



Virtualisation Security for Payment Systems

PCI DSS Conference, Sydney, Australia

October 2010

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney

Level 8, 66 King Street
Sydney, NSW 2000,
Australia

Melbourne

Level 8, 350 Collins Street
Melbourne, Victoria 3000,
Australia

T: 1300 922 923

T: +61 (0) 2 9290 4444

F: +61 (0) 2 9290 4455

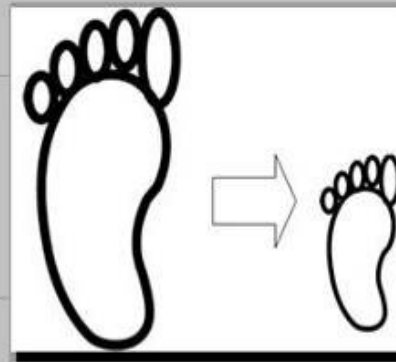
info@senseofsecurity.com.au

www.senseofsecurity.com.au

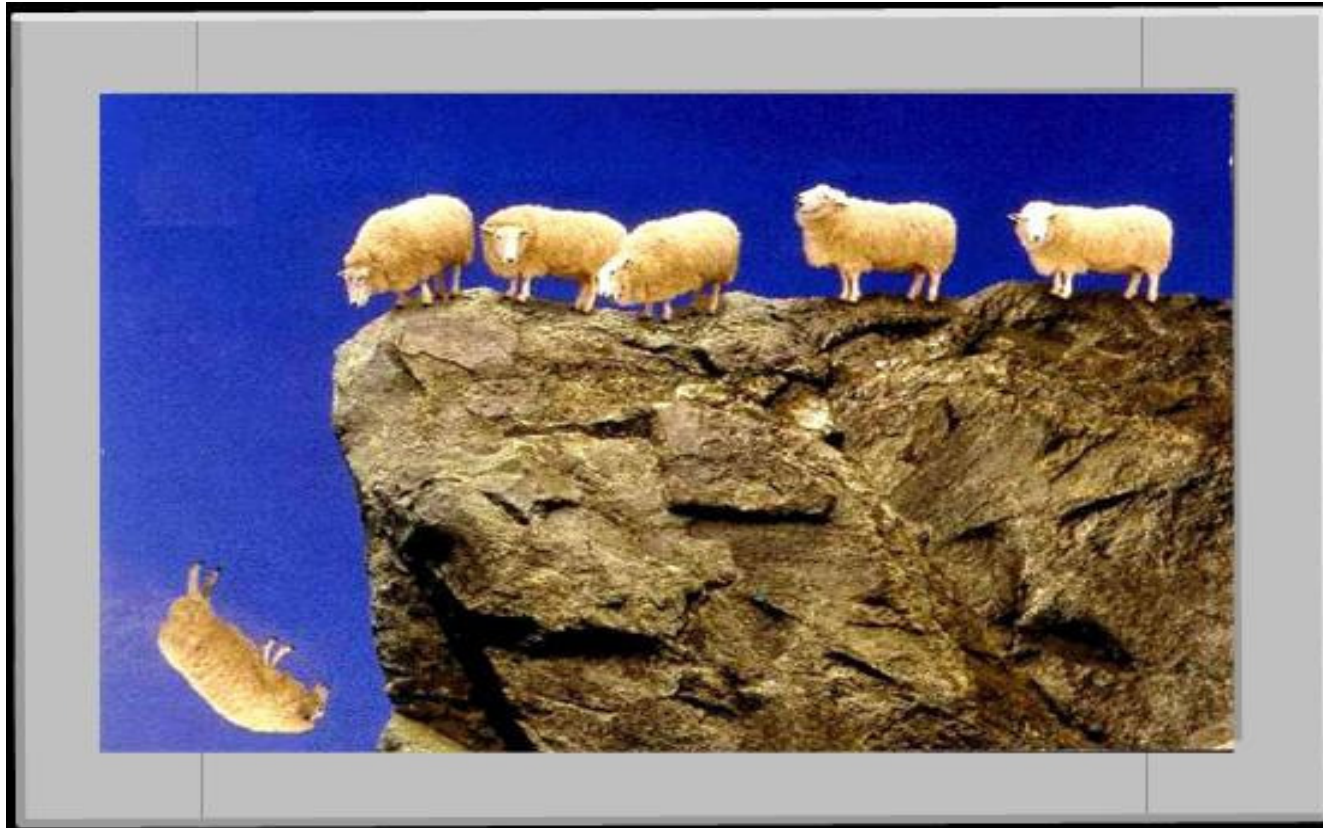
ABN: 14 098 237 908

- Brief Intro to Virtualisation Technology
- Virtualisation Security Challenges
- Implications for PCI DSS
- Be prepared
- Conclusion

