

McAfee Secure Virtualization



Proven, Comprehensive Protection for Virtualized Environments

Peter Van Eeckhout
Senior system security engineer

January 26, 2010



Data Center Cost and Consolidation Wave



70% of organizations will virtualize all or part of their DMZ by end of 2010.

58 Million virtual desktops forecasted by 2012.

*Neil MacDonald
Gartner 2009*

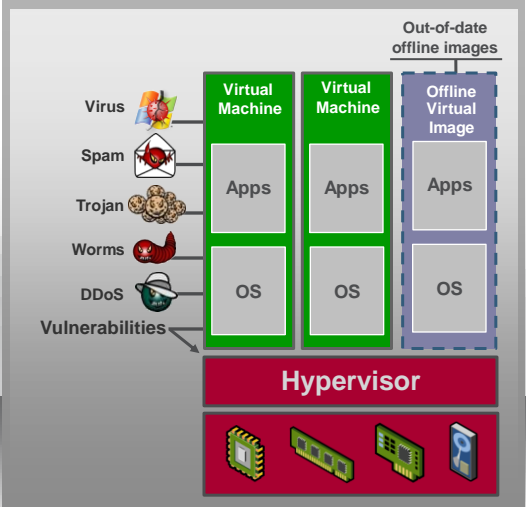
'Virtualization First' is now the default approach for new server deployments

IDC 2009

Top Market Challenges for Secure Virtualization



- Virtualization = new IT platform
 - with its own unique vulnerabilities
- Virtualization changes the definition of an endpoint
 - Virtualized systems are no longer systems, they become data
 - Virtual images built on the fly re-define the notion of an asset
- Virtualization world is vulnerable
 - Hypervisor
 - Offline Virtual Images
 - Virtualization Center Console

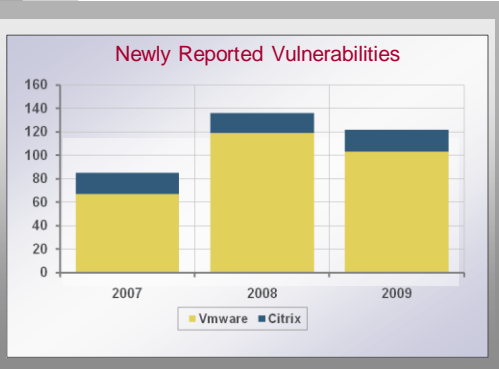


³ National Vulnerability Database

Virtualization Vulnerabilities



- #1 Threat to Security in 2009 is virtual hack – Baseline Magazine
- 60% of production VMs will be less secure than their physical counterparts through 2009 --Gartner



Source: Open Source Vulnerability Database: <http://osvdb.org>

Impact of Virtualization on Security



Some things are the same

- Malicious code
- Attackers focus on data

Some things are new

- VM Infrastructure
- Images on the move
- Moving the users from the perimeter to the datacenter

Some things are better

- Lower data loss exposure
- Virtual Security Appliances

Some things are worse

- Lack of security tools/controls
- Performance impact of security can multiply in virtualized infrastructure



What if?



Performance impact of security was not a concern?

Compliance was automatic and enforced for every new Virtual Machine?

VM Sprawl was not a security issue?


You could manage your virtual and physical systems in the same way?





McAfee's Virtualization Product Line


January 26, 2010 Confidential McAfee Internal Use Only



VirusScan Enterprise for Offline Virtual Images


Secures offline VMs without bringing them online

- Protect Offline Virtual Machines
- Identify and Remove Malware
- Automate security updates from McAfee Global Threat Intelligence



Virtualization Benefits

- Update Offline Security software and Malware Signatures without bringing VM's online
- Schedule scans via ePO along with physical machines
- VMsafe Integrated for optimized performance



10 January 26, 2010 Confidential McAfee Internal Use Only


Host Intrusion Prevention and Virtualization



Day Zero protection against Buffer Overflow Vulnerabilities

- Protects against unknown malware and zero-day vulnerabilities
- Day-zero protection for 90% of Microsoft 2009 vulnerabilities
- Reduces patching urgency
- Integrated firewall changes protection based on location
 - i.e. coffee shop vs. office





