IBM SECURITY DAY 2011

Innovare con sicurezza per aprire al futuro

Fabio Panada

La sicurezza negli ambienti virtualizzati

Virtualization – First Step in Journey to Cloud Computing

- Virtualization.
- Better hardware utilization.
- Improved IT agility.

- Rapid deployment of infrastructure and applications.
- Request-driven service management.
- Service Catalog.

Cloud Computing

- Integrated service lifecycle mgmt.
- Expose resources “as-a-Service”.
- Integrated Security infrastructure.
- Rapid provisioning of IT resources, massive scaling.
- Dynamic service mgmt.
- Energy saving via auto workload distribution.

- Server Consolidation.
- Streamline Operations – manage physical and virtual systems.
- Lower power consumption.

Virtualization Security Increasingly a Focus

- 38% of server class vulnerabilities affect the hypervisor
- Virtualization Vulnerability Disclosures stay flat in 2010
  - Virtualization systems has added 259 new vulnerabilities to the network infrastructure over the last five years (80 virtualization vulnerabilities were disclosed in 2010).
  - This trend suggests that virtualization vendors have been paying more attention to security since a couple of years.

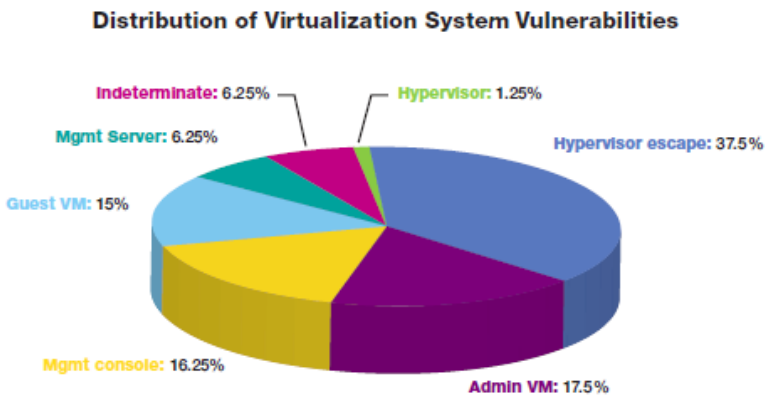
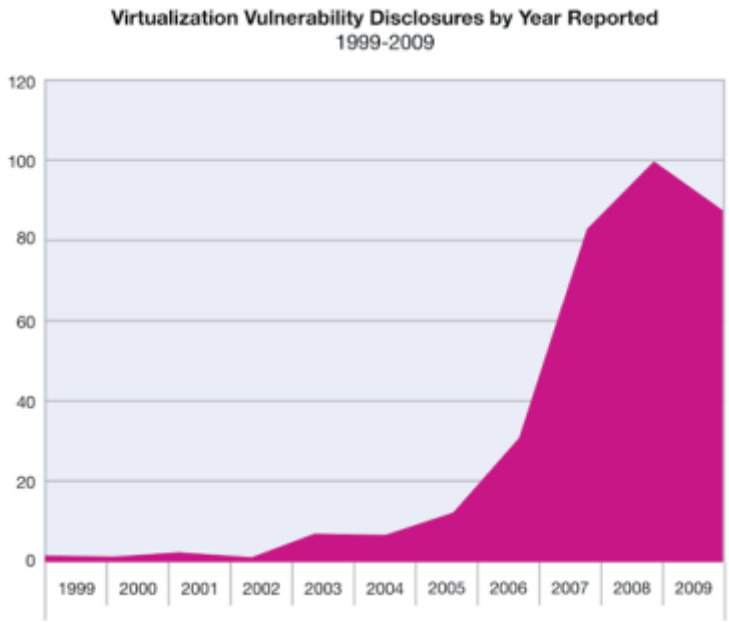


