Myths and Truths about Virtualization Security!

(Mythes et vérités de sécurité de virtualisation!)

John Reeman - CTO and Founder

Background

- Involved in IT Security for 18 years
- Contributing author to CIS (Center for Internet Security) ESX 3.5 Security benchmarks
- Developed VMinformer a unique security assessment monitoring tool for virtual environments

VirtSec Technology Landscape

- Today virtualization security is still an evolving technology space in terms of existing established security players as well as new startups & the virtualization platform vendors themselves.
- The next 12-18 months will be difficult for you the customer due to the gold rush effect
- VMsafe was announced by VMware back in early 2008, vendor take up has been good but even today there are still only a handful of solutions that are commercially ready
- There is (still) no silver bullet....

The Scoobydoo moment!

“what about security?”

Where do you start?

- The risks and threats
- Architecture and design
- Management
- Security controls
- Auditing and Monitoring

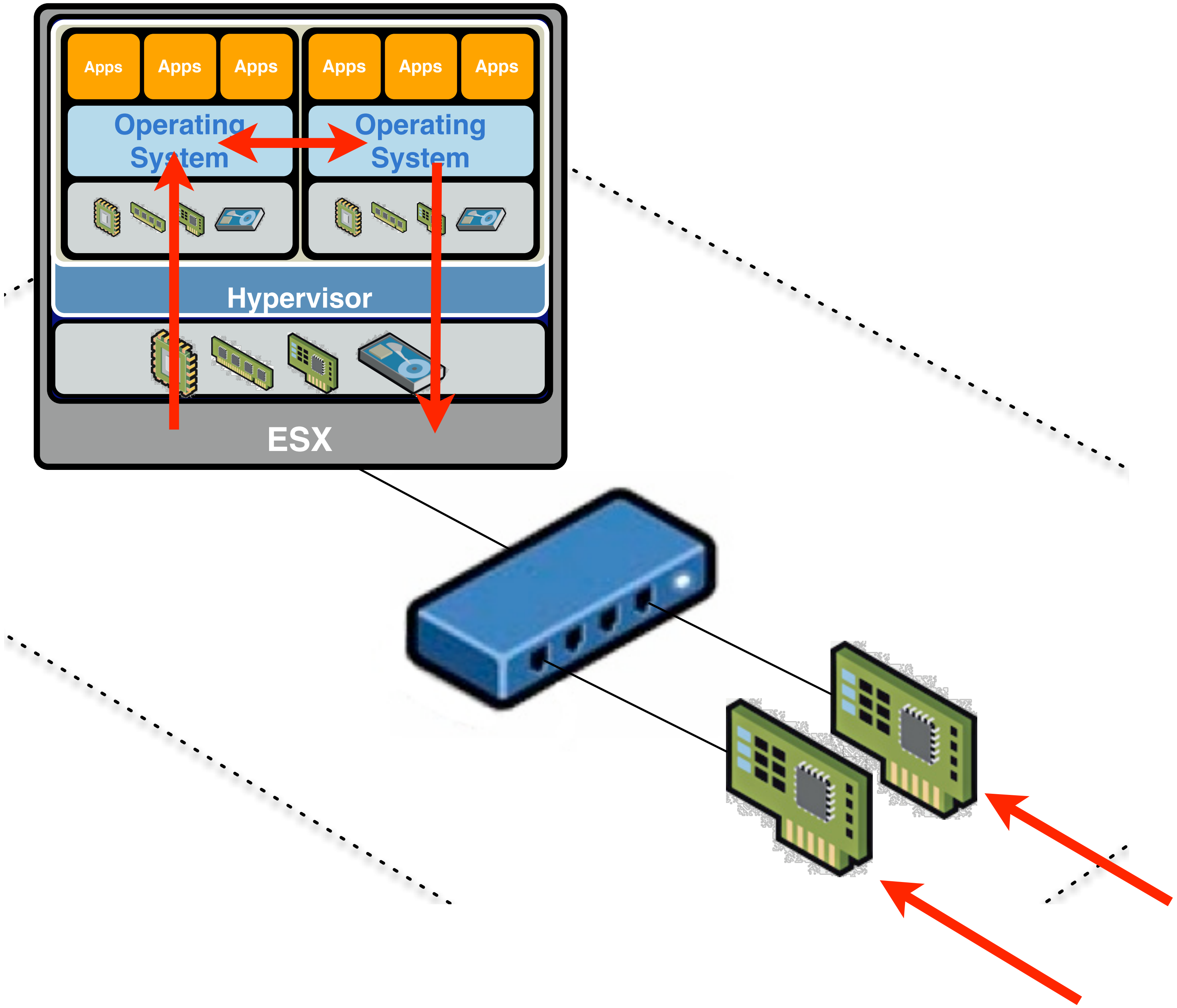
VMware Product Suite

- VMware vSphere 4
- VMotion
- Storage vMotion
- vShield Zones
- vCenter Server
- Lab Manager
- Life Cycle Manager
- Site Recovery Manager
- vOrchestrator

