

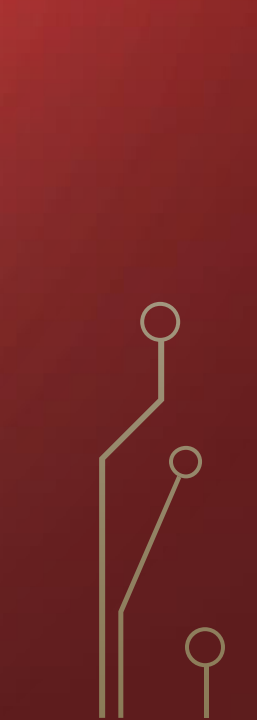


The background is a solid red color with a subtle gradient. In the four corners, there are white line-art illustrations of circuit traces or a stylized tree structure, with small circles at the end of the lines.

MODULE 5C: AUDITING VIRTUALIZED ENVIRONMENTS

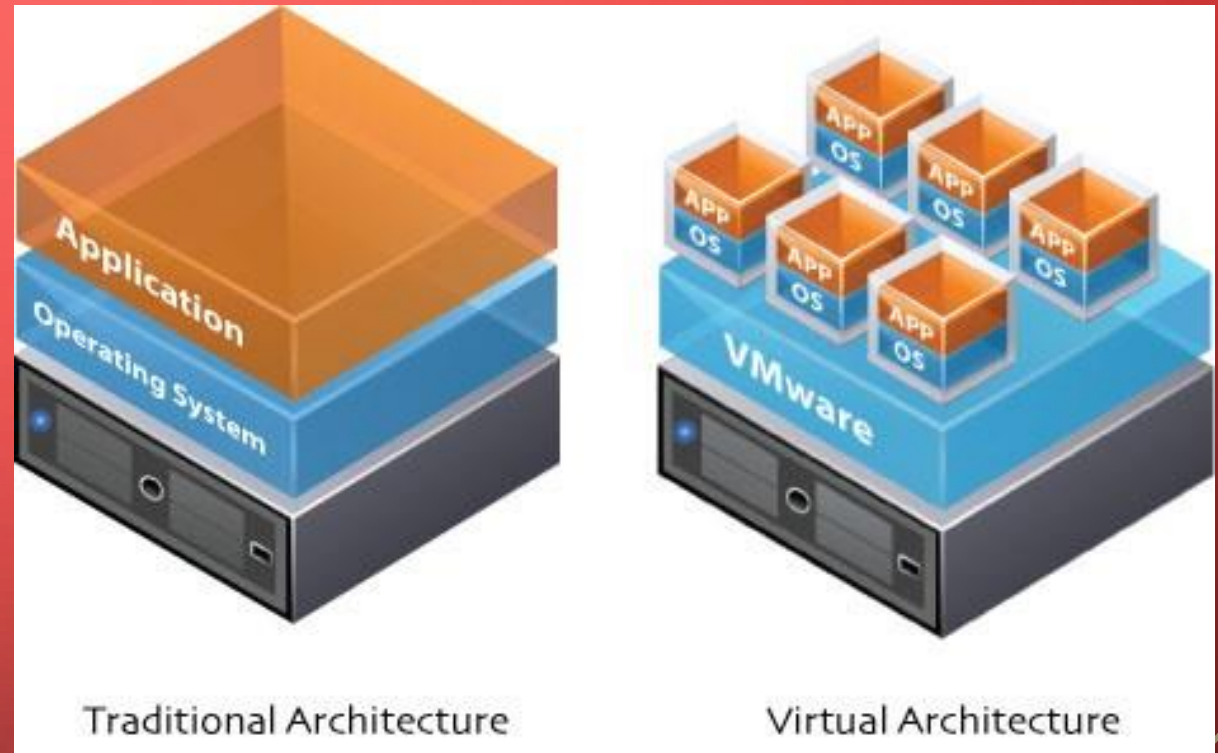


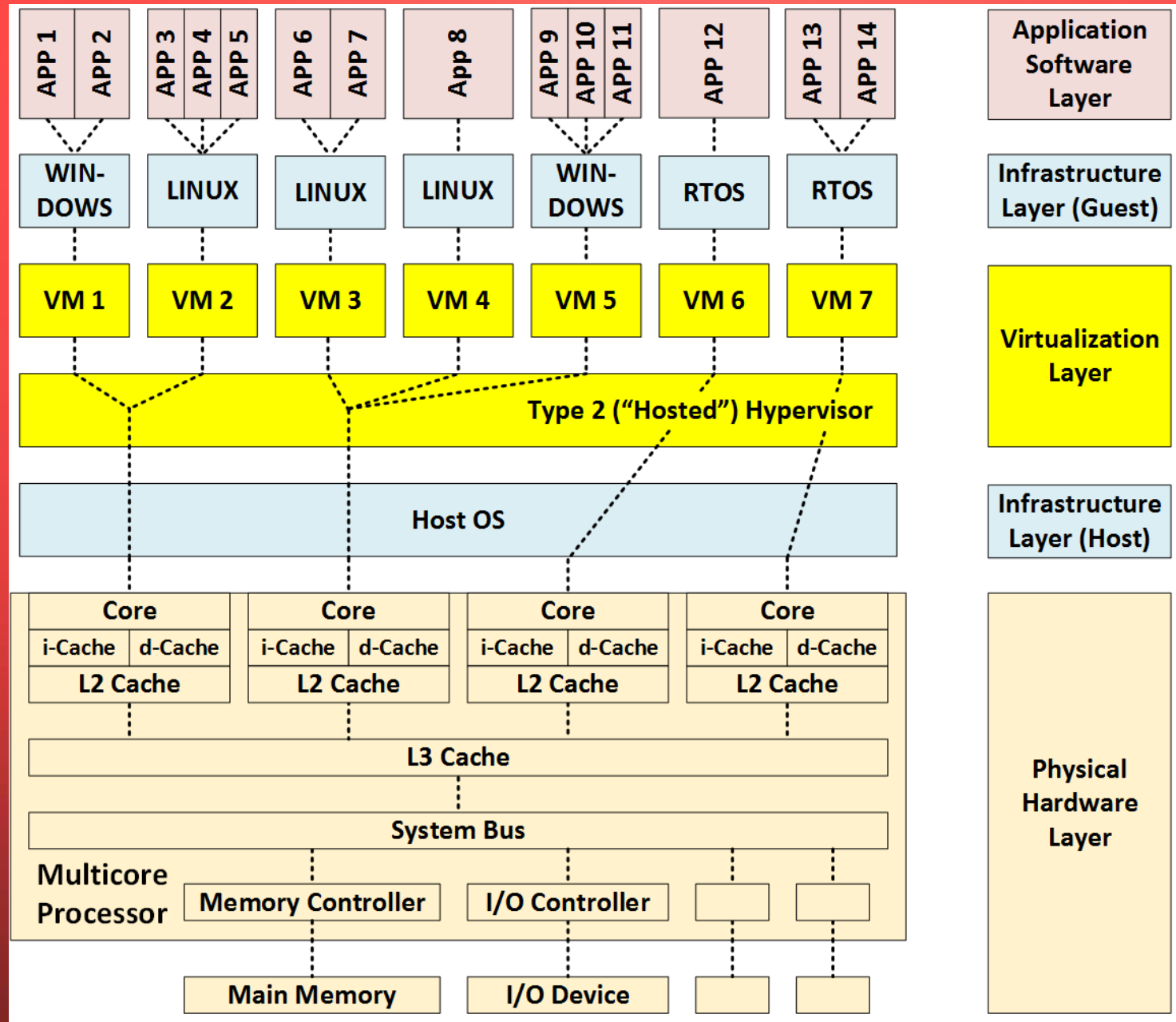
OBJECTIVES

- A brief technical overview of virtualization
 - Auditing virtualization environments
 - Tools and resources for enhancing your virtualization audits
- 
- 
- 