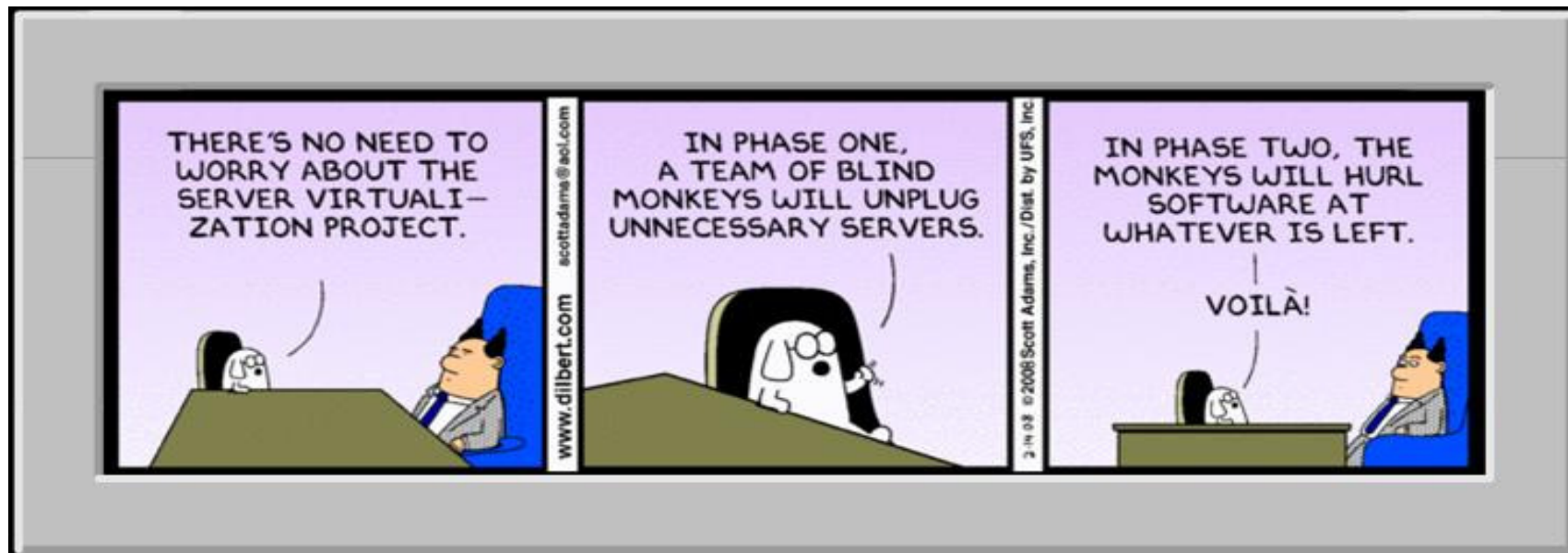
Virtualisation Benefits



It's so easy, follow me

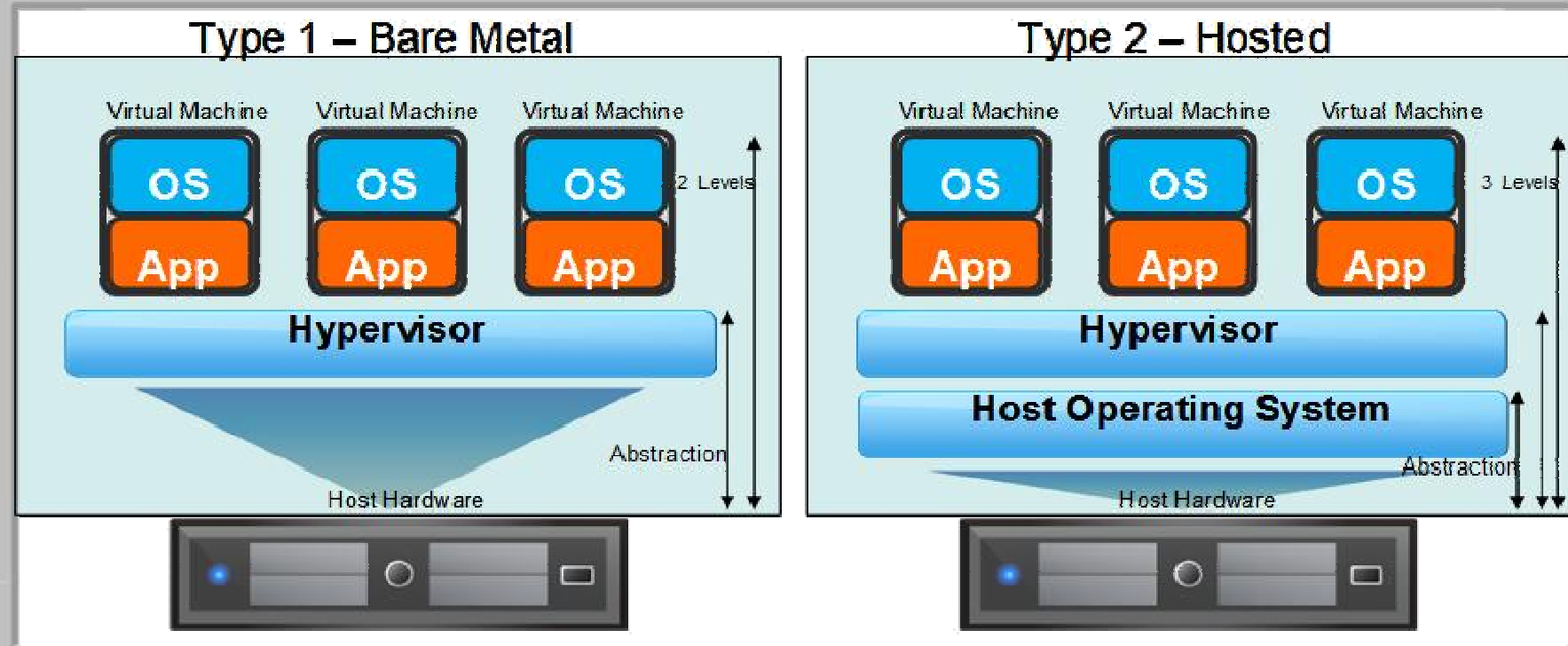


Even Dilbert's boss is onto this!

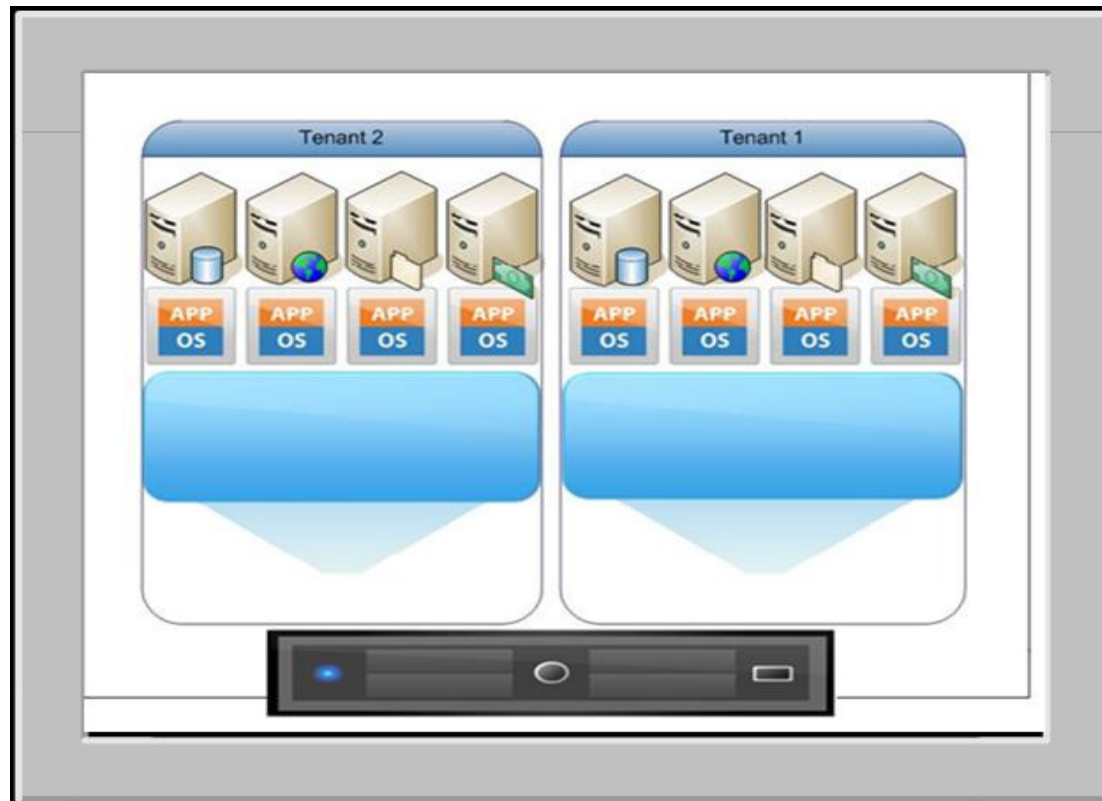


Licensed

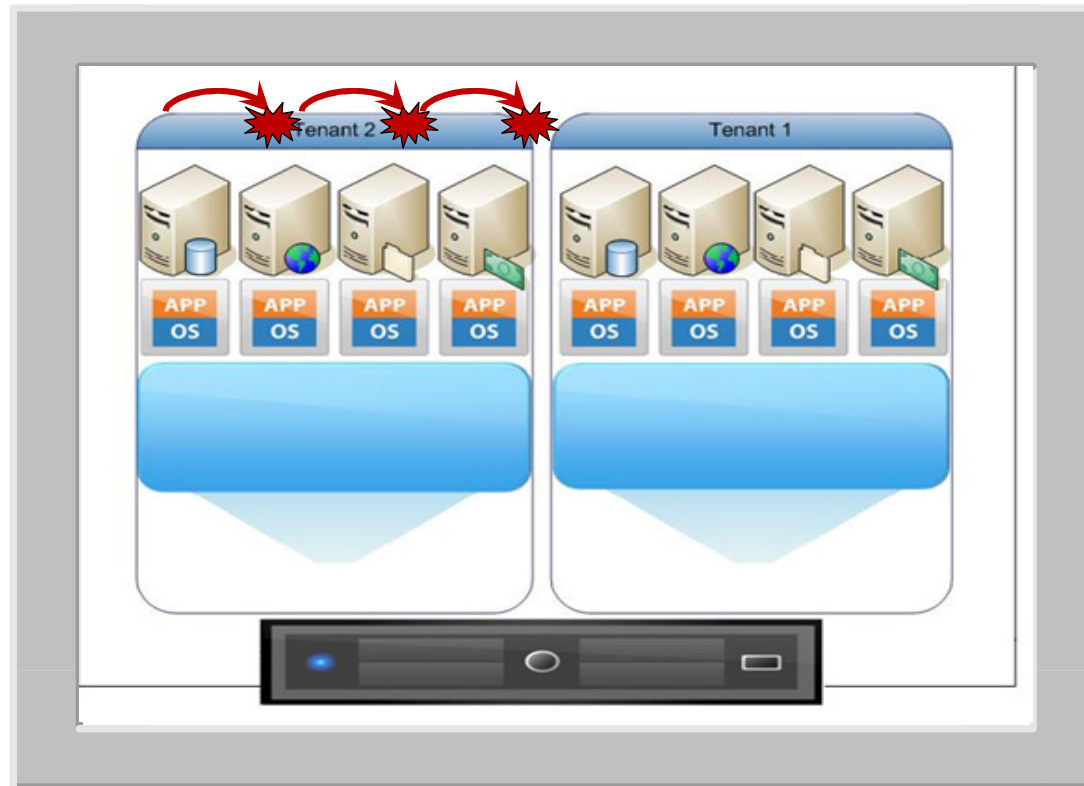
Defining Virtualisation - Hypervisor Types



