



## The Future Of Datacenter Security

Jan Tiri

SE VMware

### Disclaimer

**This session may contain product features that are currently under development.**

**This session/overview of the new technology represents no commitment from VMware to deliver these features in any generally available product.**

**Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.**

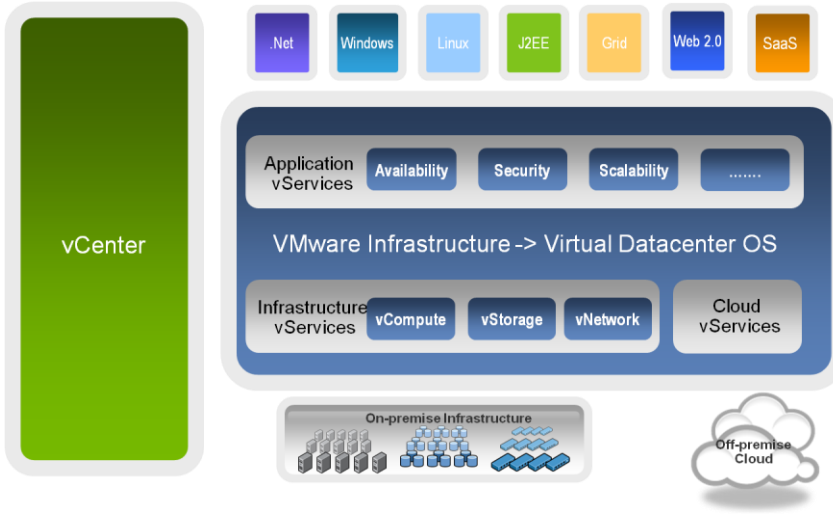
**Technical feasibility and market demand will affect final delivery.**

**Pricing and packaging for any new technologies or features discussed or presented have not been determined.**

"These features are representative of feature areas under development. Feature commitments are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind. Technical feasibility and market demand will affect final delivery."

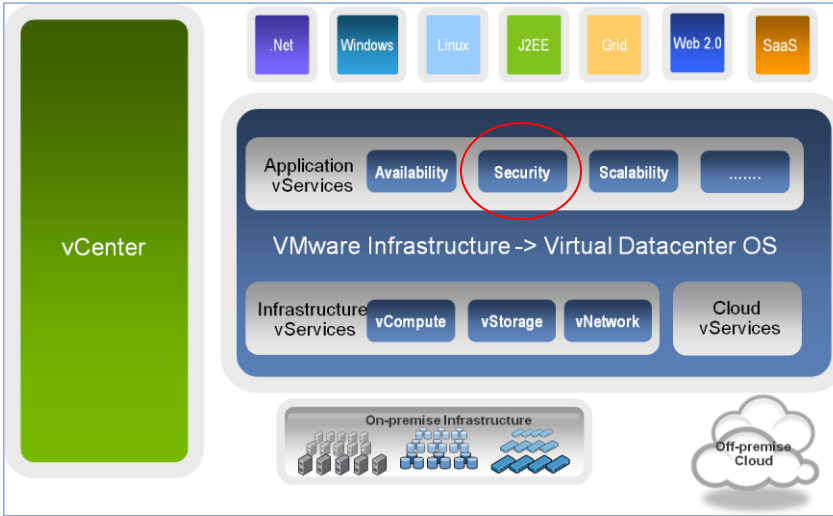


## Virtual Datacenter OS from VMware



vmware

## Where Does Security Fit In The Architecture?



vmware

## Agenda

- ← **The Impact Of Virtualization On Security Technologies**
- ← **Security Advantages of Virtualization**
- ← **New Security Architectures Through Virtualization**
- ← **Virtualization Security Futures**



## Let's Focus On The Impact Of Virtualization On Security

- > What's new?
- > Desktops That Look Like Servers
- > Insight Through Hypervisor API's
- > Appliances Go Virtual



## What's New With Virtualization?

- ← **Virtualization decouples physical resources from the OS & applications**
  - > Allows for interposition and introspection
- ← **Machines are now “freeze dried” files**
  - > Allows for online and offline operations
- ← **HW to SW machine transformation**
  - > Enables deployment flexibility and increased density
- ← **Machine mobility within the datacenter**
  - > Requires deeper integration of security products



7

## Virtualization – Any Free Lunch?

- ← **“No free lunch” rule applies to virtualization**

The Good	The other side
Easy machine creation	“VM sprawl”
Mobility	Breaks static security
Hypervisor	New layer to be secured