=

Larger Attack Surface

The potential threats

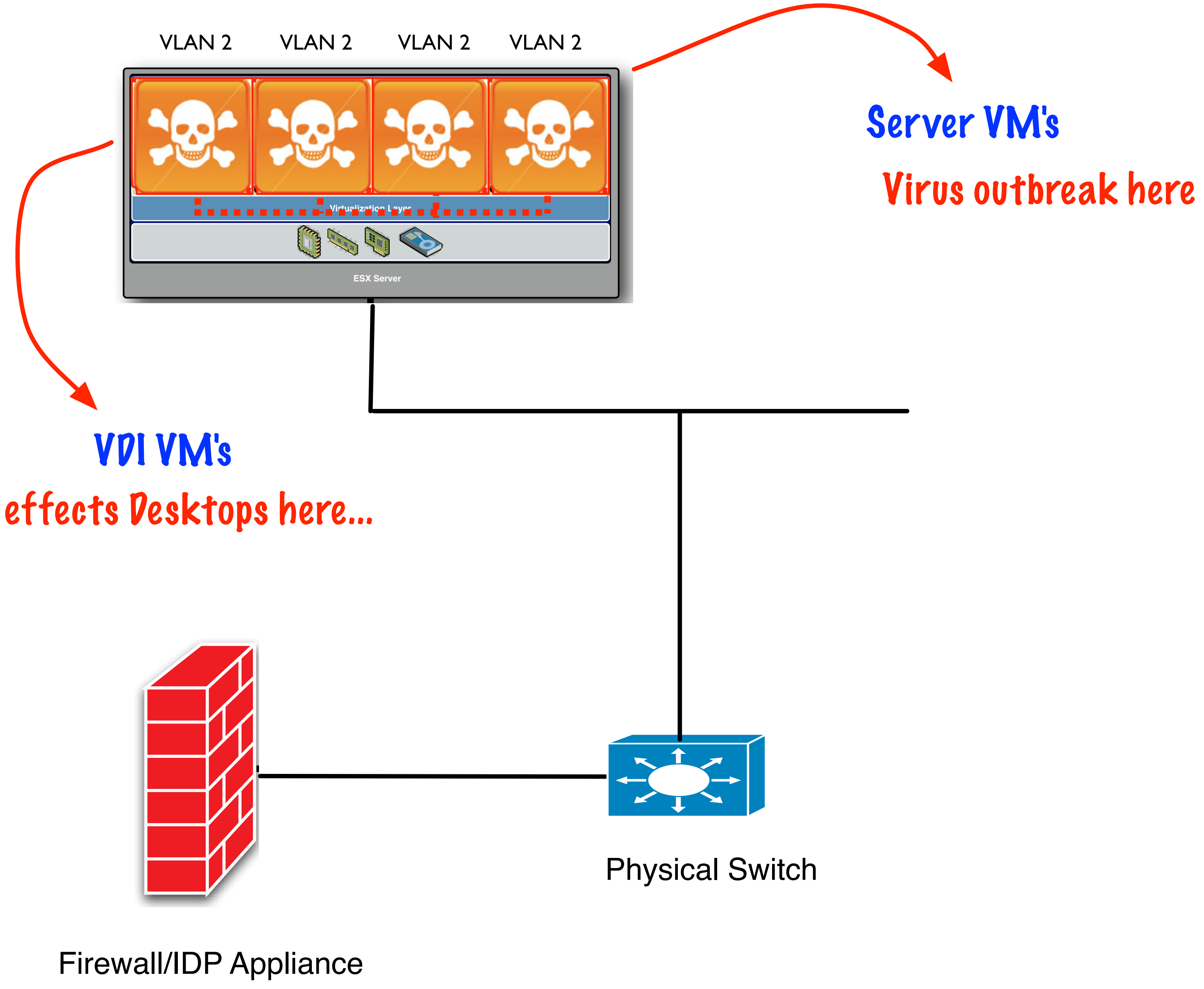


- Guest to Guest
- Host to Guest
- Guest to Host
- External to Host
- External to Guest

VMinformer
Assess Secure Comply

Don’t mix environments

No Security



Server VM's

Virus outbreak here

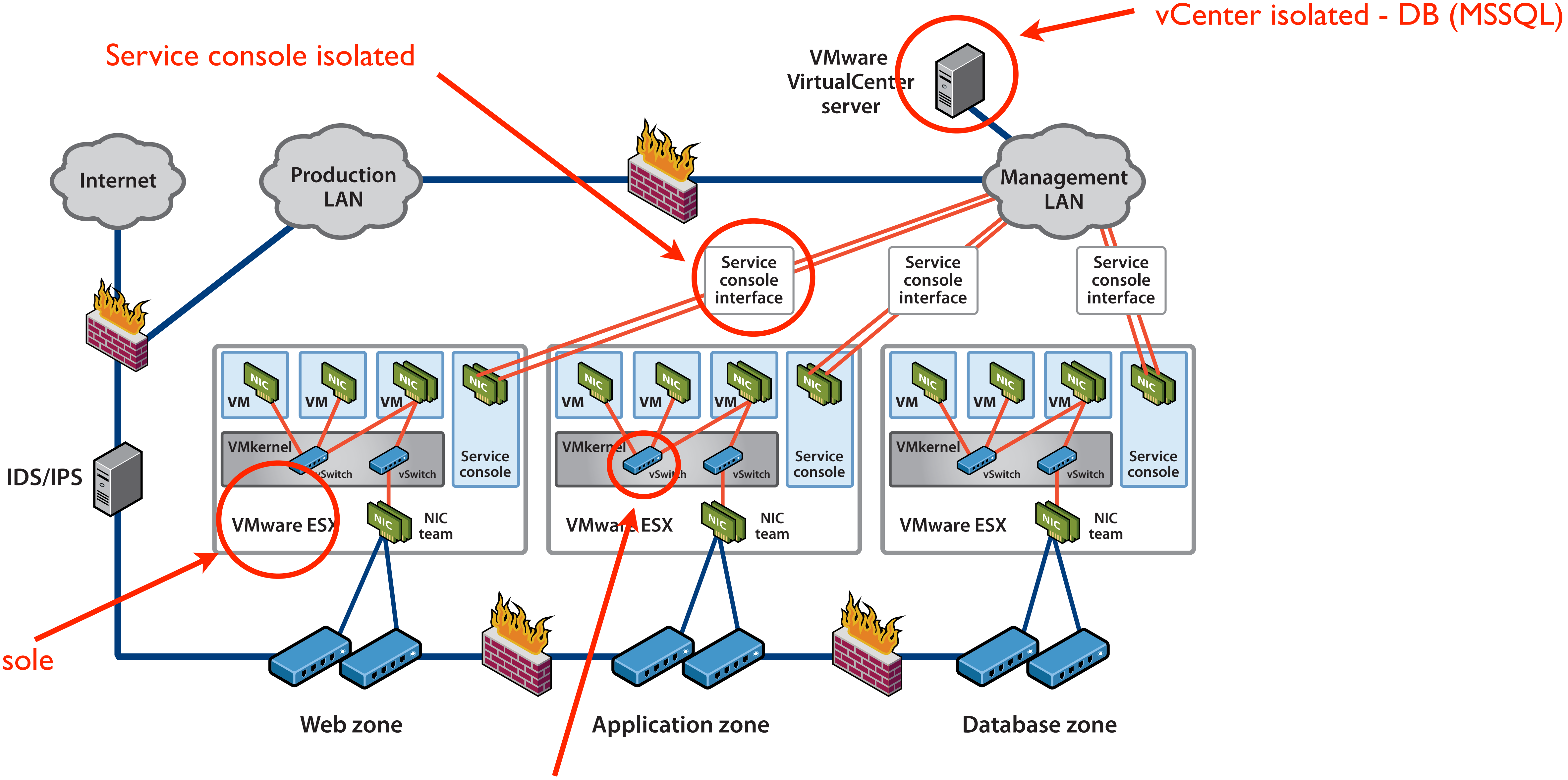
VDI VM's

effects Desktops here...

