



*The Depository Trust &  
Clearing Corporation*

# *Virtualization Challenges: Operational/Security*

Edward Wengler

Parthiv Shah, CISSP, CISM

April 30, 2008

Vice President, Distributed Infrastructure – DTCC  
ewengler@dtcc.com

Director, Information Security – DTCC  
pshah1@dtcc.com

The Depository Trust & Clearing Corporation



# *Virtualization Challenges- Operational*

## Vendor support of Virtualization

- When most vendors are questioned on their support of virtualization they provide ambiguous answers

## Performance Measurement of applications

Need to develop a methodology to understand the performance impact of an application on the virtual environment

- Local for the VM
- Resource Pool assignment
- High availability in the Computing Cluster (headroom)



# *Virtualization Challenges- Operational*

## **Disaster Recovery**

- You non have the ability to replicate the entire VM to your DR site not just you data
- Change your DR scripts for virtual servers



# *Virtualization Challenges- Operational*

## **Asset management**

- Does your asset management system understand virtual servers?

## **Charge back information**

- How does your chargeback model change when moving from physical to virtual servers?

## **OS licensing options**

- OEM licenses without Software assurance cannot be transferred to VM's
- Windows 2003 Enterprise R2 allow you to deploy 4 Virtual machines



# Virtualization challenges- Security

Threat #	Description	Preventive/Detective Control
1	<p>Virtual-machine escape/Hyperjacking: Virtual-machine escape is the phrase defining an attack where a hypervisor attack could potentially infect virtual machines that reside on the same physical host.</p> <p>Hyperjacking all involving the Hypervisor itself being exploited and used to subvert each VM it controls e.g. vmware vulnerability about file sharing CVE?</p>	<ul style="list-style-type: none"> <li>•Host based firewall e.g. IPSec/Sunscreen, Symantec etc.</li> <li>•Compliance checking for the baseline to make sure no specific file/service is altered</li> <li>•Security event monitoring using SIEM solution(s) to monitor for specific event type to identify anomaly.</li> <li>•Request secure and trusted hypervisor from vendors</li> </ul>
2	<p>Vulnerability Management per guest/host: patching/signature updates required for each application per guest/host o.s., otherwise host/guest is susceptible to an attack.</p>	<ul style="list-style-type: none"> <li>•SMS/Opware etc. software installed on each guest o.s. to apply patches for application and/or o.s.</li> <li>•Periodic vulnerability scanning of guest o.s. to identify known vulnerability by vulnerability scanners</li> </ul>



# Virtualization challenges- Security

Threat #	Description	Preventive/Detective Control
3	Separation of duty: In the legacy environment firewall person perform firewall work, network person perform switching/routing work, Systems Administrator perform O.s. work. Today, one person does all of the work, does this person know all the security parameters of all technologies in virtual environment?	<ul style="list-style-type: none"> <li>• Compliance checking for the baseline performed by info. Security team (separation of duty)</li> <li>• Security event monitoring performed by info. Security team</li> <li>• Vulnerability scanning performed by info. Security team</li> </ul>
4	Vulnerability of client software: Someone may exploit client of virtualized technology. (E.g. VMware player exploitation, Virtual PC exploitation etc.) to gain access to client O.S.	<ul style="list-style-type: none"> <li>• SMS/Opware etc. software installed on each guest o.s. to apply patches for applications and/or o.s.</li> <li>• Periodic vulnerability scanning of guest o.s. to identify known vulnerability by vulnerability scanners</li> <li>• Security event monitoring using SIEM performed by info. Security team</li> </ul>



# Virtualization challenges- Security

Threat #	Description	Preventive/Detective Control
5	Protection of management devices: There are many security products to secure Guest/Host o.s. Does everyone think of adequate controls to protect the management systems that manage virtual environments?	<ul style="list-style-type: none"> <li>• Locate management devices behind firewalls such that only limited administrators can access the management system.</li> <li>• Baseline config the management system and integrate it with SIEM solution(s)</li> </ul>
6	Lack of standards: VMWare has one type of Hypervisor, Microsoft has it's own type of hypervisor, Citrix (Xensource) have another hypervisor, Sun has it's own version of hypervisor, IBM AIX performs it's own method of virtualization, Linux versions have their own hypervisor. How do you design a secure architecture that has fundamental different hypervisors; making it difficult to standardize on controls?	<ul style="list-style-type: none"> <li>• Demand vendors for standardization.</li> <li>• Try to limit different virtualization technologies.</li> <li>• Work with vendors to make sure all different virtualization technologies are capable of sending logs to SIEM and actively monitor SIEM solution(s)</li> <li>• Evaluate additional emerging tools in the market that can help actively manage diff. technologies.</li> </ul>



# Virtualization challenges- Security

Threat #	Description	Preventive/Detective Control
7	Undetectable rouge hypervisor: running on the guest/host o.s. acting as a keylogger/malware e.g. Bluepill.	<ul style="list-style-type: none"><li>• Know your applications running on guest o.s. (Know your environment)</li><li>• Monitor threat trend data externally for different threats related to hypervisors e.g. FS-ISAC, Blackhat conferences etc.</li><li>• Work with your host based IDS provider to make sure they have ability to detect rouge hypervisor detection capabilities.</li><li>• Monitor network behavior by using network based IDS (e.g. snort type rule/signature based IDS) and behavior based IDS (e.g. Mazu type of systems) and integrate the IDS data with SIEM solution(s)</li></ul>
8	Emerging new threat <ul style="list-style-type: none"><li>• Have you considered technology challenges related to nested virtualization</li></ul>	<ul style="list-style-type: none"><li>• Request vendors prove they have created secure and trusted hypervisor.</li></ul>

