

Virtual Reality

Understanding the Security and Compliance Implications of Server Virtualization

Joshua Corman
Principal Security Strategist
IBM Internet Security Systems

INTEROP[®]



Agenda

- Introduction to Virtualization
- Key Drivers of Server Virtualization Adoption
- Understanding our Priorities
- Security and Risk Implications
- Operational and Organizational Implications
- Common Mistakes
- What Can I Do?
 - Current technologies and solutions
 - The future of virtualization and enterprise security

- PART I

Introduction to Virtualization

Basics: Disruptive Innovation

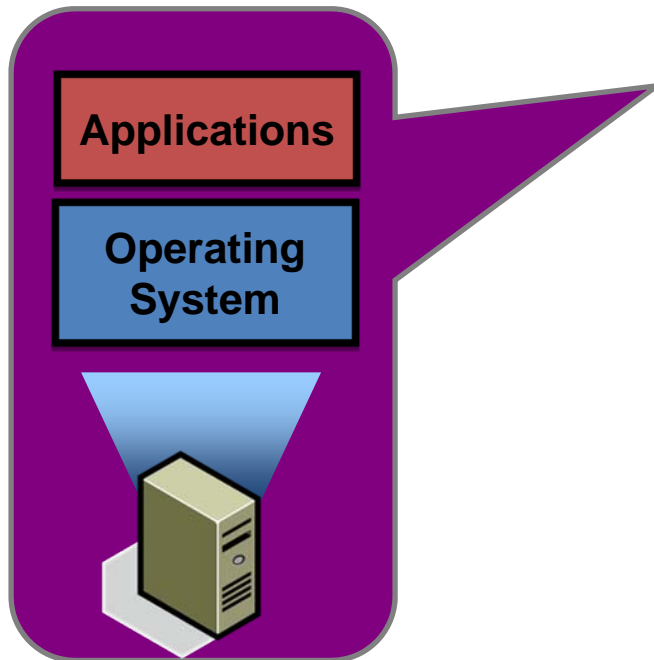
Virtualization is a **Disruptive Innovation**

Virtualization:

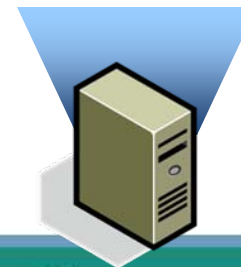
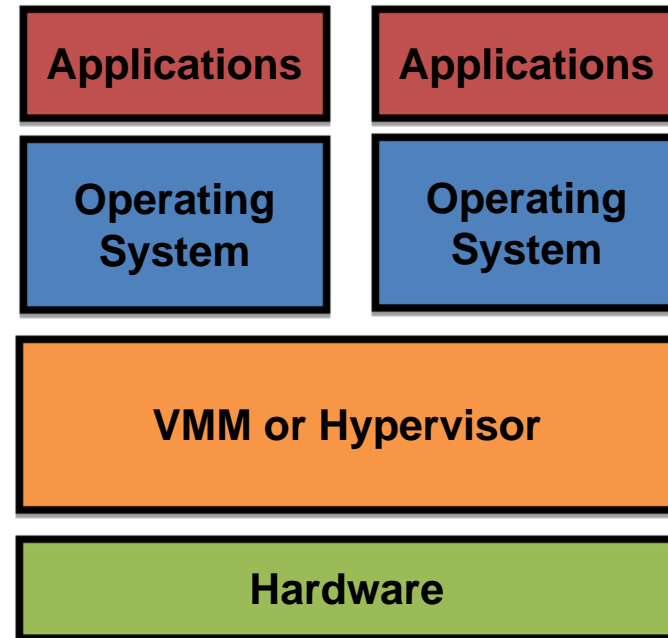
The logical abstraction of physical computing resources (OS, application, switches, storage, networks) designed to create computing environments that are not restricted by physical configuration or implementation.

