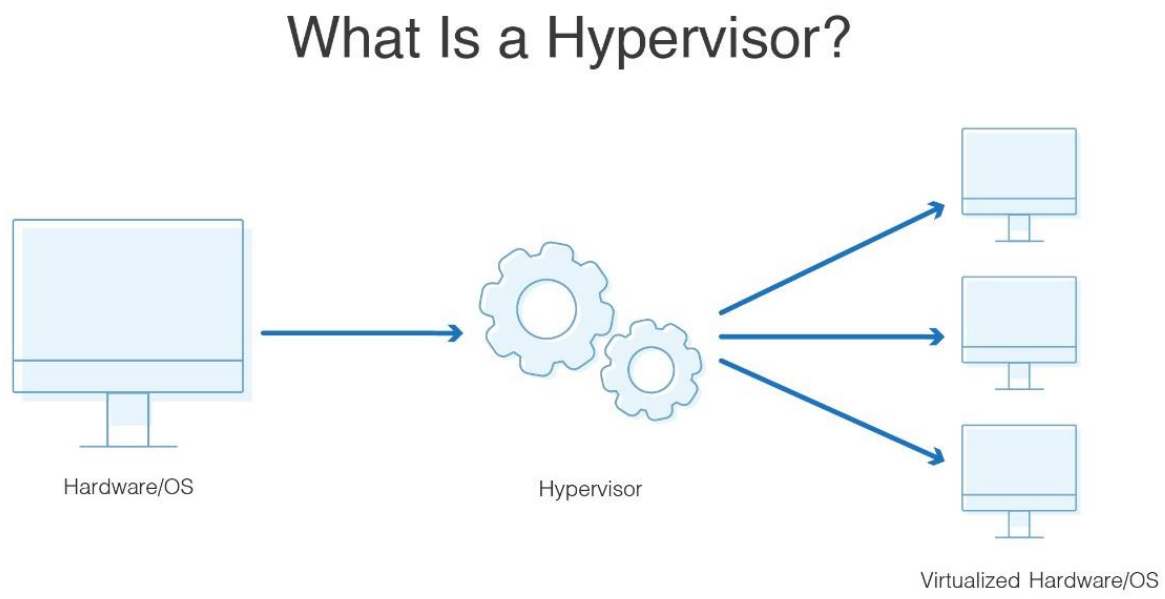
# What is a Hypervisor?

Hypervisors play an essential role in enabling server virtualization, which is itself essential to enabling cloud computing. Broadly speaking, virtualization refers to the use of software to simulate or emulate physical resources. In the case of server virtualization, a hypervisor is a software process that creates and runs virtual machines (VMs) using the resources of physical hardware. The hypervisor abstracts and isolates the VMs and their programs from the underlying server hardware, enabling a more efficient use of physical resources, simpler maintenance and operations, and reduced costs.

Discover Nutanix's AHV Virtualization solution




## Why Use a Hypervisor?

The primary technological problem that hypervisors solved was that most physical hardware could run only one operating system at a time. This constraint often led to wasted resources, as a single OS seldom fully utilized the hardware's capacity.

Hypervisors address the above constraint by aggregating the resources of virtualized physical servers (such as memory, network bandwidth and CPU cycles) and then allocating those resources to virtual environments, called virtual machines. Hypervisors are also known as virtual machine monitors (VMM). A VM is essentially a software-based computer, with access to the same resources as a physical computer, including an OS and apps. However, a hypervisor lets you run multiple VMs as guests, thereby using the physical resources of the underlying host machine much more efficiently. Each VM can act as a dedicated machine for every service, app or operating system, allowing you, for example, to run multiple different OSs on a single server.

The hypervisor also separates the VMs logically, which protects each individual VM against the effects of problems with other individual VMs on the same hypervisor, such as crashing, errors, or security attacks.

# How Hypervisors Enable the Benefits of Virtualization?

As software, hypervisors decouple the OS and apps from the physical host. This decoupling provides an array of benefits, including the ability to easily and quickly migrate the VM from one host to another without disruption. This capacity, called live migration, is essential for workload balancing. Live migration also occurs automatically in the case of node failure, providing high availability and increased uptime.

Virtualization enables cost savings through reducing physical footprint, which in turn reduces costs for electricity, cooling, and maintenance. Virtualization also greatly improves agility and speed in delivering IT services. For example, it is far easier to spin up a VM than to provision new environments to satisfy customer requests.

# Type 1 and Type 2 Hypervisors - What's the Difference?

## Type 1 Hypervisor

Type 1 hypervisors are installed directly on the physical server, which is why they are also called "bare metal" hypervisors. Direct access to the resources of the physical server makes Type 1 hypervisors highly efficient. This design also makes Type 1 hypervisors more secure, as it limits the attack surface and potential for compromise. Type 1 hypervisors are by far the most common choice within enterprise IT contexts, primarily due to their strong security, scalability, stability, and performance. Examples of the most widely used hypervisors include Nutanix AHV, VMware ESXi, Microsoft Hyper-V, and Citrix Hypervisor.

## Type 2 Hypervisor

Type 2 hypervisors differ in that they run as applications on a physical server's preexisting OS. Because they run on the host OS, which sits between the physical server and the hypervisor, they are also known as "hosted" hypervisors. Type 2 hypervisors are not ideal for server-based environments, given that they have a higher latency and risk exposure than Type 1. They are, however, relatively easy to install, and can work well in specific use cases, such as individual PC users who need to run more than one operating system, and where performance and security are not principle concerns.

# Hypervisor Security Considerations

Because a virtual machine (VM) environment is isolated from the rest of a system, whatever operates inside a VM will not affect or interfere with anything else running on the host hardware. In the unlikely event that a VM is compromised, the entire system should not be impacted.

However, cybercriminals have been known to compromise hypervisors. The impact of such a compromise can cause problems for all of the VMs that the hypervisor manages, leaving the data in each VM vulnerable.

Security protocols and requirements may vary based on the type of hypervisor.

# Top Considerations When Selecting a Hypervisor

- **Complexity** - Is it easy to deploy and manage? Is it a separate product, with a separate console, that requires full-time specialists to maintain, operate, and troubleshoot? Is it something that an IT generalist could master relatively quickly?
- **Performance** - Does it deliver enough performance to support your mission-critical applications? Check out the benchmarks for performance in production (as close to real-world conditions as possible).
- **Cost** - Does it come with licensing fees, or is it built-in to the larger solution?
- **Ecosystem** - Does it support a rich ecosystem? For example, does it support the most widely used guest operating systems? Microsoft, Suse, RedHat, Ubuntu, CentOS. Does it support leading enterprise apps and technologies such as Microsoft SQL Server, Exchange, SAP, Oracle, Citrix, Splunk, SAP, and VMware Horizon?