Physical Switch

Firewall/IDP Appliance

Architecture and Design



vCenter isolated - DB (MSSQL)

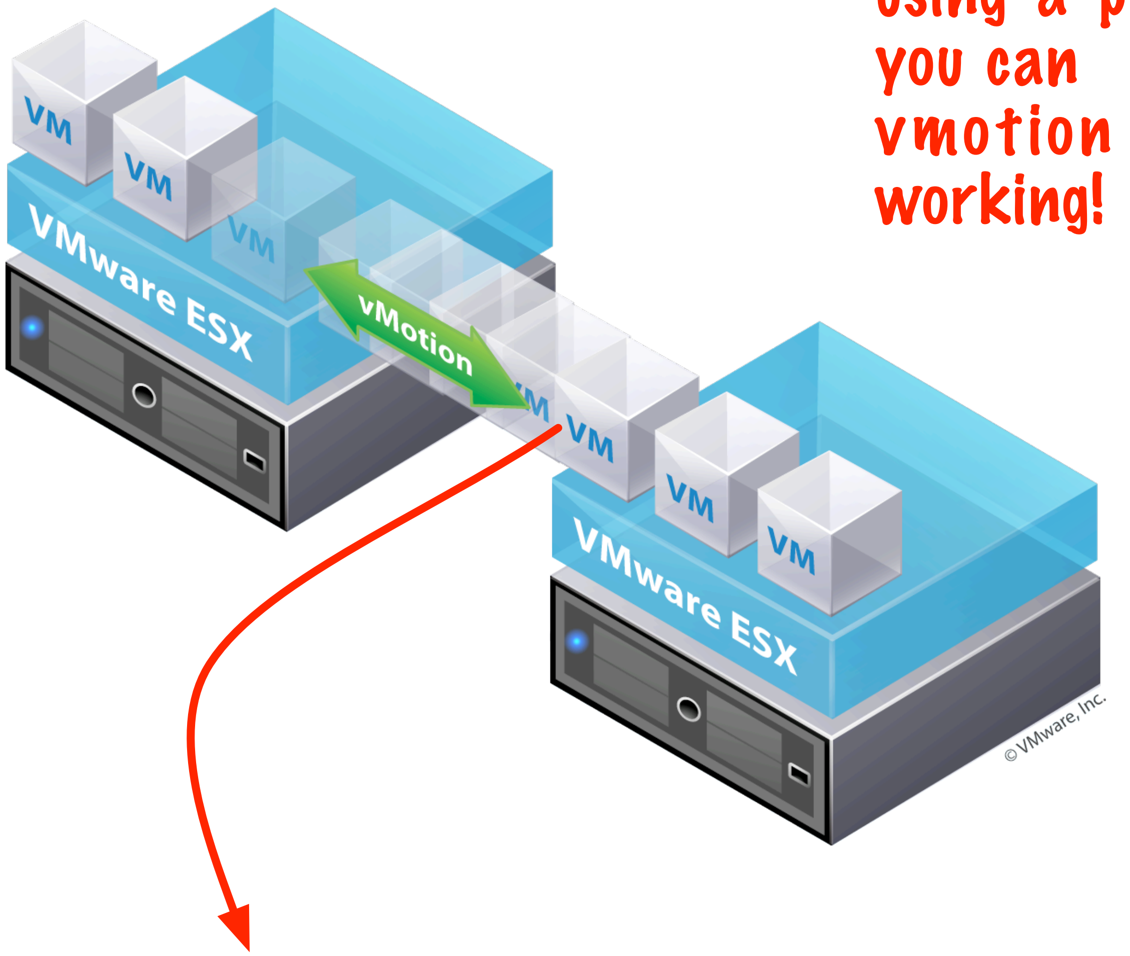
Service console isolated

ESX Host console

vSwitch Security

vMotion

using a port scanner like nmap you can by simply scanning the vmotion port stop vmotion working!



vMotion Network should be isolated
and if required encrypted using SSL

VM(in)Security Myth!

Security Team Says:

"Consolidating servers onto the same virtualized host is insecure because you cannot secure intra VM traffic!"

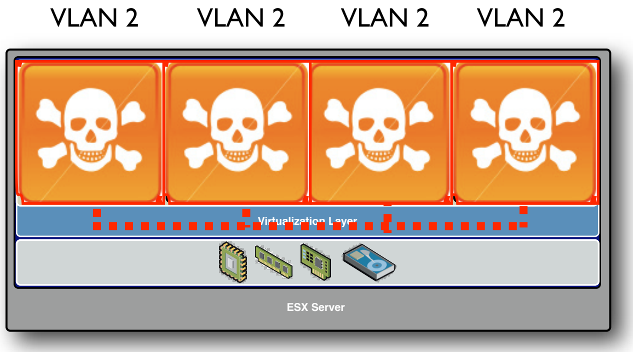
Reality Check:

"When you have two physical servers plugged into the same physical switch in the same VLAN, how do you secure intra-machine traffic?"

Response:

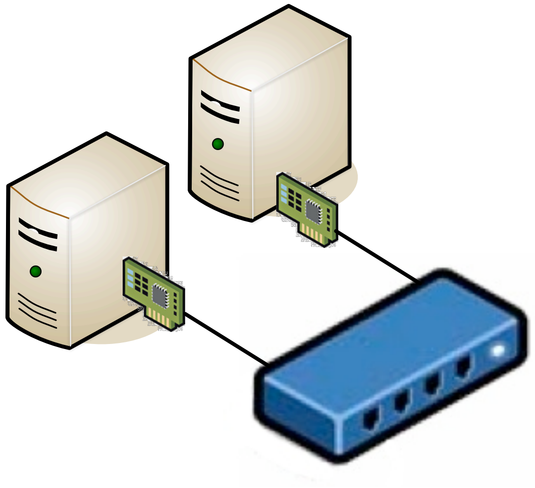
Another Scoobydoo moment!