Basics: Virtualization Architecture

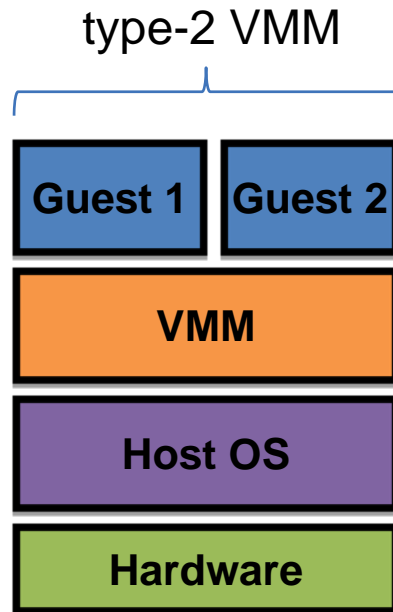
Before Virtualization



After Virtualization

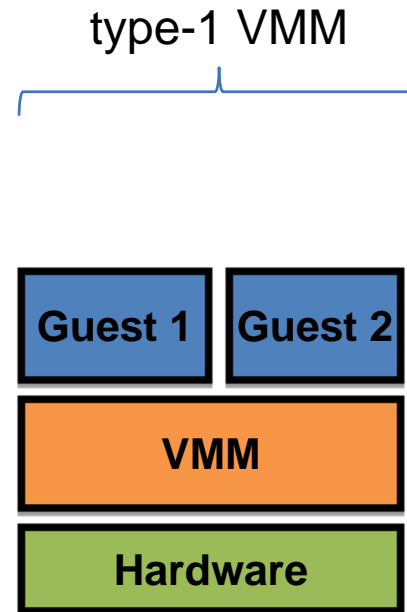


Basics: Virtualization Types



Examples:

KVM (Linux)
VMware Workstation
VMware Server
Microsoft Virtual PC



Examples:

Xen
VMware ESX
IBM pHype / LPARs
Microsoft Hyper-V

What does Virtualization Change?

- Everything
 - Dynamic, fluid data-center
 - Resource pools
 - Commoditization of everything
 - Increased efficiency
- Nothing
 - Virtual IT is still IT
 - Security, sprawl, management, complexity, heterogeneity

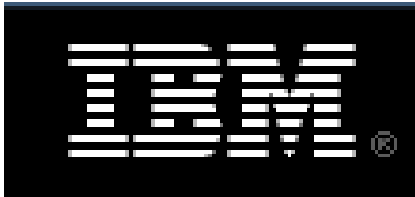
Virtualization impact on the enterprise

- Virtualization changes the enterprise landscape completely
 - Virtual networking
 - New management framework
- Security must be part of the virtual infrastructure just as it is part of the physical infrastructure
 - Defense in depth
 - Integrated protection
 - Security management
 - Audit

Major Players



- Founded in 1998
- Division of EMC
 - \$9.6B in Revenue
 - 4 million users, 20K corporate customers
- IPO (~13% shares) in 2007



- Pioneered virtualization over 40 years ago
- LPAR, sHype, Phantom



- Acquired XenSource in 2007 for \$500 million
- Based on open-source Xen hypervisor