VIRTUALIZATION

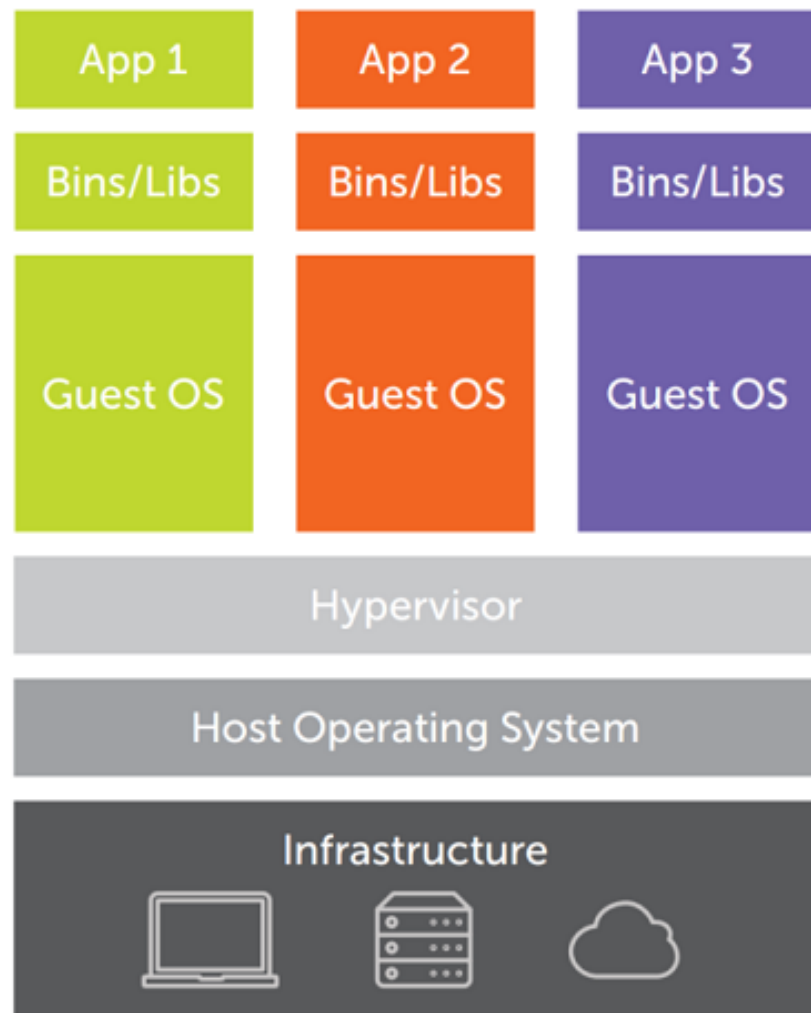
- Virtualization – The development or creation of a virtualized system. As opposed to a physical system, a virtualized system exists as purely software.