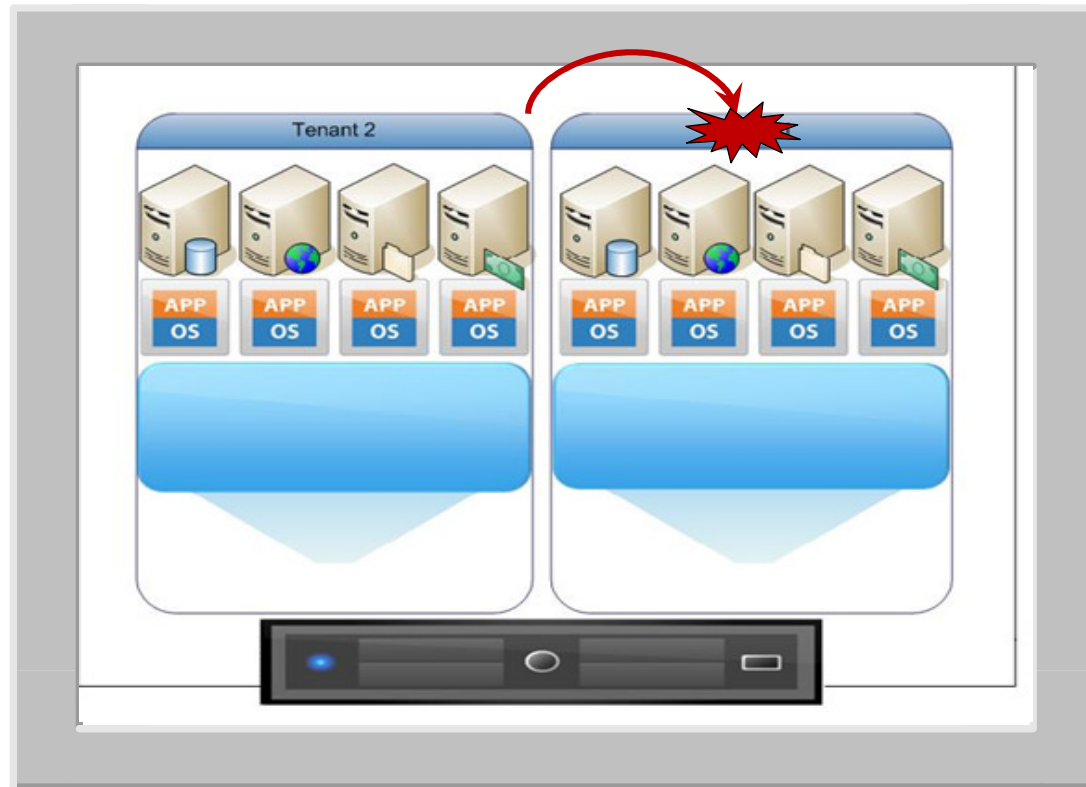
Sample Scenario - Multitenant or Internal



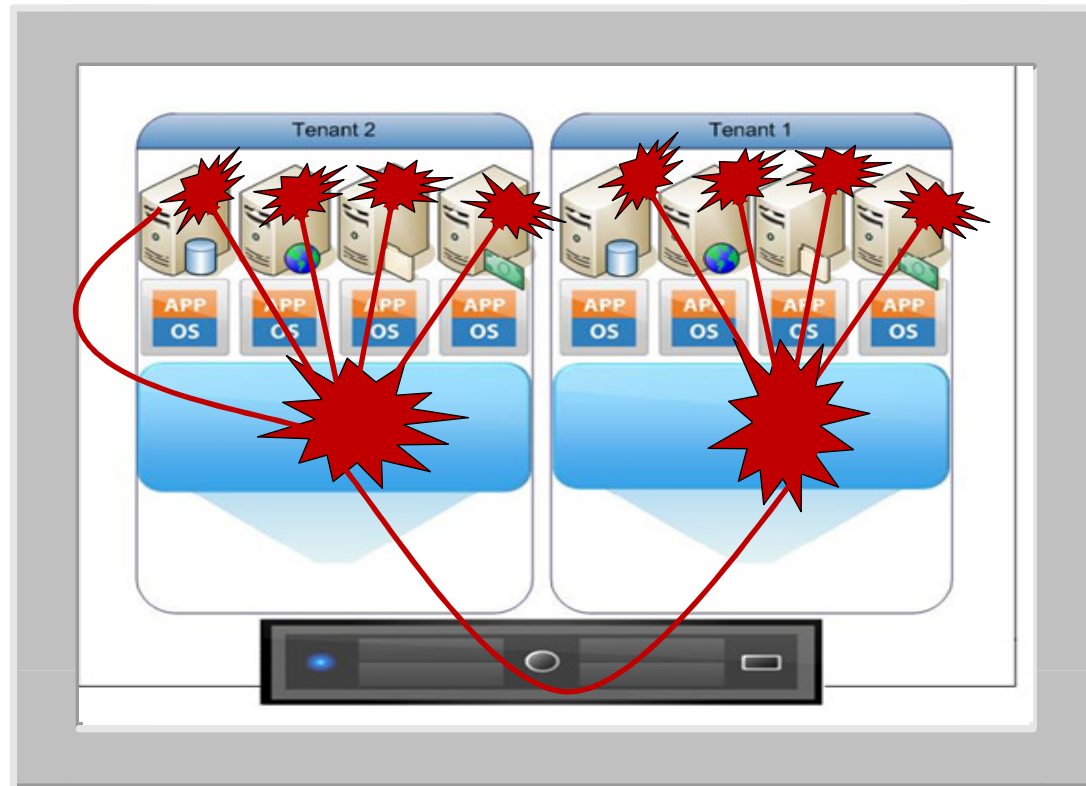
Guest to Guest Compromise



Guest to Guest - Inter-tenancy Compromise



Guest to Host (HV) - Worst Case



How does it happen?

- Hypervisor should prevent guest-to-guest or guest-to-host compromise
- However, if mis-configured isolation may not be effective
 - Poor setup of virtual networking
 - Optional features such as drag-and-drop, clipboard sharing etc. may break isolation
 - No secured management VLAN
 - Hypervisor & guest itself not secured
 - Ineffective controls to protect Hypervisor & guest (patch mgt, access control, auth)
 - Root Hypervisor Vulnerability



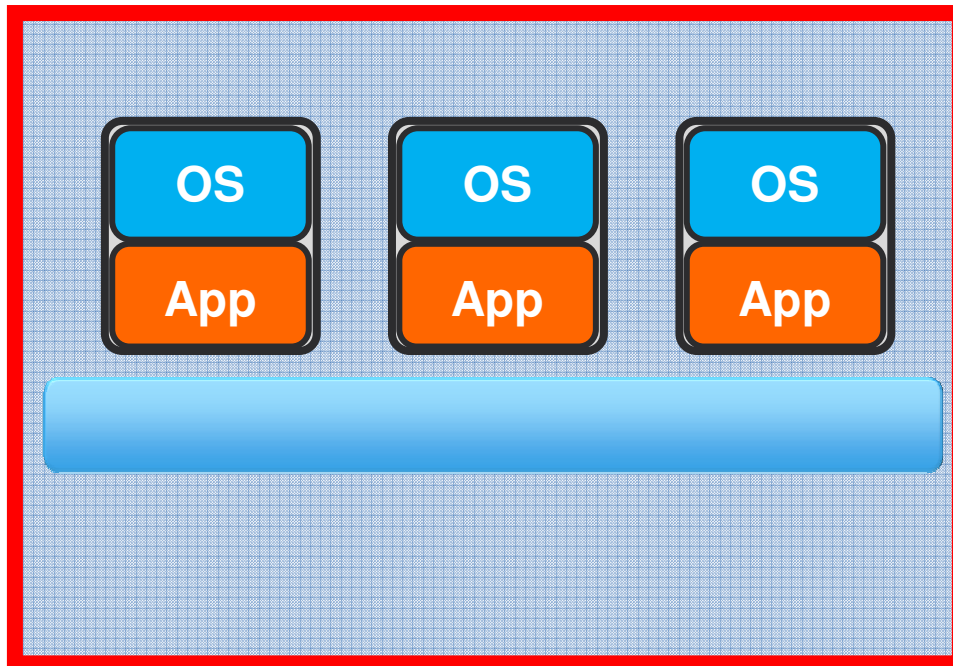
- Physically isolate CDE and non CDE?
- Co-hosted but isolated? Separate Virtual Switches?
- Risk Assessment Req 12.1.2
- Analysis by QSA, acquirer



