery (DR), security (PII, HIPAA, SARBOX, IA/CND), and records retention laws,

regulations, and policies.

- Storage availability and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, effort and cost to add availability and protection can be eliminated.
- Storage maintenance tasks, such as purchasing additional storage capacity, are offloaded to the responsibility of a service provider.
- Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a web service interface.
- Cloud storage can be used for copying virtual machine images from the cloud to on- premises locations or to import a virtual machine image from an on-premises location to the cloud image library. In addition, cloud storage can be used to move virtual machine images between user accounts or between data centers.[15]
- Cloud storage can be used as natural disaster proof backup, as normally there are 2 or 3different backup servers located in different places around the globe.
- Cloud storage can be mapped as a local drive with the WebDAV protocol. It can function as a central file server for organizations with multiple office locations.

Storage as a Service

Storage as a service (SaaS) is a cloud business model in which a company leases or rents its storage infrastructure to another company or individuals to store data. Small companies and individuals often find this to be a convenient methodology for managing backups, and providing cost savings in personnel, hardware and physical space.

As an alternative to storing magnetic tapes offsite in a vault, IT administrators are meeting their storage and backup needs by service level agreements (SLAs) with an SaaS provider, usually on a cost-per-gigabyte-stored and cost-per-data-transferred basis. The client transfers the data meant for storage to the service provider on a set schedule over the SaaS provider’s wide area network or over the Internet.

The storage provider provides the client with the software required to access their stored data. Clients use the software to perform standard tasks associated with storage, including data transfers and data backups. Corrupted or lost company data can easily be restored.

Storage as a service is prevalent among small to mid-sized businesses, as no initial budget is required to set up hard drives, servers and IT staff. SaaS is also marketed as an excellent technique to mitigate risks in disaster recovery by providing long-term data storage and enhancing business stability.

Storage as a service is fast becoming the method of choice to all small and medium scale businesses. This is because storing files remotely rather than locally boasts an array of advantages for professional users.

Top 10 advantage of Storage as a Services

1. **Cost**– factually speaking, backing up data isn’t always cheap, especially when take the cost of equipment into account. Additionally, there is the cost of the time it takes to manually complete routine backups. Storage as a service reduces much of the cost associated with traditional backup methods, providing ample storage space in the cloud for a low monthly fee.
2. **Invisibility** – Storage as a service is invisible, as no physical presence of it is seen in its deployment and so it doesn’t take up valuable office space.
3. **Security** – In this service type, data is encrypted both during transmission and while at rest, ensuring no unauthorized user access to files.
4. **Automation** – Storage as a service makes the tedious process of backing up easy to accomplish through automation. Users can simply select what and when they want to backup, and the service does all the rest.
5. **Accessibility** – By going for storage as a service, users can access data from smart phones, netbooks to desktops and so on.
6. **Syncing** – Syncing ensures your files are automatically updated across all of your devices. This way, the latest version of a file a user saved on their desktop is available on your smart phone.
7. **Sharing** – Online storage services allow the users to easily share data with just a few clicks
8. **Collaboration** – Cloud storage services are also ideal for collaboration purposes. They allow multiple people to edit and collaborate on a single file or document. Thus, with this feature users need not worry about tracking the latest version or who has made what changes.
9. **Data Protection** – By storing data on cloud storage services, data is well protected by all kind of catastrophes such as floods, earthquakes and human errors.
10. **Disaster Recovery** – as said earlier, data stored in cloud is not only protected from catastrophes by having the same copy at several places, but can also favor disaster recovery to ensure business continuity.

Advantages of Cloud Storage

- Cloud storage has given users the ability to share and access files remotely without access to their local storage systems.
- While this has opened up many doors for video teams there are some considerations that need to be made before implementing cloud storage into your video workflow.
- Below are 5 Advantages and 5 Disadvantages of Cloud Storage:

Advantages of Cloud Storage

Cost

Purchasing physical storage can be expensive. Without the need for hardware cloud storage is exceptionally cheaper per GB than using external drives.

Accessibility

Using the cloud for storage gives you access to your files from anywhere that has an internet connection.

Recovery

In the event of a hard drive failure or other hardware malfunction, you can access your files on the cloud. It acts as a backup solution for your local storage on physical drives.

Syncing and Updating

When you are working with cloud storage, every time you make changes to a file it will be synced and updated across all of your devices that you access the cloud from.

Security

Cloud storage providers add additional layers of security to their services. Since there are many people with files stored on the cloud, these providers go to added lengths to make sure your files don't get accessed by someone who shouldn't

Disadvantages of Cloud Storage

Internet Connection

Cloud based storage is dependent on having an internet connection. If you are on a slow network you may have issues accessing your storage. In the event you find yourself somewhere without internet, you won't be able to access your files.