Virtualized

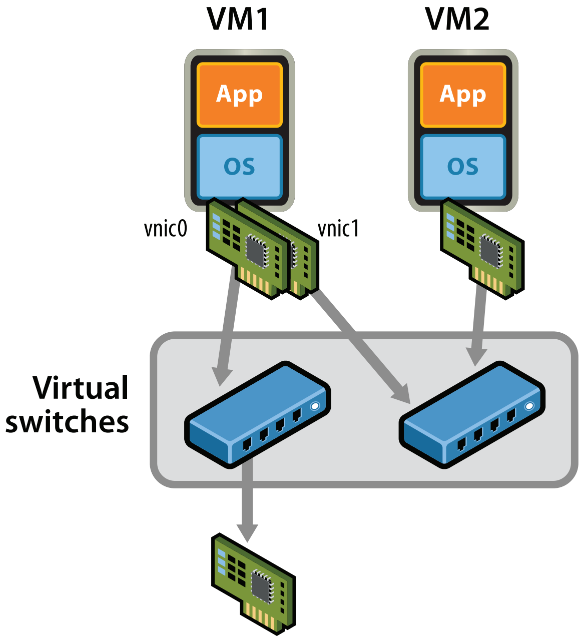


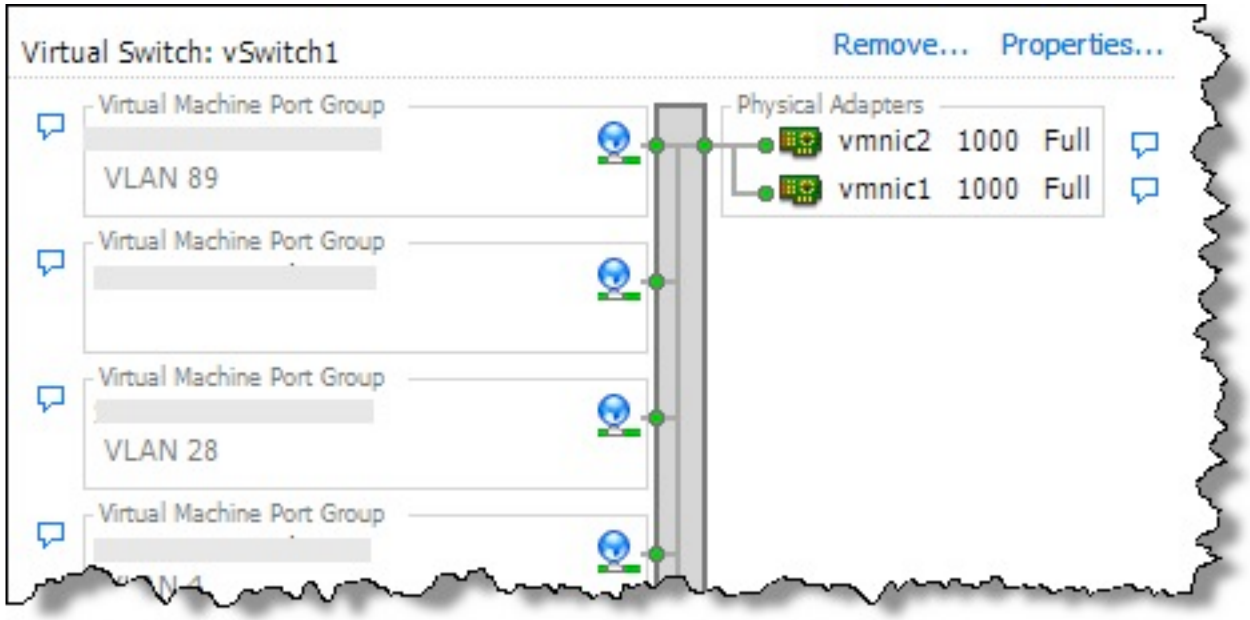
vs

Physical



nifty Security options on vSwitches





Virtual Switch: vSwitch1 Remove... Properties...

