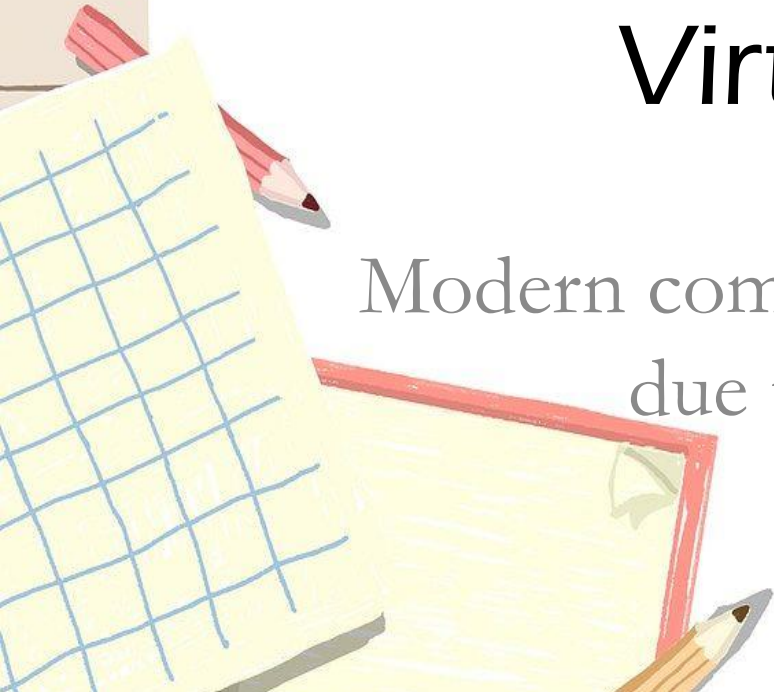


# Virtualization

Modern computing is more efficient  
due to virtualization



# Lets think like this

- Have you ever wished you could clone yourself?
- If you could, would you be more efficient? Would you do more?
- Virtualization enables computers to be more efficient in a similar fashion
- Computers that use virtualization optimize the available compute resources

# Lets ponder on this...

- Do you use a smartphone, laptop or home computer?
- Smartphones, laptops or home computers are hardware
- Similar to how your brain controls your actions, software controls hardware
- There are different types of software that control computer actions

# What is a VM

- Virtualization creates virtual hardware by cloning physical hardware
- The hypervisor uses virtual hardware to create a virtual machine (VM)
- A VM is a set of files
- With a hypervisor and VMs, one computer can run multiple OS simultaneously

# Terminologies

- **Host Operating System:** The operating system via which the Virtual Machines are run. For Type 1 Hypervisors, as in Hyper-V, the hypervisor itself is the Host OS which schedules the virtual machines and allocates memory. For Type 2 hypervisors, the OS on which the hypervisor applications run is the Host OS.
- **Guest Operating System:** The operating system that uses virtualized hardware. It can be either Fully Virtualized or Para Virtualized. An enlightened guest OS knows that its a virtualized system which can improve performance.
- **Virtual Machine Monitor:** VMM is the application that virtualizes hardware for a specific virtual machine and executes the guest OS with the virtualized hardware.

# Concepts

- Virtualization is technology that allows you to create multiple simulated environments or dedicated resources from a single, physical hardware system.
- Software called a hypervisor connects directly to that hardware and allows you to split 1 system into separate, distinct, and secure environments known as virtual machines (VMs).



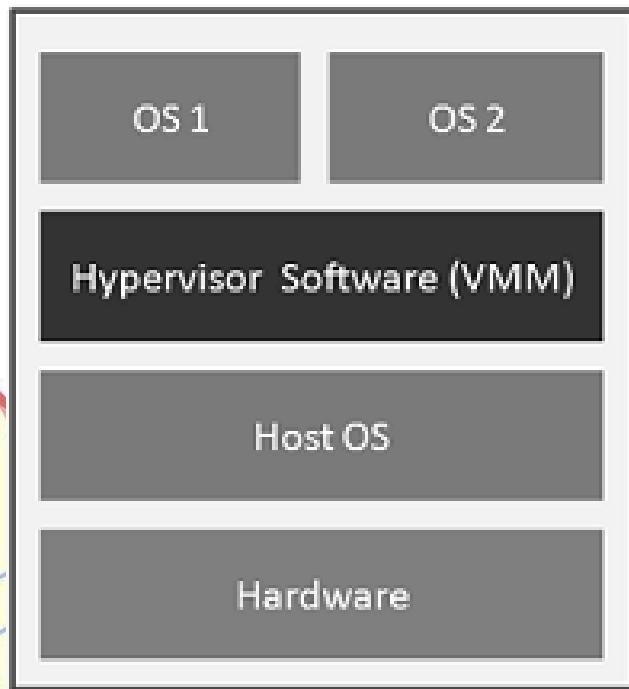
# Hypervisors

- A hypervisor is a process or a function to isolate operating system and applications from the underlying hardware.
- Though virtual machines operate on the same physical hardware, they are separated from each other. This also depicts that if one virtual machine undergoes a crash, error, or a malware attack, it doesn't affect the other virtual machines.
- Another benefit is that virtual machines are very mobile as they don't depend on the underlying hardware. Since they are not linked to physical hardware, switching between local or remote virtualized servers gets a lot easier as compared to traditional applications.