Mixed Mode - Multitenant

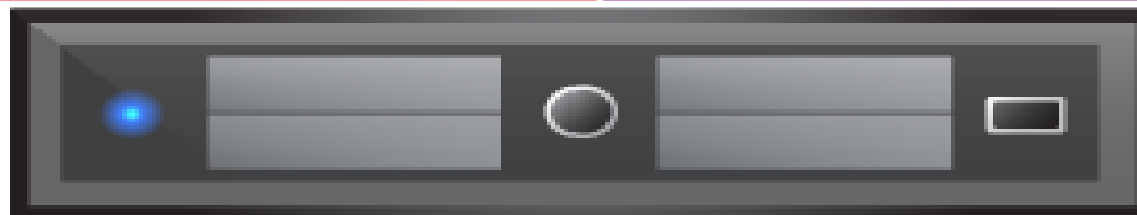
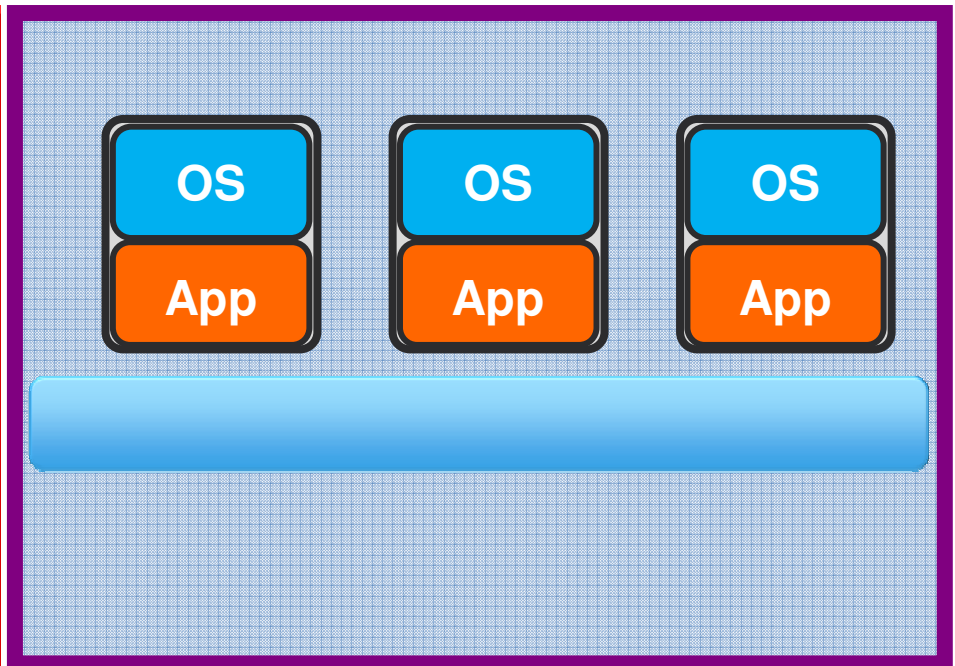
Cardholder Data Environment