8

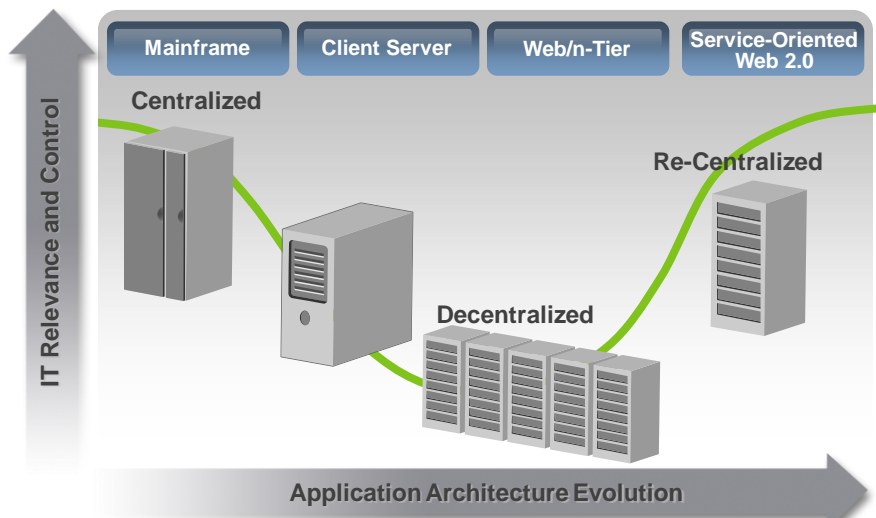
## What's The Impact

- ← **Virtualization decouples applications and OS from underlying HW**
- ← **Core hypervisor platform is increasingly “stateless” – intelligence is moved up to the next layer**
- ← **Intelligent infrastructure dynamically manages machines**
  - > Machines go online/offline
  - > Machines move in the cluster
  - > Machines are cloned and multiply
- ← **DRS & Power Management**
  - > Automatic load balancing across compute resources
- ← **Dynamic capacity for security solutions**
  - > Relieves pressure to overprovision up-front capacity



9

## Virtualization Drives Re-Centralization Of Systems



10

## Offline Access

Clients

Virtual Desktop  
Manager

VMware  
Infrastructure

- End-users can check in and out of their Virtual Desktops
- Administrators can extend security policies to the local PC
- Provides full user experience



VirtualCenter

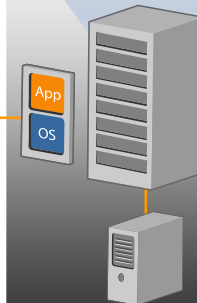


11

## Power Management & Offline VM's

Clients

VMware  
Infrastructure



VirtualCenter

Offline Ops  
Patch  
Malware Scan  
Configuration  
Backup



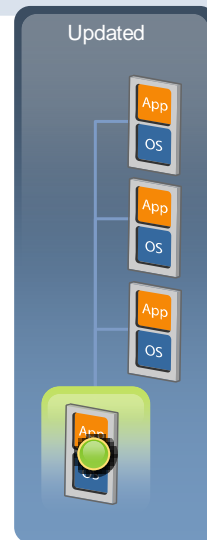
12

## “Linked Clone” Technology

← **Currently in Workstation/View products**

← **Benefits**

- > Storage cost savings
- > Quick Provisioning
- > Simplified updating



13

## What's The Impact

← **Ability to apply server-strength security to the desktop**

← **Better updates, patching, compliance, firewalling, protection, signature updates ...**

← **Security can be applied to machines through file operations**

← **Many “online” operations can be completed “offline”**

- Patching, compliance checks, configuration, etc.



14

## Insight Through Hypervisor API's

### Security solutions are facing a growing problem

- > Protection engines do not get complete visibility in and below the OS
- > Protection engines are running in the same context as the malware they are protecting against
- > Even those that are in a safe context, can't see other contexts (e.g. network protection has no host visibility).

### Virtualization can provide the needed visibility

- > Better Context – Provide protection from outside the OS, from a trusted context
- > New Capabilities – view all interactions and contexts
  - CPU
  - Memory
  - Network
  - Storage



15

## VMsafe™ Enables Application Protection

- > Virtual appliances from partners protect VMs by inspection of virtual components
- > Application-specific policies
- > Complete integration with VMotion, Storage VMotion, HA
- > Integrated security solutions within the virtual infrastructure

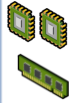


16

## VMsafe™ APIs

### API's for all virtual hardware components of the VM

#### CPU/Memory Inspection



- Inspection of specific memory pages being used by the VM or its applications
- Knowledge of the CPU state
- Policy enforcement through resource allocation of CPU and memory pages

#### Networking



- View all IO traffic on the host
- Ability to intercept, view, modify and replicate IO traffic from any one VM or all VM's on a single host.
- Capability to provide inline or passive protection

