THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by CSO

Defending the Fortress:
New Threats Meet New Defenses

THE SECURITY STANDARD™
September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY
Produced by CSO

Managing Virtualization's Security Risks

JT Jacoby, Chief Security Officer
NYC Housing Authority
john.jacoby@nycha.nyc.gov

Security Virtualization

- NYCHA Background
- Business Case
- Hidden Hardware Threat
- General Areas to Remember
- Sharing Forum – What are You Doing and Why?

NYCHA Background

- Largest public housing authority in North America: serves all 5 boroughs
- Serves 654,000 residents,178,000 dwellings in 2,600 buildings, 30% are minors under 18, average rent is $408/month.
- +/- 135,000 families on the waiting list
- 400+ satellite offices, 3 central offices, mainframe, Sun, soft phones, MS, Google?, virtualization, 12k employees, quasi-agency

Business Case

- Cost
- 60-70% of an organizations technology can be deployed virtually
- Virtualization is not for large enterprises only
- Fewer physical machines
- New, emerging methods of architecture, including more internal segmentation: chip sets, memory, etc. (not as inexpensive)

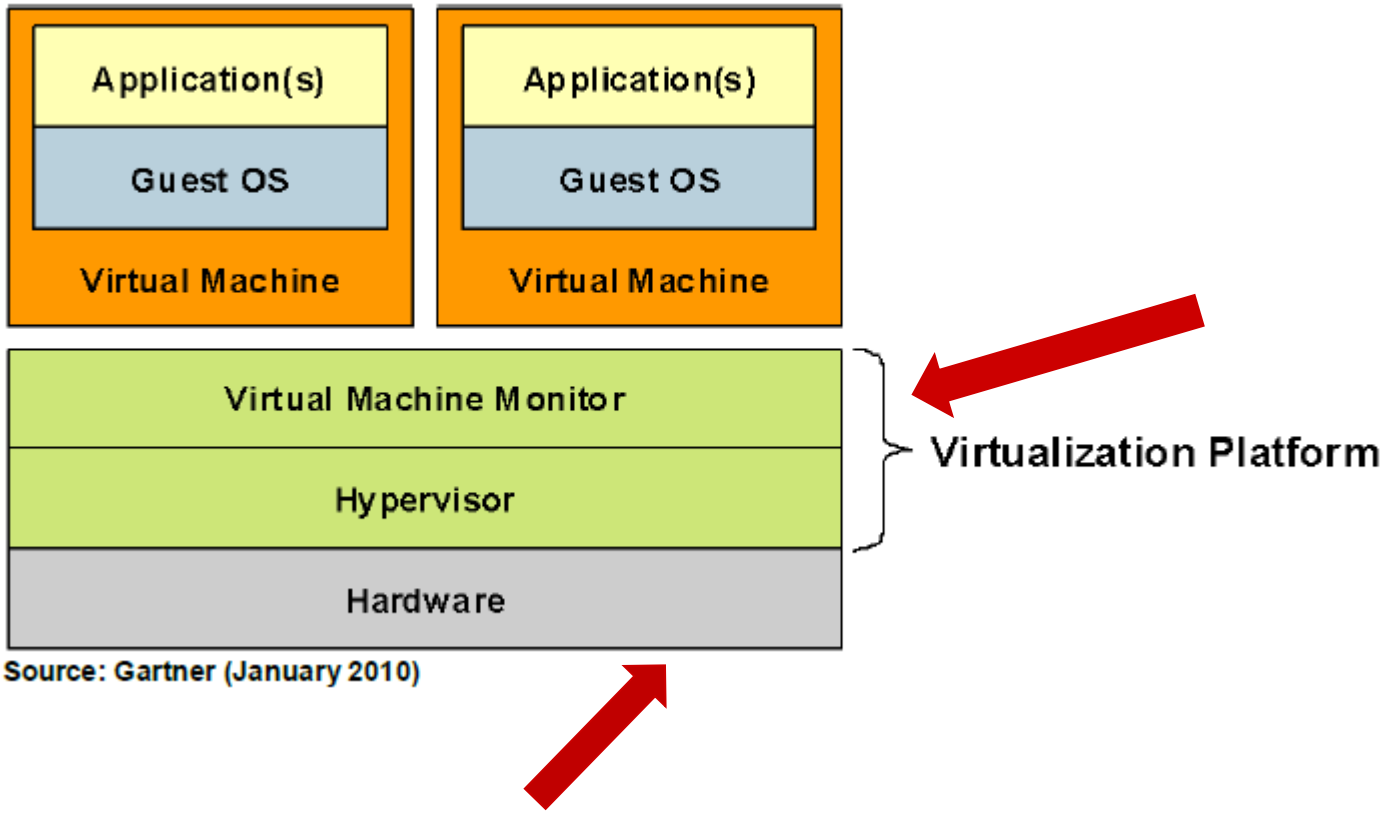
VM: Hidden Hardware Threat

- Shared resources: cards, ports
- No known spyware to date – en route
  - Co-mingling memory / swapping
- AMD-V
  - Device exclusion vector
- NSA / General Dynamics: High Assurance Platform
  - Vmware, Novell SuSE Linux and Red Hat