Figure 65: Distribution of Virtualization System Vulnerabilities

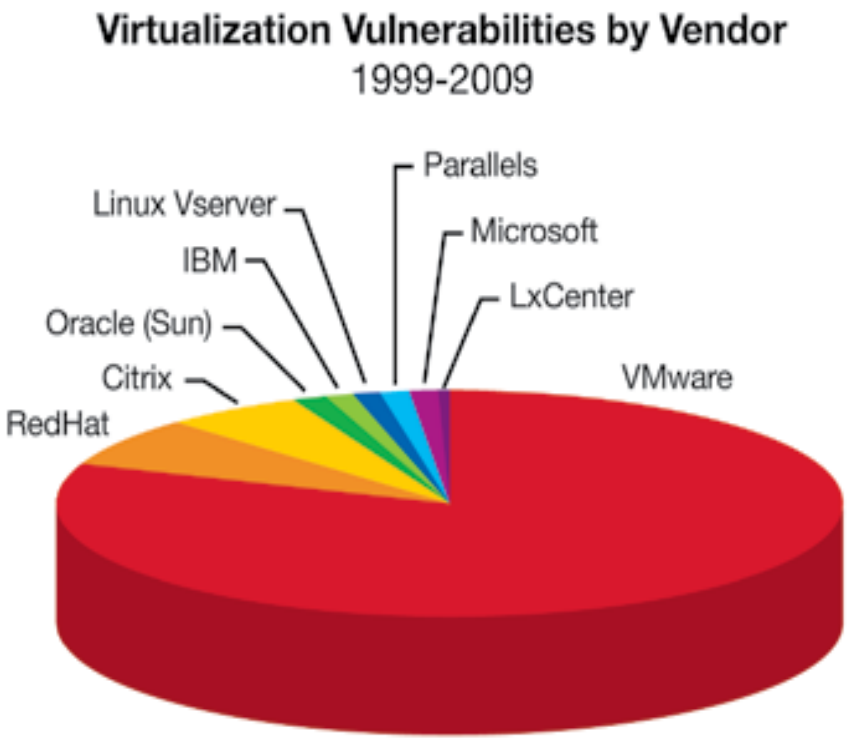


Virtualization systems have added 259 new vulnerabilities to the network infrastructure over the last five years.