#### Storage

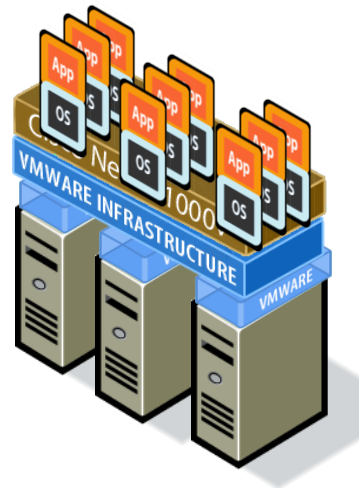


- Ability to mount and read virtual disks (VMDK)
- Inspect IO read/writes to the storage devices
- Transparent to the device and inline of the ESX Storage stack



## Another member of the Ecosystem

VMware and Cisco are collaborating to enhance workload mobility and simpler management with virtualization-aware networks



## What's The Impact

- ← **Gives security products the ability to**
  - > Introspect machines
  - > Interpose on machine activities
  - > Operate in an isolated context



18

## Virtual Appliances

- ▶ **A safer way to distribute and run applications**
- > “Just-Enough OS” (JeOS): Thin and hardened
  - Does not need to support special hardware
  - Only needs to support the specific functions needed by the service,
- > Less infrastructure needed for development
  - No dedicated hardware --- much more extensive QA possible
  - Result: a more thoroughly vetted product.
- > VMware Certified Virtual Appliances
  - Securely designed
  - Genuine
  - Guaranteed to be maintained



19

## Virtual Appliances

- ← **HW appliances already moving into VMs**
  - > Load-balancers, IDS, Firewalls, Backup, Dedupe, ...
  - > Virtualization helps manageability and capability
- ← **Partners plug into common service interface**
  - > Today's Examples: SRM, VCB, VMSafe



21

## What's The Impact

- ← **Overcomes the limitations of physical topology and architecture**
  - > Deploy anywhere
- ← **Increases the density and granularity of security within the datacenter**
  - > Leverage the same benefits of not having a hardware appliance
  - > Deploy as many appliances as necessary



22

## Security Advantages of Virtualization

### ▶ Ease of maintenance

- > Test patches on multiple configurations in contained environment before rolling them out
- > Use snapshots to save the known good state of a virtual machine before trying out something risky
- > Production VM can be cloned and then modified off-line while the original one still runs.
  - Updated VMs can be brought up in parallel with the previous version
  - both can be kept running as long as necessary to validate the new configuration

### ▶ Protect against attack of misconfiguration or attack

- > Ease of recovery
  - restoring it from last known good backup
  - patch in isolation before putting online
- > Ability to do forensics
  - Bring up hacked VM in isolation



23

## Taking Advantage Of The VMware Virtualization Platform

### ← VMware Virtualization offers rich platform and functionality

- > Waiting to be utilized to produce new products and solve old problems in new ways

### ← Expand beyond thinking of simply translating physical into virtual – “think different”

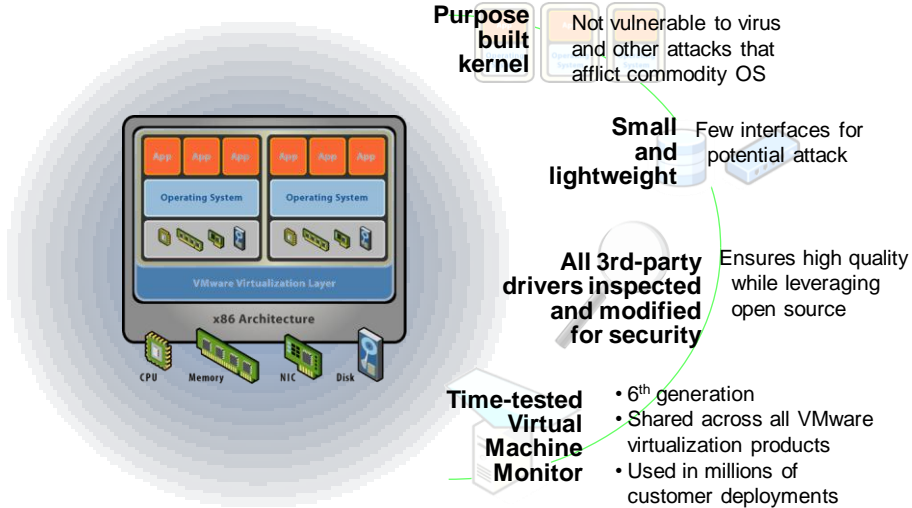
### ← Examples

- > Isolation by design
- > vMotion
- > Update management
- > Flexible security capacity



