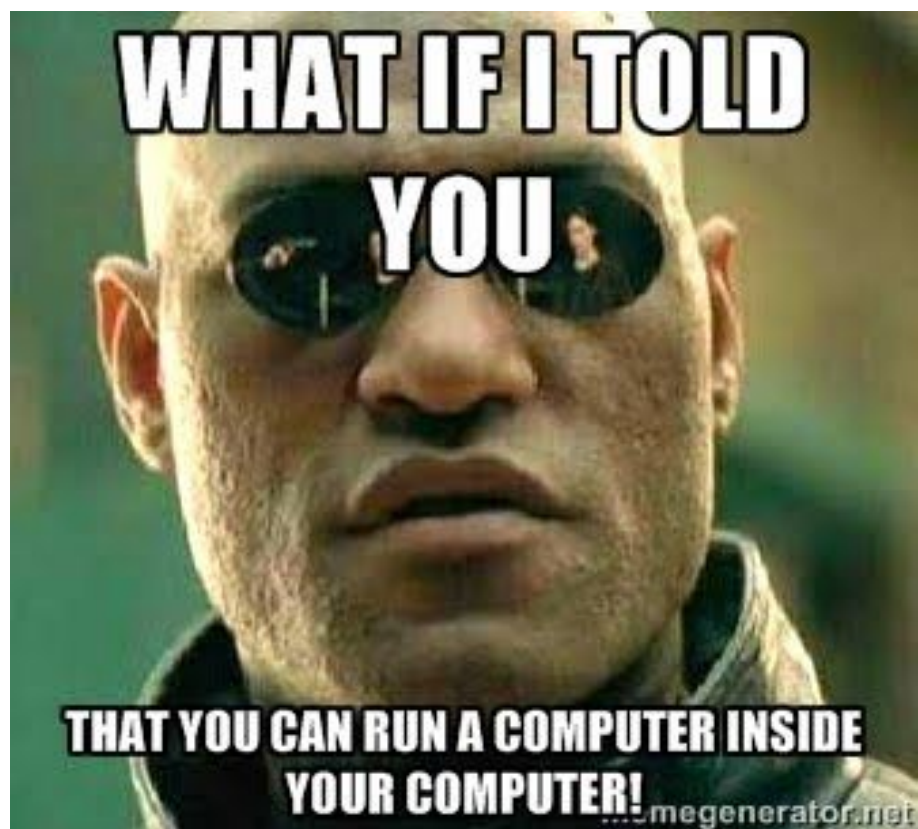# Virtualization

By: Andrew Mavrogeorgis

Hardware

- Physical components that a computer system requires to function.
- Easy to change out and upgrade.
- Large determinant of how fast your computer operates.
- Software is the programming that tells all these components what to do.

Operating System

- Core set of software that holds everything together.
- Operates systems communication with hardware.
- Handles I/O Peripherals.
- Launches and manages applications.
- Common examples includes Windows, Ubuntu and Mac OS.
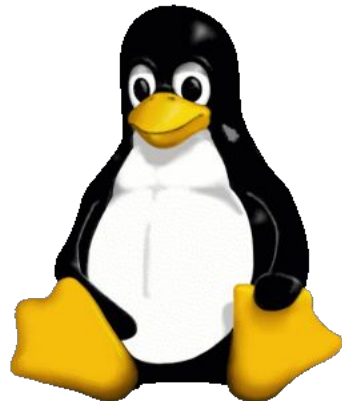
What you are probably accustomed to..
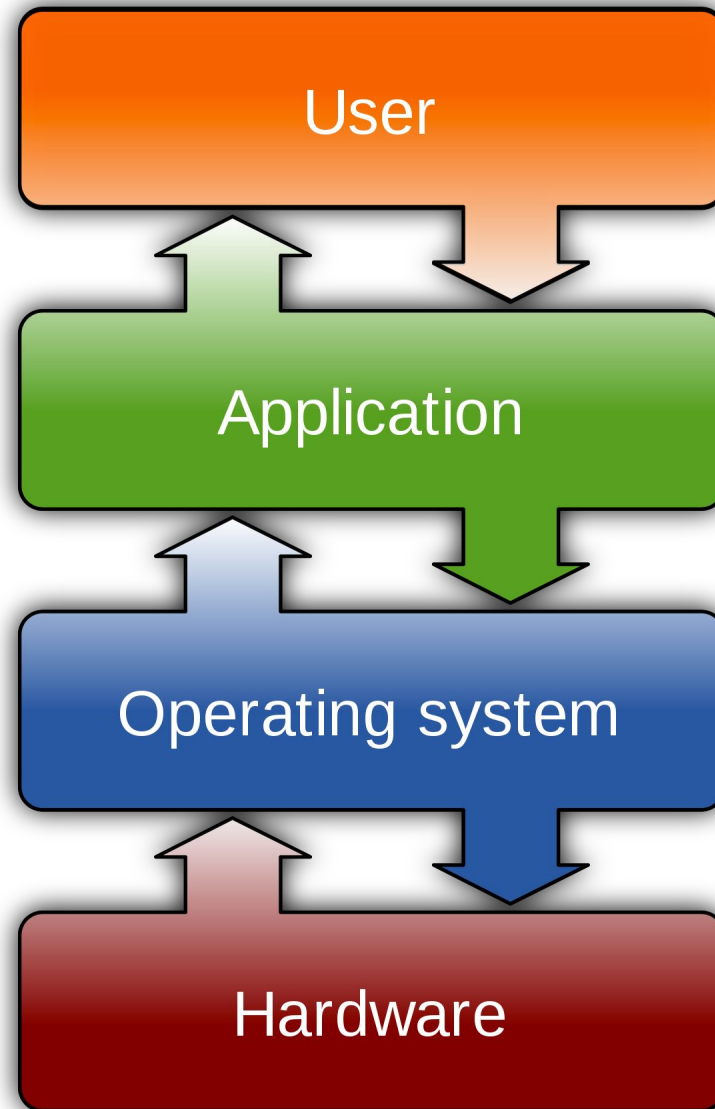
Central Processing Unit(CPU)