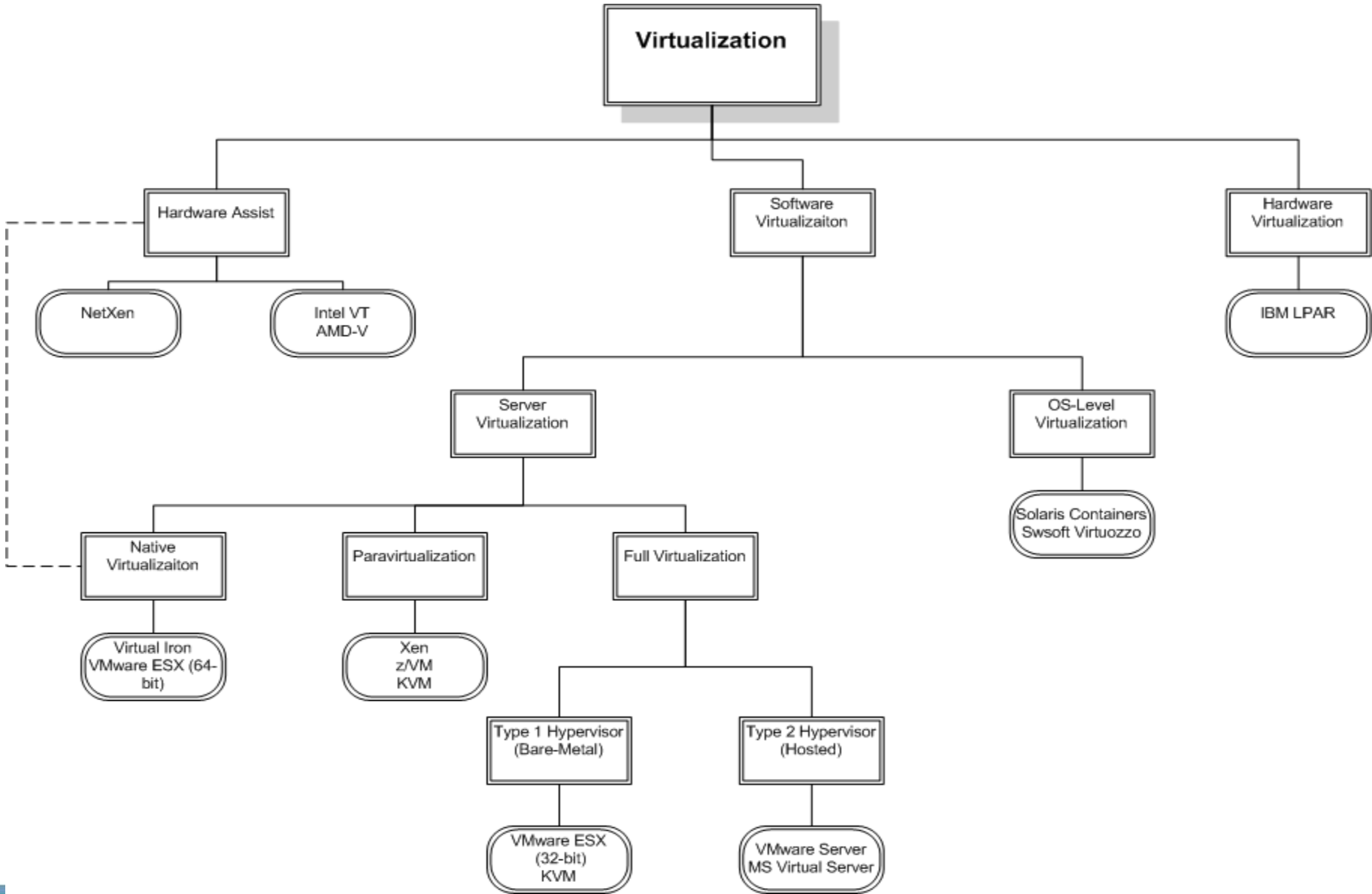


- Virtual server, acquired VirtualPC in 2003 from Connectix
- Hyper-V (fka Viridian) to be released in 2008



- Based on open-source Xen hypervisor

Platform Virtualization



Hardware Assisted Virtualization

- Intel
 - VT (Virtualization Technology or “Vanderpool” Technology)
 - VT-x (IA-32 extensions) – CPU virtualization only
 - VT-i (IA-64 extensions) – CPU virtualization only
 - Futures
 - VT-d (Directed I/O) – I/O virtualization
 - Memory virtualization
- AMD
 - AMD-V or Pacifica – CPU virtualization only
 - Futures
 - IOMMU – I/O virtualization
 - Memory virtualization
- NetXen
 - Ethernet I/O virtualization

Scope

- The scope of this presentation is x86 virtualization and its associated security implications in the Enterprise
- Primarily focused on Server uses

•PART II

Key Drivers of Server Virtualization Adoption

Virtualization Market Anecdotes

- Virtualization demand has exploded
 - “...spending on virtualization technology will reach **\$15 billion** by 2009.” – **IDC**
 - “...80% of all data centers are using virtualization in some form.” – **IDC**
 - “...Enterprises which do not leverage virtualization will pay up to 40% more in acquisition costs by 2008, and roughly 20% more in administrative costs” – **Gartner**

Virtualization Market Anecdotes

- 35% of North American and European firms use server virtualization today. An additional 11% are in the piloting process. - **Forrester**
- A separate global survey of large and SMB enterprises across a variety of vertical industries indicates that in 2006 76% of companies already use or plan to deploy server virtualization technologies.
 - 62 of the 76% have already deployed or are of the process of deploying the technology. – **Yankee Group**

Large Enterprise Perspective – Server Virtualization

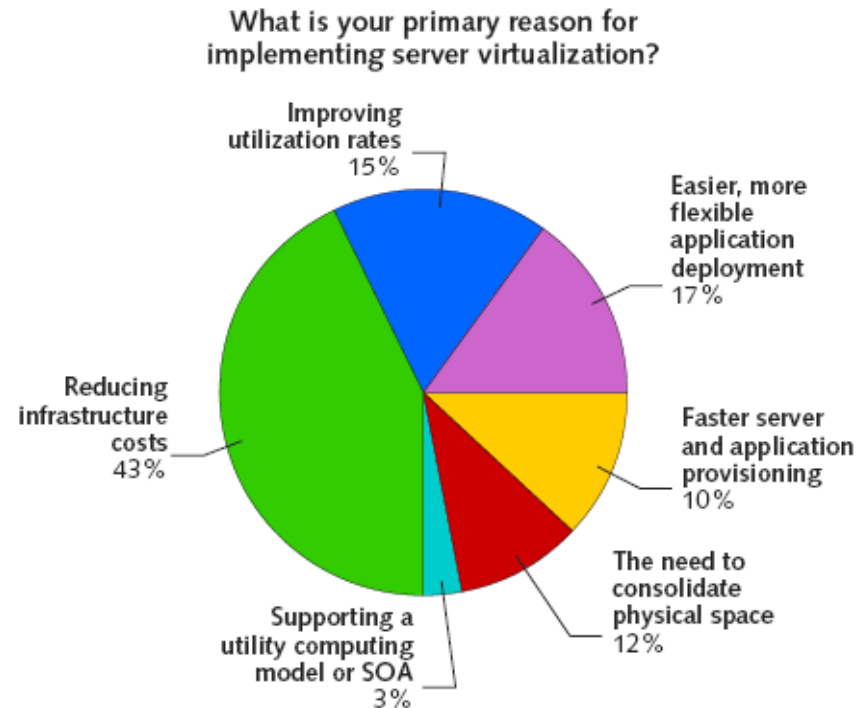
- Recent worldwide surveys of 1,221 enterprises with 1,000 employees or more. – **Forrester**
 - Twenty-six percent report they have implemented server virtualization, and another 8% plan to pilot within 12 months.
 - Global 2000 firms — those with 20,000 or more employees — had the strongest overall results in terms of awareness, adoption, and pilot plans, with 79% overall awareness, 33% already using virtualization, and 13% with plans to pilot within 12 months.
 - North American firms lead, with 41% already implemented or planning to pilot.