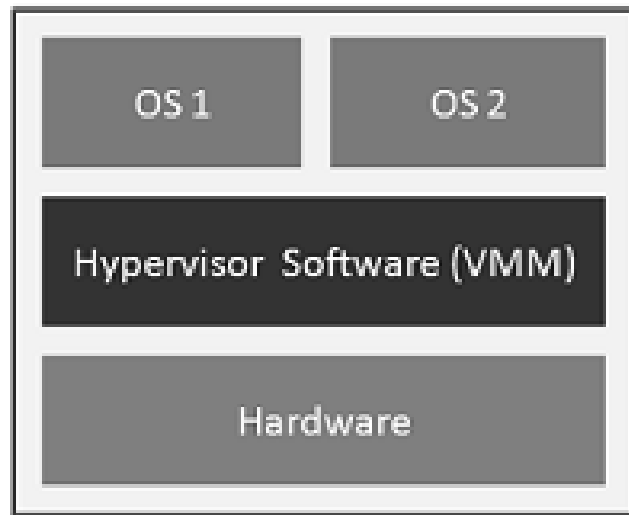
# Types of Hypervisor

- A type-I hypervisor operates directly on the host's hardware to monitor hardware and guest virtual machines, and it's referred to as the bare metal.
- A type-II, also called a hosted hypervisor because it is usually installed onto an existing operating system. They are not much capable to run more complex virtual tasks. Used for basic development, testing, and emulation.





**Hosted Architecture**



**Bare-Metal Architecture**

# Differences

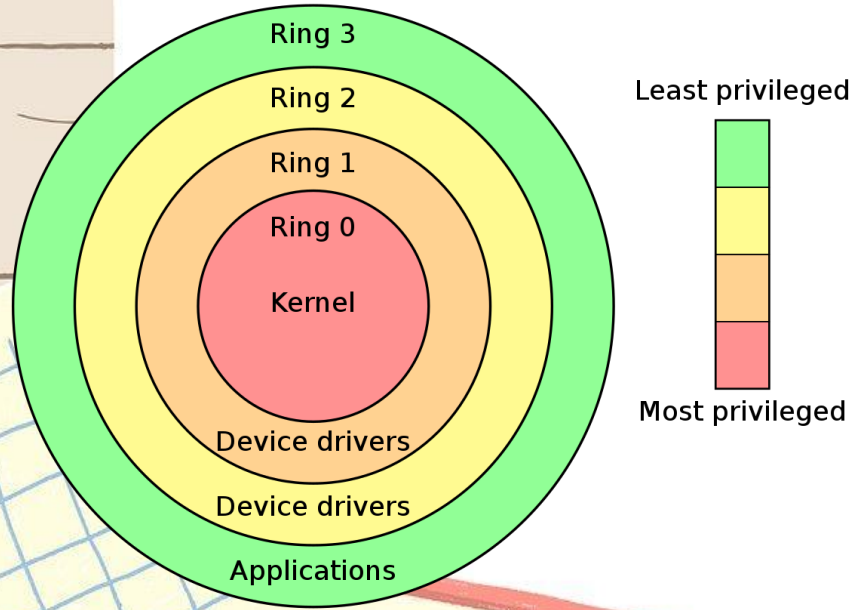
## What's the difference between virtualization and cloud computing?

- It's easy to confuse the two, particularly because they both revolve around separating resources from hardware to create a useful environment. Virtualization helps create clouds, but that doesn't make it cloud computing. Think about it like this:
- Virtualization is a technology that separates functions from hardware
- Cloud computing is more of a solution that relies on that split

# X86 Virtualization

- **x86 virtualization** refers to hardware and software-based mechanisms to support virtualization for processors based on the x86 architecture . Using a hypervisor , it allows several operating systems to be run in parallel on an x86 processor and resources to be distributed in an isolated and efficient manner between the operating systems running in parallel.

- In order to be able to allocate resources exclusively to the guest systems running in parallel, only the host operating system or the hypervisor may be granted direct access to the processor hardware, while the guest systems, like all other applications, may only have limited access rights to the hardware. In particular, it can be prevented that the guest systems can see or change memory areas that the hypervisor needs for management.
- The protected mode was introduced in the x86 world . With it, four different protection levels or *privilege levels*, *known* as rings, were introduced, which grant the code segments running on them different rights. Only with the introduction of this concept was it possible to implement virtualization based on the x86 architecture: In protected mode, the operating system kernel runs in a more privileged mode, called Ring 0 , and applications in a less privileged mode, in usually either ring 1 or ring 3.