- Stands for Central Processing Unit, carries out the instructions of a computer program(processes), executing code.

- Does this by performing basic arithmetic, logical, control and input/output commands.

- The computer's processor is like a chef, who works to prepare the food. The faster the chef, the faster food is ready.

Random Access Memory (RAM)

- Stands for Random Access Memory.
- A form of computer storage that stores data and machine code currently being used.
- Used by operating system for working applications and processes.
- The computer's RAM is like counter-top space. Everything is temporary,

Disk

- Non-volatile permanent storage.
- Stores data even when they are off.
- Where the operating system, files and application are stored
- The computer's disk is like the cupboards and refrigerator. These things hold the ingredients until the chef needs them.
- SSD, HDD, Flash

I/O

- Allows us(the humans) to interact with the computer.
- Mouse, Keyboard, CD-ROM, Printer, Video Monitor
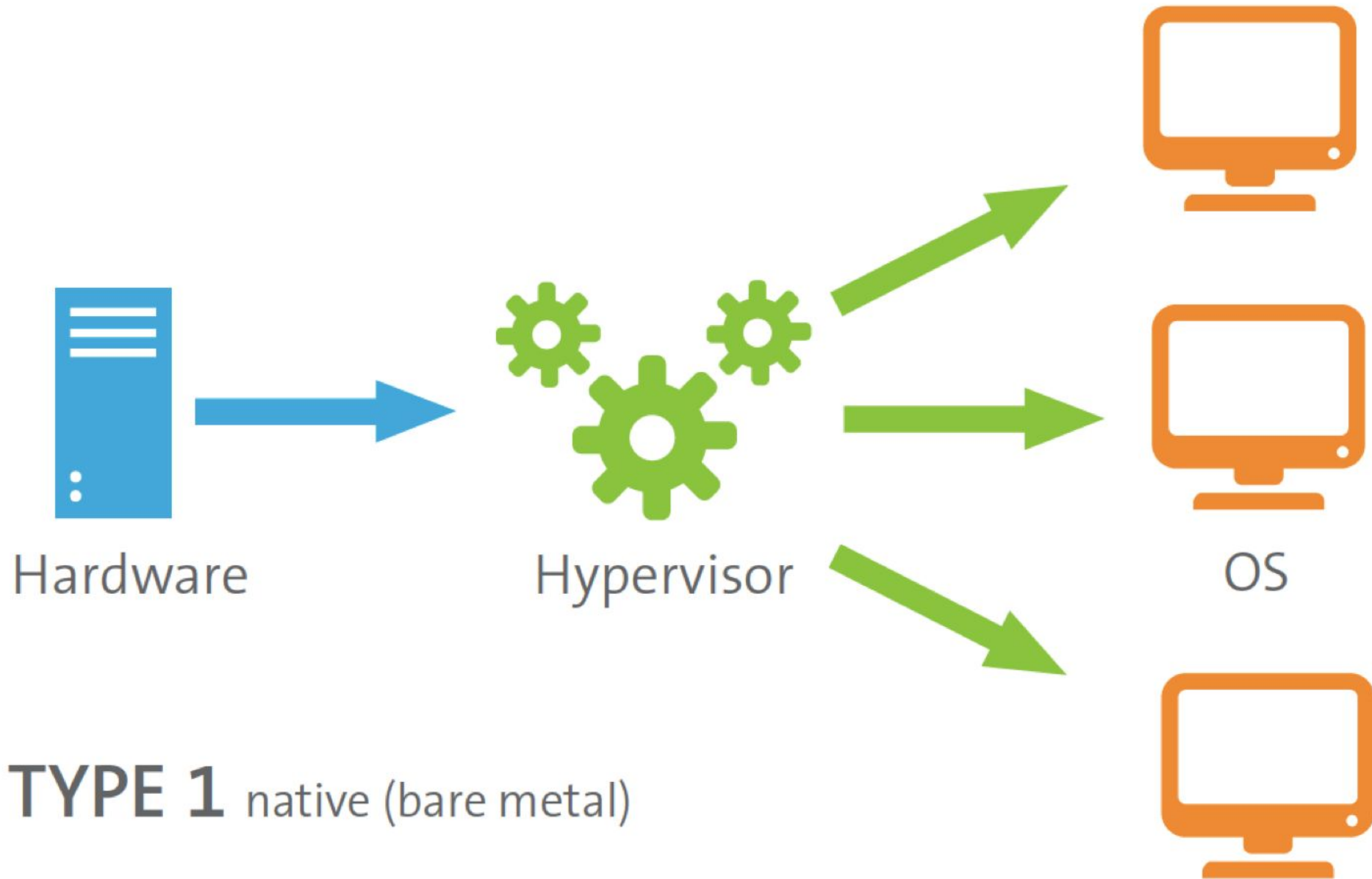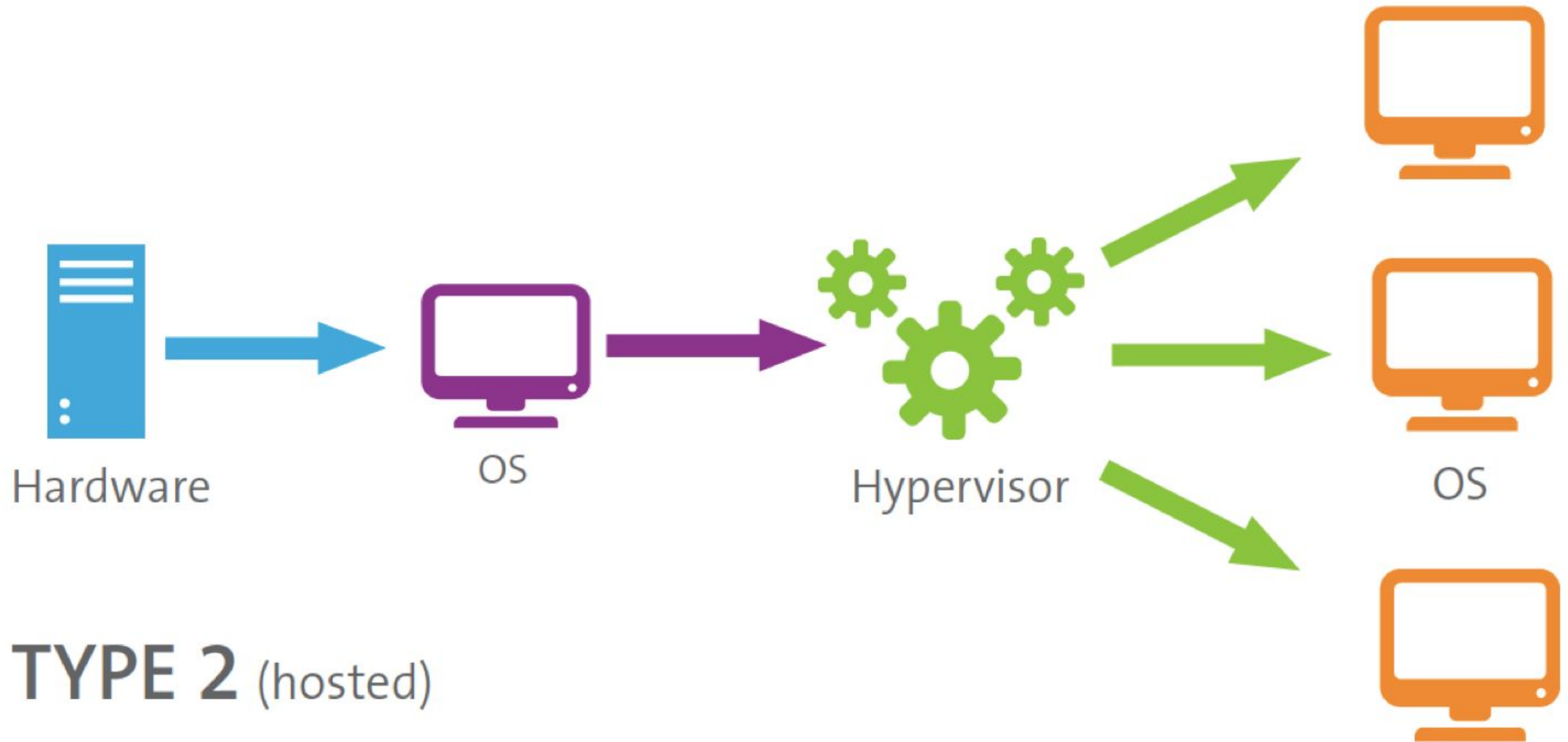- Some are one, others are both.

