Sicherheit in virtuellen Umgebungen

Christian Liebner, Solution Specialist Systems Engineer, VMware
## 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
# 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
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.
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
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
How Virtualization Affects Datacenter Security

Abstraction and Consolidation

- ↑ Capital and Operational Cost Savings
- ↓ New infrastructure layer to be secured
- ↓ Greater impact of attack or misconfiguration

Collapse of switches and servers into one device

- ↑ Flexibility
- ↑ Cost-savings
- ↓ Lack of virtual network visibility
- ↓ No separation-by-default of administration
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
“Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement”
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
Securing Virtual Machines

Provide Same Protection as for Physical Servers

Host
- Anti-Virus
- Patch Management

Network
- Intrusion Detection/Prevention (IDS/IPS)
- Firewalls
Secure Design for Virtualization Layer

Fundamental Design Principles

- *Isolate all management networks*
- *Disable all unneeded services*
- *Tightly regulate all administrative access*
Host profiles reduce setup time and allow you to manage configuration consistency and correctness.
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

Anne
Harry
Joe

Administrator
Operator
User

New Datacenter
- vCluster
  - pmsstaff-esx1.eng.vmware.com
  - pmsstaff-esx2.eng.vmware.com
- PMstaff
  - rh9-bus_2
  - rh9-bus_3
  - rh9-lsi_2
  - rh9-lsi_3
  - w2kas-busc
  - w2kent-busB
  - w2kent-busc
  - w2kent-busD
- VI-PM
  - Production VMs
    - new name
    - PMwiki
    - Sugar (win2k3)
    - Twiki4
    - VirtualCenter Server (Win2k3)
    - VM Importer 2.0 Sandbox (Win2k3)
    - w2k3ent-lsi
  - Test - Dev VMs
    - pmsstaff-esx1-rh9-lsi
    - w2kas-bus
    - w2kas-busb
    - w2kas-busB
    - w2kent-busA
You can now organize datastores in folders and control access by folder or datastore.
You can now control access by portgroup or distributed switch.
Event triggers use arguments, operators, and values to identify the triggering condition.
Use Orchestrator to create and execute workflows that automate virtual infrastructure management processes.
## Administrative Controls for Security and Compliance

<table>
<thead>
<tr>
<th>Requirement</th>
<th>VMware Products</th>
<th>Partner Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration management, monitoring, auditing</td>
<td>VMware vCenter Server&lt;br&gt;VMware vSphere Host Profiles&lt;br&gt;VMware vCenter ConfigControl (future)</td>
<td>Configuresoft ECM for Virtualization&lt;br&gt;NetIQ Secure Configuration Manager&lt;br&gt;Tripwire Enterprise for VMware</td>
</tr>
<tr>
<td>Auditable and repeatable procedures</td>
<td>VMware vCenter Orchestrator&lt;br&gt;VMware vCenter Lifecycle Manager</td>
<td></td>
</tr>
<tr>
<td>Updating of offline VMs</td>
<td>VMware Update Manager</td>
<td>Shavlik NetChk Protect</td>
</tr>
<tr>
<td>Virtual network security</td>
<td>VMware vShield Zones&lt;br&gt;vNetwork Distributed Switch</td>
<td>Cisco, Checkpoint, Reflex, Third Brigade, TrendMicro</td>
</tr>
</tbody>
</table>

Diverse and growing ecosystem of products to help provide secure VMware Infrastructure
vNetwork Distributed Switch

- Simplifies datacenter administration
- **Security Benefits**
  - Helps to mitigate misconfiguration
  - PVLAN Support
  - Inbound Bandwidth Control
- Enables networking statistics and policies to migrate with virtual machines (Network VMotion)
  - Key to enable VMsafe Appliances to Provide Stateful Security
  - Netflow Statistics Don’t Reset
- Provides for customization and third-party development
  - **Cisco’s Nexus1000V** has even more security controls build right in.
Private VLANs

PVLAN (Private VLAN)

- Enables Layer-2 isolation between VMs on the same switch, even though they are on the same subnet
- Traffic from one VM forwarded out through uplink, without being seen by other VMs
- Communication between VMs on PVLANs can still occur at Layer-3

Benefits

- Scale VMs on same subnet but selectivity restrict inter-VM communication
- Avoids scaling issues from assigning one VLAN and IP subnet per VM