- The hypervisor or the host operating system are executed with ring 0 authorization due to their privileged position in resource management. In order to guarantee the protection of the hypervisor resources, guest systems must therefore be run either at authorization level Ring 1 (in the so-called Ring 3).

# Types of Hardware Virtualization

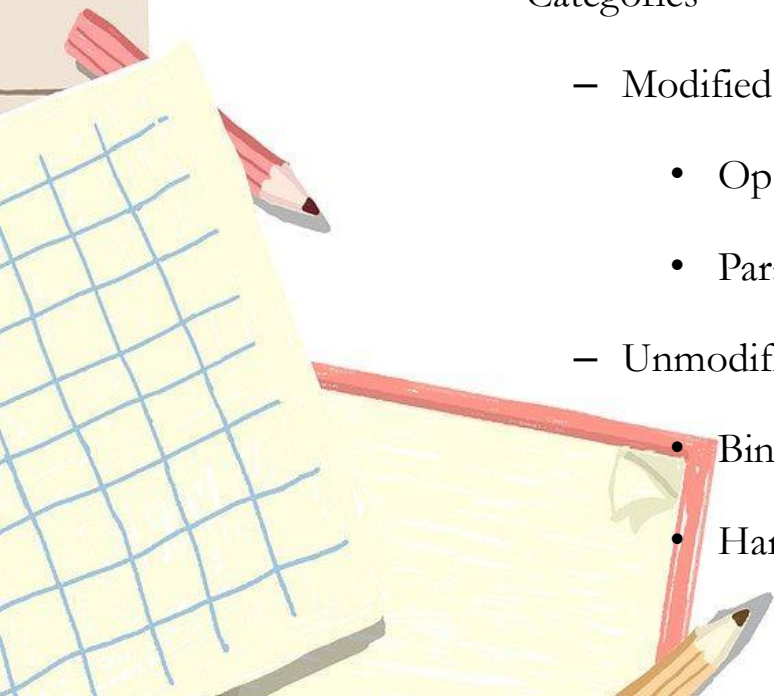
- Full Virtualization
- Para-virtualization
- Hardware Assisted Virtualization

