VMware Security Briefing

Matt Northam

Systems Engineer – Security Specialist

Northern EMEA

VMware Security Strategy

Core Platform Security

- New platform hardening features further enhance robust security capabilities
- Thin-hypervisor strategy
- Memory Protection
- Kernel Module Protections

Operationalize Security

- Integrate VMware products into existing operational policies in the enterprise

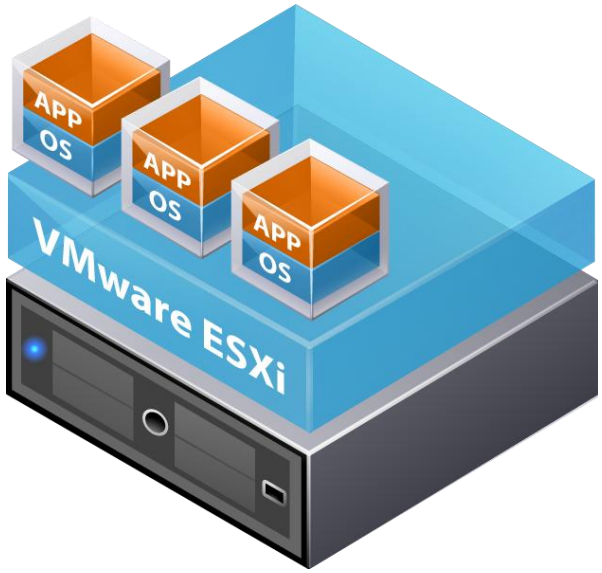
Security Virtual Appliances

- Enable broad-based security for every VM in the environment
- “Democratize” security

Better Than Physical

- Self-describing, Self-configuring security
- Impact security by taking advantage of unique VMware technologies
- Focus on products and operations