Implementation

- Available when using Distributed Switch
Cisco Nexus 1000V Security Features

Private VLAN
• Promiscuous port
• Isolated port
• Community port

Security Features
• Access Control List
• Port Security
• DHCP Snooping
• IP Source Guard
• Dynamic ARP Inspection
• ERSPAN

SGACL Matrix

<table>
<thead>
<tr>
<th>Source Group</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
## 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
vShield Zones

Capabilities

• Bridge, firewall, or isolate VM zones based on familiar VI containers
• Monitor allowed and disallowed activity by application-based protocols
• One-click flow-to-firewall blocks precise network traffic

Benefits

➢ Well-defined security posture within virtual environment
➢ Monitoring and assured policies, even through Vmotion and VM lifecycle events
➢ Simple zone-based rules reduces policy errors
vShield Zones: Architecture

vShield Host Appliance
• Virtual Network Monitoring
• Virtual Network Firewall

vShield Manager
• Centralized Monitoring
• Centralized Policy Assignment
Logical Hierarchy of Zones

VM Flow: Monitoring
- Can monitor and audit traffic at all levels of hierarchy

VM Wall: Blocking
- Can define rules at Cluster, VLAN, Datacenter level
  - Network packet processed according to first match
- Policy maintained automatically even for inventory changes, e.g.
  - New VM provisioned
  - VLAN extended to host
VM Flow - Virtual Network Visibility

- Network flows at DC, Cluster, VLAN and down to the guest VM level
- Take guess work out of troubleshooting firewalls: see allowed and blocked traffic
- Identify malicious traffic: visibility for rogue services, botnets, improper server configuration

<table>
<thead>
<tr>
<th>Application</th>
<th>Sessions</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLOWED</td>
<td>3266</td>
<td>3,338</td>
<td>413,933</td>
</tr>
<tr>
<td>UDP</td>
<td>3266</td>
<td>3,338</td>
<td>413,933</td>
</tr>
<tr>
<td>INCOMING</td>
<td>166</td>
<td>177</td>
<td>29,734</td>
</tr>
<tr>
<td>CATEGORYIZED</td>
<td>166</td>
<td>177</td>
<td>29,734</td>
</tr>
<tr>
<td>NBNS-Broadcast</td>
<td>62</td>
<td>94</td>
<td>8,460</td>
</tr>
<tr>
<td>W2K3 VM6(10.91.252.30)</td>
<td>42</td>
<td>48</td>
<td>4,320</td>
</tr>
<tr>
<td>W2K3 VM5(10.91.252.31)</td>
<td>40</td>
<td>46</td>
<td>4,140</td>
</tr>
<tr>
<td>NBDG-Broadcast</td>
<td>63</td>
<td>83</td>
<td>21,274</td>
</tr>
<tr>
<td>W2K3 VM6(10.91.252.30)</td>
<td>40</td>
<td>40</td>
<td>10,318</td>
</tr>
<tr>
<td>W2K3 VM5(10.91.252.31)</td>
<td>43</td>
<td>43</td>
<td>10,956</td>
</tr>
<tr>
<td>UNCATEGORIZED</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>OUTGOING</td>
<td>3101</td>
<td>3,161</td>
<td>304,199</td>
</tr>
<tr>
<td>CATEGORYIZED</td>
<td>3101</td>
<td>3,161</td>
<td>304,199</td>
</tr>
<tr>
<td>DNS</td>
<td>85</td>
<td>125</td>
<td>7,843</td>
</tr>
<tr>
<td>10.91.252.1</td>
<td>43</td>
<td>60</td>
<td>3,908</td>
</tr>
<tr>
<td>10.91.252.2</td>
<td>62</td>
<td>65</td>
<td>3,935</td>
</tr>
<tr>
<td>DHCP-Server</td>
<td>24</td>
<td>48</td>
<td>15,912</td>
</tr>
<tr>
<td>10.91.252.1</td>
<td>24</td>
<td>48</td>
<td>15,912</td>
</tr>
<tr>
<td>NBNS-Broadcast</td>
<td>2118</td>
<td>2,124</td>
<td>176,184</td>
</tr>
<tr>
<td>NBDG-Broadcast</td>
<td>664</td>
<td>864</td>
<td>184,260</td>
</tr>
<tr>
<td>UNCATEGORIZED</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>INTRA</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
VM Wall - Virtual Firewall