Virtualization Benefits

- Cost savings
 - Space, power, cooling
- More efficient use of hardware resources
- Common hardware environments
- Instant provisioning
- Disaster recovery
- Data partitioning
- Distributed resource scheduling
 - Load balancing

Infrastructure Consolidation Drives Server Virtualization Adoption

Source: Yankee Group 2006 Global Server Virtualization Survey



•PART III

Understanding our Priorities

INTEROP[®]



Priorities...

- Security Trade Offs...
- What Drives our Security Decisions...
- For Servers... Rank these Objectives:
 - Confidentiality
 - Integrity
 - Availability
- Isolation, Isolation, Isolation
- Compliance, Compliance, Compliance

Security Trade Offs... by Bruce Schneier

There are several specific aspects of the security trade-off that can go wrong. E.g. :

1. The severity of the risk.
2. The probability of the risk.
3. The magnitude of the costs.
4. How effective the countermeasure is at mitigating the risk.
5. How well disparate risks and costs can be compared.

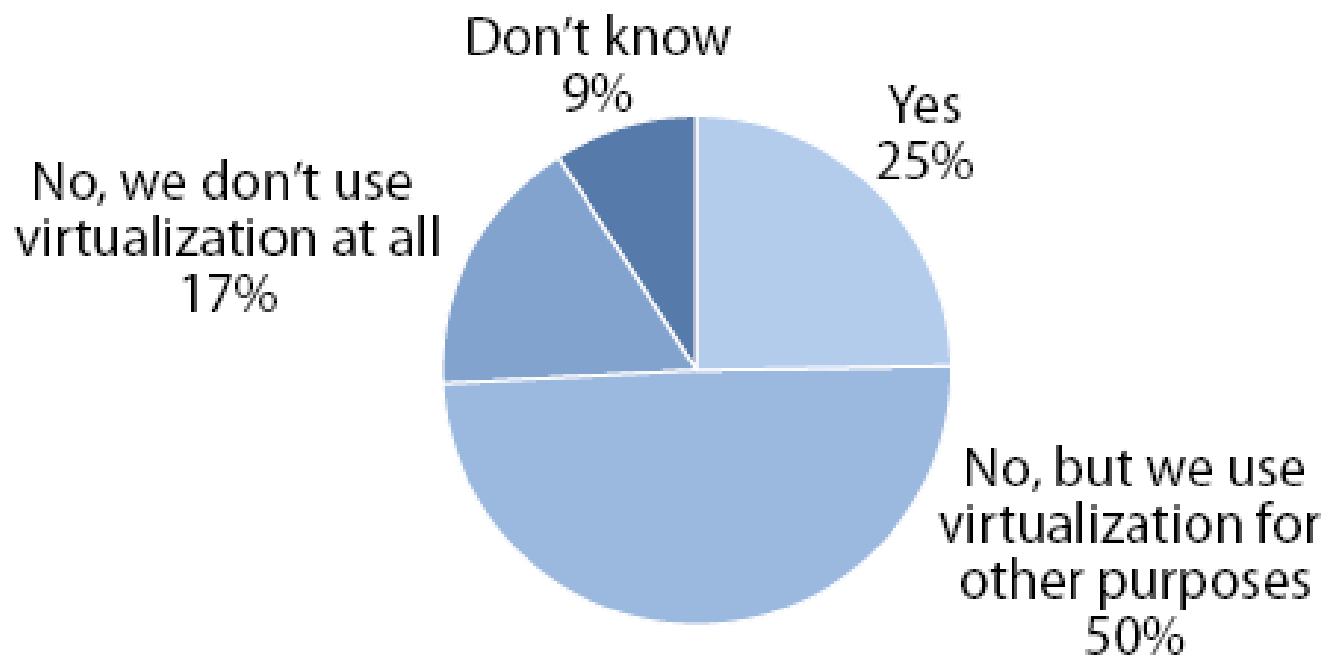
– As mentioned in *The Psychology of Security* keynote from Black Hat USA 2007

- PART IV

Security and Risk Implications

Virtualization and Security

“Do you use server virtualization to address security issues?”



Base: 93 security managers
(percentages do not total 100 because of rounding)

Source: Forrester Research, Inc.