Costs

There are additional costs for uploading and downloading files from the cloud. These can quickly add up if you are trying to access lots of files often.

Hard Drives

Cloud storage is supposed to eliminate our dependency on hard drives right? Well some business cloud storage providers require physical hard drives as well.

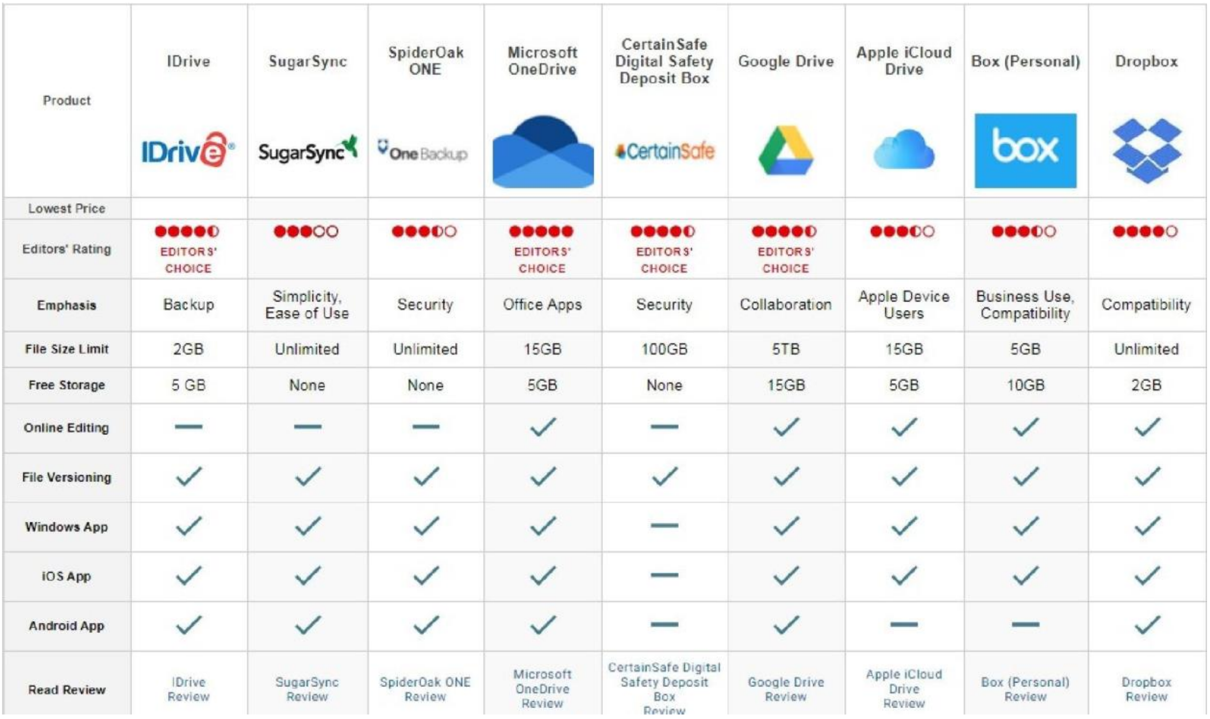
Support

Support for cloud storage isn't the best, especially if you are using a free version of a cloud provider. Many providers refer you to a knowledge base or FAQs.

Privacy

When you use a cloud provider, your data is no longer on your physical storage. So who is responsible for making sure that data is secure? That's a gray area that is still being figured out.

Cloud Storage Providers



Product	IDrive	SugarSync	SpiderOak ONE	Microsoft OneDrive	CertainSafe Digital Safety Deposit Box	Google Drive	Apple iCloud Drive	Box (Personal)	Dropbox
Lowest Price									
Editors' Rating	●●●●◐ EDITORS' CHOICE	●●●○○	●●●◐○	●●●●● EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●◐○	●●●◐○	●●●●○
Emphasis	Backup	Simplicity, Ease of Use	Security	Office Apps	Security	Collaboration	Apple Device Users	Business Use, Compatibility	Compatibility
File Size Limit	2GB	Unlimited	Unlimited	15GB	100GB	5TB	15GB	5GB	Unlimited
Free Storage	5 GB	None	None	5GB	None	15GB	5GB	10GB	2GB
Online Editing	—	—	—	✓	—	✓	✓	✓	✓
File Versioning	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows App	✓	✓	✓	✓	—	✓	✓	✓	✓
iOS App	✓	✓	✓	✓	—	✓	✓	✓	✓
Android App	✓	✓	✓	✓	—	✓	—	—	✓
Read Review	IDrive Review	SugarSync Review	SpiderOak ONE Review	Microsoft OneDrive Review	CertainSafe Digital Safety Deposit Box Review	Google Drive Review	Apple iCloud Drive Review	Box (Personal) Review	Dropbox Review