Vendor Disclosures Include Some Surprising Results

- Low percentages for Oracle, IBM, and Microsoft

VMware: 80.9%	RedHat: 6.9%	Citrix: 5.8%
Oracle: 1.8%	IBM: 1.1%	Microsoft: 0.9%



Virtualization and Enterprise Security

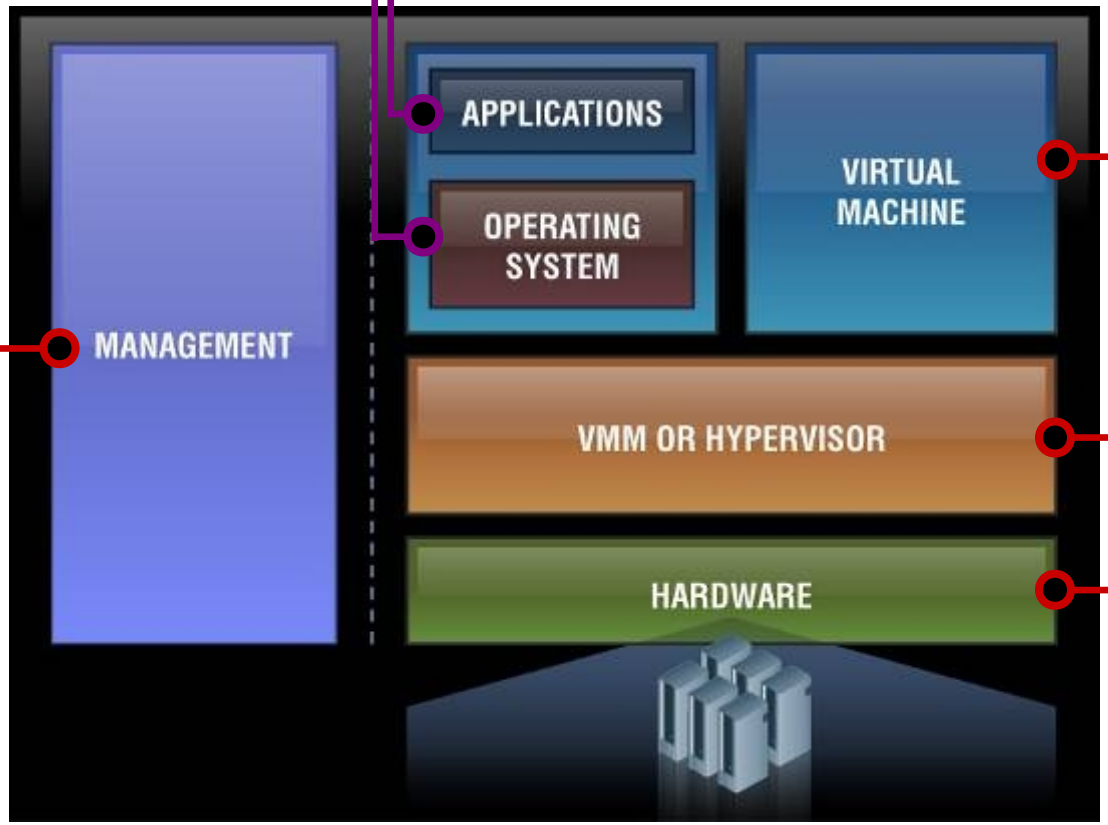
- Virtualization != Security
  - Standard servers are as secure as standard VMs
- Partitioning divides VMs, but does not secure them
- Same principles apply
  - Defense in depth
  - Network design and segmentation
  - Unified security management

- Virtualization <u>does</u> impact security posture
- “Traditional” tools are still relevant
- New products adapted for virtual environments are available
- No single product for everything

