

# Securing the Virtual Infrastructure – Achieving a Trusted Cloud

- Ana Seijas, Security & Compliance Specialist, VMware, Inc.
- [aseijas@vmware.com](mailto:aseijas@vmware.com)



# Agenda

- **Cloud Computing**
- **VMware and Security**
  - Network Security
- **Use Case**
  - Securing View Deployments
- **Questions**

# IT consumption is changing



# Enterprise IT is Aligning to Consumption

Empowered,  
Secure Mobile  
Workforce



Faster  
Time-to-Market  
for Modern  
Applications



A More Flexible,  
Scalable, Efficient  
Infrastructure  
for All Apps



Existing Datacenters



Public Cloud Services

Paul Maritz  
CEO



“VMware enables our customers’ success by simplifying and automating IT in the Cloud Era.”

# Future of Cloud Computing



**80%**

of new commercial enterprise apps will be deployed on cloud platforms in 2012

predicted cloud computing market in 2020

**\$241 B**



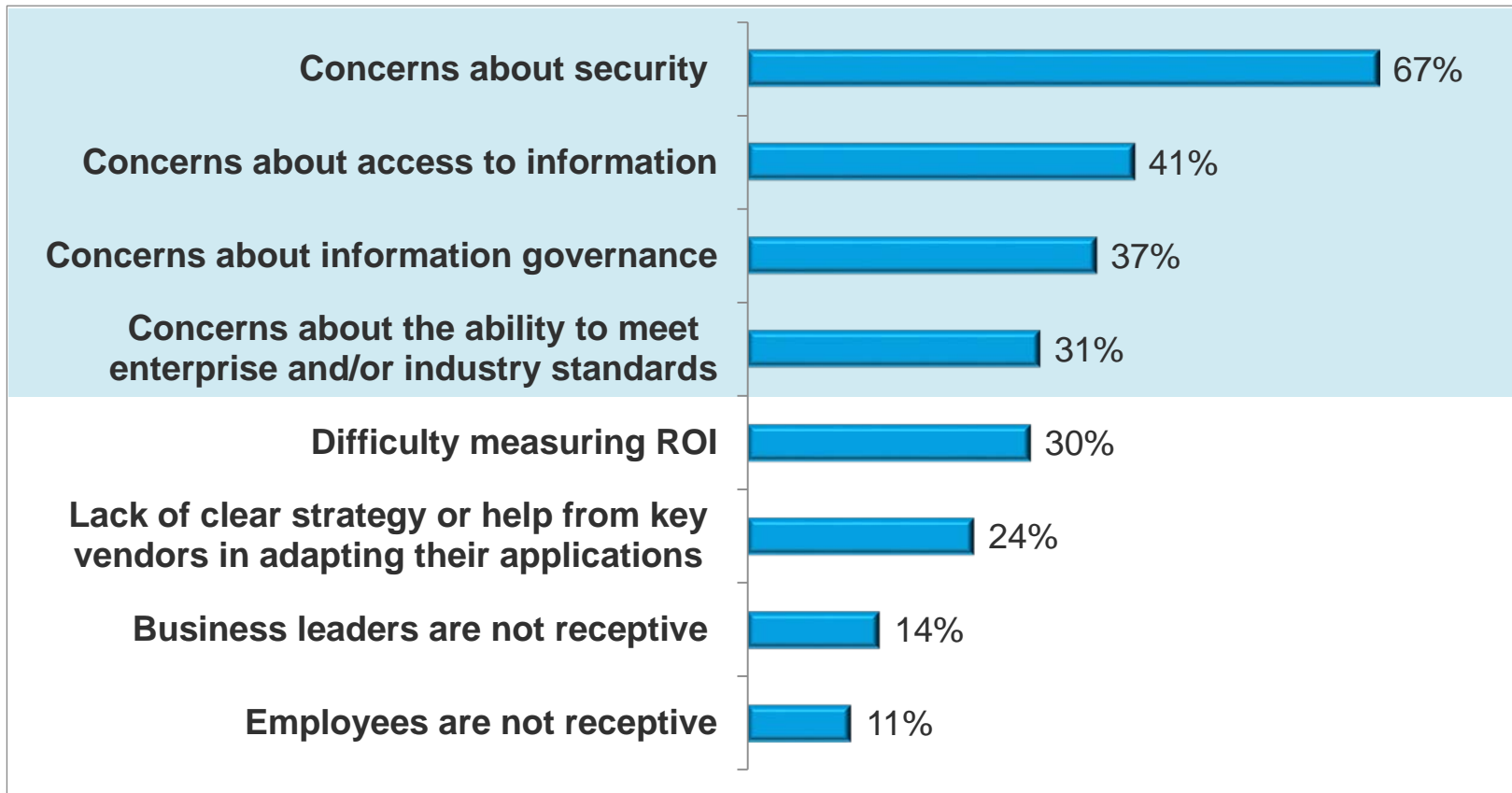
**2.7ZB**

predicted volume of digital content, up 48% from 2011

Source: IDC, "Predictions 2012: Competing for 2020," December 2011; Forrester, "Sizing the Cloud," April 2011

# Security and Compliance are Key Concerns for Organizations Considering Cloud Migrations

Q. What are the top challenges or barriers to implementing a cloud computing strategy?



**Top 4 Concerns Relate to Security or Compliance**

Source: 2010 IDG Enterprise Cloud-based Computing Research, November 2010

# Security Concerns in Virtualized Environments

How can I **secure my applications** in the virtual environment?

I have major concerns about **confidential & regulated data** being secure in our virtual environment.

Users are complaining about poor performance of their desktop due to **anti-virus processing**.

Infrastructure Team



Security Team &  
Compliance Officer

Virtualization adds a whole new level of complexity. No one can tell me the state of our **compliance**.

Operations Team



THE AUDITOR

**Both Security and Proof of Compliance are required to build Trust in the Cloud**

# VMware and Security



## Virtualization Security

- Secure hypervisor architecture
- Platform hardening features
- Secure Development Lifecycle



## Audit and Compliance

- Hardening Guidelines - Prescriptive guidance for deployment and configuration
- Enterprise controls for security and compliance



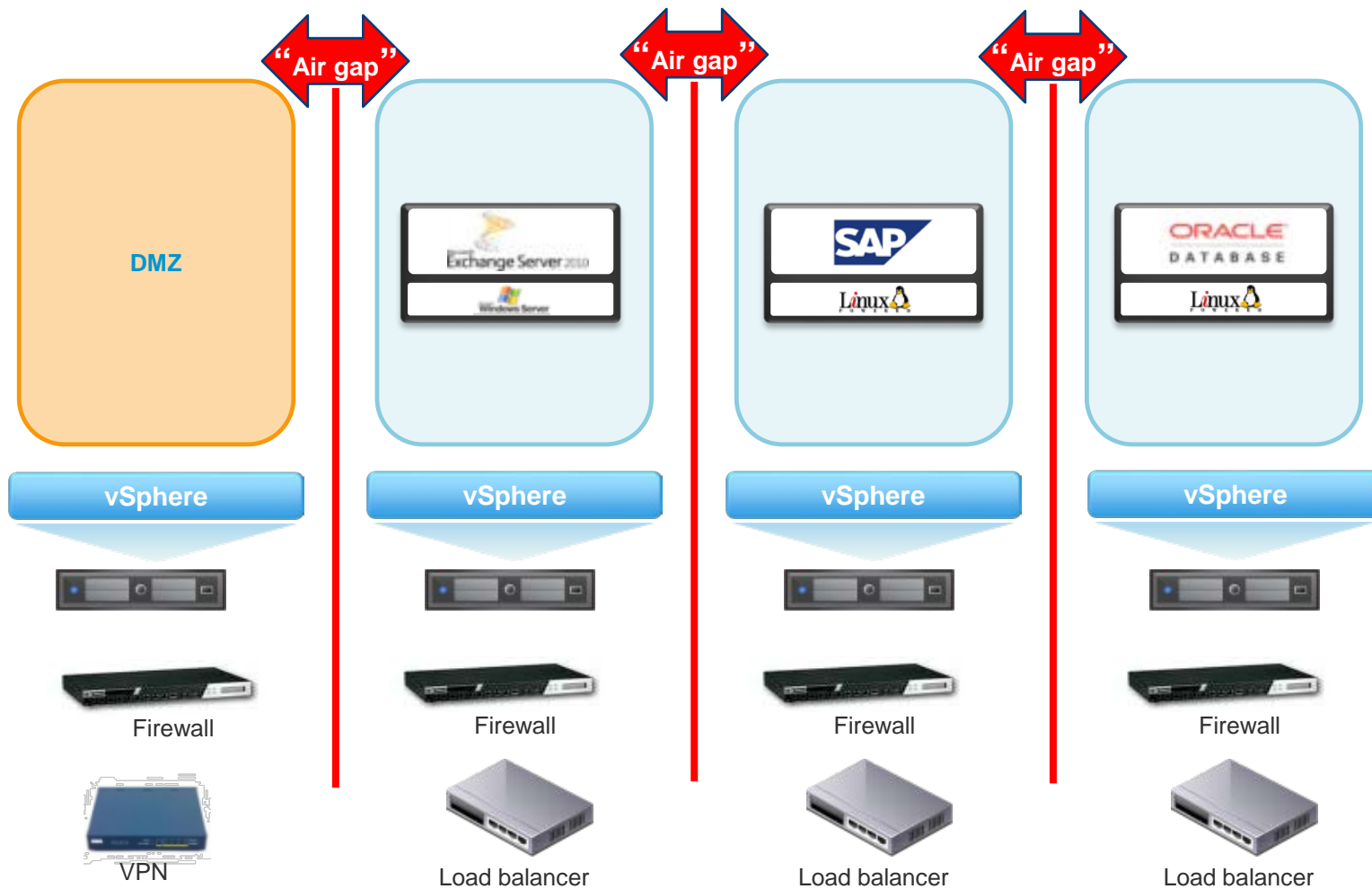
## Network Security in the Data Center/ Cloud