Virtual Machine Port Group
VLAN 89

Virtual Machine Port Group

Virtual Machine Port Group
VLAN 28

Virtual Machine Port Group

Physical Adapters

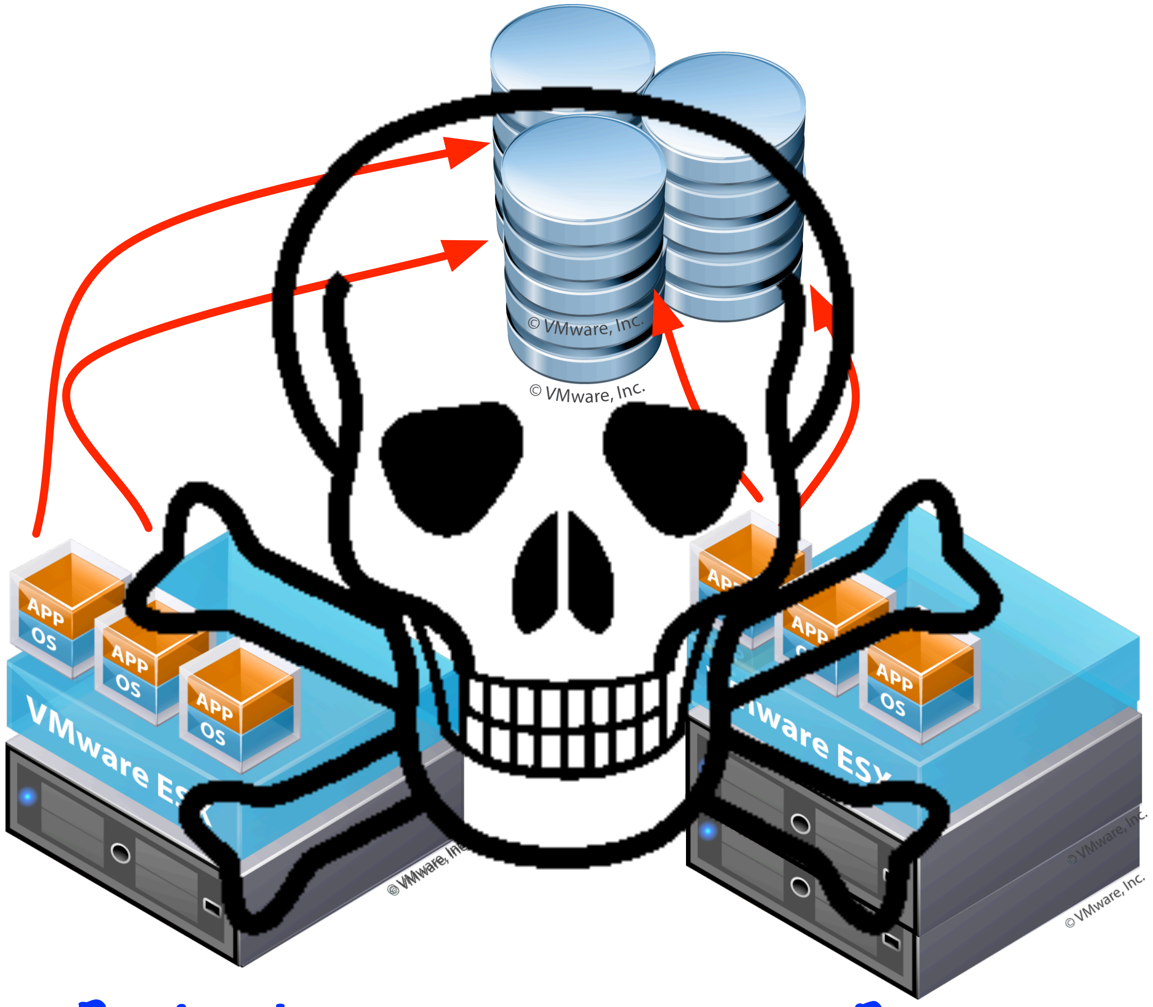
vmnic2	1000	Full
vmnic1	1000	Full

- Protect against Forged Transmits - Enable
- Protect against MAC Address Spoofing - Enable
- Promiscuous mode - DISABLE
- By DEFAULT none of the above are set

VMinformer
Assess Secure Comply

Storage Layer

- Where is the data stored?
- How important is the data?
- Encryption?



Production

Production

Demo

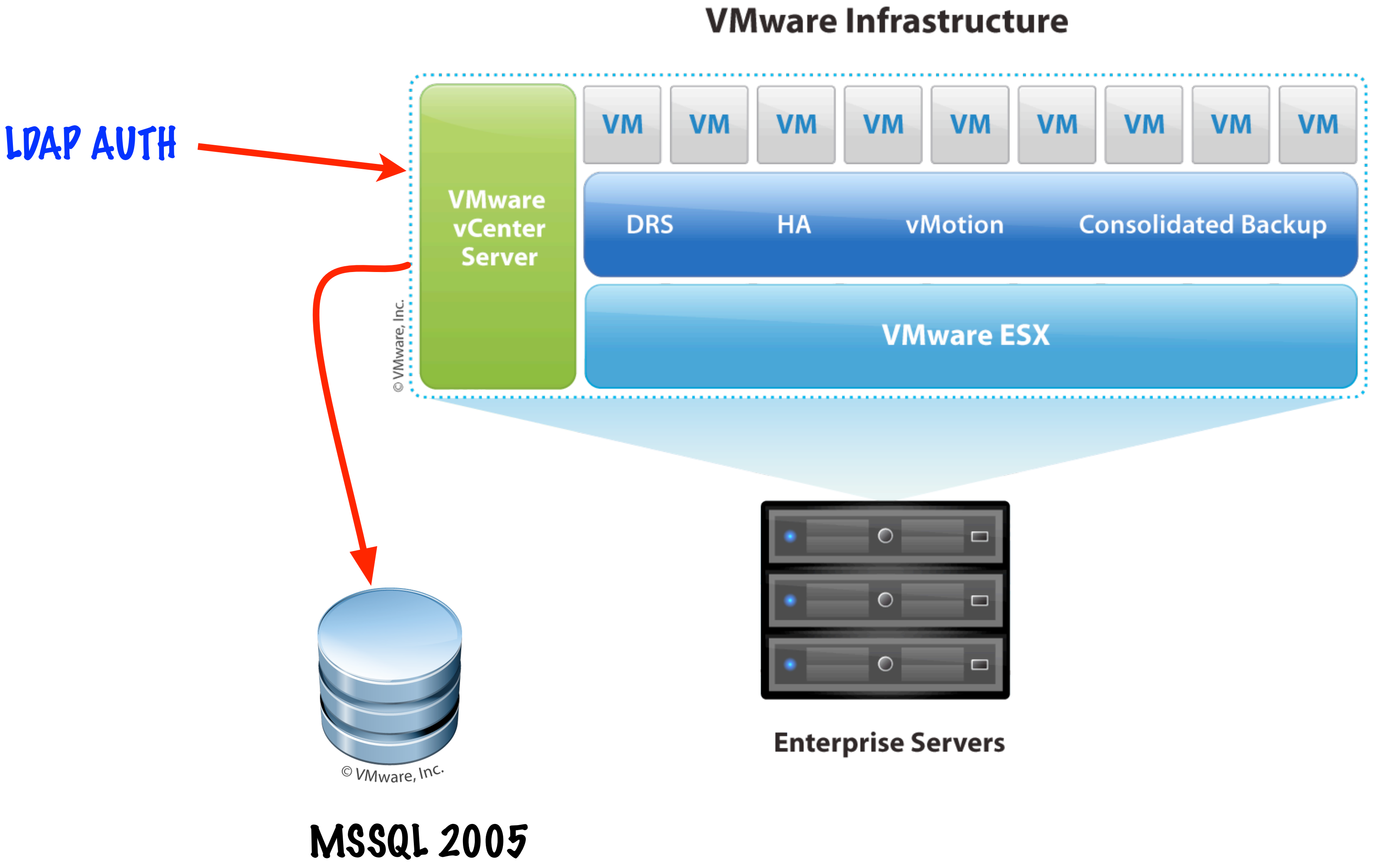
Demo

"Isolate data according to environment"

Management

- VI Client - ESX or vCenter
- API's - over 10+ currently available (VMCI Sockets)
- Web interface - ESX or vCenter
- Console (ESX)

Management - vCenter Security



Potential Risks

- Man in the middle attacks
- Brute force attacks
- sslsniff
- SQL Injection

Good Design

- Isolate vCenter on a management network
- Change the default SSL Cert
- Lock down MSSQL
- Work on the principle of least privilege

VMinformer
Assess Secure Comply

Management - Protocols and Ports

902,903

2050-2250

5988

SSH

8042-8045

5989

HTTP

Can control using ESX Firewall

CIM (427)