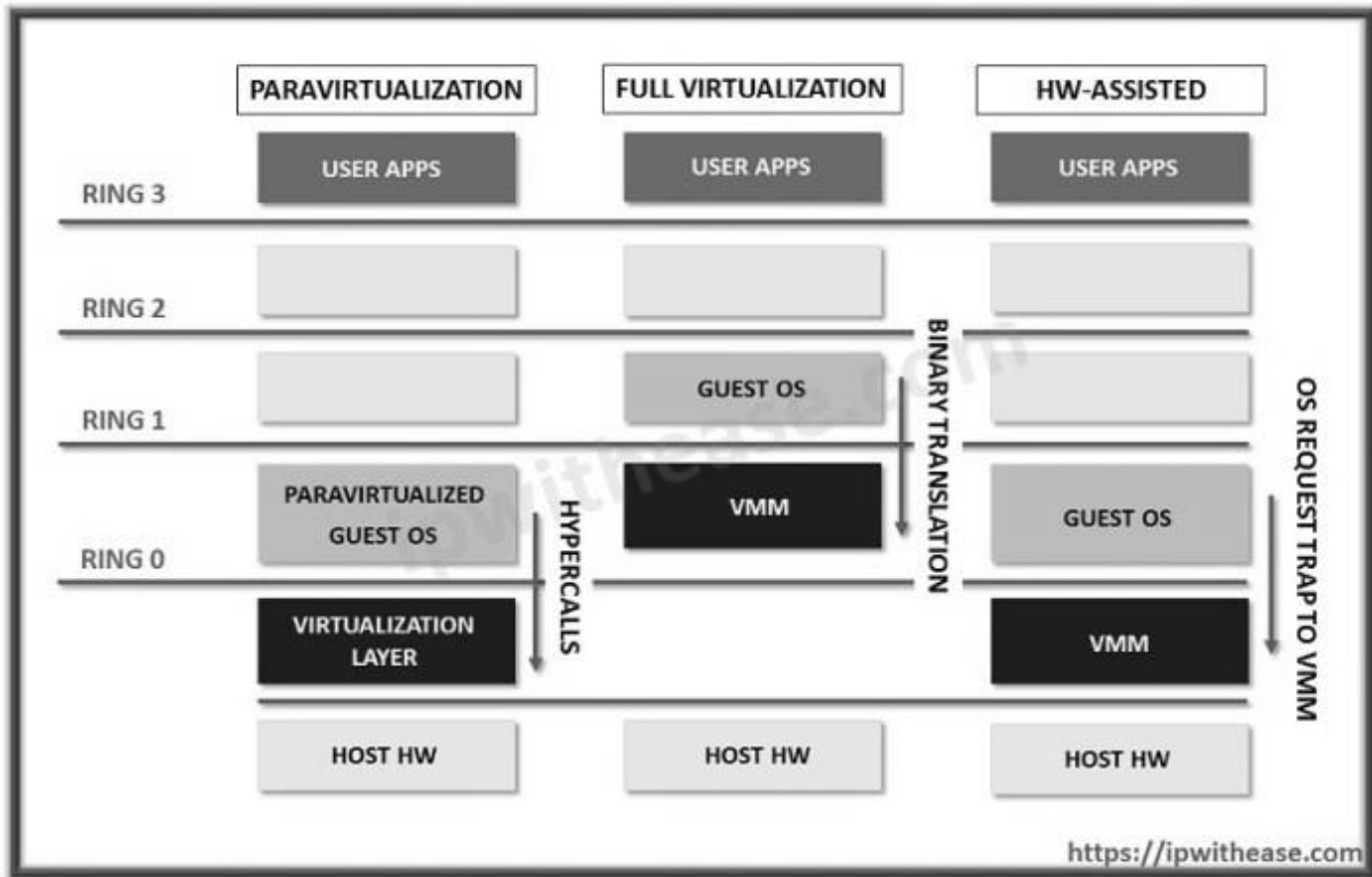




# What to change

- Based on how much change is required and at what level
- Categories
  - Modified Guest OS
    - Operating system level
    - Para-virtualization.
  - Unmodified Guest OS
    - Binary Translations
    - Hardware assisted





# Full virtualization

- In this scenario, data is completely abstracted from the underlying hardware by the virtualization layer. In this technique guest, OS is unaware that it is a guest and hypervisor translate all OS calls on-the-fly. It provides flexibility and no hardware assistance or modification is required.
- The advantages of full virtualization are that the emulation layer isolates VMs from the host OS and from each other. It also controls individual VM access to system resources, preventing an unstable VM from impacting system performance.
- It also provides the total VM portability by emulating a consistent set of system hardware, VMs have the ability to transparently move between hosts with dissimilar hardware without any problems. The products support this virtualization are VMware, Microsoft, and KVM.

# Para Virtualization

- It is an enhancement of virtualization technology in which a guest OS is recompiled prior to installation inside a virtual machine. In para-virtualization, the guest OS is modified to enable communication with the hypervisor to improve performance and efficiency.
- Its advantages are that the guest system comes closer to native performance than a fully virtualized guest and also it does not require the latest virtualization CPU support. It also allows for an interface to the virtual machine that can differ somewhat from that of the underlying hardware.
- VMware and Xen are supported by this type of virtualization.

# Hardware-assisted Virtualization

- It enables full virtualization with help of utilizing of a computer's physical components to support the software that creates and manages virtual machines. In this technique of virtualization unmodified guest OS and no API are made. The sensitive calls are trapped by the hypervisor and in 2006 it was added to x86 processors (Intel VT-x or AMD-V).
- The products supporting hardware-assisted virtualization are VMware, Xen, Microsoft, and Parallels.
- There is additionally a mix of para-virtualization and full virtualization called **Hybrid Virtualization** where parts of the visitor working on paravirtualization for certain hardware drivers, and the host utilizes full virtualization for different highlights. This frequently delivers prevalent execution on the visitor without the requirement for the visitor to be totally par-virtualized.

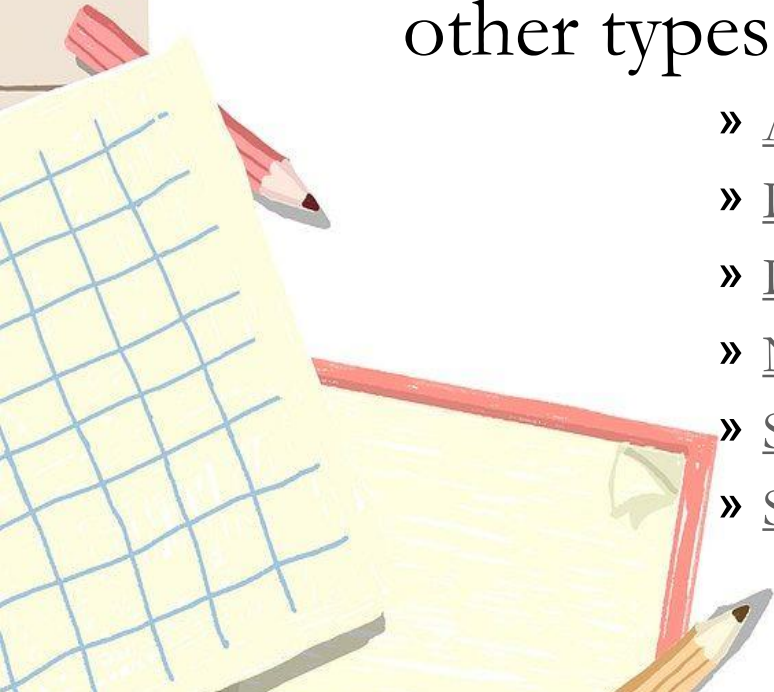
# Comparisons

PARAMETER	FULL VIRTUALIZATION	PARA VIRTUALIZATION	HARDWARE ASSISTED VIRTUALIZATION
Generation	1st	2nd	3rd
Performance	Good	Better in certain cases	Fair
Used By	VMware, Microsoft, KVM	VMware, Xen	VMware, Xen, Microsoft, Parallels
Guest OS modification	Unmodified	Codified to issue hypercalls	Unmodified
Guest OS hypervisor independent?	Yes	XenLinux runs only on Hypervisor	Yes
Technique	Direct execution	Hypercalls	Exit to root mode on privileged instruction
Compatibility	Excellent	Poor	Excellent