- Virtualization-aware security
- Products taking Unique Advantage of virtualization



# Traditional Security in Virtual Environments

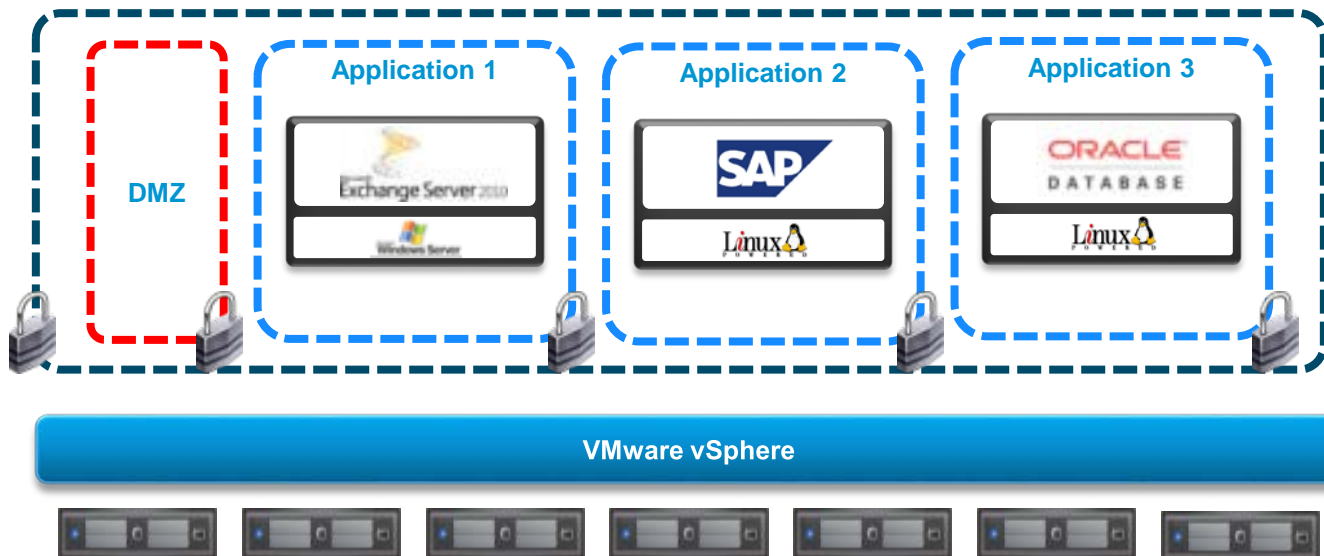
## Physical Security Devices and Airgaps