Virtualization Benefits

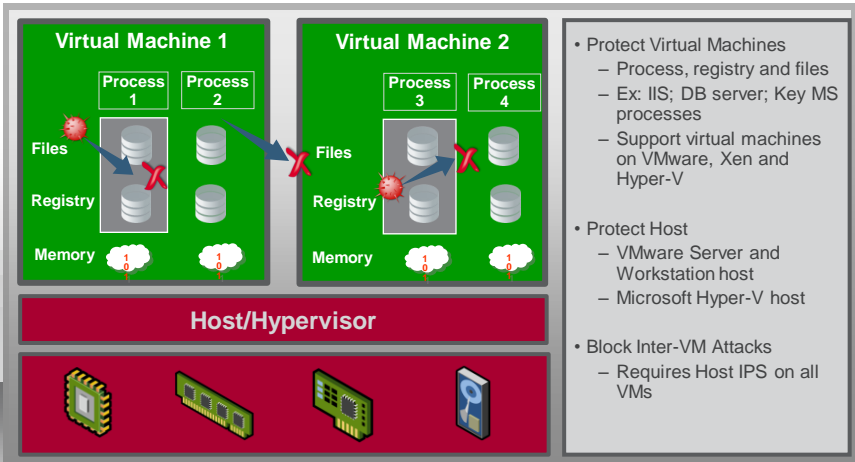
- Protect Virtual Machines
 - Process, registry and files
 - Ex: IIS; DB server; Key MS processes
 - Support virtual machines on VMware, Xen and Hyper-V
- Protect Host
 - VMware host, Microsoft Hyper-V host
- Block Inter-VM Attacks

11

January 26, 2010

Confidential McAfee Internal Use Only

Host IPS Protects Virtualized Servers



12

January 26, 2010

Confidential McAfee Internal Use Only


Application Control and Virtualization



Ensures only trusted applications run on servers and endpoints

- Dynamic whitelisting trust model reduces cost of ownership
- Zero day threat protection reduces patching cycles
- Blocks unwanted applications and their risks
- Extend the lifespan of legacy systems





Virtualization Benefits
 Minimal endpoint impact on Virtual Desktop and Virtualized Application Servers

- Consumes less than 10MB of RAM and minimal CPU
- No online scanning
- No Signature Updates
- Minimal Disk footprint

13 January 26, 2010 Confidential McAfee Internal Use Only


Network Access Control and Virtualization



Ensure endpoint compliance prior to and after network access

- Prevent users from disabling security tools
- For unmanaged (guest) endpoints, integrates with McAfee NAC Appliance and NAC Add-on to Network Security Platform





Virtualization Benefits

- Ensures VM's are compliant before they come online
- Checks for patches, application status and more

14 January 26, 2010 Confidential McAfee Internal Use Only

ePolicy Ochestraator

Centrally manage security for physical and virtual environments



World's most scalable security and compliance mgmt platform

- Manages 60M+ endpoints in 35,000+ enterprises with largest deployment > 5M endpoint
- 3 of 4 Global 2000 companies use ePO

Deploy, manage and report on

- Online and offline virtual images
- Endpoint security
- Data protection
- Web and messaging security
- Integration with network IPS and vulnerability management
- Threat alerts from McAfee Labs



“ePO has historically been the standard for centralized administration consoles.”
Peter Firstbrook,
 2008 Endpoint Protection Platform Magic Quadrant

15

January 26, 2010

Confidential McAfee Internal Use Only

McAfee Vulnerability Manager and Virtualization



- Automatically discover all assets
 - Physical or virtual; managed or unmanaged
- Risk based approach to threats
 - Most important systems remedied first
- Leverages virtualization benefits
 - Reduced TCO by deploying in virtual environments
 - Disaster recovery and high availability



Virtualization Benefits

- Assesses Virtual Machines and the hypervisor layer for security issues remotely without impact
- Supports VMware ESX and Citrix Xen
- Over 100 unique checks – patches, vulnerabilities, ssh/ssl certificates and more

16

January 26, 2010

Confidential McAfee Internal Use Only

McAfee Network Intrusion Prevention and Virtualization



- Award-winning, network-class protection for absolute security confidence
- 10-Gigabit Ethernet performance
- Real-time risk-aware IPS
- System-aware IPS with McAfee ePO™ integration
- Dynamic network access control



Virtualization Benefits

- Dozens of vulnerability behavioral signatures specific to VMware, Citrix and Microsoft
- Virtual IPS allows you to create separate policies for each VM Image.

17 January 26, 2010 Confidential McAfee Internal Use Only



McAfee Enterprise Firewall Virtual Appliance



- Software firewall for VMWare ESX Server
 - Unlimited instances per server
- Includes virtualized IPS, as well as AV, URL filtering, SSL decryption
- Designed for your server consolidation projects
 - Security within ESX platform and inter VM
- Manage and report individually



Virtualization Benefits

- Lower Cost
- Greater Convenience
- Maximize Hardware Usage

18 January 26, 2010 Confidential McAfee Internal Use Only




VMware Ready Products



Endpoint Security products are tested by McAfee to work with VMware products

VMware Tested Products



- VirusScan Enterprise for Offline Virtual Images*
VMsafe™ integrated
- Total Protection for Virtualization
- McAfee Network Access Control
- McAfee Policy Auditor
- McAfee Enterprise Firewall Virtual Appliance
- McAfee Web Security Virtual Appliance
- McAfee Email Security Virtual Appliance

*Compatible with VMware® Vsphere, ESX™ and VCenter™

Citrix Ready Certification



The Citrix Ready program identifies trusted, third-party solutions that add the greatest value in the Citrix Delivery Center™ infrastructure.