24

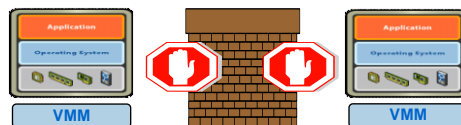
## Built Secure from the ground up



vmware

25

## Virtual Machine Isolation



### ► Design Highlights

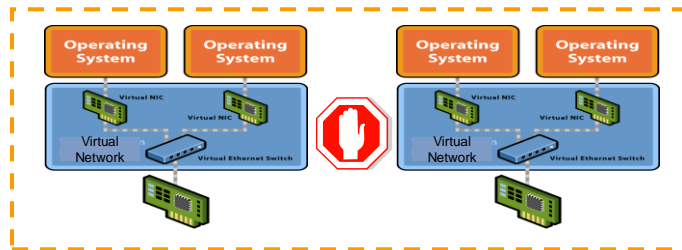
- > **VMs have limited access to CPU**
  - Most instructions run natively for performance
  - Privileged instructions are trapped and translated
- > **Memory pages zeroed out before being used by a VM**
  - Shared memory pages marked as copy-on-write --- no possibility of information leakage
- > **VMs have no direct access to I/O hardware devices**
  - only have visibility to virtual I/O devices

vmware

## Virtual Network Isolation

### ← Design Highlights

- > No code exists to link virtual switches
- > Virtual switches provide protection by design against attack:
  - MAC flooding, 802.1q and ISL tagging attacks, Double-encapsulation attacks, Multicast brute-force attacks, Spanning-tree attacks, Random frame attacks
  - Can restrict malicious network behavior:
    - MAC address change, impersonation
  - Such protection not possible with physical switches



## Containment: constrain guest behavior

### ▶ Prevent malicious intent

- > Privileged instructions within a VM are “de-privileged” and run within an isolated virtual memory space
- > Binary translation makes no assumptions about the code running in VM
  - no special OS modifications are necessary for running on VMware
- > Few places exist where code running in VM is processed directly
  - buffer overflow checking is done in these cases

## Containment: constrain guest behavior

### ► Prevent resource Denial-of-Service

- > Load balancing of CPU according to sharing policy
- > Storage I/O limited according to sharing policy.
- > Traffic-shaping available for virtual networks

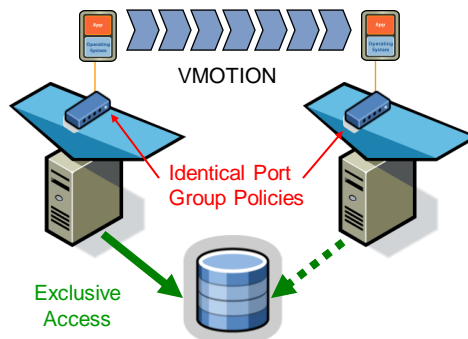


28

## Secure Management

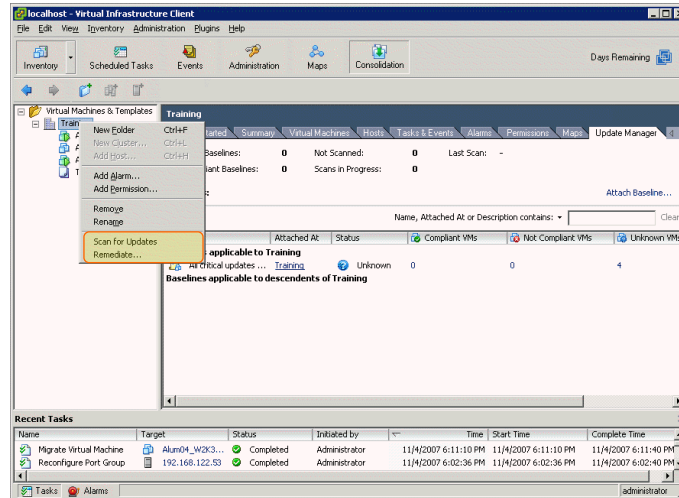
### ► Distributed Virtualization

- > vMotion Preserves Security: policies defined at the port group (network) level carries forth when a VM moves from one host to another
- > VMFS enforces single ownership of virtual disks at any one time