3260

Most TCP based some UDP

HTTPS

VNC

636

NTP

2049

SNMP

514

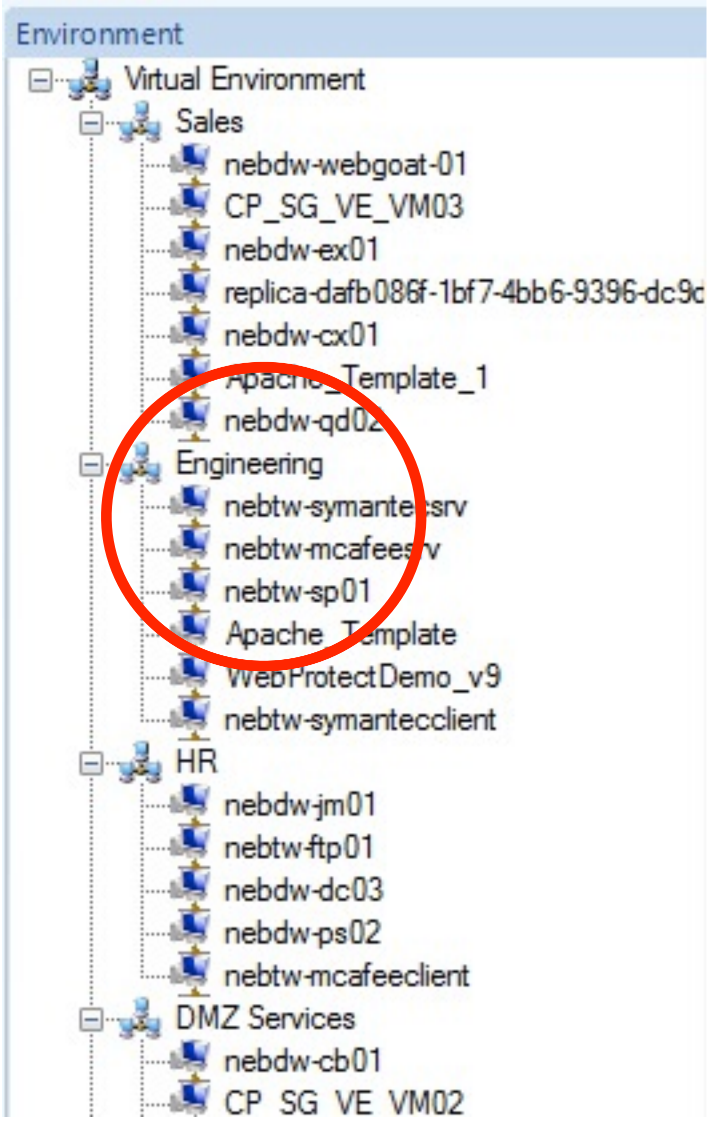
NFS

8000

SMTP

other considerations - Business Assets

- VM's are business assets
- What function do they perform?
- Standard VMware management tools do not provide a business view



Environment

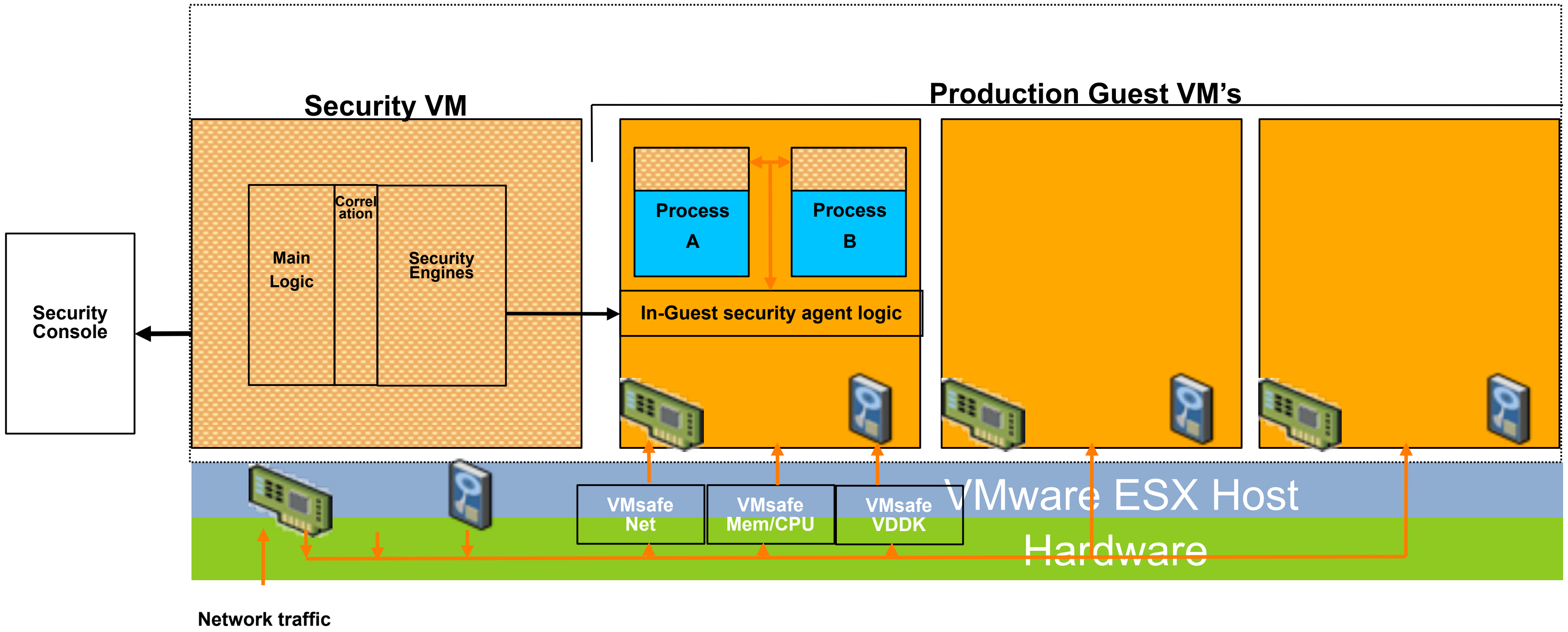
- Virtual Environment
  - Sales
    - nebdw-webgoat-01
    - CP_SG_VE_VM03
    - nebdw-ex01
    - replica-dafb086f-1bf7-4bb6-9396-dc9c
    - nebdw-cx01
    - Apache_Template_1
    - nebdw-qd02
  - Engineering
    - nebtw-symantecsrv
    - nebtw-mcafeesrv
    - nebtw-sp01
    - Apache_Template
    - WebProtectDemo_v9
    - nebtw-symantecclient
  - HR
    - nebdw-jm01
    - nebtw-ftp01
    - nebdw-dc03
    - nebdw-ps02
    - nebtw-mcafeeclient
  - DMZ Services
    - nebdw-cb01
    - CP_SG_VE_VM02