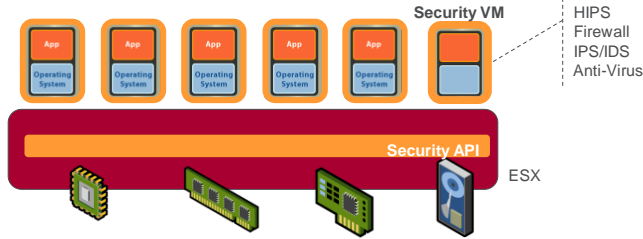
Citrix Certified Products

- VirusScan Enterprise for Offline Virtual Images*
- VirusScan Enterprise*
- AntiSpyware Enterprise*
- ePolicy Orchestrator
- Vulnerability Manager

www.citrixready.com

Compatible with Citrix® XenApp™

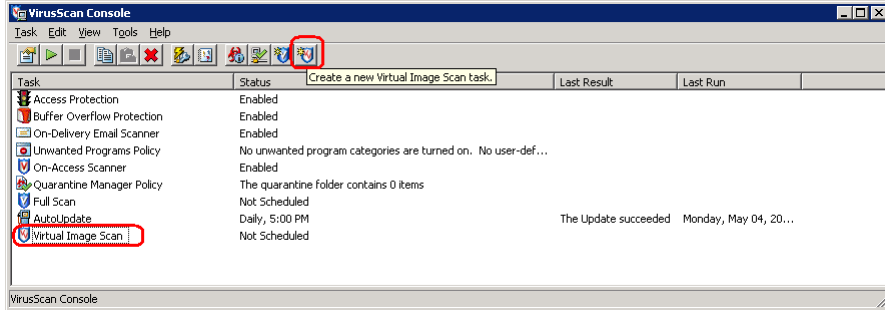
Introducing VMsafe™



- 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

Confidential McAfee Internal Use Only

Add-on to regular VSE product



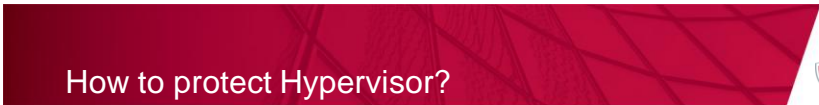
- OVI is an add-on for VSE
- OVI modifies VSE's console to add new toolbar icons and menu items
- Can create scan tasks for VM images
 - Similar to VSE's "On-Demand" scan tasks

Confidential McAfee Internal Use Only



Best Practices

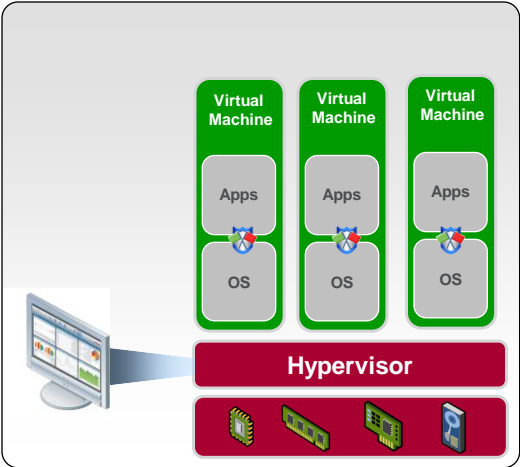
Confidential McAfee Internal Use Only



How to protect Hypervisor?



- Lock down management network access
- Have a stringent access control policies for VI administration
- Lock down VMs
 - AVs
 - Host IPS



Confidential McAfee Internal Use Only

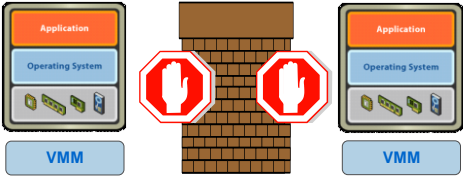
Network Protection - Lock down Open Ports



- Limited ports open.
- The following ports are open on ESX3i by default:
 - 80 (reverse proxy)
 - 443 (reverse proxy)
 - 427 (service location protocol).
 - 902 (old VIM API, MKS etc).
 - 5989 (CIM XML server - sfcdb)

Confidential McAfee Internal Use Only

VM Isolation



Design

- Privileged instructions within a VM are “de-privileged” and run within an isolated virtual memory space
- VMs have no direct access to hardware, only have visibility to virtual devices
- VMs can only communicate with each other through Virtual Switches
- Resource reservations and limits guarantees performance isolation
- OS and applications within a VM run as is with no modification (hence no recertification required)

Production Use Proof Points

- Passed security audit and put into production by the largest Financial Institutions
- Passed Defense and Security Agencies scrutiny and audit (NetTop and HAP)
- Large number of customers run mission critical and transaction processing applications
- CC EAL 2 certification (for ESX 2.5)
- CC EAL 4+ certification (for VI 3.0)

Confidential McAfee Internal Use Only

Thank You!



For more information, please visit:

http://www.mcafee.com/us/enterprise/products/virtualization_security/index.html

January 26, 2010