Remember

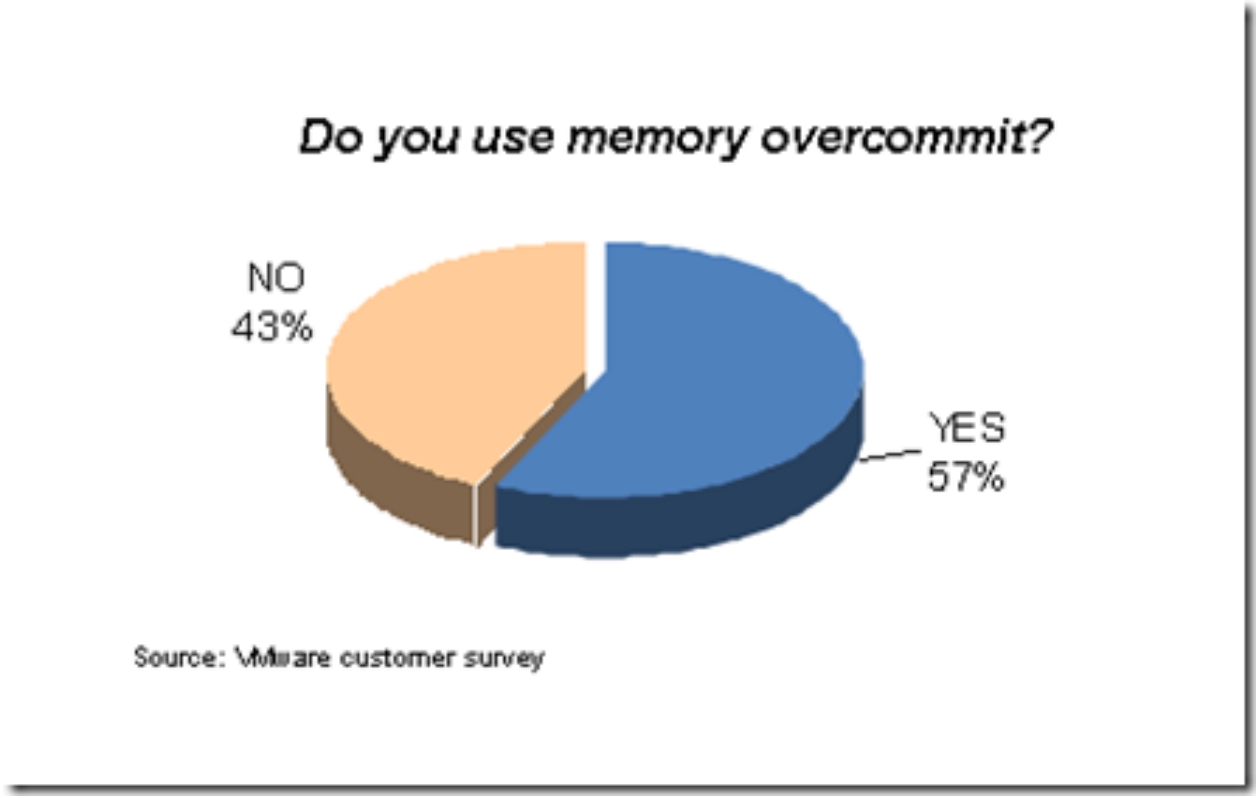
- There are trade-offs: cost, security, uptime
- Major control areas:
  - Physical
  - VM Management Console
    - Access controls
  - Each VM is its own machine
    - Resources are shared I (memory is key)

Remember: VM Architecture



Source: Gartner (January 2010)

Remember: Shared Memory



Remember:

- Network Isolate Special purpose Farms
- Anti-Virus on VMs
  - Malware detection
- IPSEC or Encryption between Host and VMs
- No Internet Browsing
- System Hardening
- Turn off un-utilized VMs

Remember:

- VMs must be part of enterprise security policy
- Favor systems with isolated hypervisors
- Disable unnecessary hardware ports
- Monitor use of shared resources: RAM, CPU, hard disk, cards, etc.
- Dedicate 1 NIC:VM
- Event logging – often overlooked on VMs

Remember:

- Host security – 1: Many
- Beware excessive privileges (network and users)
- Beware slower patching

Remember:

- Licensing:
  - protection for legacy revenue streams
- Virtual Aware Systems
- Secure the management console
- Segregate disk partitions
- Replication / continuity methods

Information Sharing

- What are the major reasons to use virtualization?
- What are the major concerns?
- What are some of the best technologies to manage / implement secure virtualization

Thank you!!