INTEROP[®]



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

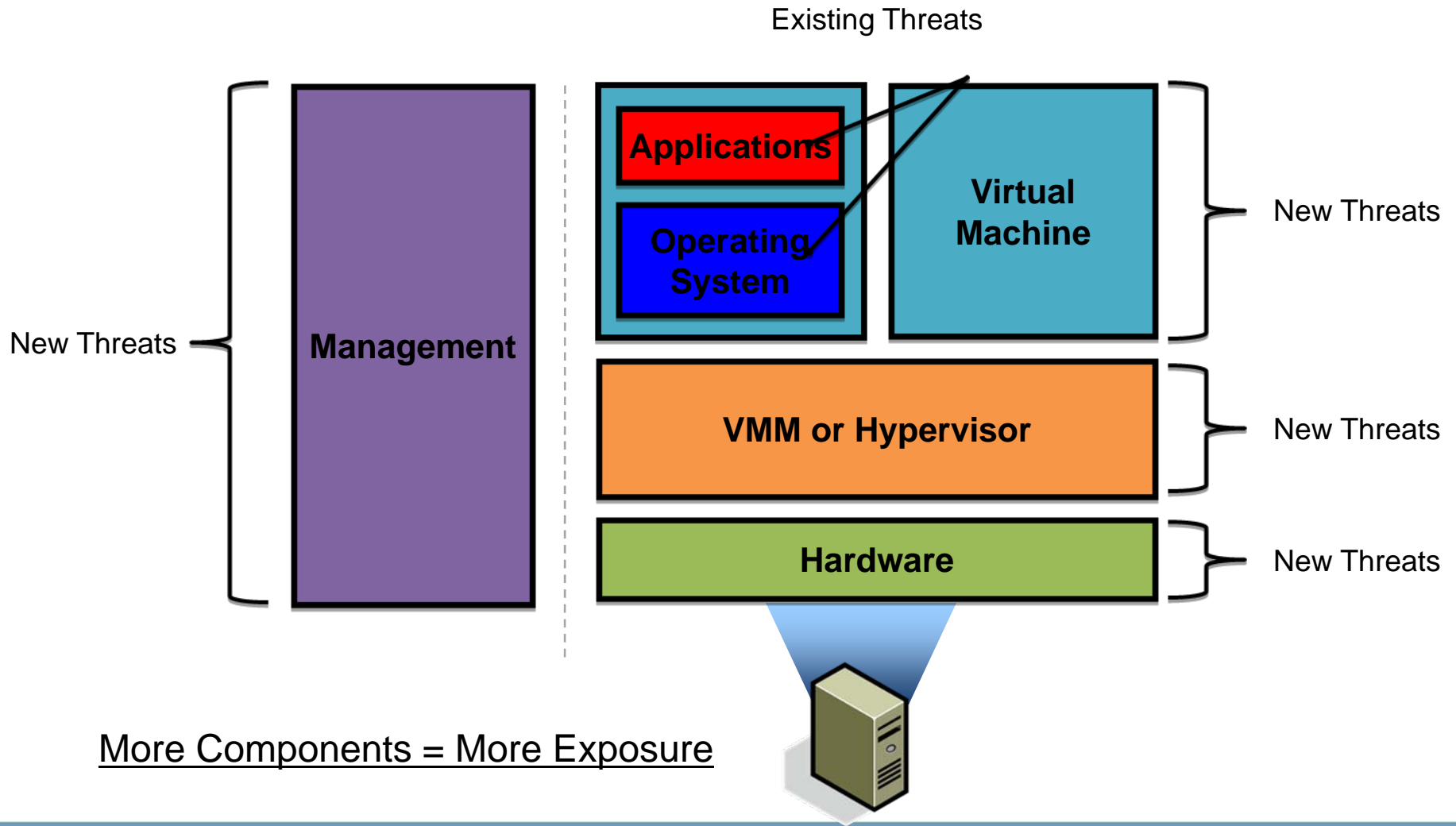
Threat Landscape

- New Swath of **Availability** Attacks
 - Owning a single guest
 - Breaking out of the guest
 - Compromise of Virtual Console/Management
 - Provision my own evil guest(s)
 - Adjust resource quotas
 - Shut OFF guest(s)
 - Compromise of the VMM/Hypervisor
 - IsGameOver()

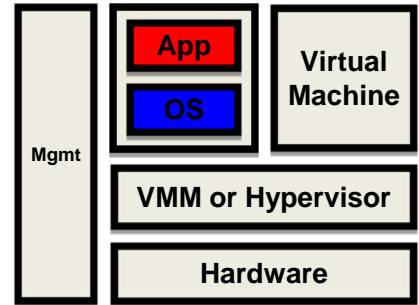
Threat Landscape (cont.)