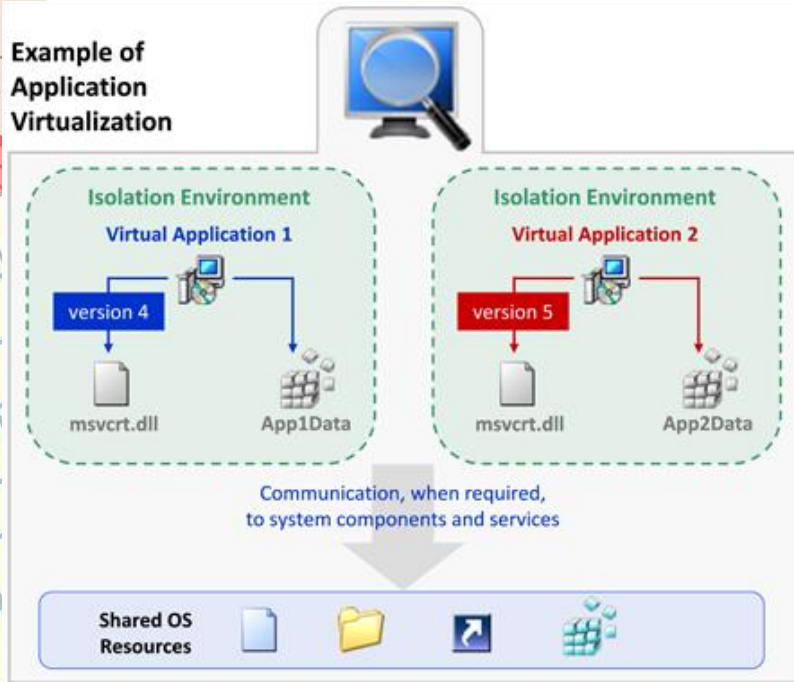


# Types of Virtualization

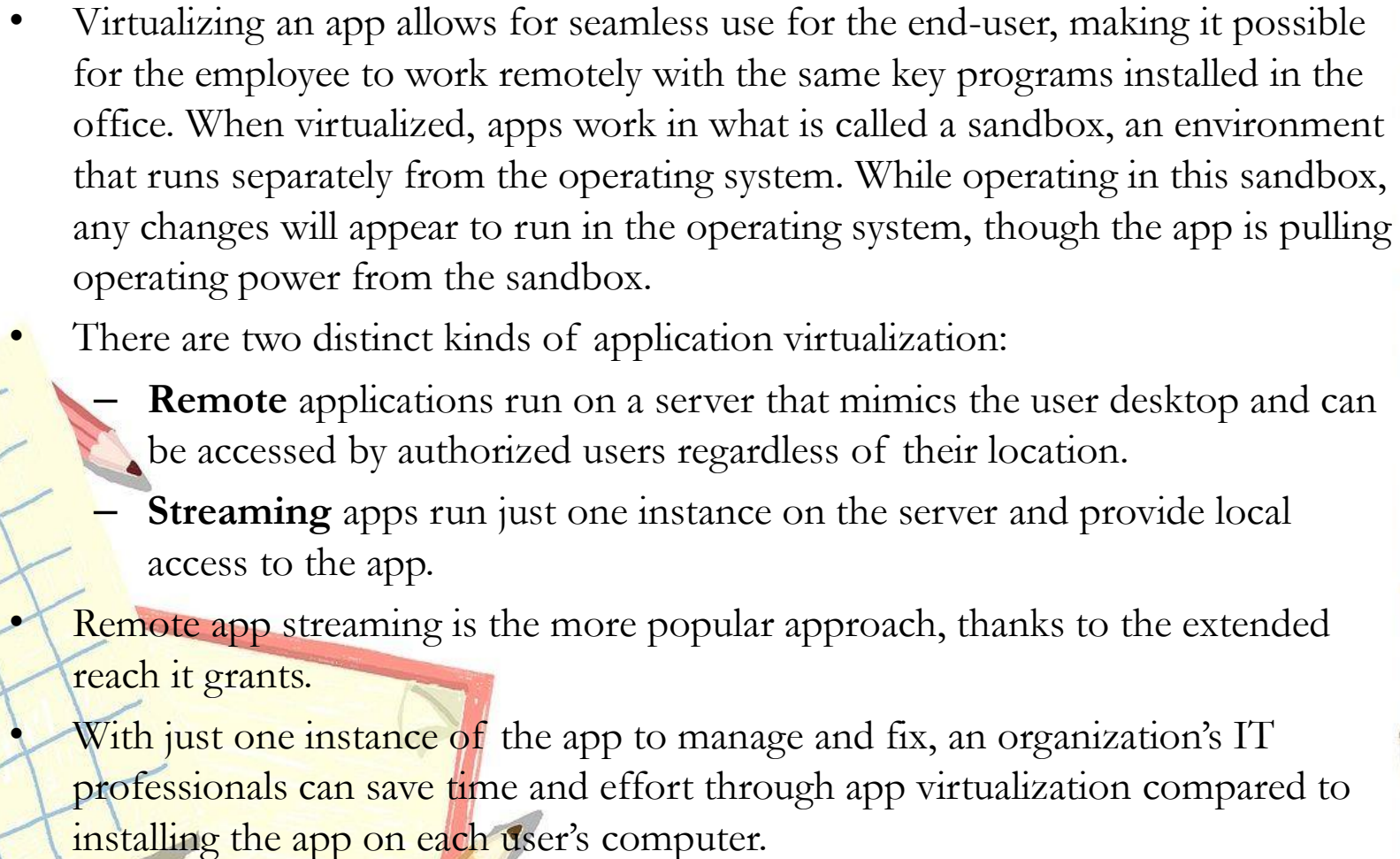
- Apart from hardware virtualization, other types of virtualization include:
  - » Application Virtualization
  - » Data Virtualization
  - » Desktop Virtualization
  - » Network Virtualization
  - » Server Virtualization
  - » Storage Virtualization