# Customers Want to Virtualize More....

## Increased interest in Mixing Trust Zones

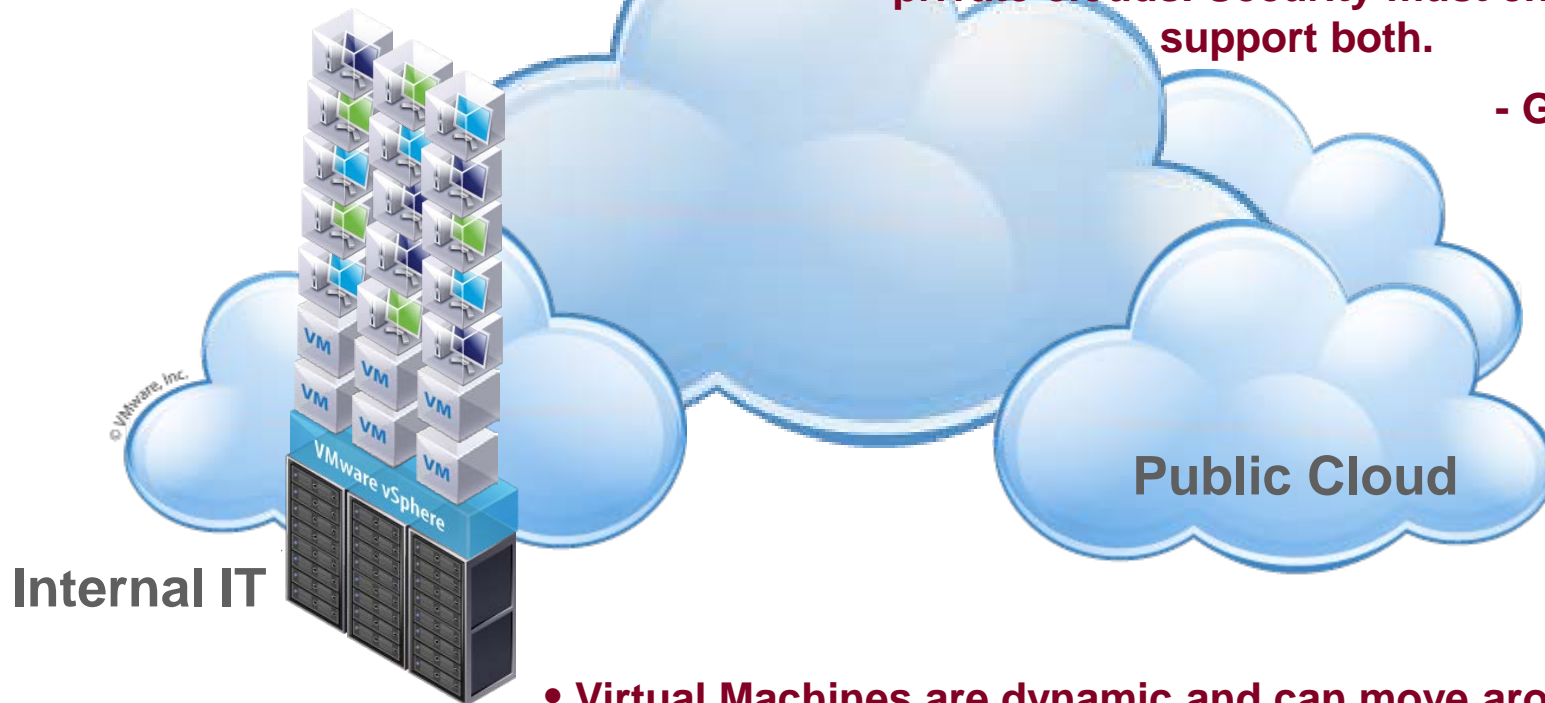
- PCI
- Tier 1 Apps
- DMZ



# New Challenges with Cloud Computing

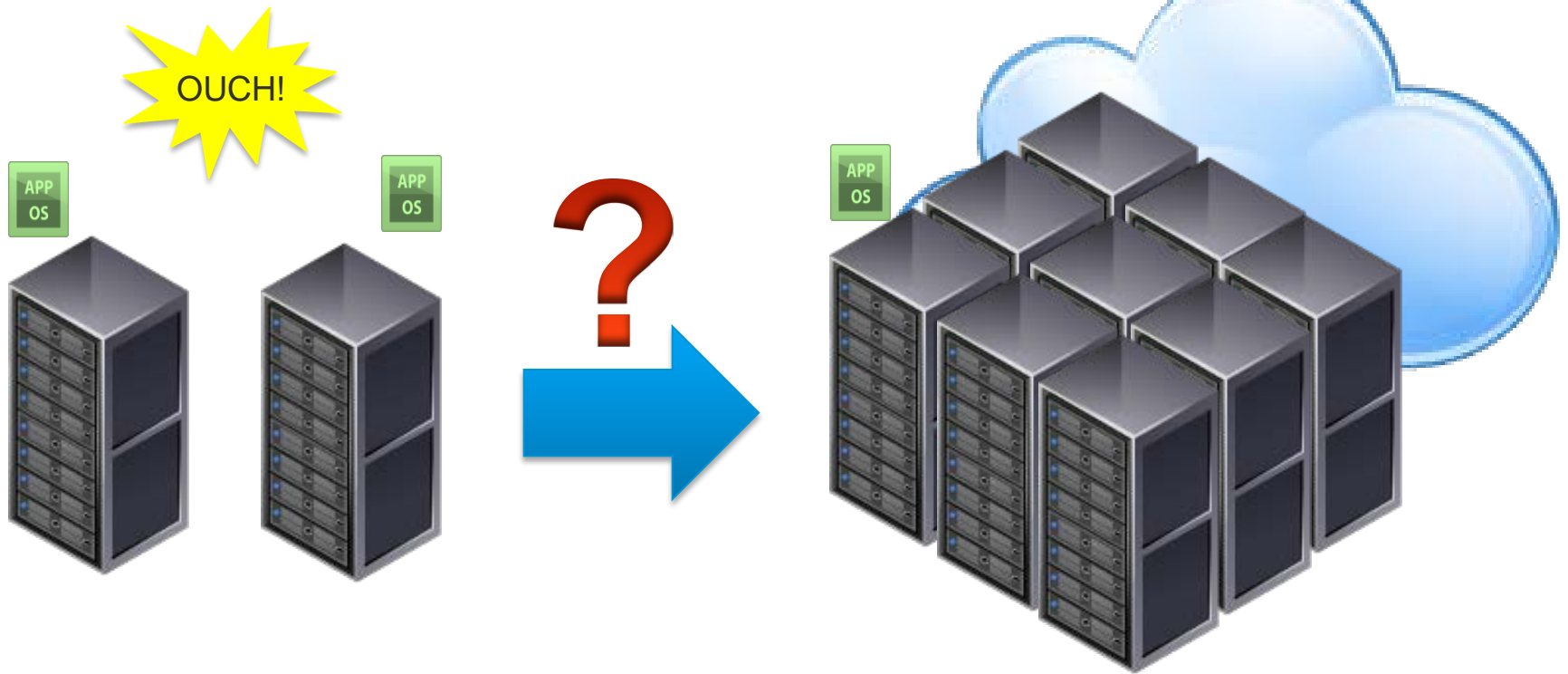
Virtualization forms the foundation for building private clouds. Security must change to support both.

- Gartner 2010

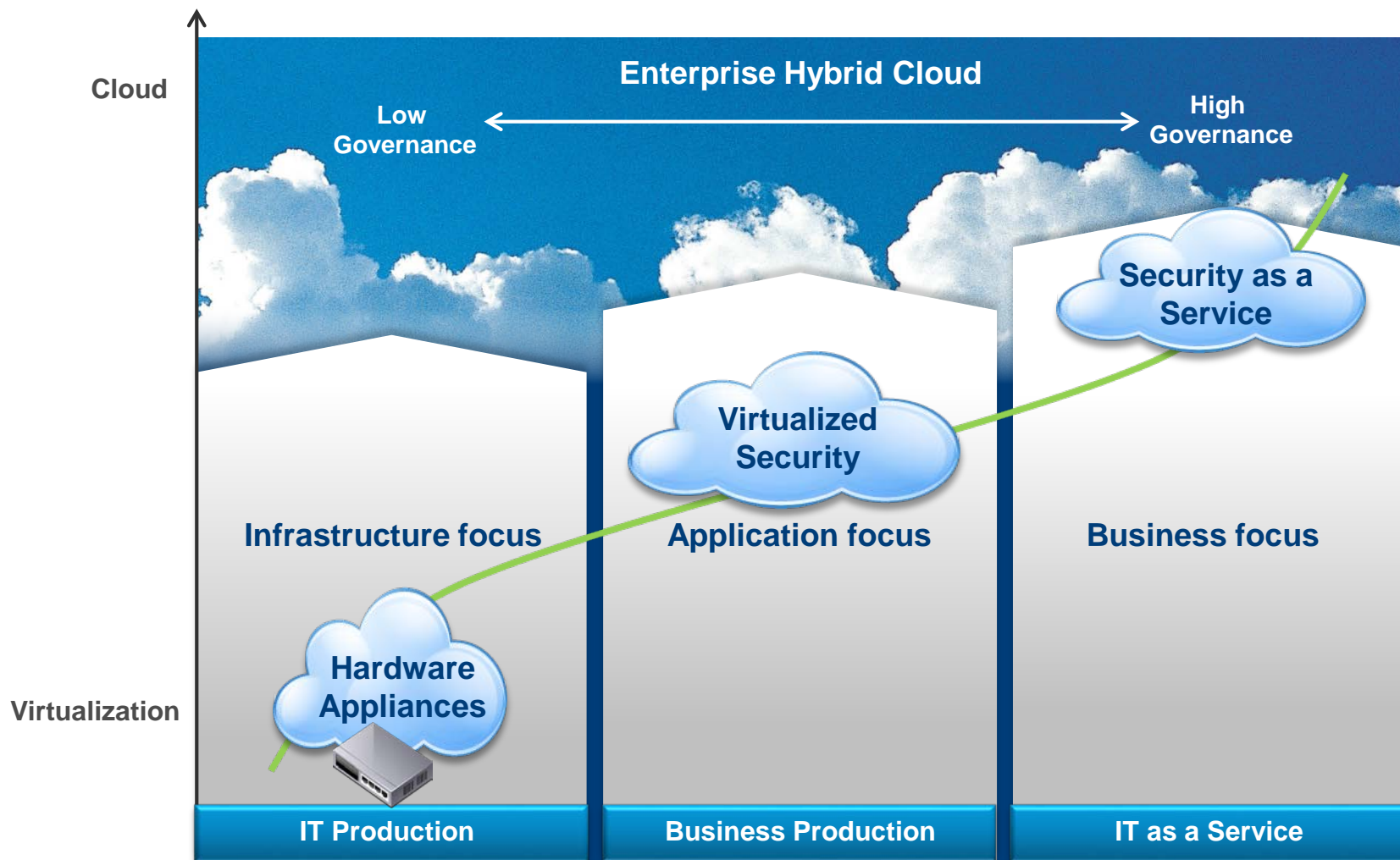


- Virtual Machines are dynamic and can move around
- Virtual Machines are easily created and can be self provisioned by non IT staff
- Increased workloads with large amount of virtual desktops in datacenter