Tenant 1



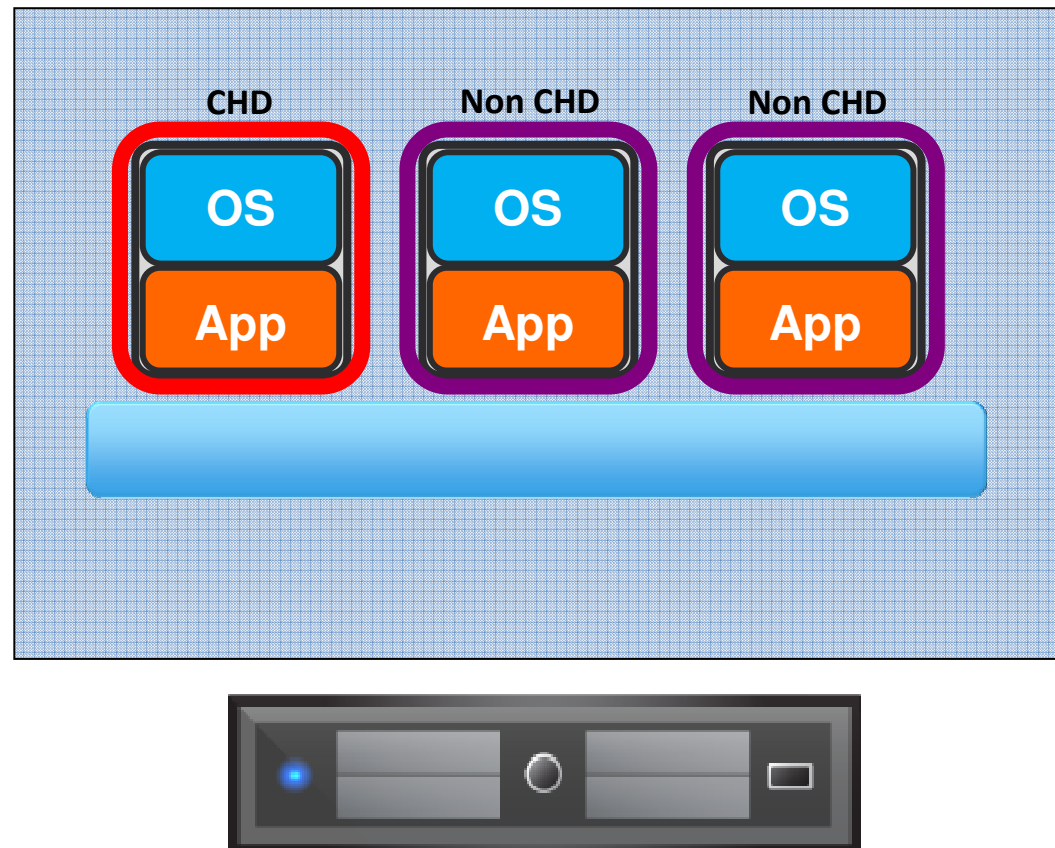
Non Cardholder Data Environment

Tenant 2

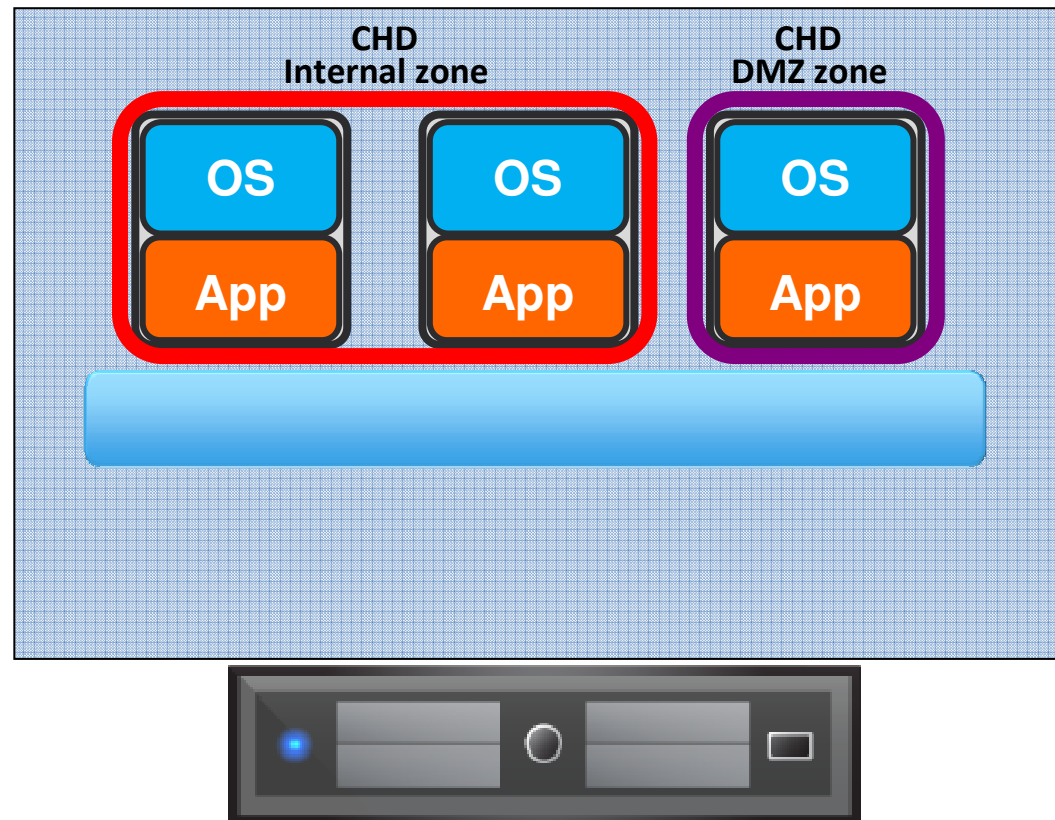


Mixed Mode Single Tenant

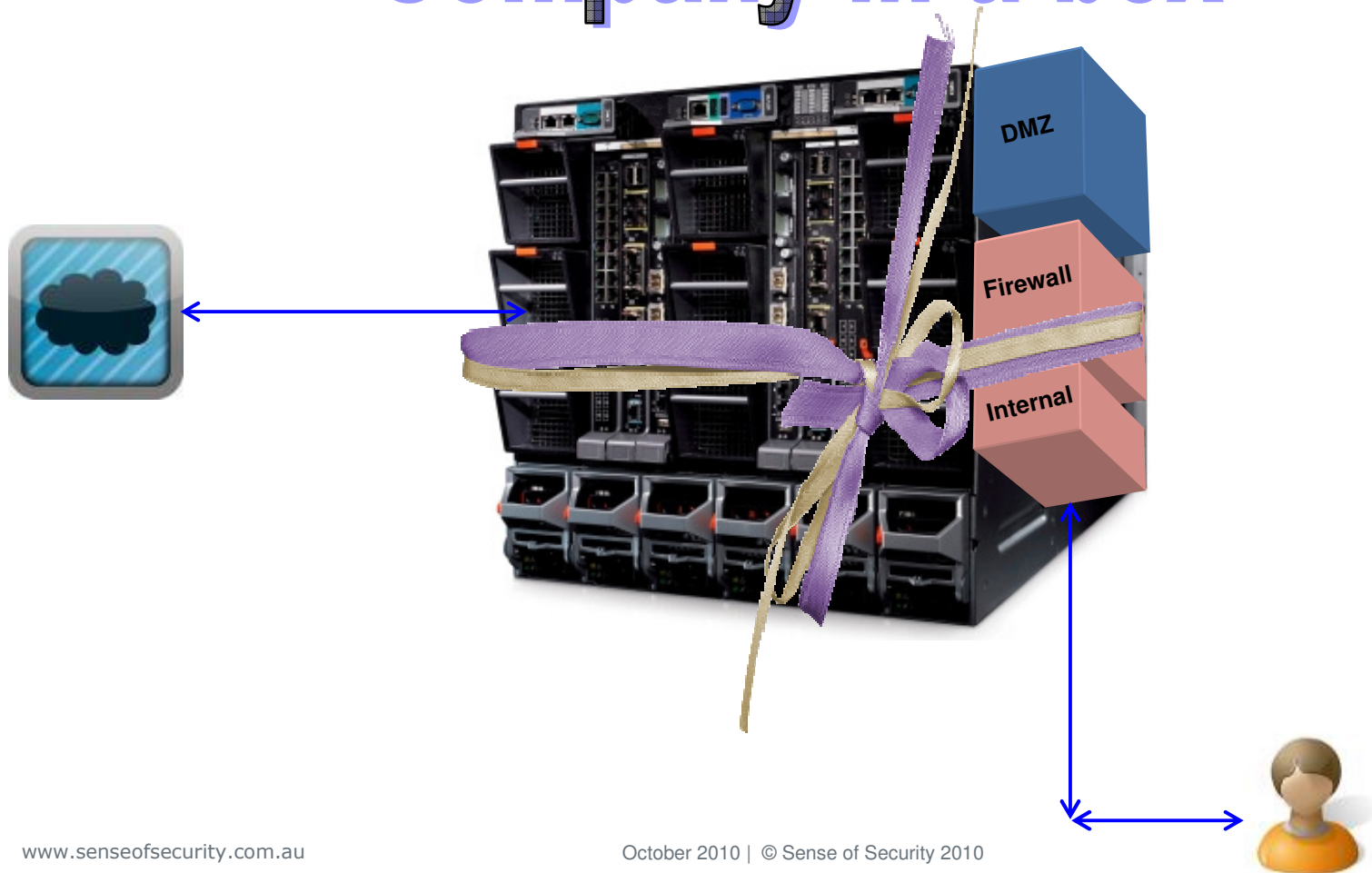
Tenant 1



Mixed Mode CHD Environment



Company in a box



Is it getting crowded in there?