Security Challenges with Virtualization: New Risks

- Traditional Threats
- New threats to VM environments

Traditional threats can attack VMs just like real systems



Management Vulnerabilities

Secure storage of VMs and the management data

Requires new skill sets

Virtual server sprawl

Dynamic relocation

Dynamic state

VM stealing

Loss of visibility

Resource sharing

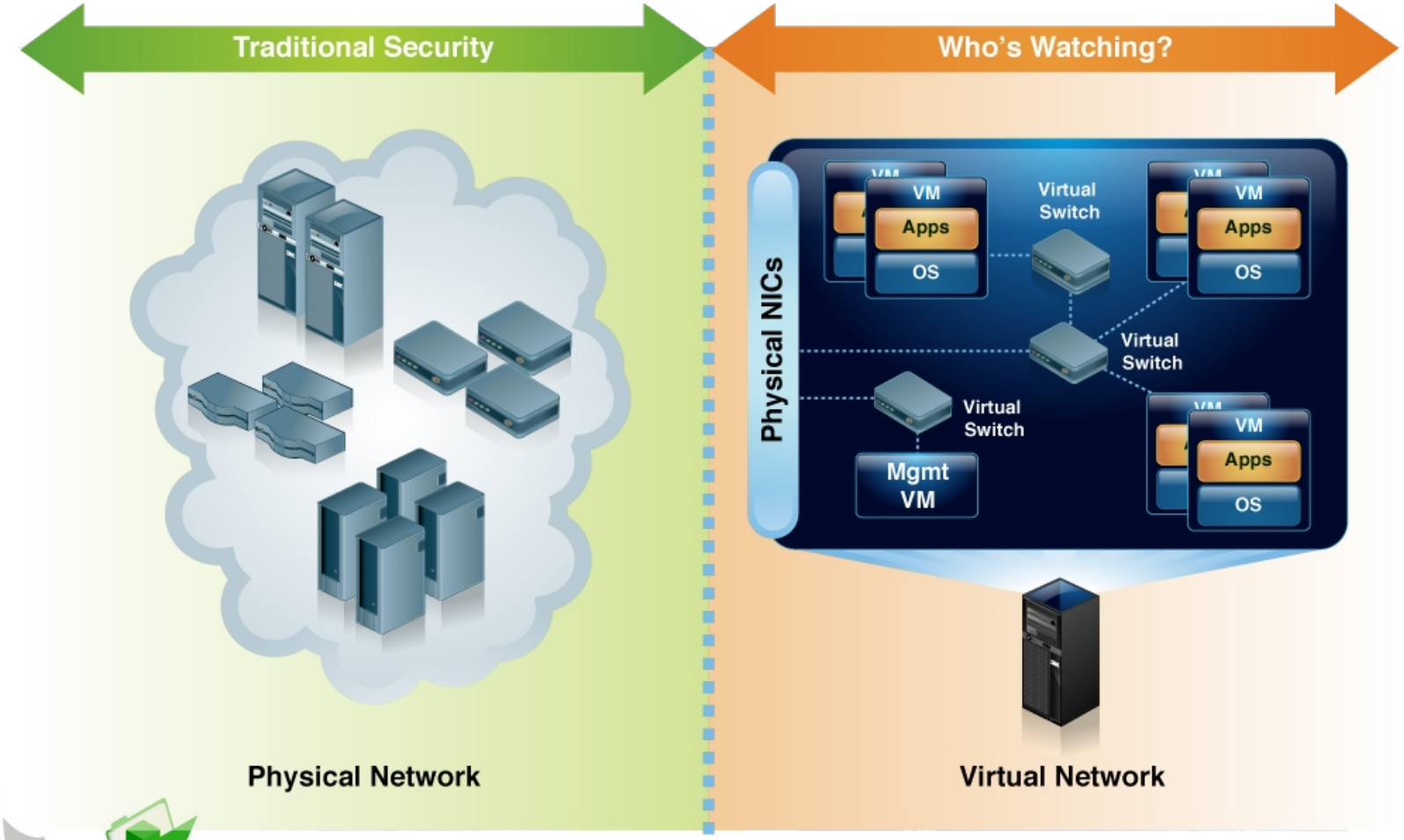
Single point of failure

Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

MORE COMPONENTS = MORE EXPOSURE

Server and Network Convergence



Security Must Evolve

Physical	
Network IPS	Blocks threats and attacks at the perimeter
Server Protection	Secures each physical server with protection and reporting for a single agent
System Patching	Patches critical vulnerabilities on individual servers
Security Policies	Policies are specific to critical applications in each network segment and server

Virtualized	
Network IPS	Should protect against threats at perimeter and between VMs
Server Protection	Securing each VM as if it were a physical server adds time, cost and footprint
System Patching	Needs to protect against vulnerabilities that result from VM state changes
Security Policies	Policies must be able to move with the VMs