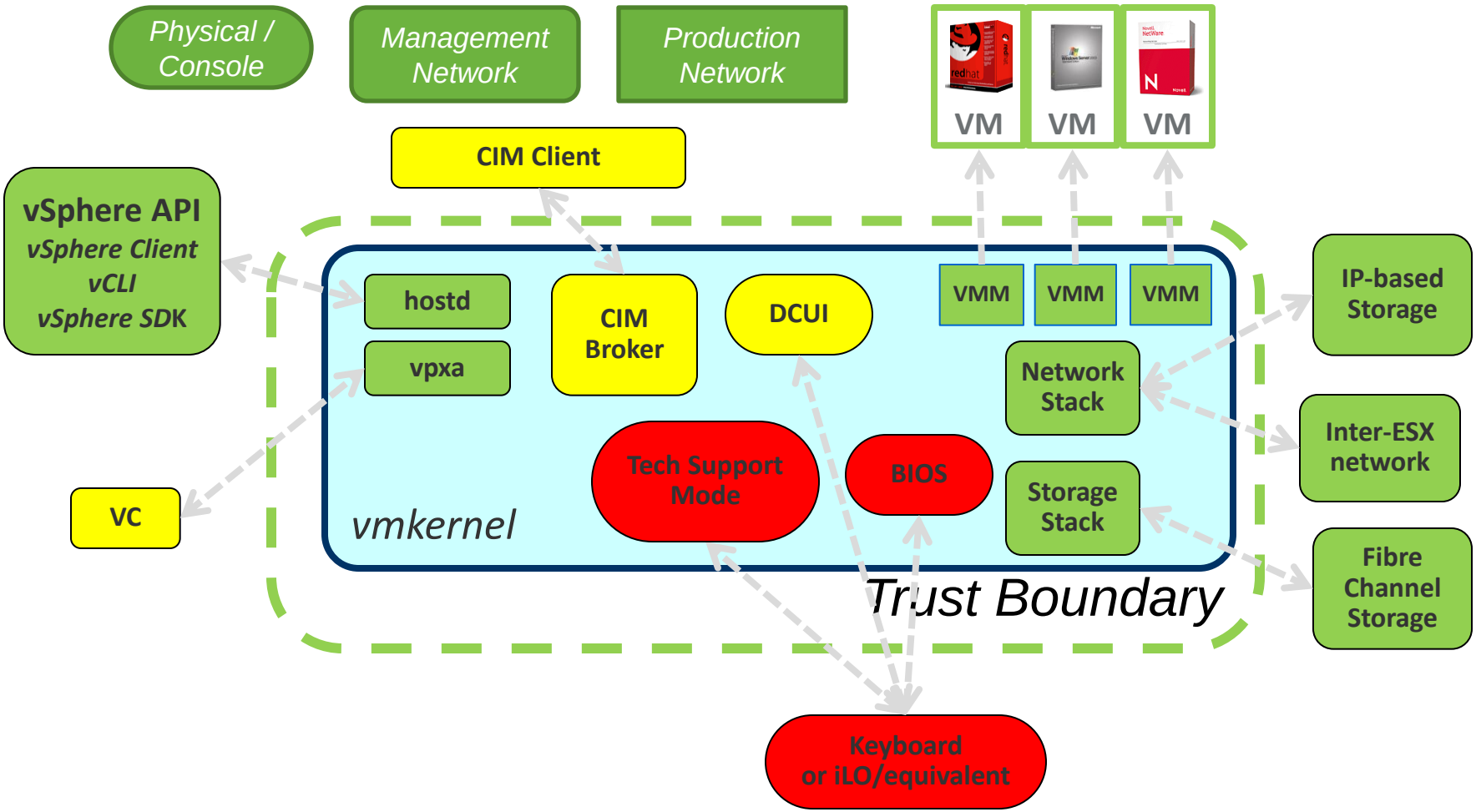
Secure Implementation



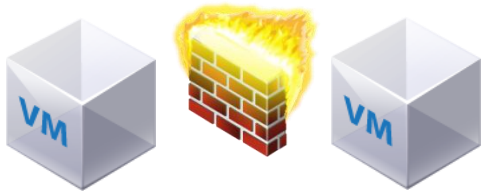
VMware ESXi

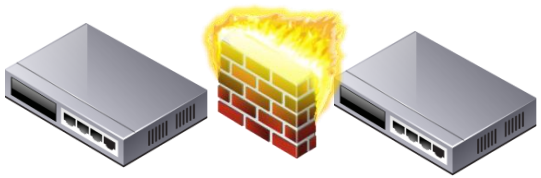
- Compact 100MB footprint
  - Fewer patches
  - Smaller attack surface
- Absence of general-purpose management OS
  - No arbitrary code running on server
  - Not susceptible to common threats

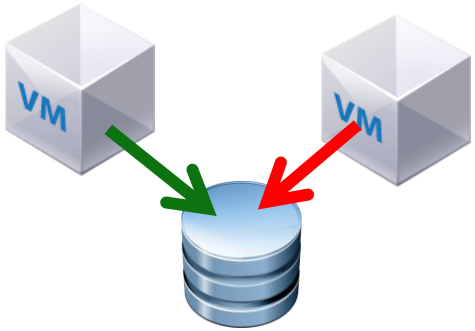
ESXi Security Model



Isolation by Design







CPU & Memory

- VMs have limited access to CPU
- Memory isolation enforced by Hardware TLB
- Memory pages zeroed out before being used by a VM

Virtual Network

- No code exists to link virtual switches
- Virtual switches immune to learning and bridging attacks

Virtual Storage

- Virtual Machines only see virtual SCSI devices, not actual storage
- Exclusive virtual machine access to virtual disks enforced by VMFS using SCSI file locks