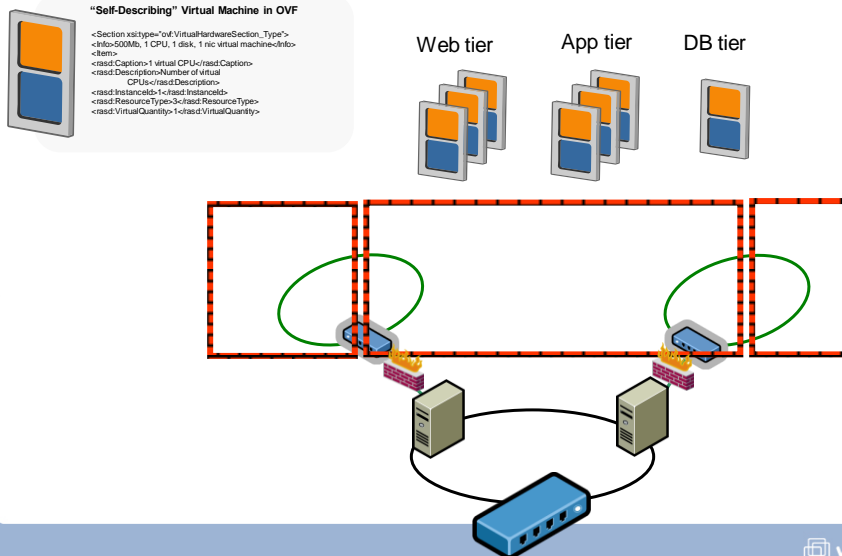


29

## Scanning and Remediating



## Auto-Configuration Of App Security

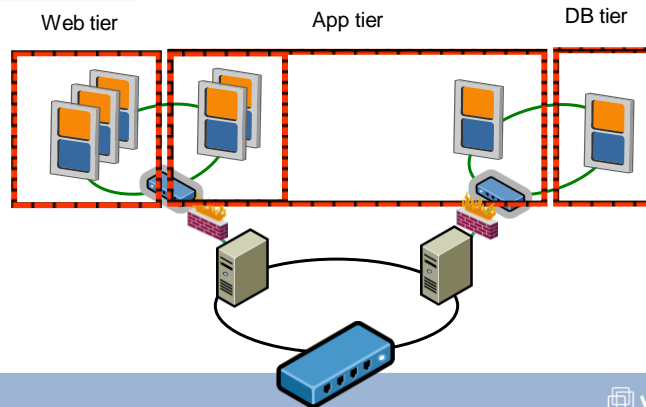


## Dynamic Capacity, Mobility Awareness



### "Self-Describing" Virtual Machine in OVF

```
<Section xsi:type="ovf:VirtualHardwareSection_Type">
  <Info>500MB, 1 CPU, 1 disk, 1 nic virtual machine</Info>
  <Item>
    <rasd:Caption>1 virtual CPU</rasd:Caption>
    <rasd:Description>Number of virtual
      CPU</rasd:Description>
    <rasd:InstanceId>1</rasd:InstanceId>
    <rasd:ResourceType>3</rasd:ResourceType>
    <rasd:VirtualQuantity>1</rasd:VirtualQuantity>
  </Item>
</Section>
```



93

## VMware's Security Response Policy

- ◀ **VMware has a strong security response policy:**
  - > Monitoring of public repositories such as CERT
  - > Acknowledgement and initial analysis: Posting of KB article with mitigation or workaround
  - > Fix and issuance of a patch if needed
  - > Customer Notification: Customers with SNS (Subscription and Support) notified of patch via e-mail
  - > Code is audited regularly by external resources and resulting recommendations are implemented.
- ◀ **VMware's security response policy can be found at:**
  - > [http://www.vmware.com/support/policies/security\\_response.html](http://www.vmware.com/support/policies/security_response.html)
  - > The VMTN Security Center: <http://www.vmware.com/security>



94

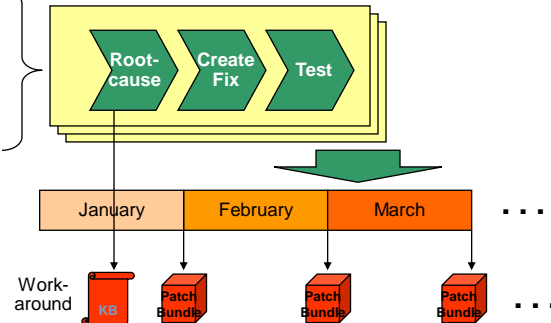
## Patch Release Process

### ← Patches are released in a predictable monthly schedule

- ▶ Each patch is individually installable and released through the monthly patch release train
- ▶ High impact patches may be released out of cycle
- ▶ For time critical issues, usually a KB article describing the issue and workaround is sent before the patch release

#### Security issues and bugs reported from:

- Customers
- Internal Testing
- Security Bulletins
- Security Auditors
- Public forums
- Partners



35

## VMware Security Validation Efforts

### ▶ Common Criteria Certification EAL (Evaluation Assurance Level)

- > CC EAL 2 certification (completed for ESX 2.5)
- > CC EAL 4+ certification (completed for ESX 3.0)