- Other Threats...
 - Regulatory
 - Auditors
 - Org-Charts...
 - Separation of Duties
 - Politics

Points of Exposure



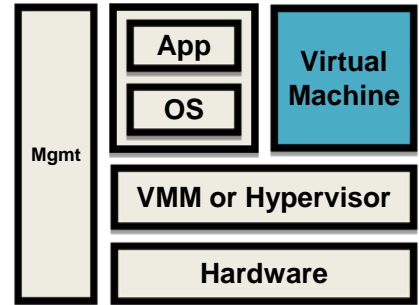
Operating Systems and Applications



- Traditional threats remain:
 - Malware: Viruses, Worms, Trojans, Rootkits
 - DoS/DDoS attacks
 - Buffer Overflows, SQL Injection, XSS
 - Data Leakage
 - Access Control, Compliance, Integrity
- Virtualized OSeS and Apps threats remain:
 - Disaster Recovery and Sandboxing are notable arguments
 - However, they do not increase native resistance to OS/Application threats

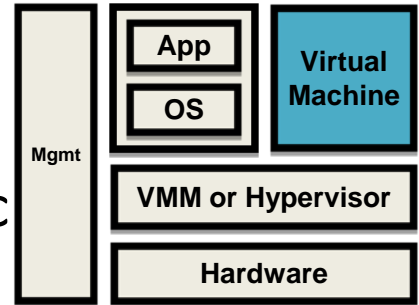
Virtual Machines

- Compliance and Patching
 - Ability to “Suspend” / “Activate” VMs alters update lifecycle.
- Virtual Sprawl and Identification
 - Difficult to keep track of VMs. Unmanaged, rogue VMs.
- Dynamic Relocation (Live Migration)
 - Are VMs moving to less secure machines, networks, datacenters, etc?
 - Static security policies no longer apply.

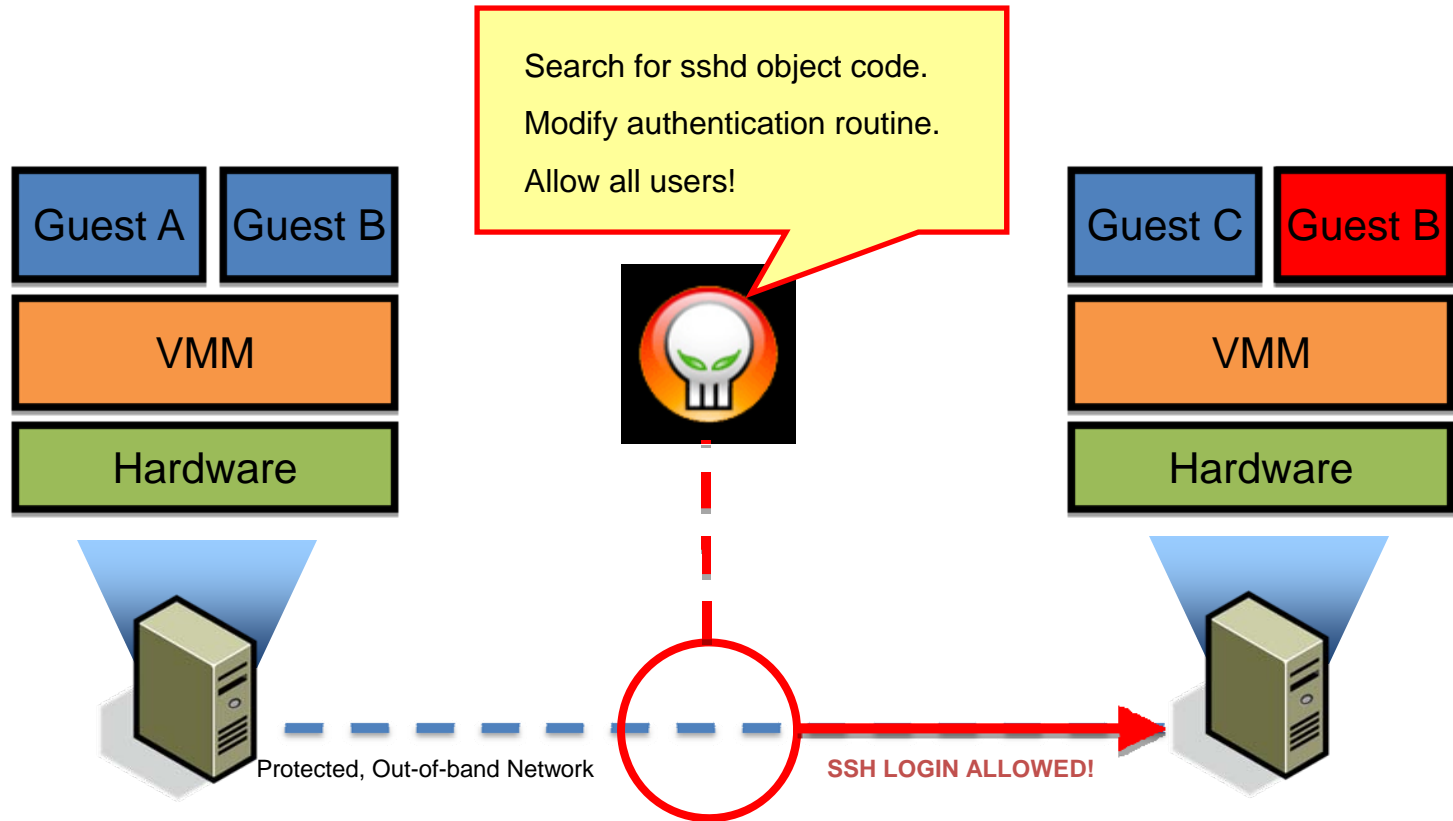


Virtual Machines (cont.)