# How Do We Transform Rigid Silos Into Secure Elastic Clouds?



# The Security Evolution - From Appliances to Security as a Service



# VMware vShield – Foundation for Trusted Cloud

## Securing the Cloud From Edge to Endpoint

### vShield Edge

Secure the edge of the virtual datacenter

### vShield App

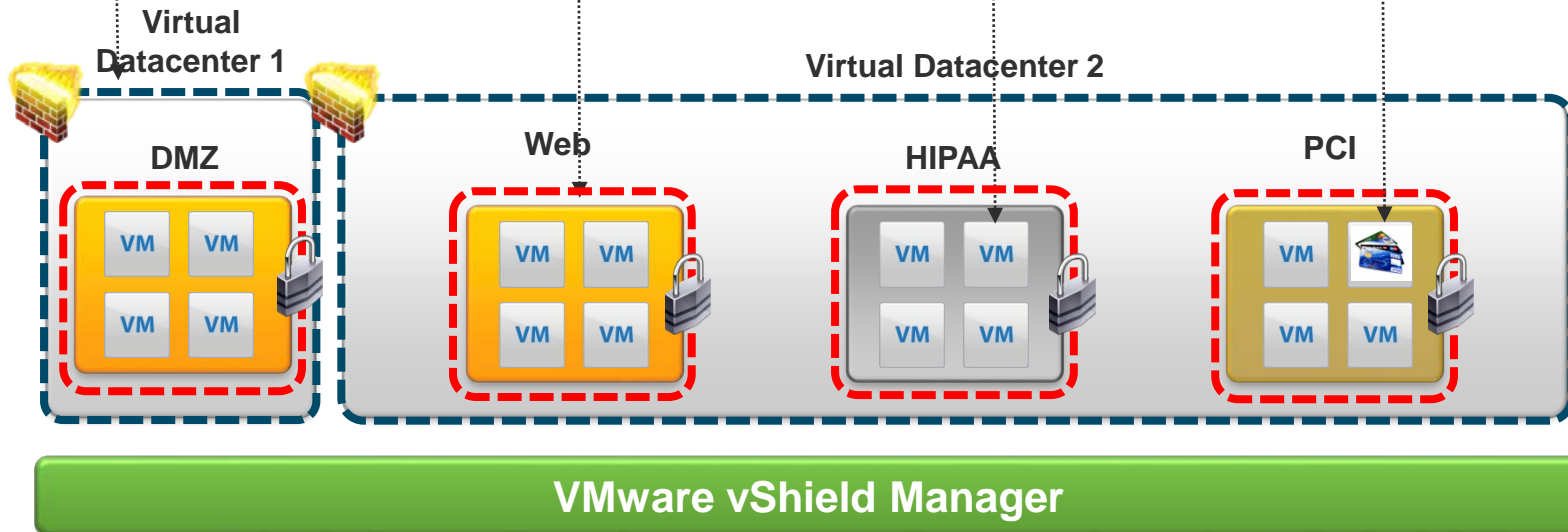
Protect applications from threats with trust zones

### vShield Endpoint

Streamline and accelerate anti-virus solutions

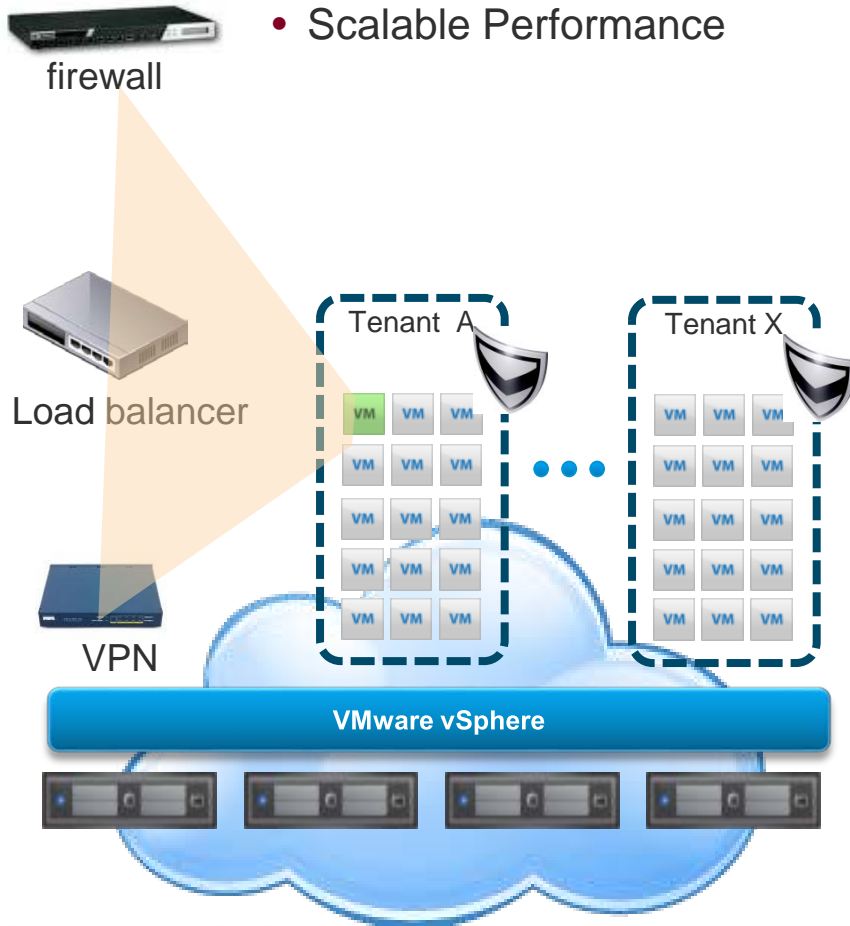
### vShield Data Security

Protect against data leaks



## Secure the Edge of the Virtual Data Center

- 'Auto-wired' Security for VDCs – VPN, Load Balancer, DHCP, NAT, Firewall
- Eliminate 'Air-Gapped' sprawl
- Scalable Performance

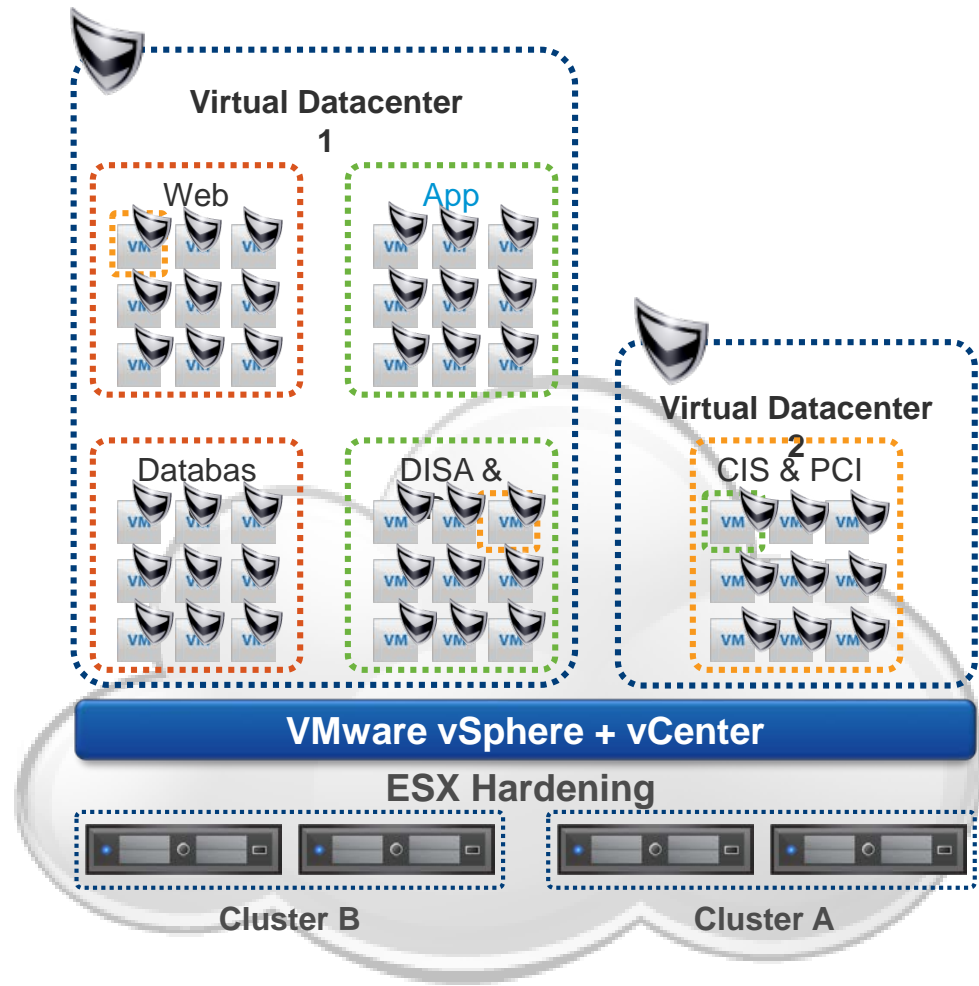


## Features

- Multiple edge security services in one appliance
  - Stateful inspection firewall
  - Network Address Translation (NAT)
  - Dynamic Host Configuration Protocol (DHCP)
  - Site to site VPN (IPsec)
  - Web Load Balancer
- Policy management through UI or REST APIs
- Logging and auditing based on industry standard syslog format

## Enforce Micro-segmentation Inside the vDC

- **Protect applications against Network Based Threats**
  - **Full Stateful Packet Inspection** firewall
  - Control on **per-VM/per vNIC** level
  - See **VM-VM traffic** within the same host with **Robust Flow Monitoring**
  - Security groups **enforced with VM movement**
  - **Logging and auditing via Syslog**
  - **REST APIs for automation**