What is virtualization?

- Virtualization is the process of creating a software-based, or virtual, representation of something, such as virtual applications, servers, storage and networks.

- This practice allows IT organizations to operate multiple operating systems, more than one virtual system and various applications on a single server.

- Most effective way to reduce IT expenses while boosting efficiency and agility.

- Allows you to use a physical machine's full capacity by distributing its capabilities among many users or environments.

How does virtualization work?

- A thin software layer, known as a hypervisor, reproduces the functions and actions of the underlying hardware for the abstracted hardware or software.
- It will appear that a individual virtual machine will have its own memory and processor.
- The hypervisor is actually the one that are allocating those resources to the virtual machines.
- It is important to note that there are two different types of hypervisors.
- Type 1 that runs on bare metal(ie:Vmware esxi,Microsoft Hyper-V), and type 2(Virtual Box, Vmware Fusion, etc) that sits on top of an operating system.

Hardware → Hypervisor → OS

TYPE 1 native (bare metal)

Photo Source: Flexiant.com

Hardware → OS → Hypervisor → OS

TYPE 2 (hosted)

Virtualization Key Terms

Virtual Machine - a software computer comprised of configuration files and backed by the physical resources of a host

Hypervisor - A Hypervisor is an OS that separates a computer's operating system and applications from the underlying physical hardware

Host System - OS installed on physical hardware Guest System - Virtualized OS on top of Host System.

Guest System- Virtualized OS on top of host system

So what are the benefits of Virtualization?

Security	→	Separates application from interfering with each other.
Testing	→	Open unknown, potentially malicious files.
Learning	→	Try out new programs without having to worry.
Optimization	→	Use what you have more efficiently

Characteristics of Virtual Machines

- **Partitioning**
  - Run multiple operating systems on one physical machine.
  - Divide system resources between virtual machines.
- **Isolation**
  - Provide fault and security isolation at the hardware level.
  - Preserve performance with advanced resource controls.
- **Encapsulation**
  - Save the entire state of a virtual machine to files.
  - Move and copy virtual machines as easily as moving and copying files.
- **Hardware Independence**
  - Provision or migrate any virtual machine to any physical server.

Source: Frank Baitia

What is paravirtualization?

- Rather then emulating a complete hardware environment, guest operating systems work together to utilize resources and work well together.
- This is able to happen because we modify the kernel of the guest operating system to run directly on the hypervisor.
- The hypervisor in turn performs tasks on behalf of the guest's kernel.
- In essence, as opposed to traditional virtualization this allows the guest to gain direct access to the underlying architecture.
- Two benefits, Performance and not limited to drivers of virtualization software.
- Limitations, requires modifications so operating system can interact with hypervisor so operating system should be introduce significant support and maintainability issues in production environments as it requires deep OS kernel modifications