- Replay Attacks and Data Retention
 - VM replay may foster advanced cryptographic attacks.
 - Is sensitive data being cached in unknown areas for replay purposes?
- Virtual Machine Stealing
 - VMs are just as files, its trivial to steal a full system or groups of systems.



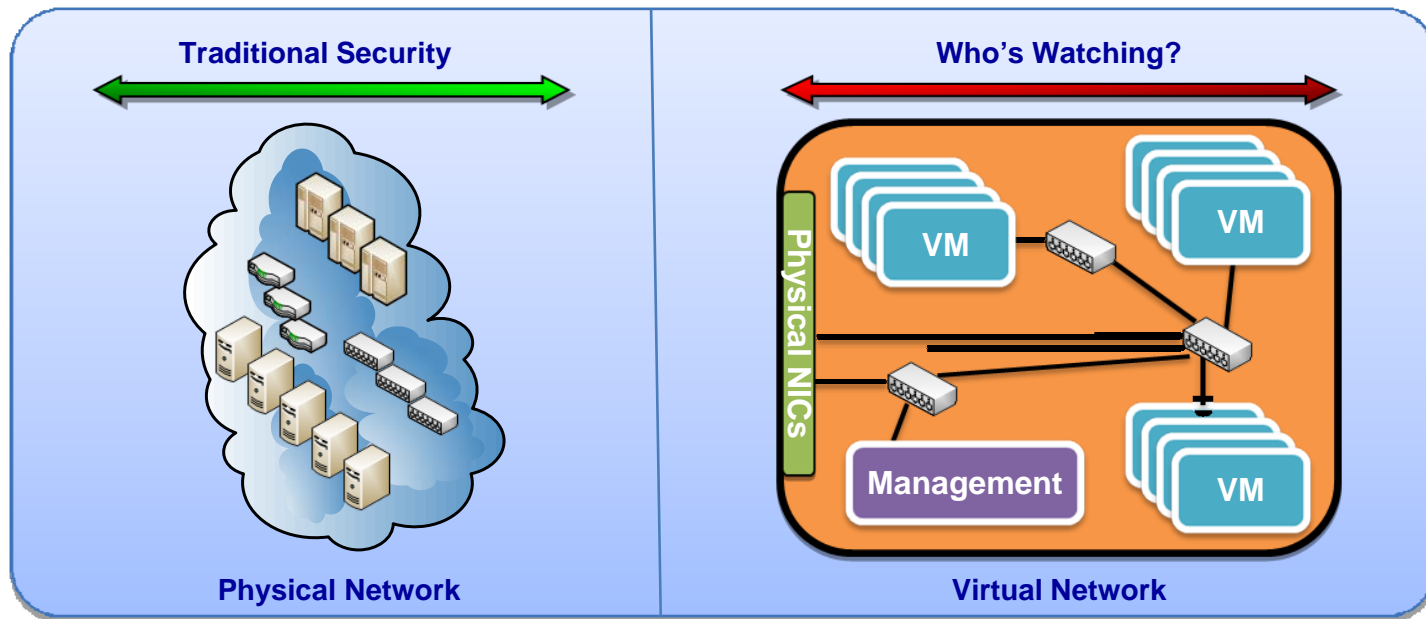
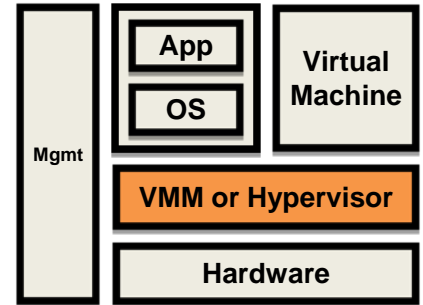
Exploiting Live Migration: Xensploit



By default, live migration traffic is sent in plain text across the network. A man-in-the-middle attack can be used to own endpoints in limitless ways.