# Visibility into Sensitive Data to Address Regulatory Compliance

## vShield Data Security

**Select Regulations**

Selected | All

Regulations	Category	Region	
<input type="checkbox"/> ABA Routing Numbers	PCI,PII	ALL	Details
<input type="checkbox"/> Arizona SB-1338	PHI,PCI,PII	NA	Details
<input type="checkbox"/> Australia Bank Account Numbers	PII	APAC	Details
<input type="checkbox"/> Australia Business and Company Numbers	PII	APAC	Details
<input type="checkbox"/> Australia Medicare Card Numbers	PHI,PII	APAC	Details
<input type="checkbox"/> Australia Tax File Numbers	PII	APAC	Details
<input type="checkbox"/> California AB-1298	PHI,PCI,PII	NA	Details
<input checked="" type="checkbox"/> California SB-1386	PHI,PCI,PII	NA	Details
<input type="checkbox"/> Canada Drivers Licence Numbers	PII	NA	Details
<input type="checkbox"/> Canada Social Insurance Numbers	PHI,PII	NA	Details
<input checked="" type="checkbox"/> Colorado HB-1119	PHI,PCI,PII	NA	Details
<input checked="" type="checkbox"/> Connecticut SB-650	PHI,PCI,PII	NA	Details

Cloud Infrastructure  
(vSphere, vCenter, vShield, vCloud Director)

### Overview

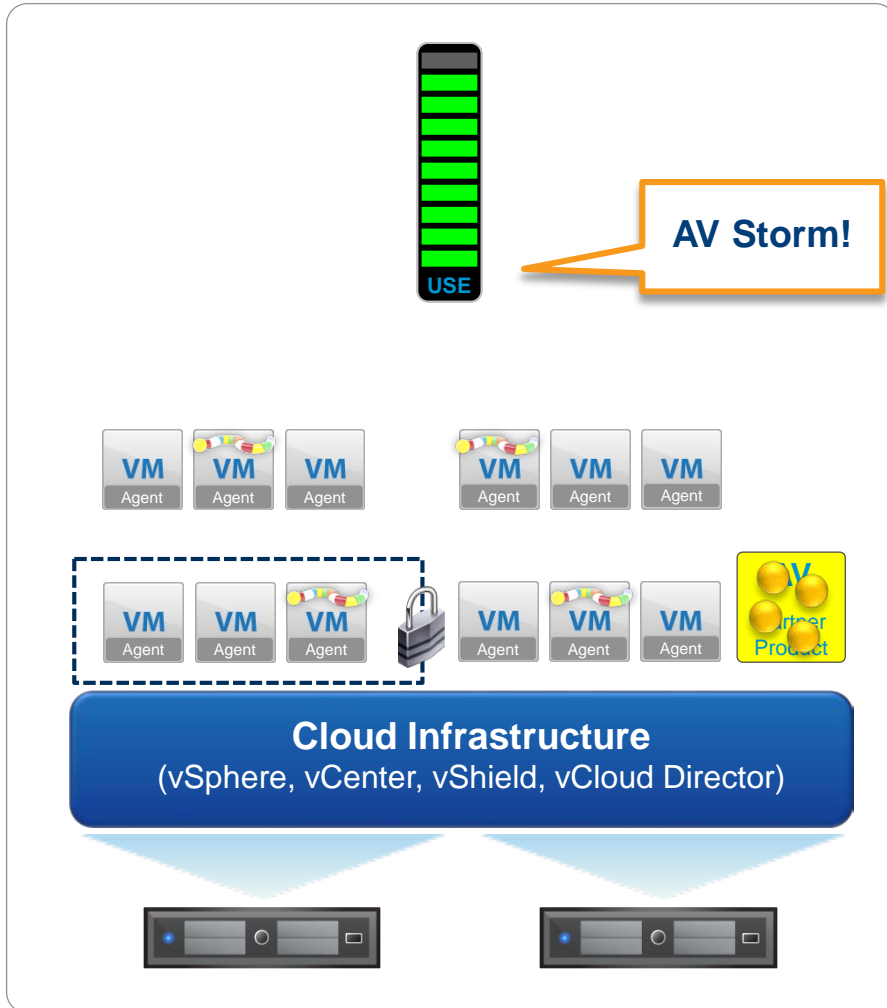
- More than 80 pre-defined templates for country/industry specific regulations
- Accurately discover and report sensitive data in unstructured files with analysis engine
- Segment off VMs with sensitive data in separate trust zones

### Benefits

- Quickly identify sensitive data exposures
- Reduce risk of non-compliance and reputation damage
- Improve performance by offloading data discovery functions to a virtual appliance

# Efficient Protection Against Malware

## vShield Endpoint



## Overview

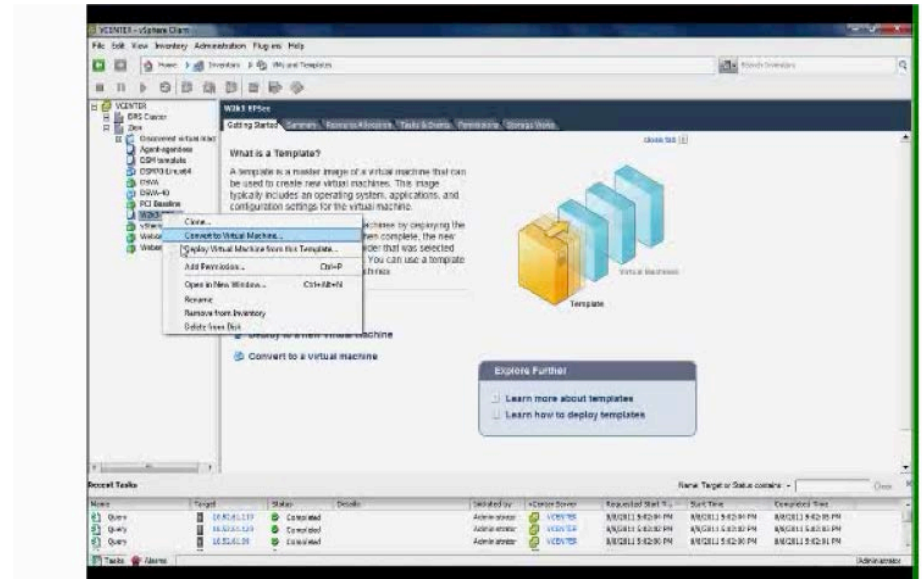
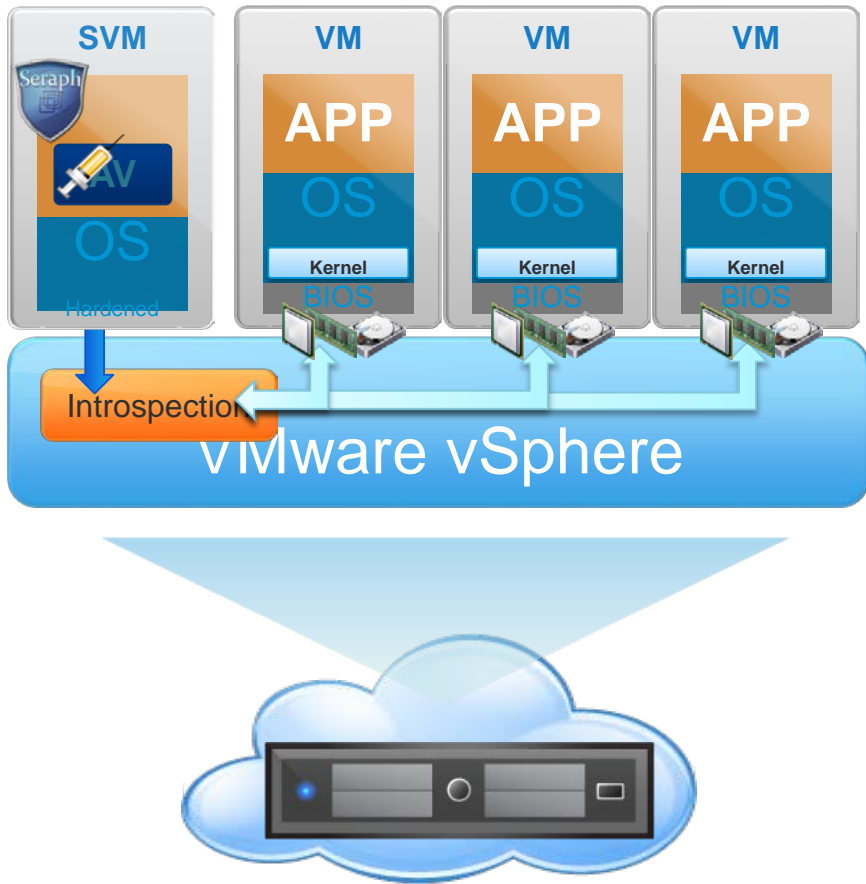
- Offloaded anti-virus protection
- Leverage 3rd party anti-virus solutions
- Eliminate security agent from guest VM
- Partner provides security virtual appliance for endpoint security such as anti-virus, file integrity monitoring, OS event logging