Virtualization Security Evolution

Existing solutions certified for protection of virtual workloads

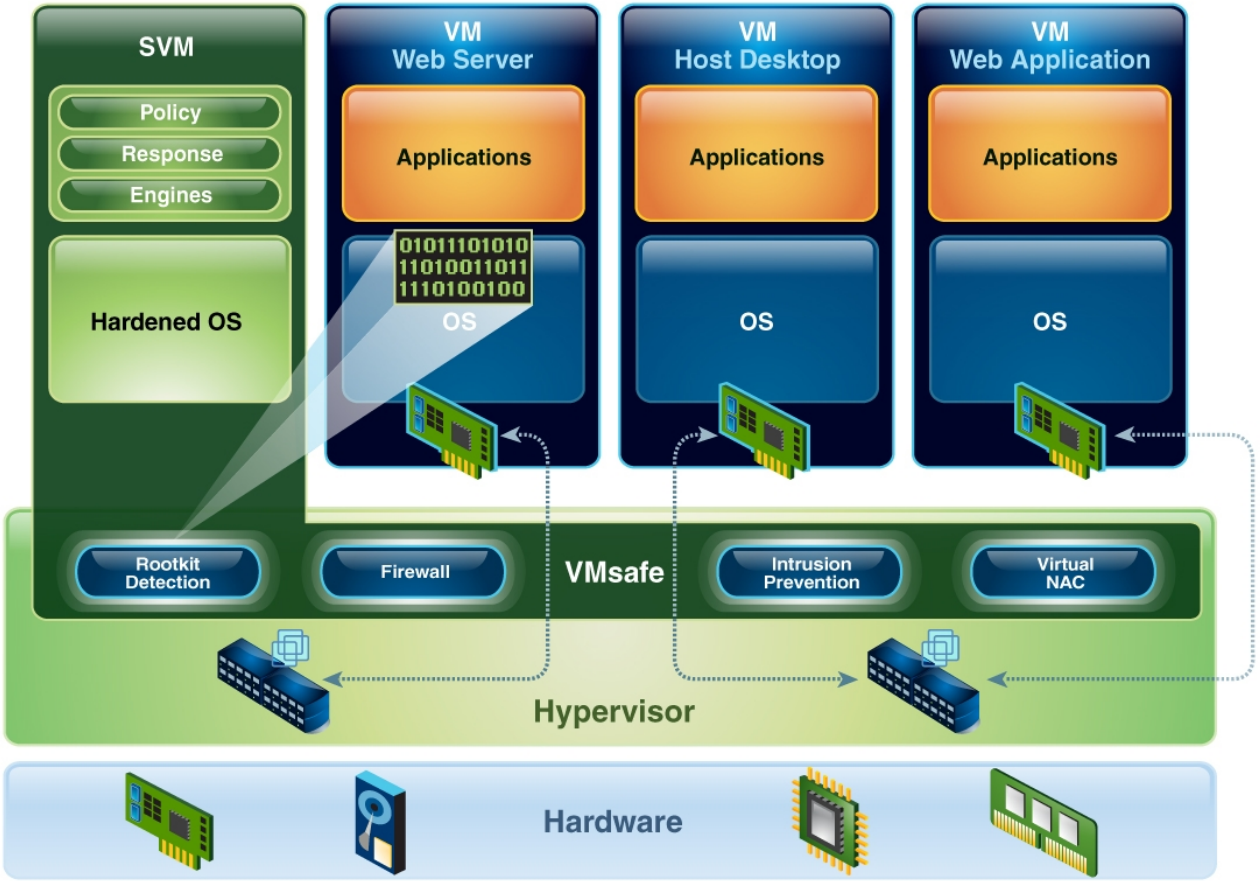
Threat protection delivered in a virtual form-factor

Integrated virtual environment-aware threat protection

IBM Security
Virtual Server Protection for VMware

IBM Virtual Server Security for VMware

Integrated threat protection for VMware ESX and ESXi



- VMsafe Integration
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- Virtual Network Access Control

IBM Virtual Server Protection for VMware helps to meet compliance best practices

1. **Configuration and change management processes should be extended to encompass the virtual infrastructure**
   - Automatic discovery and protection as a VM comes online
   - Dashboard visibility into the virtual host OS and the virtual network to identify vulnerabilities.
   - IBM Virtual Patch® technology protects vulnerabilities on virtual servers regardless of patch strategy
2. **Maintain separate administrative access control although server, network and security infrastructure is now consolidated**
   - Virtual network access control
     - Quarantines or limits network access from a virtual server until VM security posture has been confirmed
   - Virtual Infrastructure auditing
3. **Provide virtual machine and virtual network security segmentation**
   - Network-level workload isolation
4. **Maintain virtual audit logging**
   - Virtual Infrastructure monitoring and reporting

*Source: RSA Security Brief: Security Compliance in a Virtual World http://www.rsa.com/solutions/technology/secure/wp/10393_VIRT_BRF_0809.pdf