National Information Assurance Partnership  
Common Criteria Evaluation and Validation Scheme

27 March 2006  
CCEVS-0019-06



36

## VMware Security Validation Efforts

### ▶ 3<sup>rd</sup> party inspection

- > Penetration testing by third-party (completed for ESX 3.0 and VC 2.0 prior to release)
- > Threat modeling and source code audit by third-party (completed for ESX 3.0 and VC 2.0)



37

## New Security Architectures Through Virtualization

### Use the Principles of Information Security

- > Hardening and Lockdown
- > Defense in Depth
- > Authorization, Authentication, and Accounting
- > Separation of Duties and Least Privileges
- > Administrative Controls



38

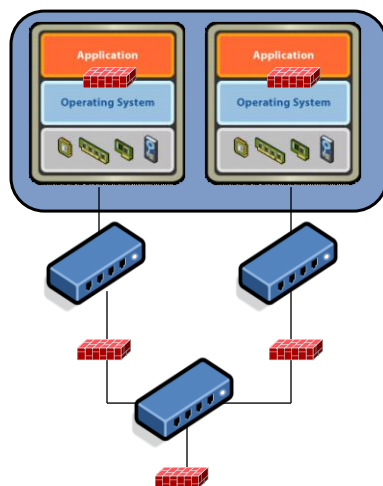
## Proper IT Processes for Virtualized Environment

- ← **Hardening and operations guidelines**
  - > Isolate all management interfaces
  - > Continue applying Guest OS security
  - > Enable & utilize only those features needed for your environment
  - > Enforce separation of duties & strictly limit administrative capabilities
  
- ← **Detailed Prescriptive Guidance (VMware & 3<sup>rd</sup>-party)**
  - > VMware Infrastructure 3 Security Hardening (<http://www.vmware.com/vmtn/resources/726>)
  - > Managing VMware VirtualCenter Roles and Permissions (<http://www.vmware.com/resources/techresources/826>)
  - > STIG (Secure Technology Implementation Guide) draft (<http://iase.disa.mil/stigs/draft-stigs/index.html>)
  - > CIS (Center for Internet Security) Benchmark in-progress (<http://www.cisecurity.org/development.html>)
  - > ... and more



39

## Securing Virtual Machines



*Provide Same Protection as for Physical Servers*

- ← **Host**
  - > Anti-Virus
  - > Patch Management
- ← **Network**
  - > Intrusion Detection/Prevention (IDS/IPS)
  - > Firewalls



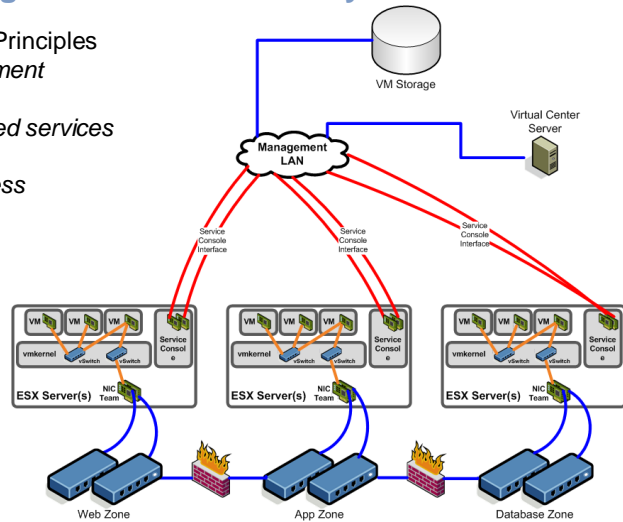
40

40

## Secure Design for Virtualization Layer

### Fundamental Design Principles

- *Isolate all management networks*
- *Disable all unneeded services*
- *Tightly regulate all administrative access*



## Concern: Virtualizing the DMZ / Mixing Trust Zones

### Three Primary Configurations:

- Physical Separation of Trust Zones
- Virtual Separation of Trust Zone with Physical Security Devices
- Fully collapsing all servers and security devices into a virtual infrastructure