Docker

- Popular paravirtualization tool designed to make it easier to create, deploy, and run applications by using containers
- Provides a lightweight environment to run your application code
- These containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and ship it all out as one package.
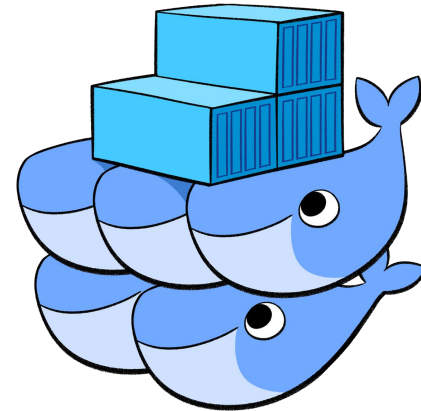
Source:
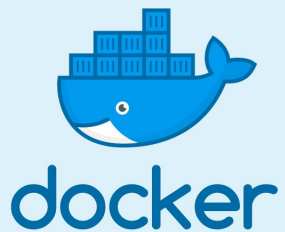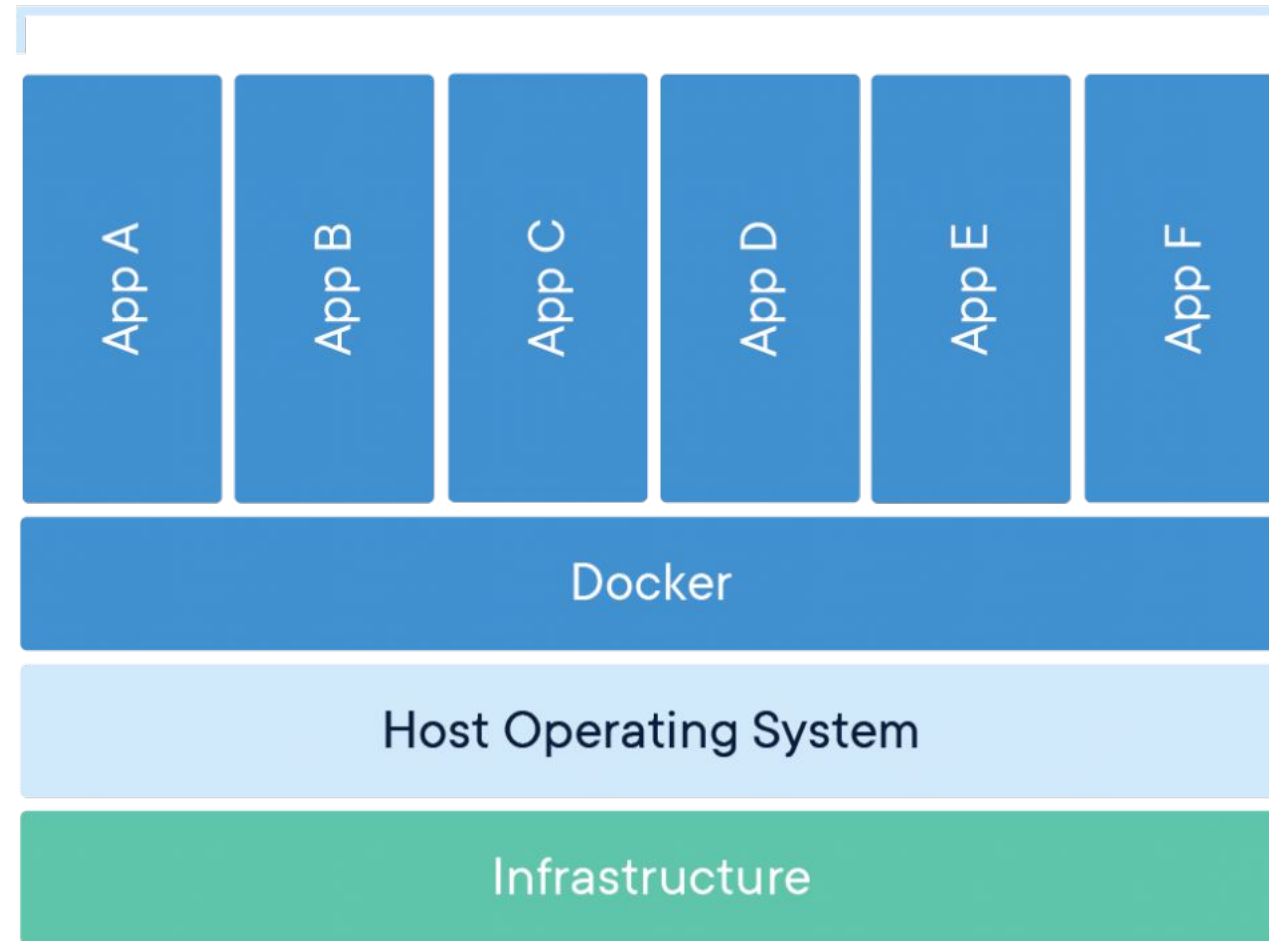
Benefits of Containerization over Virtualization

- Much more portable.
- Save space due to small size.
- Much more stable, predictable environment.
- Gives you exactly what you need, no less and no more.
- Performance benefits.