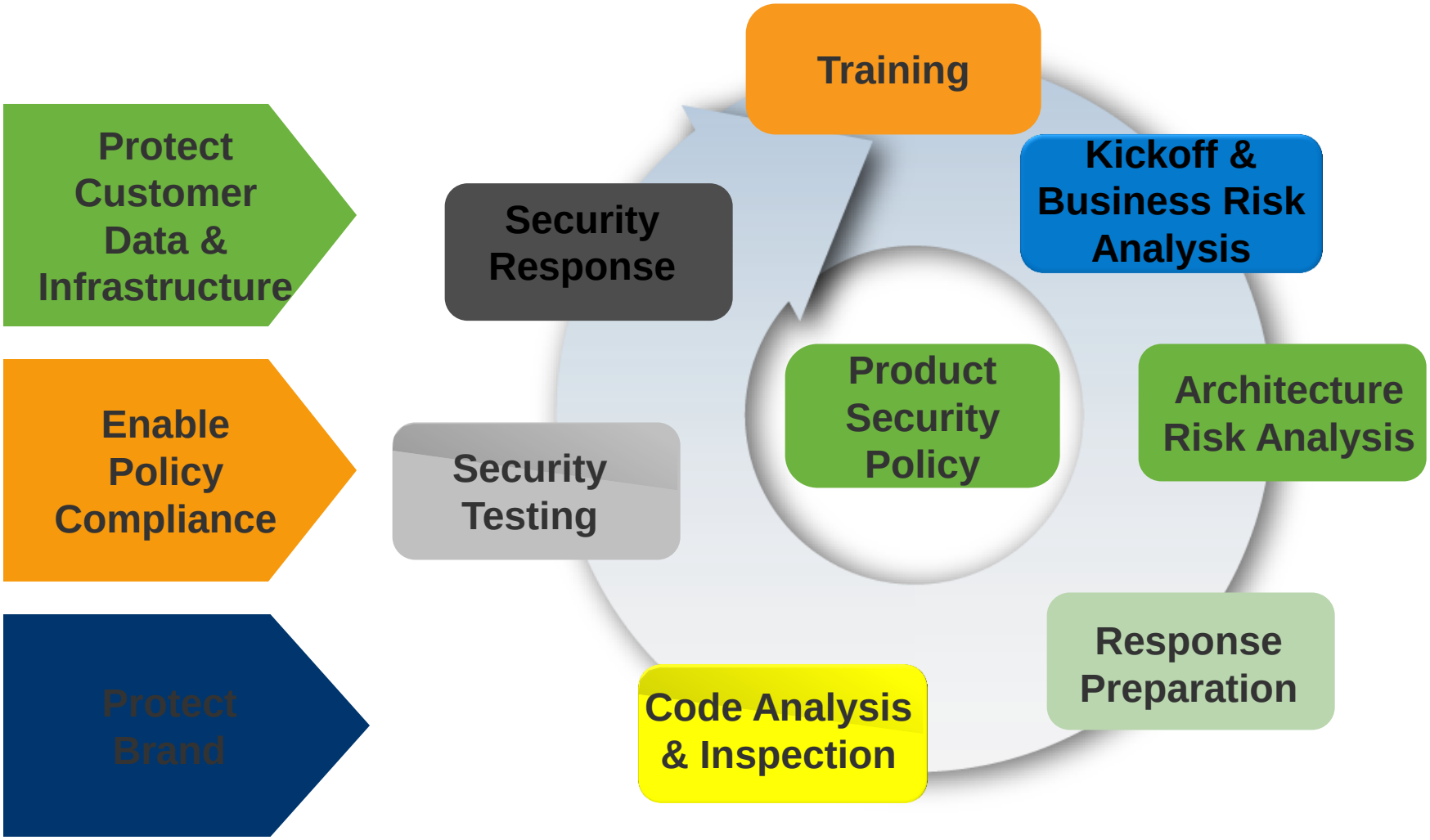
Security Design of the VMware Infrastructure 3 Architecture
http://www.vmware.com/resources/techresources/727

Secure Implementation

Platform Hardening

- Integrity in Memory Protection
  - NX/XD – Marks writable areas of memory as non-executable
  - ASLR – Randomizes where core kernel modules load into memory
- Kernel Module Integrity
  - Digital signing – ensures the integrity and authenticity of modules, drivers and applications as they are loaded by the VMkernel.
  - Module signing – allows ESX to identify the providers of modules, drivers, or applications and whether they are VMware-certified.