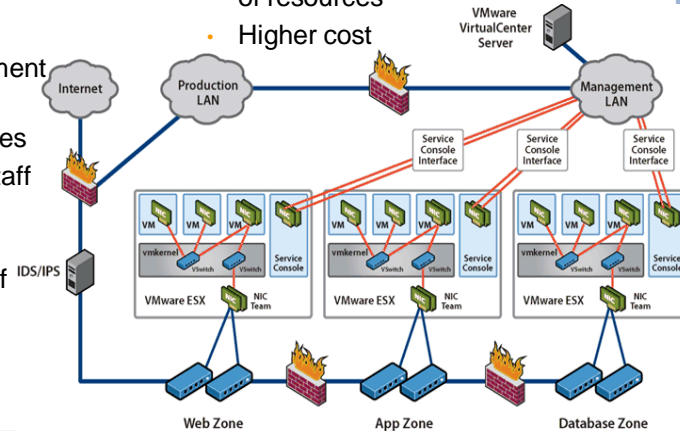
## Physical Separation of Trust Zones

### Advantages

- Simpler, less complex configuration
- Less change to physical environment
- Little change to separation of duties
- Less change in staff knowledge requirements
- Smaller chance of misconfiguration

### Disadvantages

- Lower consolidation and utilization of resources
- Higher cost



vmware

43

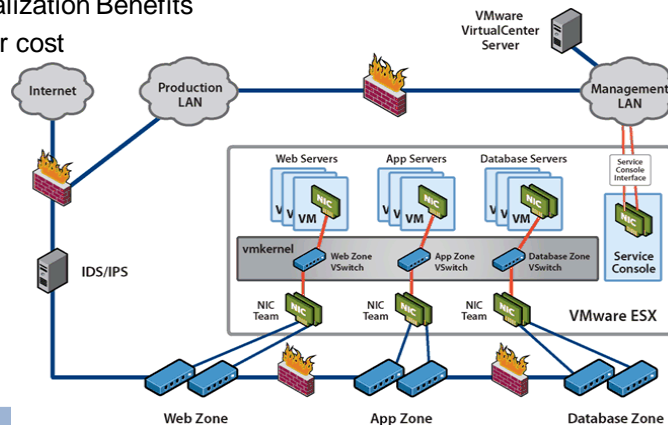
## Virtual Separation of Trust Zones with Physical Devices

### Advantages

- Better utilization of resources
- Take Full Advantage of Virtualization Benefits
- Lower cost

### Disadvantages (can be mitigated)

- More complexity
- Greater chance of misconfiguration



vmware

44

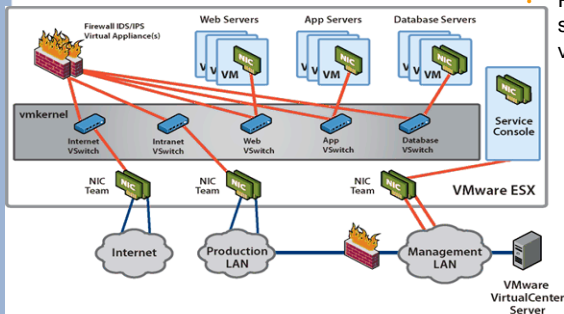
## Fully Collapsed Trust Zones Including Security Devices

### Advantages

- Full utilization of resources, replacing physical security devices with virtual
- Lowest-cost option
- Management of entire DMZ and network from a single management workstation

### Disadvantages (can be mitigated)

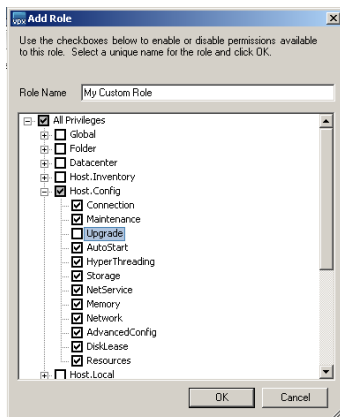
- Greatest complexity, which in turn creates highest chance of misconfiguration
- Requirement for explicit configuration to define separation of duties to help mitigate risk of misconfiguration; also requires regular audits of configurations
- Potential loss of certain functionality, such as VMotion (Being mitigated by vendors and VMsafe)



vmware

45

## Secure Management

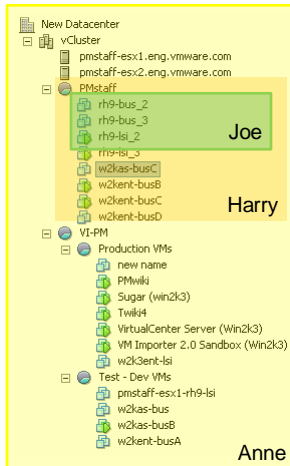


### VirtualCenter: primary management tool

- > Encrypted communication
- > Integration with global security framework, e.g.
  - Authentication via Active Directory
  - Detailed auditing
- > Extensive roles system for fine-grained separation-of-duties
- > Operational Best Practices for maximum security, e.g.
  - Dedicated management network
  - Lock-down of Administrator access

vmware

## Enforce Strong Access Controls



Security Principle	Implementation in VI
Least Privileges	Roles with only required privileges
Separation of Duties	Roles applied only to required objects