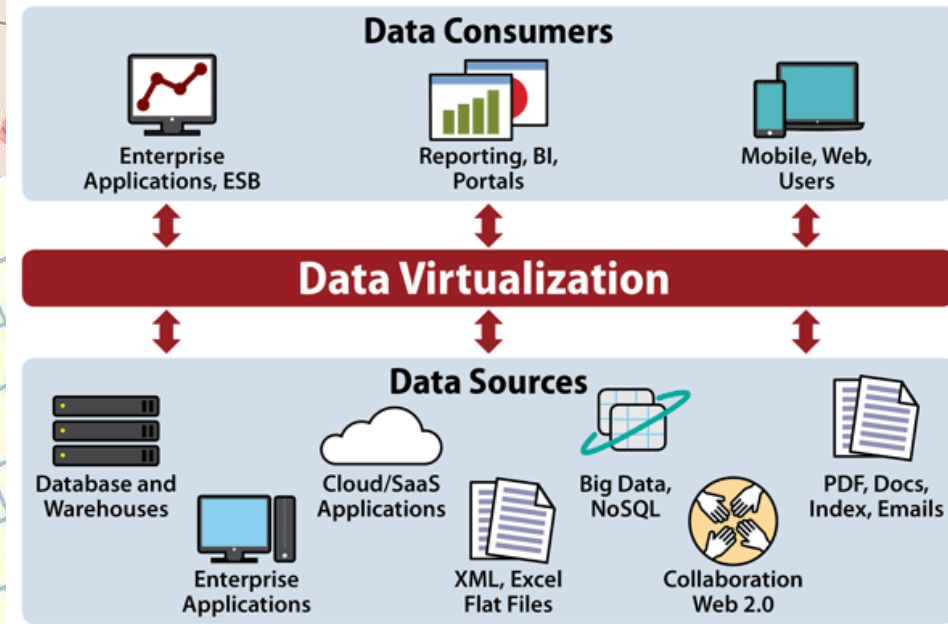
# Application virtualization



- The process of installing an application on a central server (single computer system) that can virtually be operated on multiple systems is known as application virtualization. For end users, the virtualized application works exactly like a native application installed on a physical machine. With application virtualization, it's easier for organizations to update, maintain, and fix applications centrally. Admins can control and modify access permissions to the application without logging in to the user's desktop.

- 
- Virtualizing an app allows for seamless use for the end-user, making it possible for the employee to work remotely with the same key programs installed in the office. When virtualized, apps work in what is called a sandbox, an environment that runs separately from the operating system. While operating in this sandbox, any changes will appear to run in the operating system, though the app is pulling operating power from the sandbox.
  - There are two distinct kinds of application virtualization:
    - **Remote** applications run on a server that mimics the user desktop and can be accessed by authorized users regardless of their location.
    - **Streaming** apps run just one instance on the server and provide local access to the app.
  - Remote app streaming is the more popular approach, thanks to the extended reach it grants.
  - With just one instance of the app to manage and fix, an organization's IT professionals can save time and effort through app virtualization compared to installing the app on each user's computer.

# Data Virtualization



- Data virtualization is a data management approach. It retrieves, segregates, manipulates, and delivers data without any data specifications.
- Any technical details of the data like its exact location and formatting information are not needed to access it. It allows the application to get a singular view of the overall data with real-time access.
- Data virtualization software helps with data warehouse management and eliminates latency. It also provides users with on-demand integration, quick analysis, and real-time search and reports capabilities.