Gartner's Perspective on Secure Virtualization

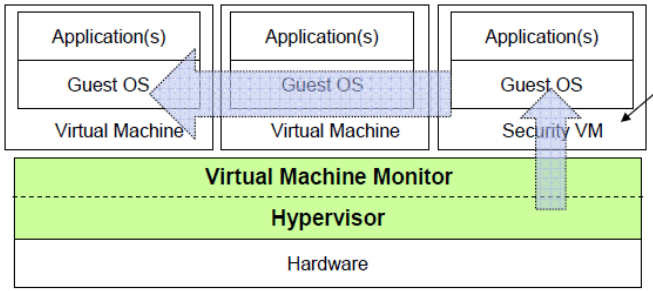
Most Common Security Risks in Virtualization Projects

1. Information Security Isn't Initially Involved in the Virtualization Projects
2. A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads
3. The Lack of Visibility and Controls on Internal Virtual Networks Created for VM-to-VM Communications Blinds Existing Security Policy Enforcement Mechanisms
4. Adequate Controls on Administrative Access to the Hypervisor/VMM Layer and to Administrative Tools Are Lacking
5. There Is a Potential Loss of SOD for Network and Security Controls When These are Virtualized

-Neil MacDonald, Gartner

"IBM has the first commercial implementation of a rootkit detection/prevention offering that works from outside of the virtual machine it is protecting..."

-Neil MacDonald, Gartner



"Virtual Security Partition" in this case a "Security VM":

- Network firewall
- Application-level firewall
- Identity-aware network access control
- E-mail security platform
- Web security platform
- Unified Threat Management
- Directory server

Neil MacDonald, Gartner

IBM Security Virtual Server Security Benefits

- **Automated Protection as each VM comes online**
  - Automatic Discovery
  - Automated vulnerability assessment
  - IBM Virtual Patch® technology
- **Non-intrusive**
  - No reconfiguration of the virtual network
  - No presence in the guest OS
    - Improved stability
    - More CPU/memory available for workloads
    - Decreased attack surface
- **Protection for any guest OS**
  - Reduction is security agents for multiple OSs

- **Less presence in guest OS**
  - More CPU/memory available for workloads
  - Decreased attack surface
- **Less management overhead eliminates redundant processing tasks**
  - One Security Virtual Machine (SVM) per physical server
  - 1:many protection-to-VM ratio
  - CPU-intensive processing removed from the guest OS and consolidated in SVM
- **Centralized Management**
  - IBM Proventia® Management SiteProtector™ system

IBM Office Last Week

- Customer: “Hello Mr. Panada, yesterday we had a serious problem in our Datacenter, can we talk about ?”
- Me: “ Sure Mr Customer, how can help you ?”
- Customer: “ I am part of our Cloud Computing team; our cloud environment is based on VMware technology. We think one of our virtual server brought a Worm in the system and we are looking something to mitigate the issue and to avoid it to happen again.
- Me: “I think we have a solution for you. Can we show you how it works ?”
- Customer: “Yes, thanks. Let’s do it as soon as possible”

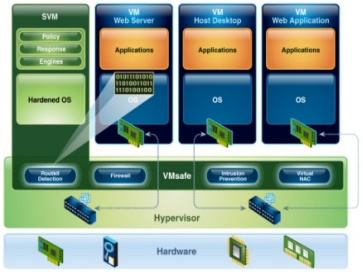
The problem : Serious Security problem in a virtual environment

The context: Cloud Computing Service

The Solution: <u>IBM Security Virtual Server Protection for VMware</u>

Summary

Need	How IBM Virtual Server Protection helps
Mitigate new risks and complexities introduced by Virtualization	Provides dynamic protection for every layer of the virtual infrastructure
Maintain compliance standards and regulations	Helps meet regulatory compliance by providing security and reporting functionality customized for the virtual infrastructure
Drive operational efficiency	Increases ROI of the virtual infrastructure




Thank
You