## Benefits

- **Efficiency** - Improve performance and consolidation ratios from 30-100%\*. Eliminate anti-virus 'storms'
- **Manageability** - Streamline deployment and monitoring of endpoint security
- **"Better than physical"** – VM protected the moment it comes online, no agent susceptible to attack

\* Depending on whether workload stresses the AV solution – Source: Tolly Group 2010

# vShield Endpoint



# Securing View Deployment

vShield App and View Use Case: <http://blogs.vmware.com/security/2011/05/desktop-security-zones-and-the-desktop-dmz.html>

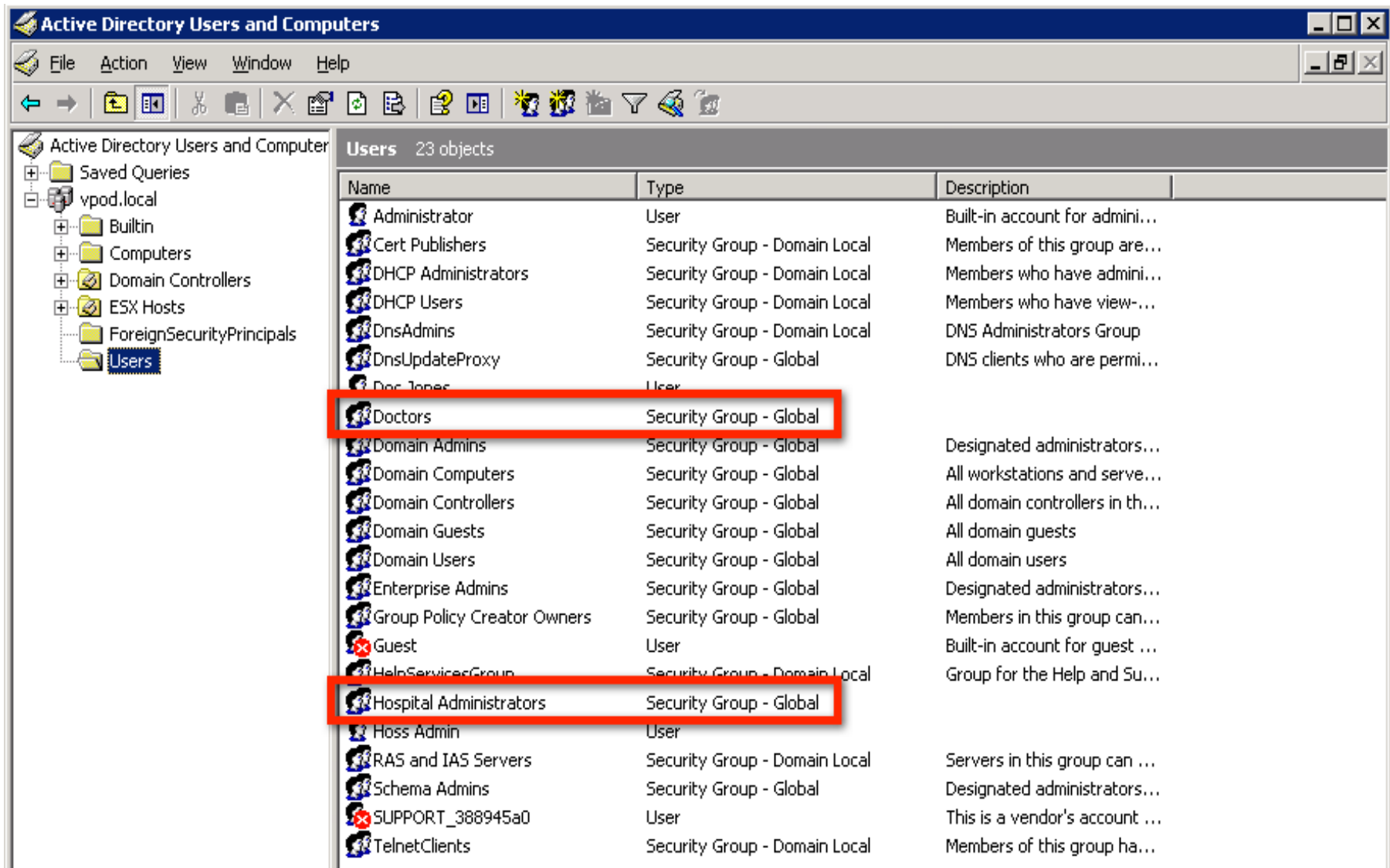
## Case study- Remote Desktop Segmentation with View

---

**We are going to have three sets of virtual desktops for different types of hospital users:**

- Doctor Desktops- have remote desktops with patient information and PII sensitive information
- Hospital Administrator Desktops- remote desktop with restricted access for administration purposes only
- Web Browsing Desktops- General hospital terminals for web browsing with no patient-sensitive data

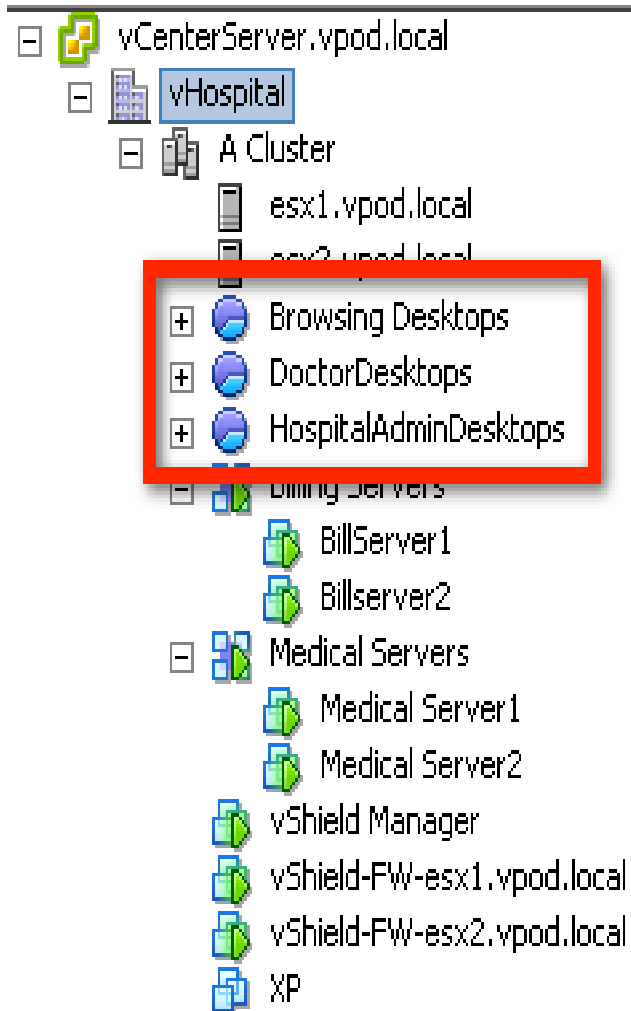
# AD groups are simply “Doctors” and “Hospital Administrators”



The screenshot shows the Active Directory Users and Computers console. The left pane shows the tree structure with 'Users' selected under 'ypod.local'. The right pane displays a list of 23 objects in a table format. Two entries are highlighted with red boxes: 'Doctors' and 'Hospital Administrators'.

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group - Domain Local	Members of this group are...
DHCP Administrators	Security Group - Domain Local	Members who have admini...
DHCP Users	Security Group - Domain Local	Members who have view-...
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permi...
Doc Jones	User	
<b>Doctors</b>	<b>Security Group - Global</b>	
Domain Admins	Security Group - Global	Designated administrators...
Domain Computers	Security Group - Global	All workstations and serve...
Domain Controllers	Security Group - Global	All domain controllers in th...
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Global	Designated administrators...
Group Policy Creator Owners	Security Group - Global	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group - Domain Local	Group for the Help and Su...
<b>Hospital Administrators</b>	<b>Security Group - Global</b>	
Hoss Admin	User	
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can ...
Schema Admins	Security Group - Global	Designated administrators...
SUPPORT_388945a0	User	This is a vendor's account ...
TelnetClients	Security Group - Domain Local	Members of this group ha...