Stealing a Physical Machine

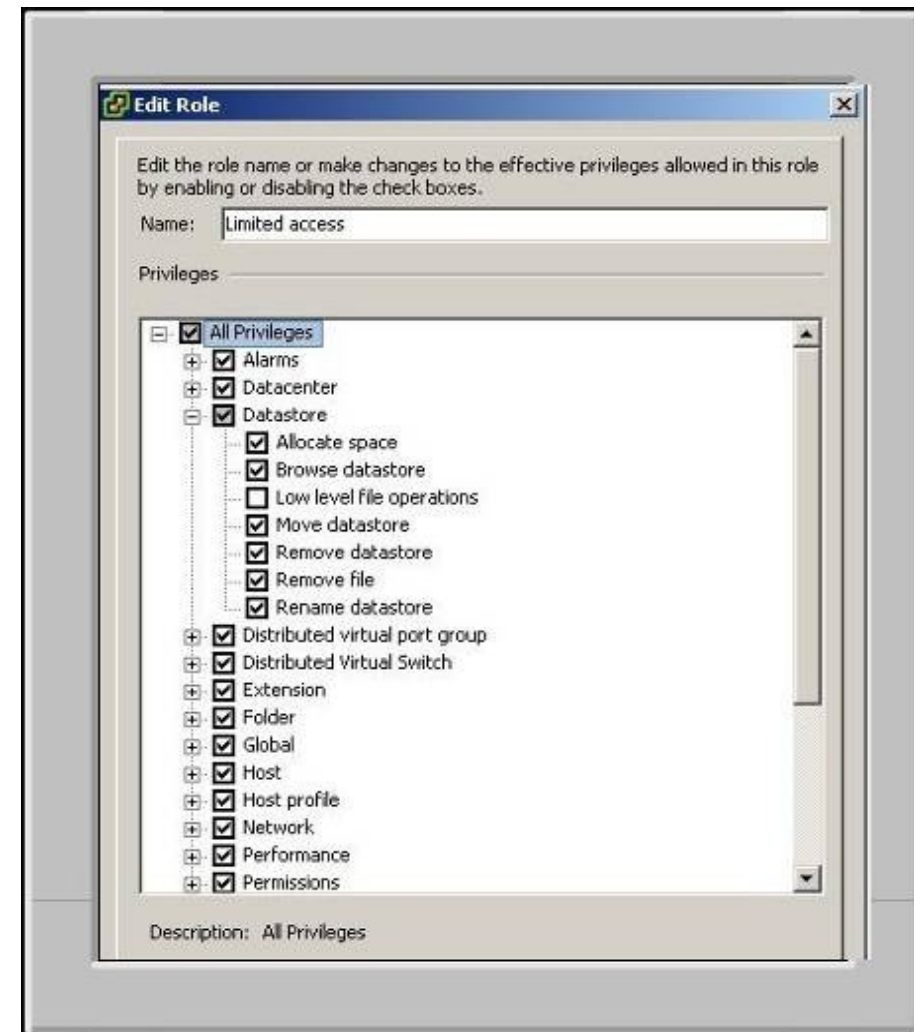


Stealing a Virtual Machine

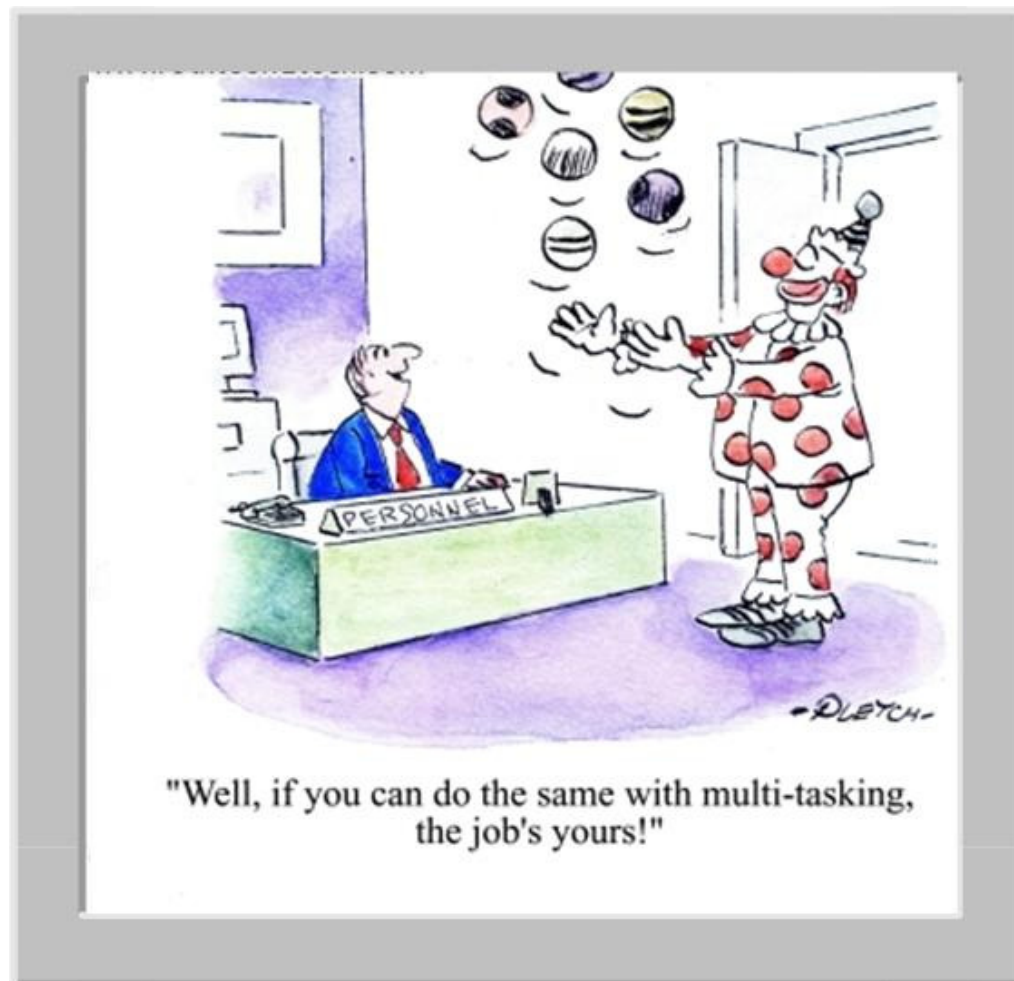
- Take a snapshot of the machine
- After snapshot virtual disk is unlocked
- Copy to removable media
- Mount VM, access to virtual disk
- If credentials are not known - boot using recovery tool; change admin password
- If credentials are known - power on with player

See video at: <http://www.senseofsecurity.com.au/consulting/virtualisation-security>

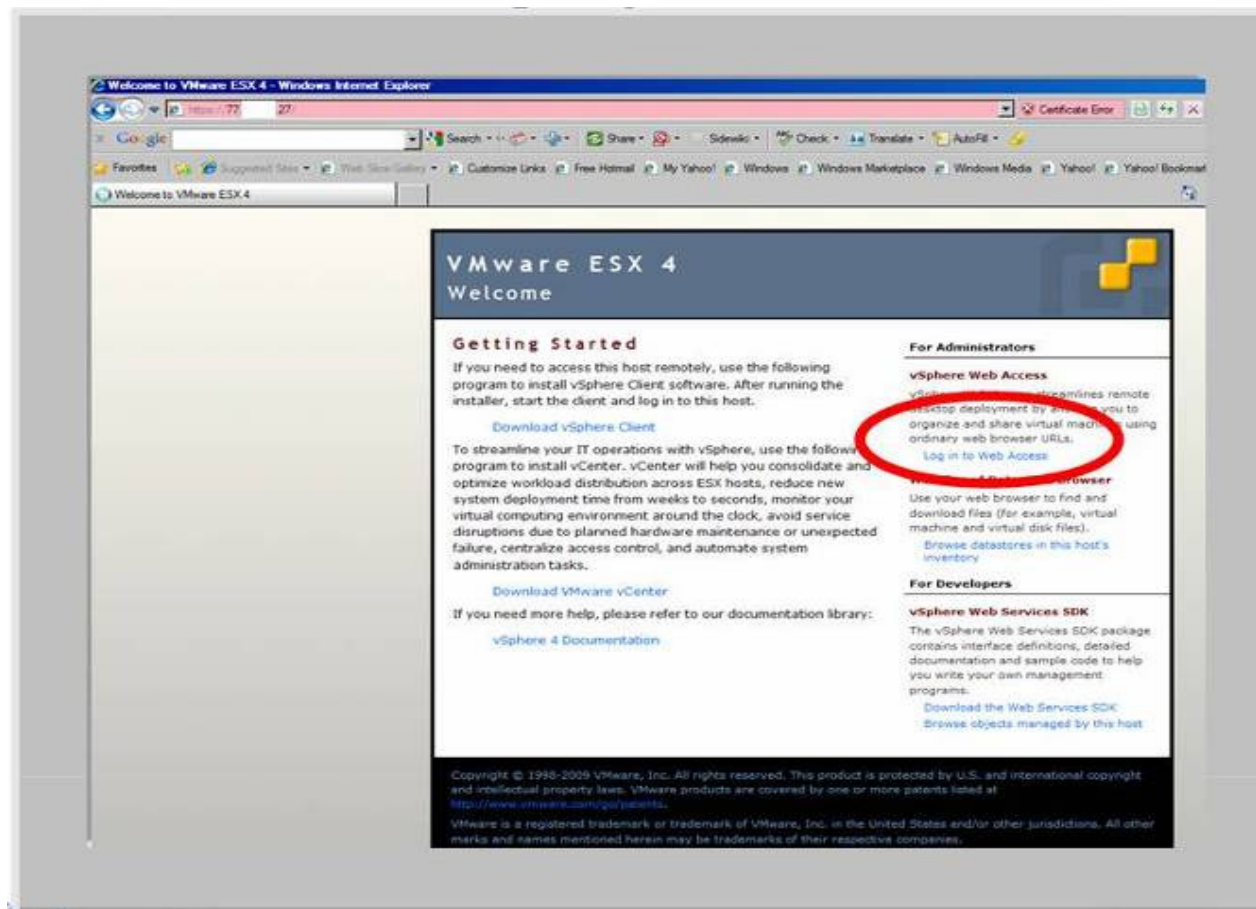
- Encrypt Data
- Improve RBAC - restrict access to low level file ops
- Restrict access to Service Console
- Implement controls for access, accountability, and visibility



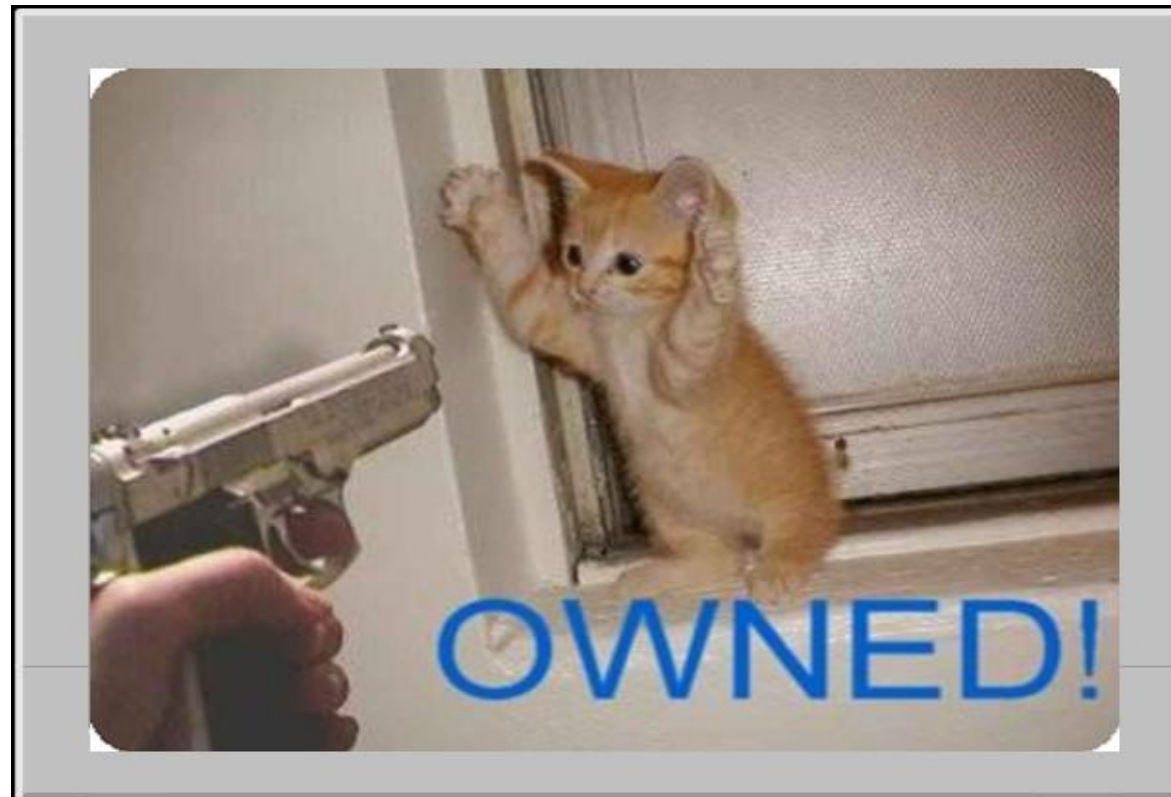
Who manages the system?