Security Controls

- Vendor provided - eg. VMsafe, vShield Zones
- Inbuilt Firewall on each ESX Host, IPTABLES
- 3rd Party Vendors, Firewall's, IPS, Anti-Virus etc
- Configuration and lockdown
- Entitlement - Roles and Permissions

VMsafe Security API's - quick overview

VMsafe Architecture – Closer Look



➡ VMsafe-Net - allows visibility of all I/O traffic on the host, inline protection or passive monitoring as well as ability to intercept, view, modify and replicate I/O traffic from one, many or all VM's

➡ VMsafe-Introspect (CPU-MEM) - Inspection of specific memory pages being used by the VM or its applications, knowledge of CPU state, policy enforcement, little or no performance impact

➡ VMsafe-Disk(VDDK) - Ability to mount and read disks, inspect I/O read/writes to the storage device

VMsafe sample use cases

- Verify-Before-Execute - in-line memory based introspection of guest code execution
- Virtual networks - distributed and full-grain network monitoring stack for guest communication
- File scanning - scheduled scanning of offline and online VM's.
- Correlation - multi-layered correlation engines in guest granularity
- In-guest guarantees: protecting in-guest components from in-guest malware
- Early integrity checks - early launch protection mechanisms for increased trust

Vulnerabilities - VMescape / VMbackdoor

- No known in the wild security vulnerabilities with the hypervisor yet
- There have been proof of concept VMescape exploit (Cloudburst) that target weaknesses in the virtual device drivers allowing guests to breakout and read data from the host or interact with other guests (has since been patched)
- This has happened with other virtualization platform vendors as well such as Citrix Xen server, blue pill, red pill, scooby etc

So what's going on?

- Should you monitor?
- Do you monitor?
- VM Sprawl an issue?
- Policy Baselines?

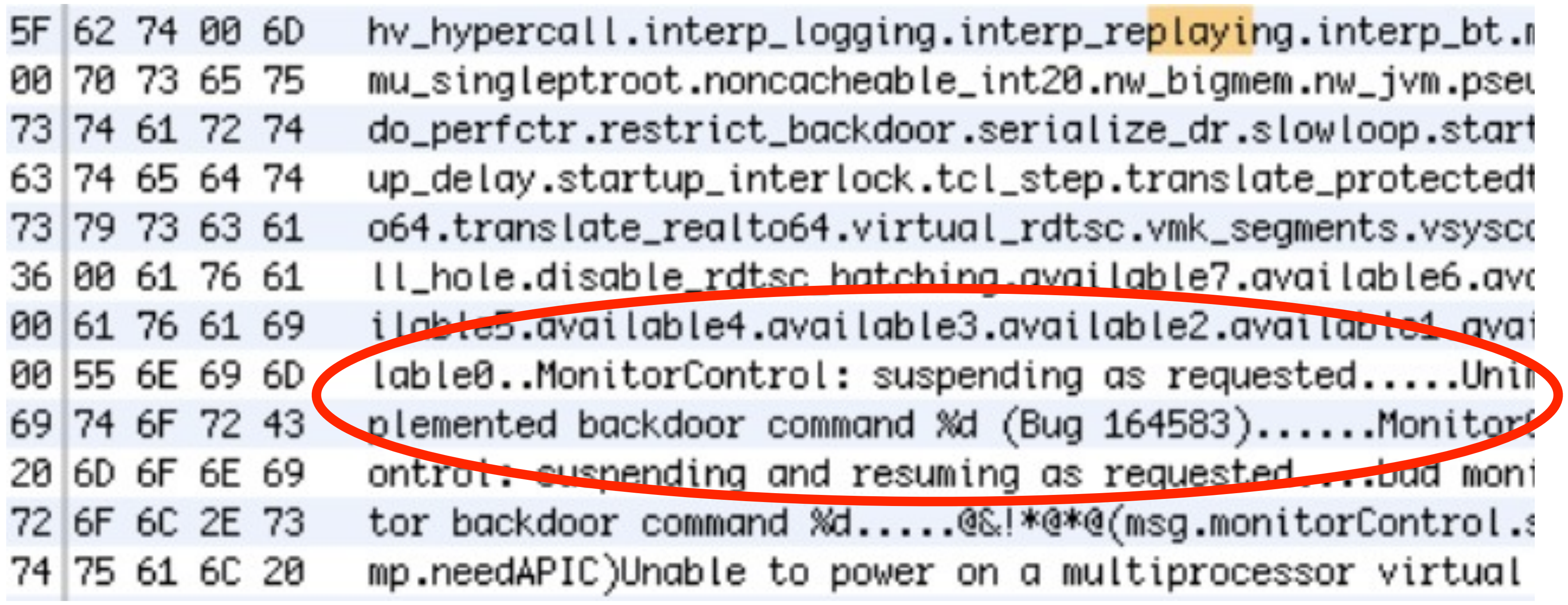
Time for the Demo!!

VMinformer techie stuff

- Written in C# and .NET
- Policy files written in XML
- VM API Checks are user extensible
- SSH checks are closed except for file permissions
- DB Checks are user extensible

VMinformer Policies

- CIS Benchmarks
- ISO 27005
- DISA STIG
- My Own Research (undocumented key pairs)



```
5F 62 74 00 6D   hv_hypercall.interp_logging.interp_replaying.interp_bt.
00 70 73 65 75   mu_singleptroot.noncacheable_int20.nw_bigmem.nw_jvm.pseu
73 74 61 72 74   do_perfctr.restrict_backdoor.serialize_dr.slowloop.start
63 74 65 64 74   up_delay.startup_interlock.tcl_step.translate_protectedt
73 79 73 63 61   o64.translate_realto64.virtual_rdtsc.vmk_segments.vsysca
36 00 61 76 61   ll_hole.disable_rdtsc_batching.available7.available6.ava
00 61 76 61 69   ilable5.available4.available3.available2.available1.avai
00 55 6E 69 6D   lable0..MonitorControl: suspending as requested.....Unin
69 74 6F 72 43   plemented backdoor command %d (Bug 164583)......Monitor
20 6D 6F 6E 69   ontrol: suspending and resuming as requested....bad moni
72 6F 6C 2E 73   tor backdoor command %d.....@&!*@*@(msg.monitorControl.
74 75 61 6C 20   mp.needAPIC)Unable to power on a multiprocessor virtual
```