# Desktop virtualization

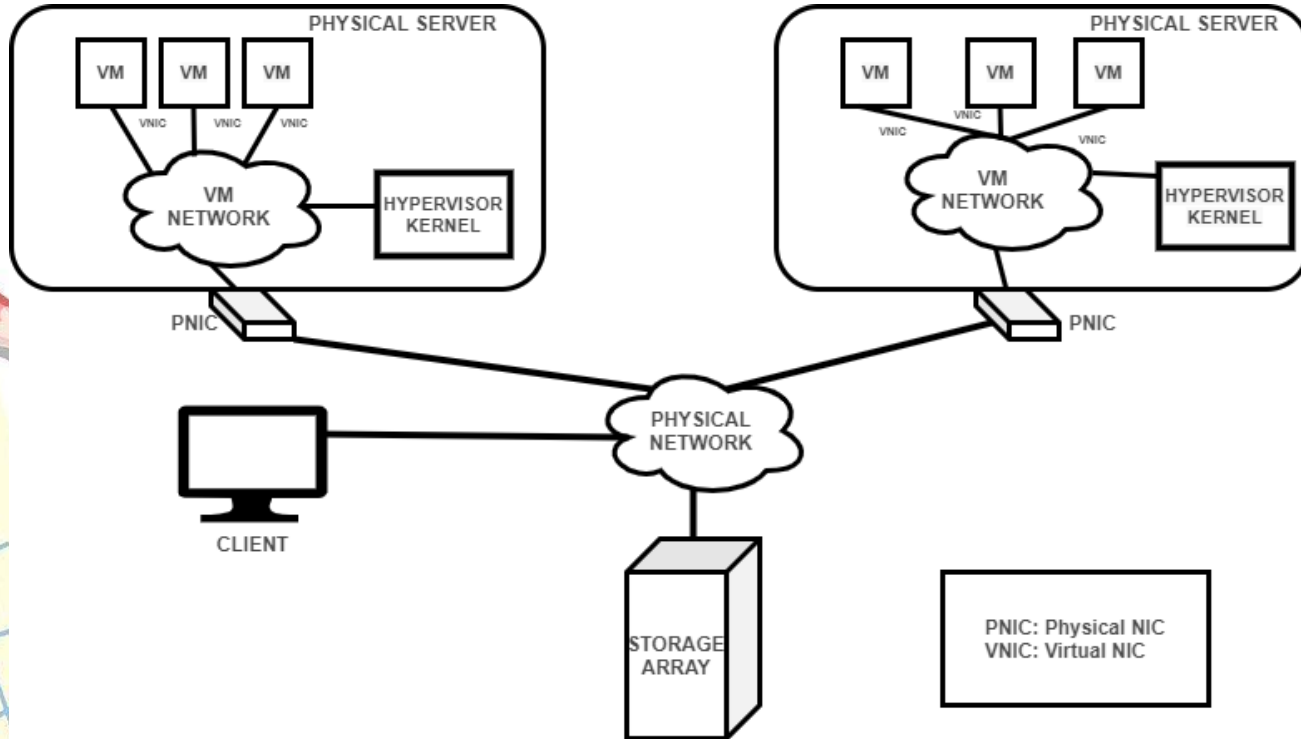
## Desktop Virtualization



- Creating a virtual desktop infrastructure, or VDI, makes it possible to work and store files in locations that everyone in your team can easily access no matter where they work.
- Desktop virtualization allows people to access multiple applications and operating systems (OS) on a single computer because the applications and OSs are installed on virtual machines that run on a server in the data centre.
- **When it comes to desktop virtualization, there are two main methods: local and remote. Local and remote desktop virtualization** are both possible depending on the business needs.
- Remote desktop virtualization is more robust and popular in the marketplace, with users running operating systems and applications accessed from a server located inside a secure data center.