- Server, storage, network, and security duties are collapsed
 - Critical considerations:
 - Role-mapping within IT
 - RBAC capabilities of virtualisation platform
 - Layered controls (prevent, detect, respond)
 - Must enforce least privilege
 - Roles and Responsibilities
 - Review of 75 discrete responsibilities assigned to 3 or 4 roles
- (Per VMWare)



This is a good start to getting



System Components

- The PCI DSS security requirements apply to all system components that are included in or connected to the cardholder data environment.
- For virtualised environments this should include:
 - ANY Virtual Machine
 - Network Component (Vswitch; router)
 - Server (One Primary Function per VM)
 - Application
 - Virtual Appliance
 - Servicing CDE
 - Hooks into hypervisor
 - Security Appliances (Firewall, IPS, AV etc)
 - Hypervisor
 - Third Party Components
 - Virtual Applications (e.g. for Point of Sales)

- Choice of Hypervisor
 - See industry radar at <http://virtualization.info/en/radar/>
- Secure Configuration (Hardening, Disable unnecessary services etc) (2.2.X)
- Encryption of non-console administrative traffic (2.3)
- Patch Management, HV is a new dimension (6.1)
- Identify new vulnerabilities (6.2)
- Restrictive access (7)
- Effective user authentication (8.5)
- Audit trails for all changes (10)

Other Virtualisation Considerations

- Management Tools
 - Remote management (see previous graphic of exposed interfaces)
 - Mobile handset clients – convenience vs security
 - Incorporate two-factor authentication for remote access (8.3)
- Patch Management
 - Active and dormant machines

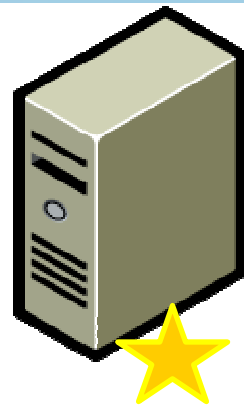
- Dormant VM's
 - Audit trails required for access to all dormant machines (10)
 - May include Cardholder Data, encryption keys (3)
 - How do you address retention and destruction? (9.10)
- Virtual Media
 - SAN/NAS ? Management Networks?
 - If NAS will require additional isolation and controls
 - VM's are just files on disks
 - Access controls apply (7)
 - Master images, images with CHD
 - Physical controls apply (9)

- Change Management
 - VMSprawl must be managed particularly for VM's with CHD
 - Movement from Dev to Test to Production must be controlled
 - Snapshot and rollback may inadvertently reinstate a non-compliant image
 - Enrolment & retirement must be controlled

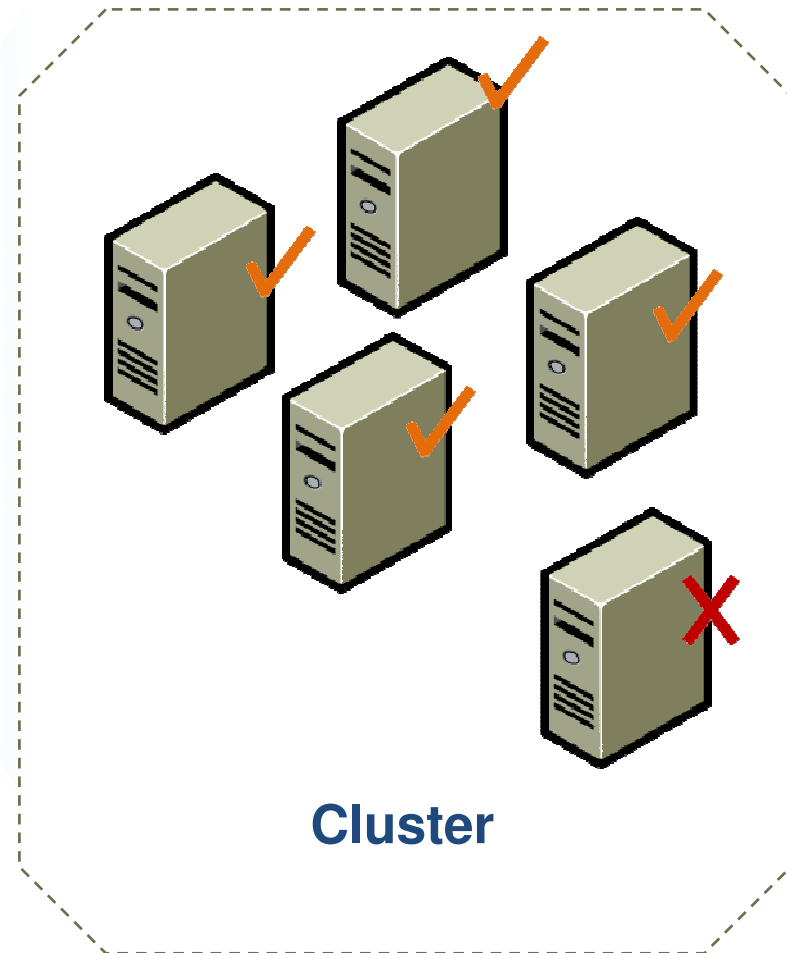
- Defense-in-Depth
 - Apply controls to data, control and management planes
 - Create as many zones of trust as required
 - Enforce zones of trust (virtualised or physical firewalls)
 - If using Virtual Firewalls confirm they meet all of PCI Req 1
 - DMZ, Stateful, NAT, Inbound/Outbound Rules
 - Recommend dedicated admin/management segments
 - Firewalled; RBAC for admins
 - Very important for Service Providers

- Audit and Logging
 - The entire environment should be auditable
 - All activity should be logged and monitored
 - Administrators/Auditors should be able to produce compliance reports at any point in time
 - Native and Commercial tools can be used

Host profiles reduce setup time and allow you to manage configuration consistency and correctness.