# vCenter resource pools for virtual desktops



- The next step happens in vCenter where we need to create some resource pools for the housing of our different desktop pools.
- These will be necessary for our vShield App rule creation later.
- We need to create three resource pools for our different virtual desktops:
  - “Browsing Desktops”
  - “DoctorDesktops”
  - “HospitalAdminDesktops”

# View Manager Desktop pools creation

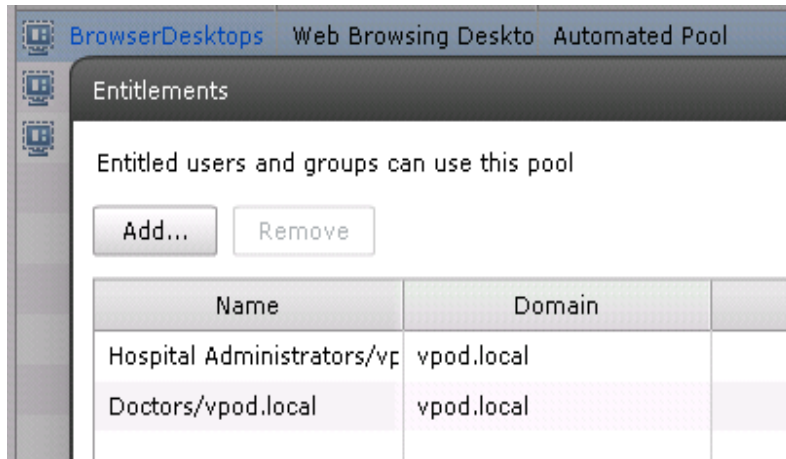
The screenshot displays the VMware View Administrator interface. The top navigation bar includes the VMware logo, the text 'VMware View Administrator', and links for 'About', 'Help', and 'Logout (administrator)'. Below the navigation bar, there is a status bar showing 'Updated 04/14/2011 21:14 PM' and a refresh icon. The main content area is titled 'Pools' and features a toolbar with buttons for 'Add...', 'Edit...', 'Delete...', 'Entitlements...', 'Status', 'Folder', and 'More Commands'. Below the toolbar is a search section with a 'Filter' dropdown, 'Find' and 'Clear' buttons, and a 'Folder' dropdown set to 'All'. The central part of the interface is a table listing desktop pools. The table has columns for ID, Display Name, Type, Source, User Assi..., vCenter Server, Entitled, Enabled, and Sessions. Three rows are visible, each representing a desktop pool: 'BrowserDesktops' (Web Browsing Desktop), 'DocDesktops' (Doctor Desktops), and 'HosAdminDesktops' (Hospital Admin Desktop). These three rows are highlighted with a red border. The 'Sessions' column for all three pools shows '0 Remote'. The left sidebar contains a navigation menu with options like 'Dashboard', 'Users and Groups', 'Inventory', 'Pools', 'Desktops', 'Persistent Disks', 'ThinApps', 'Monitoring', 'Policies', and 'View Configuration'. The 'Pools' option is currently selected.

ID	Display Name	Type	Source	User Assi...	vCenter Server	Entitled	Enabled	Sessions
BrowserDesktops	Web Browsing Desktop	Automated Pool	vCenter (linked clone	Floating	vcenterserver.vpod.loc	✓	✓	0 Remote
DocDesktops	Doctor Desktops	Automated Pool	vCenter (linked clone	Floating	vcenterserver.vpod.loc	✓	✓	0 Remote
HosAdminDesktops	Hospital Admin Desktop	Automated Pool	vCenter (linked clone	Floating	vcenterserver.vpod.loc	✓	✓	0 Remote

- We need to create the Desktop Pools within the View Manager.
- We will create three desktop pools to matchup with the roles we talked about earlier.



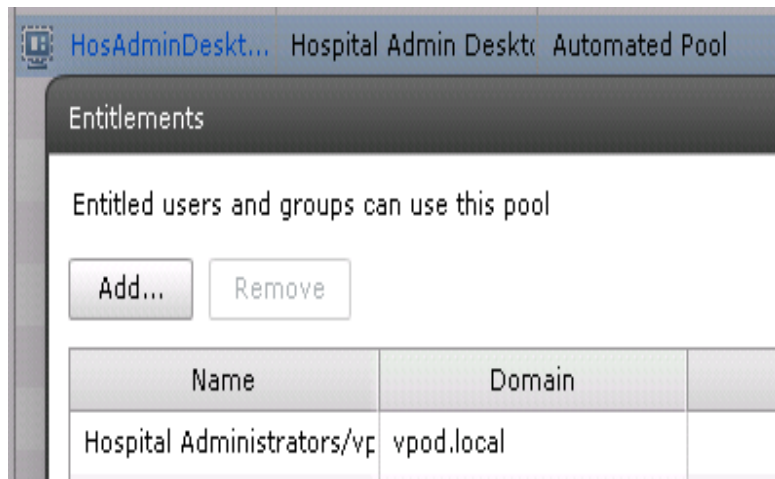
# User based entitlement to give access to specific desktops



The screenshot shows the vSphere interface for configuring entitlements for a desktop pool named "BrowserDesktops". The pool is currently in an "Automated Pool" state. The "Entitlements" section is active, displaying a list of entitled users and groups. Below the list are "Add..." and "Remove" buttons.

Name	Domain
Hospital Administrators/vp	vpod.local
Doctors/vpod.local	vpod.local

- We configure the entitlements to give the user access to their desktop specific to their roles and the browsing desktop.



The screenshot shows the vSphere interface for configuring entitlements for a desktop pool named "HosAdminDeskt...". The pool is currently in an "Automated Pool" state. The "Entitlements" section is active, displaying a list of entitled users and groups. Below the list are "Add..." and "Remove" buttons.

Name	Domain
Hospital Administrators/vp	vpod.local

# Intuitive Firewall rules with pre-populated groups

ANY	ANY	DoctorDesktops	PCoIP	4172	TCP	ALLOW
ANY	ANY	DoctorDesktops	PCoIP	4172	UDP	ALLOW
DoctorDesktops	ANY	172.16.0.80/32	JMS	4001	TCP	ALLOW
ANY	ANY	HospitalAdminDesktops	PCoIP	4172	TCP	ALLOW
ANY	ANY	HospitalAdminDesktops	PCoIP	4172	UDP	ALLOW
HospitalAdminDesktops	ANY	172.16.0.80/32	JMS	4001	TCP	ALLOW
ANY	ANY	Browsing Desktops	PCoIP	4172	TCP	ALLOW
ANY	ANY	Browsing Desktops	PCoIP	4172	UDP	ALLOW
Browsing Desktops	ANY	ANY	JMS	4001	TCP	ALLOW

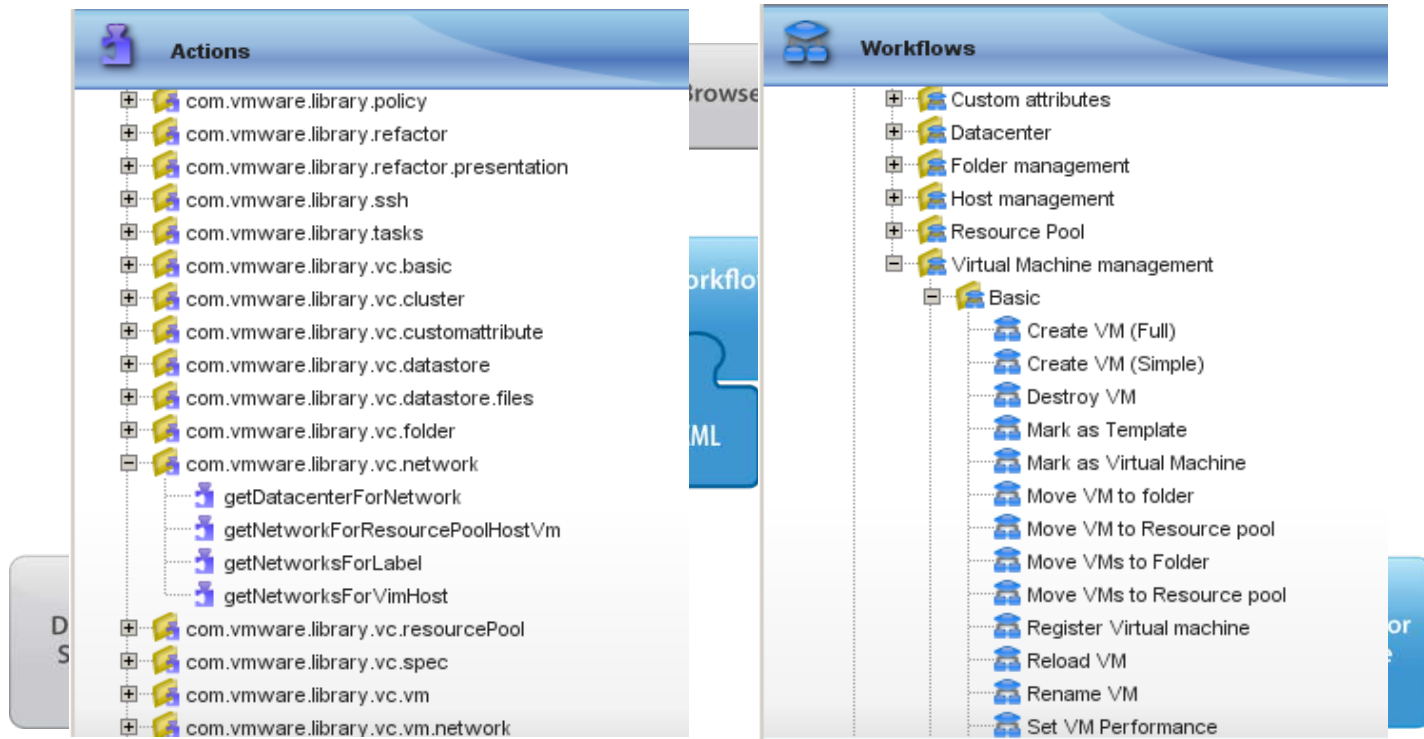
Resource Pools as  
"Doctor Desktops"  
"Hospital Administrator Desktops"  
Directly populated from the  
vCenter