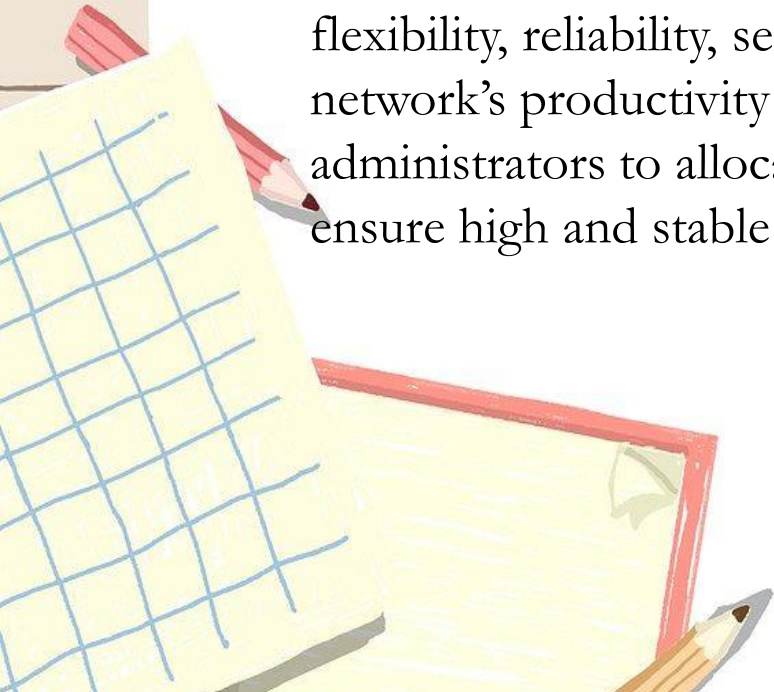


# Network virtualization



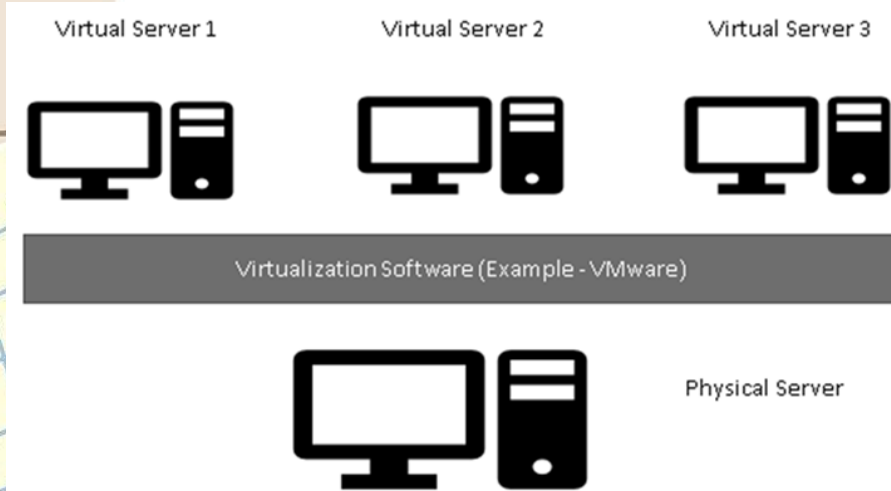


- Network virtualization helps manage and monitor the entire computer network as a single administrative entity. Admins can keep a track of various elements of network infrastructure such as routers and switches from a single software-based administrator's console. Network virtualization helps network optimization for data transfer rates, flexibility, reliability, security, and scalability. It improves the overall network's productivity and efficiency. It becomes easier for administrators to allocate and distribute resources conveniently and ensure high and stable network performance.

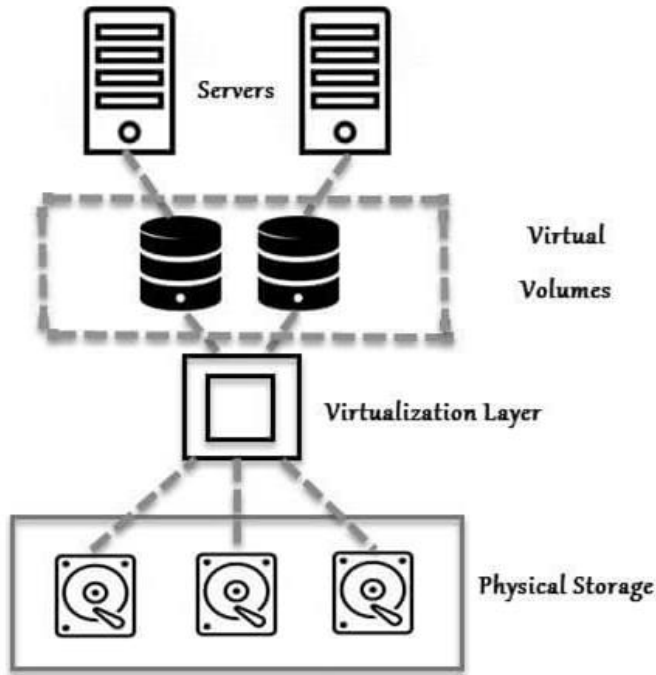


# Server virtualization

Server virtualization is a process of partitioning the resources of a single server into multiple virtual servers. These virtual servers can run as separate machines. Server virtualization allows businesses to run multiple independent OSs (guests or virtual) all with different configurations using a single (host) server. The process also saves the hardware cost involved in keeping a host of physical servers, so businesses can make their server infrastructure more streamlined.



# Storage virtualization



- Storage virtualization performs resource abstraction in a way that the multiple physical storage arrays are virtualized as a single storage pool with direct and independent access.
- The storage virtualization software aggregates and manages storage in various storage arrays and serves it to applications whenever needed.
- The centralized virtual storage increases flexibility and availability of resources needed. This data virtualization and centralization is easily manageable from a central console. It allows users to manage and access multiple arrays as a single storage unit.