VMware Secure Development Lifecycle Process

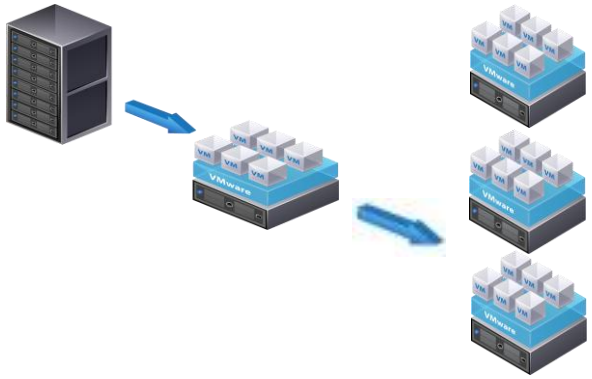


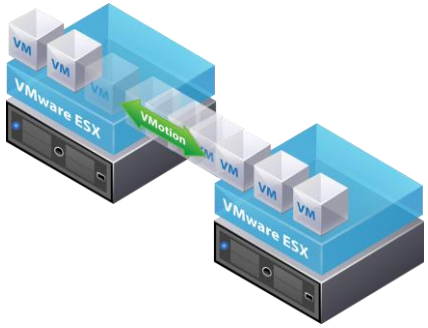
VMworld 2009 Session TA2543:
VMware's Secure Software Development Lifecycle

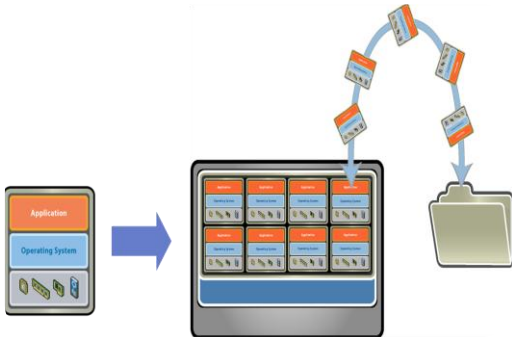
Independently validated

- Common Criteria Certification EAL (Evaluation Assurance Level)
  - CC EAL 4+ certification
    - Highest recognized level
    - Achieved for ESX 3.0; in process for ESX 3.5
    - Current Submission for vSphere
- DISA STIG for ESX
  - Approval for use in DoD information systems
- NSA Central Security Service
  - guidance for both datacenter and desktop scenarios

How Virtualization Affects Datacenter Security







Faster deployment of servers

- ↑ IT responsiveness
- ↓ Lack of adequate planning
- ↓ Incomplete knowledge of current state of infrastructure
- ↓ Poorly Defined Procedures
- ↓ Inconsistent Configurations

VM Mobility

- ↑ Improved Service Levels
- ↓ Identity divorced from physical location

VM Encapsulation

- ↑ Ease of business continuity
- ↑ Consistency of deployment
- ↑ Hardware Independence
- ↓ Outdated offline systems
- ↓ Unauthorized Copy

Biggest Security Risk: Misconfiguration

Neil MacDonald – "How To Securely Implement Virtualization"

Gartner

"Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement"

What *not* to worry about

Hypervisor Rootkits

- Examples: Blue Pill, SubVirt, etc.
- These are ALL theoretical, highly complex attacks
- Widely recognized by security community as being only of academic interest

Irrelevant Architectures

- Example: numerous reports claiming guest escape
- Apply only to hosted architecture (e.g. Workstation), not bare-metal (i.e. ESX)
- Hosted architecture deliberately include numerous channels for exchanging information between guest and host.