Administrator

Operator

User



47

47

## Virtualization Security Futures

### ← Current network security issues disappear

- > Intra-virtual network communication will now be visible with VMsafe-Net API's
- > Ability to firewall and protect individual machines, even between machines on a single switch
- > VMotion awareness

### ← Stronger VM protection available through VMsafe Host API's

- > Guarantee for security products to run before malware

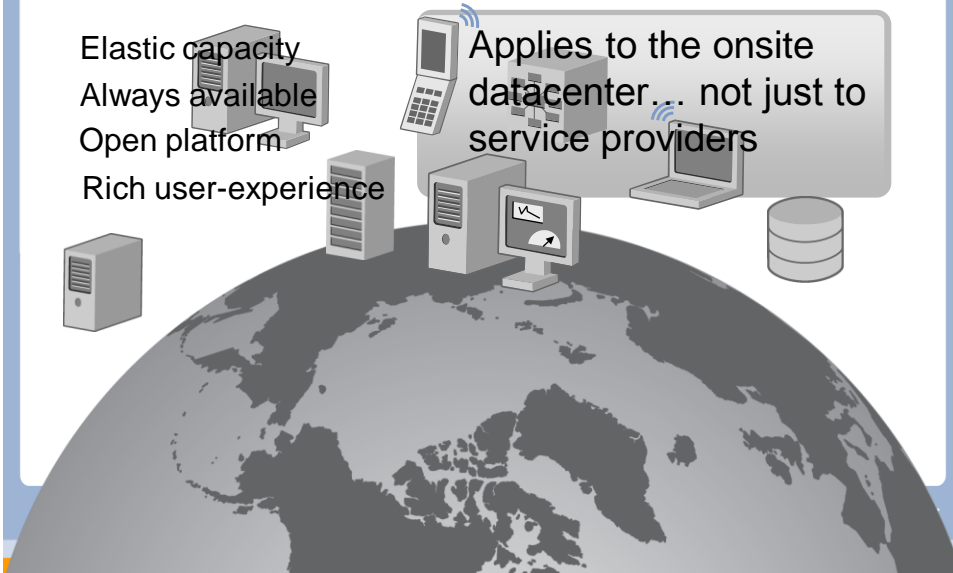


48

## Future - Cloud Computing

Elastic capacity  
Always available  
Open platform  
Rich user-experience

Applies to the onsite  
datacenter... not just to  
service providers



## Key Cloud Computing Security Issues

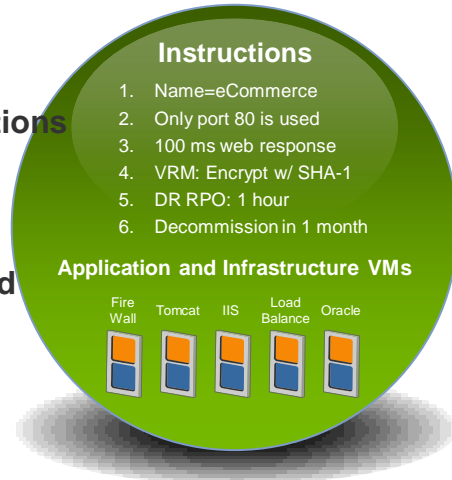
- ← **Cloud computing security issues are going to be vastly different**
- > Data protection
- > Transport concerns and considerations
- > Identity & Access Control
- > Policy storage, transportation and enforcement

## Future - Impact Of OVF (Open Virtualization Format)

← Pushed by VMware

← OVF includes instructions for the infrastructure

← Contract is maintained across VM deployments and VMotions



51

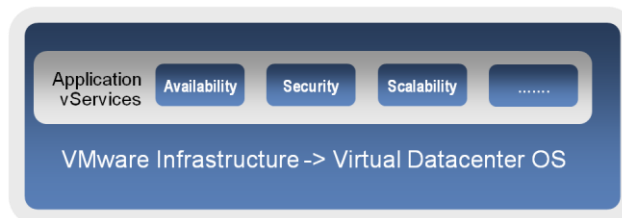
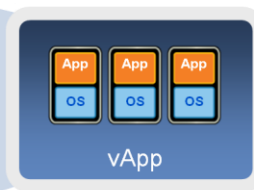
## vApp – New Model for Describing and Deploying Applications

Availability = 99.99%

Security = High

Performance = 500 msec

SLA Definitions 



52

## Summary: Pulling it All Together

- ▶ Virtual can be more secure than physical computing
- ▶ Need to have a broader perspective about virtualization – utilize everything that's different
- ▶ The “Next Generation” of datacenter is coming – and so are the security products



## Q&A