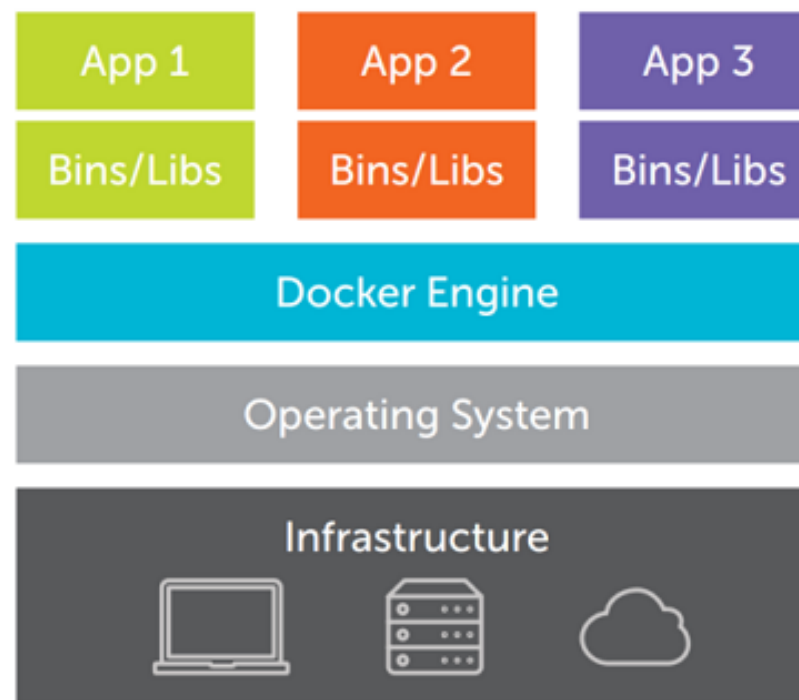


VIRTUAL MACHINES

- Two Categories:
- System Virtual Machine – A complete platform meant to take the place of an entire computer, enabling you to run an entire OS virtually.
- Process Virtual Machine – Designed to run a single application, such as a virtual web browser.
 - Can also host a single process as well. New tech called “containers”
 - Docker for Linux
- Virtual Machines are often stored within a single file such as .vdx file.



Virtual Machines



Containers

VIRTUAL APPLIANCE

- A VM image that is designed to run on virtualized platforms.
- VMWare.
- An image that usually provides a specific function.

HYPERVISOR

- Allows multiple virtual operating systems to run at the same time on a single computer.
- Think of the Hypervisor as the interface between the physical system and your virtualized systems.
- There are two types of Hypervisors:
 - Type-1
 - Type-2

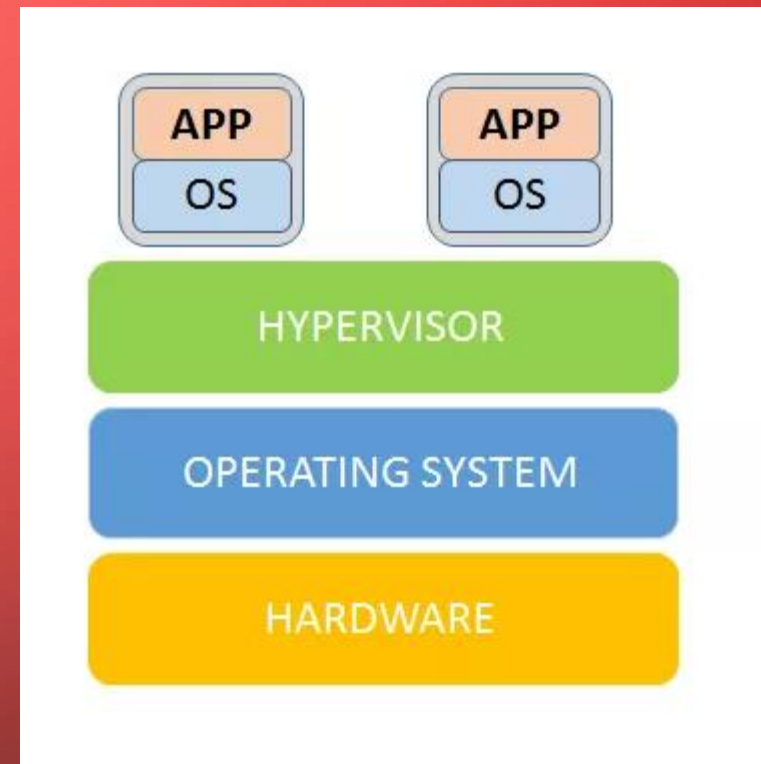
TYPE-1 HYPERVISOR (BARE METAL)

- A Type-1 Hypervisor is installed on a system that typically does not contain an operating system. The hypervisor provides the interface between the hardware and virtual machines directly.
 - Microsoft Hyper-V
 - Citrix XenServer
 - vCenter, Vmware
 - ESXi
- The hypervisor is the physical system's "OS"