Contrived Scenarios

- Example: VMotion intercept
- Involved exploits where
  - Best practices around hardening, lockdown, design, for virtualization etc, not followed, or
  - Poor general IT infrastructure security is assumed

Security Advantages of Virtualization

- 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

Security of VMware Infrastructure

KEYS TO A SECURE VIRTUALIZED DEPLOYMENT

How do we secure our Virtual Infrastructure?

Use the Principles of Information Security

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

For virtualization this means:

- Secure the Guests
- Harden the Virtualization layer
- Setup Access Controls
- Leverage Virtualization Specific Administrative Controls

Leveraging Virtualization To Solve Security Problems

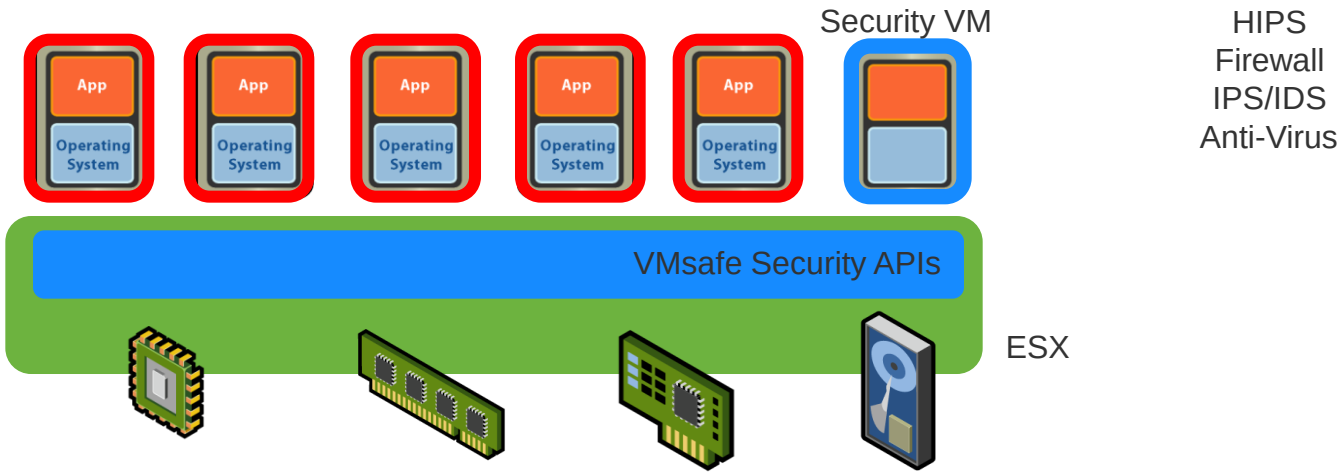
Security solutions are facing a growing problem

- 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

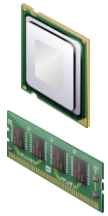
VMsafe™ APIs



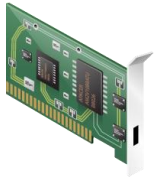
- New security solutions can be developed and integrated into VMware virtual infrastructure
- Protect the VM by inspection of virtual components (CPU, Memory, Network and Storage)
- Complete integration and awareness of VMotion, Storage VMotion, HA, etc.
- Provides an unprecedented level of security for the application and the data inside the VM

VMsafe™ APIs

API's for all virtual hardware components of the VM



- CPU/Memory Inspections
  - Inspection of specific memory pages being used by the VM or it 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

VMware Security Strategy

Core Platform Security

- New platform hardening features further enhance robust security capabilities
- Thin-hypervisor strategy
- Memory Protection
- Kernel Module Protections

Operationalize Security

- Integrate VMware products into existing operational policies in the enterprise

Security Virtual Appliances

- Enable broad-based security for every VM in the environment
- “Democratize” security

Better Than Physical

- Self-describing, Self-configuring security
- Impact security by taking advantage of unique VMware technologies
- Focus on products and operations