[Virtual Machine Escape Wikipedia](https://en.wikipedia.org/wiki/Virtual_machine_escape)

Do not connect your virtual machine back to your host computer

You can run a virtual machine within a virtual machine without performance issues

You can run as many VMs as you like, provided your host machine has enough resources (usually ram) available

A VM is just a file that sits on the host machine but acts independently as if it were a separate computer.

A VM can be configured to use a different type of CPU, storage drive or NIC than its host

Hypervisor is the software that creates and runs VMs

Type 1 “bare metal” hypervisor: run directly on top of the host hardware. Eg

* Citrix XenServer, VMware ESXi/vSphere, Microsoft Hyper-V, KVM

Type 2 hosted hypervisor is known as a VMM (Virtual Machine Monitor). An application program existing on top of a conventional OS. Virtual machines are created and managed by VMM through the host. Eg

* VMWare Workstation, VMWare Player, Parallels Desktop (MacOS), Oracle Virtualbox

Threat isolation and VMs

VMs can also be used for system backup and recovery: You can create multiple virtual copies of an OS and restore the copy if something goes wrong

Disadvantages to Virtualization:

* Performance is compromised
* Increased complexity, it’s more difficult than managing physical machines
* There is a big risk if we keep all our eggs in one basket. If the host fails, all VMs fail too “single point of failure”
* License cost: prices are going down but should still be considered

Virtualized networking: physical servers with type 1 hypervisor

Virtual switch: mapped to physical NICs on the server

Virtual machines: mapped to the vSwitch with virtual NICs

Virtual router that communicates with the vSwitches

Virtual Firewall that protects your VM

Use cases for virtualization:

* Virtualization server: if we had physical standalone servers, we’d have one for a domain controller, another for a backup, an email server, a DNS server, print server, etc. Physical to virtual migration creates a virtualization server
* Virtual Desktop Infrastructure (VDI): virtualization of desktops/OS that run in a data center. Endpoints are usually thin clients that access their virtual machine via the network. VDIs are easier to manage than thick clients. There’s more security because our desktops are in a data center, not on the physical machine. Decreased cost
* Data center & cloud: data centers benefit from virtualization because of the ability to run more services and software with a smaller footprint. Public cloud computing is all about accessing services and resources from a remote data center and only paying for what you use (metered service)
  + Virtualization and high speed networking truly enable the era of cloud computing