TYPE 2 HYPERVISOR – OS-HOSTED

- The Hypervisor runs on top of the OS.
 - Virtual Box
 - Vmware Fusion
 - Parallels
 - Hyper-V
- Slower than Type 1

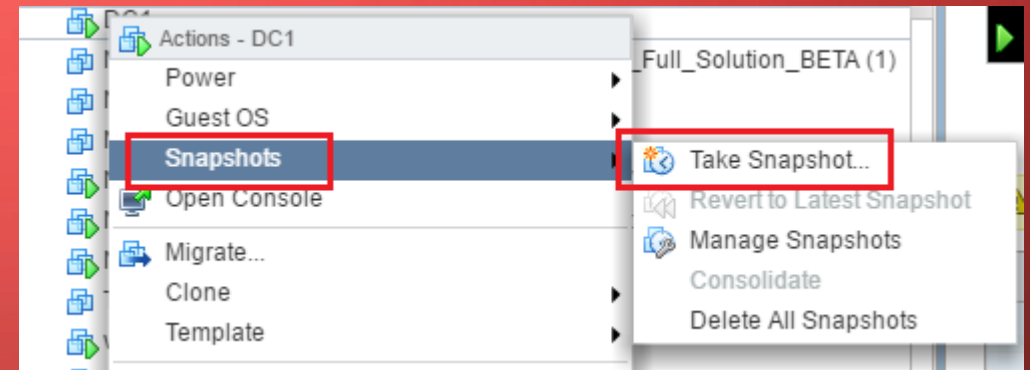


SECURING VIRTUAL MACHINES

- The securing of a VM OS is similar to a physical machine's OS.
 - Update the VM to the latest OS build, ensure it has security patches.
 - Ensure AV is installed and has latest definitions
 - Ensure hypervisors are updated
 - If VMs interact with each other, ensure their traffic is secured, especially over networks.
 - While VMs are generally isolated, this is not foolproof to hackers.

VM SNAPSHOTS

- A snapshot is basically a preserved state of a virtual machine at a particular instance in time.



AUDITING VIRTUALIZED SYSTEMS

What to look for?

- Change management process
- Systematic management of VMs
- Hypervisor & VM patching/updates
- Snapshot and Backup management & security
- Technical and Administrative controls
- **Sys Admins are extremely key!**

Checklist for Auditing Virtualization

- ☐ 1. Document the overall virtualization management architecture, including the hardware and supporting network infrastructure.
- ☐ 2. Obtain the software version of the hypervisor and compare with policy requirements.
- ☐ 3. Determine what services and features are enabled on the system and validate their necessity with the system administrator.
- ☐ 4. Review and evaluate procedures for creating accounts and ensure that accounts are created only when a legitimate business need has been identified. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
- ☐ 5. Verify the appropriate management of provisioning and deprovisioning new virtual machines, including appropriate operating system and application licenses.
- ☐ 6. Evaluate how hardware capacity is managed for the virtualized environment to support existing and future business requirements.
- ☐ 7. Evaluate how performance is managed and monitored for the virtualization environment to support existing and anticipated business requirements.
- ☐ 8. Evaluate the policies, processes, and controls for data backup frequency, handling, and offsite management.
- ☐ 9. Review and evaluate the security of your remote hypervisor management.
- ☐ 10. Review and evaluate system administrator procedures for monitoring and maintaining the state of security on the system.
- ☐ 11. Verify that policies and procedures are in place to identify when patches are available and to evaluate and apply applicable patches. Ensure that all approved patches are installed per your policy requirements.
- ☐ 12. Review and evaluate the security around the storage of virtual machine data.
- ☐ 13. Verify that network encryption of data-in-motion is implemented where appropriate.
- ☐ 14. Evaluate the low-level and technical controls in place to segregate or firewall highly sensitive data on critical virtual machines from the rest of the virtualization environment.
- ☐ 15. Evaluate the use of baseline templates and the security of guest virtual machines as appropriate to the scope of the audit.
- ☐ 16. Perform the steps from Chapter 5 and Chapter 12 as they pertain to the environment you are auditing.