PCOIP and other  
application list from the  
drop down menu

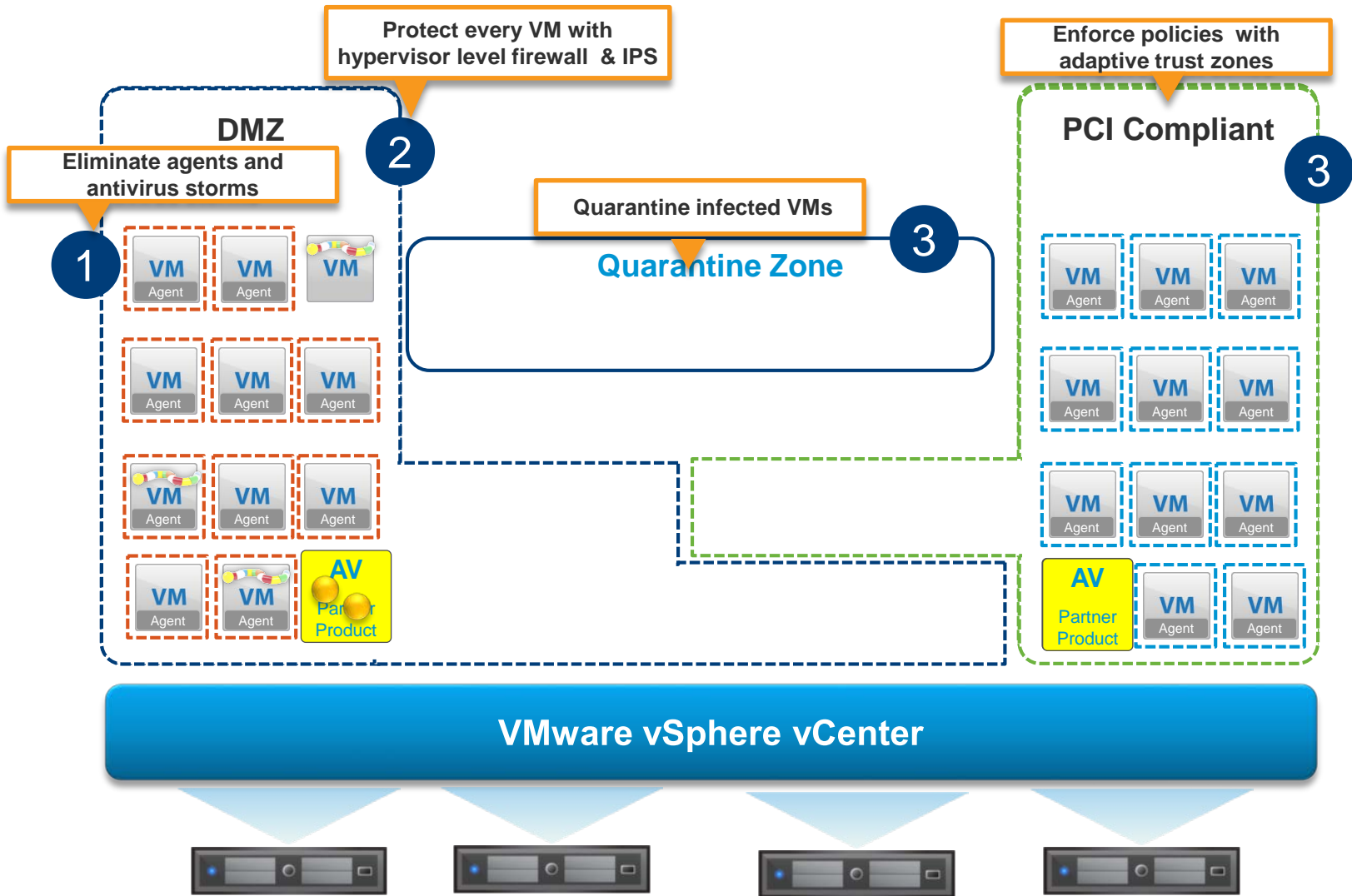
# vCO – Security Automation

# Automate Workflows with vCenter Orchestrator

- Use Orchestrator to create and execute workflows that embed access controls, auditing, notifications, etc.
- Capture and Automate Best Practices
- Leverage Out the Box Workflows and Actions for managing vSphere
- Integrate with VMware and 3rd party products



# Automating Security Processes



# Enhancing Security through Virtualization and Automation

---

- Allows Automation of Many Manual Error Prone Processes
- Cleaner and Easier Disaster Recovery/Business Continuity
- Better Forensics Capabilities
- Faster Recovery After an Attack
- Patching is Safer and More Effective
- Better Control Over Desktop Resources
- More Cost Effective Security Devices
- App Virtualization Allows de-privileging of end users
- Better Lifecycle Controls
- Security Through VM Introspection
- Automated and Continuous Compliance

**Virtualization + Automation = Better Security**

**Deployments on VMware can be More Secure than Physical**

## Where to learn more...

---

Security Specialist Team's Everything security.....

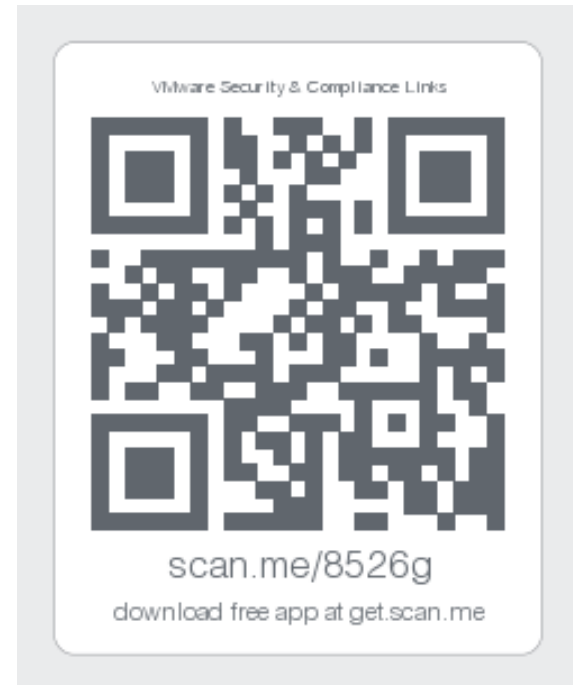
[http://portal.sliderocket.com/ATOHL/VMware-Security-Links\\_v2](http://portal.sliderocket.com/ATOHL/VMware-Security-Links_v2)

Or

<http://tinyurl.com/VMwareSecurityLinks>



Use it as a reference – visit often.....



A landscape photograph of a road stretching into the distance under a sunset sky. The road is overlaid with a vibrant, geometric pattern of triangles in shades of blue, green, and yellow. The background shows rolling hills and a field of tall grass.

# Thank you

## Question & Answer Session

vmware