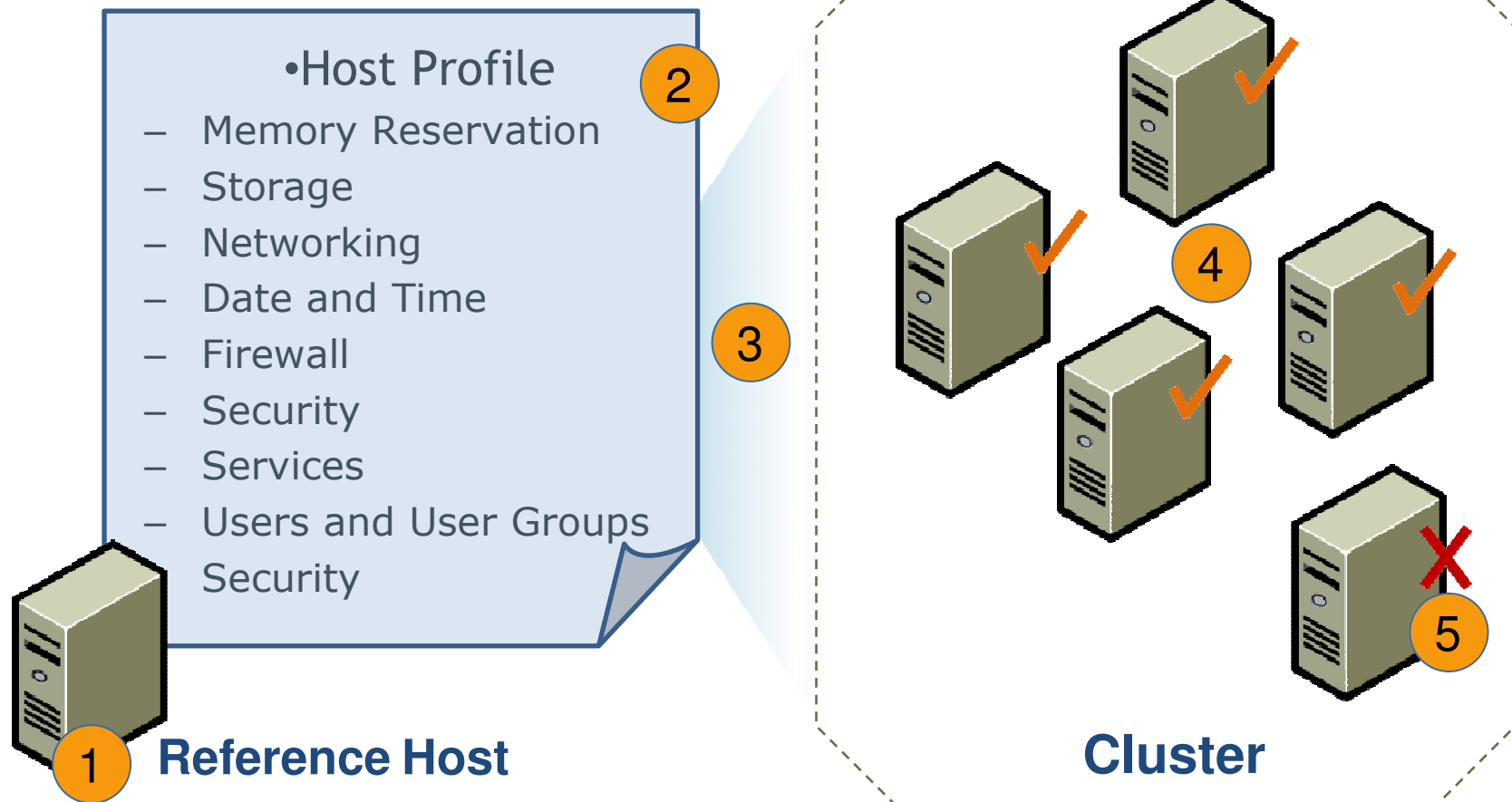


Reference Host

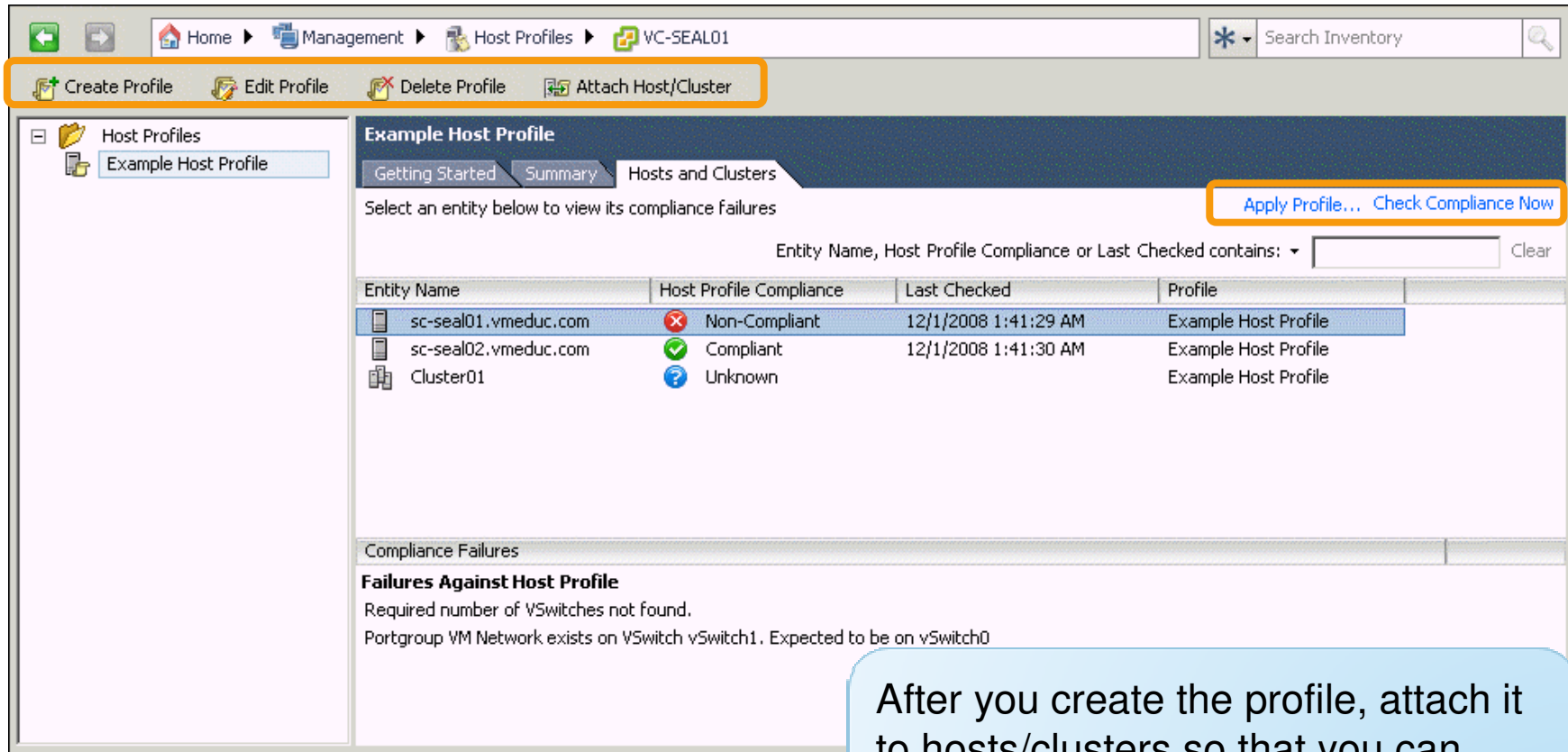


Cluster

This slide courtesy VMware



This slide courtesy VMware



Home > Management > Host Profiles > VC-SEAL01

Create Profile Edit Profile Delete Profile Attach Host/Cluster

Host Profiles

Example Host Profile

Example Host Profile

Getting Started Summary Hosts and Clusters

Select an entity below to view its compliance failures

Entity Name, Host Profile Compliance or Last Checked contains: Clear

Entity Name	Host Profile Compliance	Last Checked	Profile
sc-seal01.vmeduc.com	Non-Compliant	12/1/2008 1:41:29 AM	Example Host Profile
sc-seal02.vmeduc.com	Compliant	12/1/2008 1:41:30 AM	Example Host Profile
Cluster01	Unknown		Example Host Profile

Compliance Failures

Failures Against Host Profile

Required number of vSwitches not found.
Portgroup VM Network exists on vSwitch vSwitch1. Expected to be on vSwitch0

Apply Profile... Check Compliance Now

After you create the profile, attach it to hosts/clusters so that you can check compliance and apply it to hosts not in compliance.

This slide courtesy VMware

- PCI DSS V.20 (Oct 2010)
- PCI SSC Virtualization Special Interest Group - Information Supplement - Securing Virtual Payment Systems (expected Nov 2010)
 - Provide guidance on the use of Virtualization within payment systems so you can receive the benefits of the technology while maintaining compliance.
- Virtualization Mapping Tool (expected Nov 2010)
 - Spreadsheet based mapping; provide detailed guidance on allowed/disallowed usage of virtualization.



Thank you

Murray Goldschmidt
Chief Operating Officer
Sense of Security
murrayg@senseofsecurity.com.au
+61 2 9290 4444

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

Head office is level 8, 66 King Street, Sydney, NSW 2000, Australia. Owner of trademark and all copyright is Sense of Security Pty Ltd. Neither text or images can be reproduced without written permission.

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au