Container Orchestration

- Container orchestration is all about managing the lifecycles of containers, especially in large, dynamic environments.

- Software teams use container orchestration to control and automate many tasks.

- Used for provisioning, configuration and maintenance in short.

- Tools to do this include Kubernetes, AWS ECS, Docker Swarm

Cloud Computing

- Storing, accessing and delivering data and programs over the Internet instead of your computer's hard drive
- Makes available a virtualized pool of resources from raw compute power to application functionality available on demand.
- The key techniques to creating a cloud are abstraction and orchestration.
- Can be Multi-Tenant or Single Tenant.
- Offers tremendous potential benefits in agility, resiliency, and economy
- Can provide additional security benefits.

Cloud Abstraction

- Allowing workloads and applications within the cloud to not be confined to the physical boundaries of server hardware.

- Instead of having one physical machine interacting with one operating system and its own set of hardware components, we can have a resource pool which can be diverted as needed.

- Abstraction enables greater resource utilization and can be used with concepts like multi-tenancy.

Source: Channelpro.co.uk

Cloud Orchestration

- Involves end-to-end automation and coordination of multiple processes to deliver desired service to the client.

- As opposed to simple cloud automation which concerns itself around tasks, orchestration is focused around workflows or whole processes.

- Tool used to do this include Ansible, Terraform, Puppet, Chef, JuJu
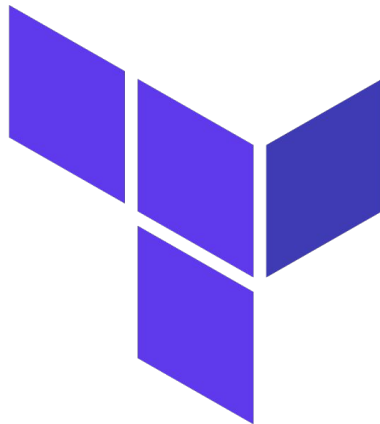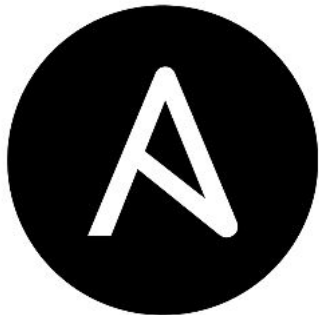
Characteristics of Cloud Computing

According to the National Institute of Standards and Technology's (NIST), there are 5 characteristics of cloud computing.

- On-demand Self Service
  - Cloud computing resources can be provisioned without human interaction from the service provider.
  - Able to provision additional computing resources as needed without going through the cloud service provider Ie)storage space, virtual machine, databases, etc.

- Broad Network Access
  - Cloud computing resources are available over the network such as the internet or in some cases (Private Cloud) the LAN.

- Multi-Tenancy and Resource Pooling
  - allows multiple customers to share the same applications or the same physical infrastructure while retaining privacy and security over their information.

Continued...

- Rapid elasticity and scalability
  - Ability to quickly provision resources and remove as needed often responding to business needs.

- Measured Service
  - Cloud resource usage is metered and users pay according to what they used.

Different Models of Cloud Computing

- NIST defines three service models of cloud computing which describe the different categories of services

- SaaS, Software as a Service – a full application manage/hosted by the provider. Consumers can access through a web browser, mobile app or a lightweight client app. Ie) Salesforce

- IaaS, Infastructure as a Service - a virtual provision of computing resources over the cloud. An IaaS cloud provider can give you the entire range of computing infrastructures such as storage, servers, networking hardware alongside maintenance and support. Ie) AWS, Azure, Google Cloud, AliCloud

- PaaS, Platform as a Service – a cloud base where you can develop, test and organize the different applications for your business. Ie)Red Hat Openshift, Google App Engine, AWS Elastic Beanstalk

Cloud Deployment Models

NIST defines the following four cloud deployment models.

- Public Cloud-The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

- Private Cloud- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Continued..

- Community Cloud- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

- Hybrid Cloud- The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).