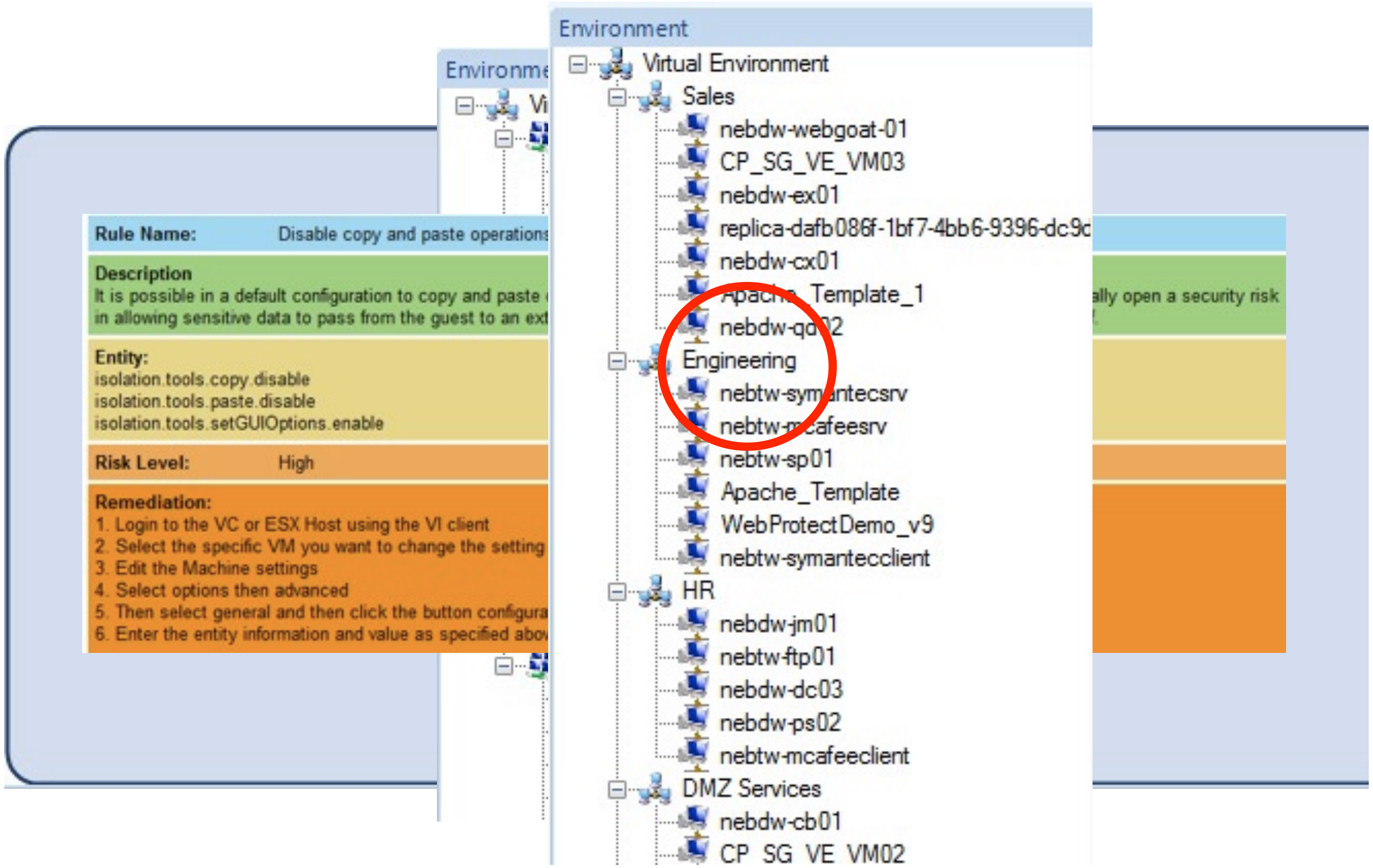
VMinformer
Assess Secure Comply

Futures for VMinformer

- SIEM Integration
- Helpdesk Integration
- NMAP Support
- Deeper checks for VM Guests (VMsafe API)
- Scheduling
- Policy baselines

VMinformer

- Assess
- Identify
- Classify
- Context
- Report
- Remediate



Environment

Virtual Environment
- Sales
  - nebdw-webgoat-01
  - CP_SG_VE_VM03
  - nebdw-ex01
  - replica-dafb086f-1bf7-4bb6-9396-dc9c
  - nebdw-cx01
  - Apache_Template_1
  - nebdw-qa02
- Engineering
  - nebtw-symantecsrv
  - nebtw-mcafeesrv
  - nebtw-sp01
  - Apache_Template
  - WebProtectDemo_v9
  - nebtw-symantecclient
- HR
  - nebdw-jm01
  - nebtw-ftp01
  - nebdw-dc03
  - nebdw-ps02
  - nebtw-mcafeeclient
- DMZ Services
  - nebdw-cb01
  - CP_SG_VE_VM02

Rule Name: Disable copy and paste operations

Description
It is possible in a default configuration to copy and paste … ally open a security risk
in allowing sensitive data to pass from the guest to an ext… t.

Entity:
isolation.tools.copy.disable
isolation.tools.paste.disable
isolation.tools.setGUIOptions.enable

Risk Level: High

Remediation:
1. Login to the VC or ESX Host using the VI client
2. Select the specific VM you want to change the setting
3. Edit the Machine settings
4. Select options then advanced
5. Then select general and then click the button configura
6. Enter the entity information and value as specified abov

Some Final thoughts....

- Remember there is no silver bullet
- Virtualization Security could end up costing you more if not planned well
- Design well, think about what you are trying to achieve or find someone who can help
- Thoroughly evaluate existing and emerging technologies to determine value vs disruption
- Use risk assessment and threat modeling
- VMware is NOT inherently INSECURE, its us damn humans that can mess it up!
- Monitoring and Auditing is IMPORTANT, don't become complacent...
- Push the virtualization platform providers to reveal roadmaps, don't always believe the hype!

Merci

communaute edition disponible @

www.vminformer.com/community

john@vminformer.com