- **Shorthand rule notation**: use cluster, VLAN as container groups
- **Hierarchical rule assignment**: scope of rules can be datacenter, zone, default
- **Application-aware rules**: opens dynamic / ephemeral ports as needed and specify app names – not ports
## 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

---

### Table of Security Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New platform hardening features</td>
<td>Further enhance robust security capabilities</td>
</tr>
<tr>
<td>Thin-hypervisor strategy</td>
<td></td>
</tr>
<tr>
<td>Memory Protection</td>
<td></td>
</tr>
<tr>
<td>Kernel Module Protections</td>
<td></td>
</tr>
<tr>
<td>Integrate VMware products</td>
<td>Integrate VMware products into existing operational policies</td>
</tr>
<tr>
<td>Security Virtual Appliances</td>
<td>Enable broad-based security for every VM in the environment</td>
</tr>
<tr>
<td>Better Than Physical</td>
<td>Self-describing, Self-configuring security</td>
</tr>
<tr>
<td></td>
<td>Impact security by taking advantage of unique VMware technologies</td>
</tr>
<tr>
<td></td>
<td>Focus on products and operations</td>
</tr>
</tbody>
</table>
VMware vSphere 4 – Cloud OS

VMware vSphere 4 - The Industry’s First Cloud Operating System

Application Services
- Availability
  - Clustering
  - Data Protection
- Security
  - Firewall
  - Anti-virus
  - Intrusion Prevention
  - Intrusion Detection
- Scalability
  - Dynamic Resource Sizing

Infrastructure Services
- Compute
  - Hardware Assist
  - Enhanced Live Migration Compatibility
- Storage
  - Storage Management & Replication
  - Storage Virtual Appliances
- Network
  - Network Management
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 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 VMs on a single host.
  - Capability to provide inline or passive protection

• Storage
  - Ability to mount and read virtual disks
<table>
<thead>
<tr>
<th>Category</th>
<th>Partner</th>
<th>Solution</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Check Point</td>
<td>VPN1-VE</td>
<td>Early Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UTM - Firewall, IPS, App FW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALTOR</td>
<td>VF 3.0</td>
<td>GA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firewall, network monitoring</td>
<td></td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>ISS</td>
<td>IBM ISS Proventia</td>
<td>Beta</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hybrid host/network IPS + Anti-rootkit + Virtual NAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trend Micro</td>
<td>Third Brigade Deep Security 7</td>
<td>Pre-beta</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hybrid host/network IPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reflex</td>
<td>VMC</td>
<td>GA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vTrust network zoning, network IPS, virtualization mgmt</td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td>McAfee</td>
<td>Virusscan for Offline Virtual Images (OVI) 2.0</td>
<td>Beta</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Offline AV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trend Micro</td>
<td>Core Protection for Virtual Machines 1.0</td>
<td>GA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Online / Offline AV</td>
<td></td>
</tr>
</tbody>
</table>
Where to Learn More

Security

- Hardening Best Practices
- Implementation Guidelines
  http://vmware.com/go/security

Compliance

- Partner Solutions
- Advice and Recommendation
  http://vmware.com/go/compliance

Operations

- Peer-contributed Content
  http://viops.vmware.com
### VMware Security Strategy

<table>
<thead>
<tr>
<th>Core Platform Security</th>
<th>Operationalize Security</th>
<th>Security Virtual Appliances</th>
<th>Better Than Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>• New platform hardening features further enhance robust security capabilities</td>
<td>• Integrate VMware products into existing operational policies in the enterprise</td>
<td>• Enable broad-based security for every VM in the environment</td>
<td>• Self-describing, Self-configuring security</td>
</tr>
<tr>
<td>• Thin-hypervisor strategy</td>
<td></td>
<td>• “Democratize” security</td>
<td>• Impact security by taking advantage of unique VMware technologies</td>
</tr>
<tr>
<td>• Memory Protection</td>
<td></td>
<td></td>
<td>• Focus on products and operations</td>
</tr>
<tr>
<td>• Kernel Module Protections</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions?

Christian Liebner, Solution Specialist Systems Engineer, VMware