Virtual Machine Manager / Hypervisor

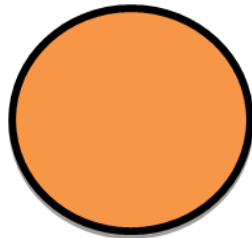
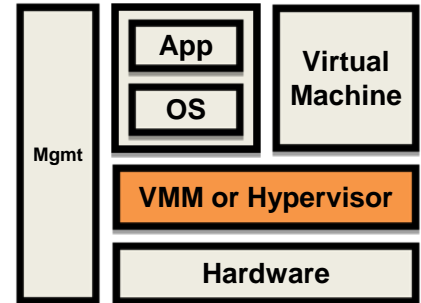
- Single Point-of-Failure/Attack
- Mandatory Access Control / Resource Sharing
 - Can we guarantee isolation, sharing and communication?
- Inter-VM Traffic Analysis:



VMM / Hypervisor (cont.)

- Attacks against the VMM / Hypervisor.

- There are going to be bugs that lead to security risks.
- Shrinking size of VMMs is good for security, but does not make them immune to risk. Features demand complex code.



VMware ESX 3
~2GB Surface Area
Lines of Code: Millions



VMware ESX 3i
~32MB Surface Area
Lines of Code: ~200,000

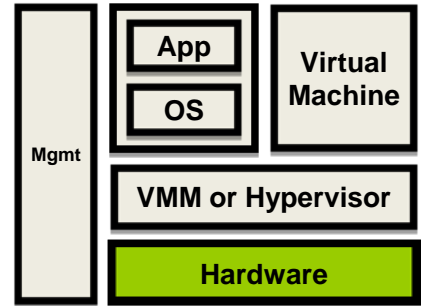
- Hypervisor Services

- Network – DHCP, vSwitching, general packet processing
- Communication – Inter-domain communication APIs (VMCI, XenSocket)
- Other Services – Security (VMsafe), Disaster Recovery (vMotion), etc.

Virtualization-Aware Hardware

- Hardware Assist (Intel-VT, AMD-V)

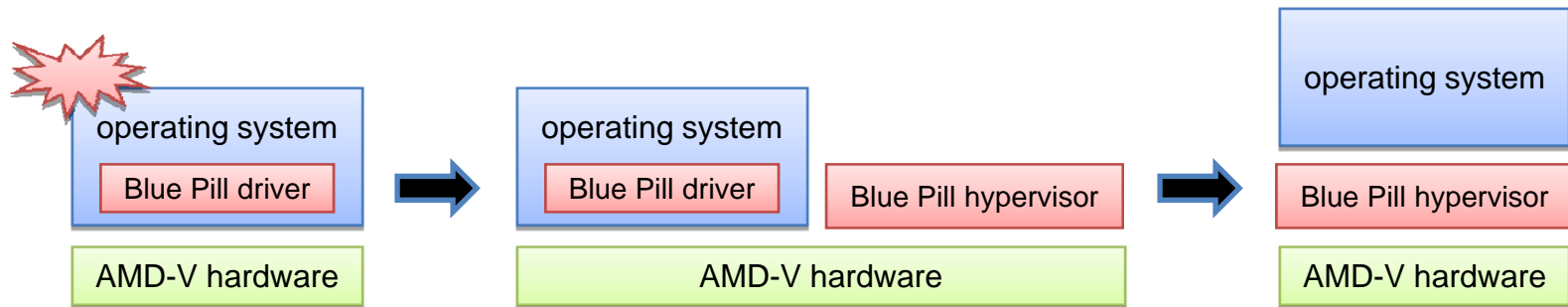
- Techniques (e.g. rootkits) with stealth capabilities.
- Low-level makes detection more difficult.
- Risk to non-virtualized deployments.
 - Blue Pill: Malicious hypervisor injection for AMD-V
 - Vitriol: Leverages Intel VT-x



- I/O Virtualization

- VMs natively share virtualization-aware I/O devices.
 - Virtual Ethernet Cards (vNICs), Virtual FC HBAs (vHBAs), etc.
- How do we secure a new class of on-demand, dynamic and virtualized allocation of resources?

HVM-based Rootkits: Blue Pill



Blue Pill exploits the OS and inserts a malicious driver into the kernel.

The driver enables SVM, sets up the VMCB, and loads the Blue Pill hypervisor into memory. Execution is transferred to the hypervisor and VMRUN is called.

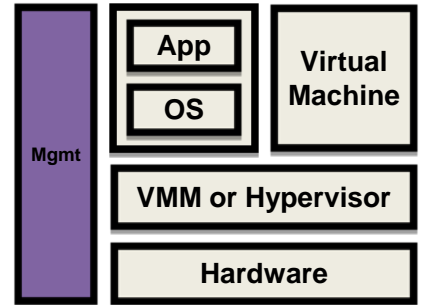
The OS now runs in a VM. Execution is transferred back to the driver for removal.

- Blue Pill requires hardware-enabled machines not running virtualization.
- Blue Pill exploits Operating System / Software bugs to install.
- **New research aims to accommodate nested virtualization.**

Management Infrastructure

- Software Threats:

- Keys to the castle.
- Vulnerabilities in management applications.
- Secure storage of Virtual Machines and management data.

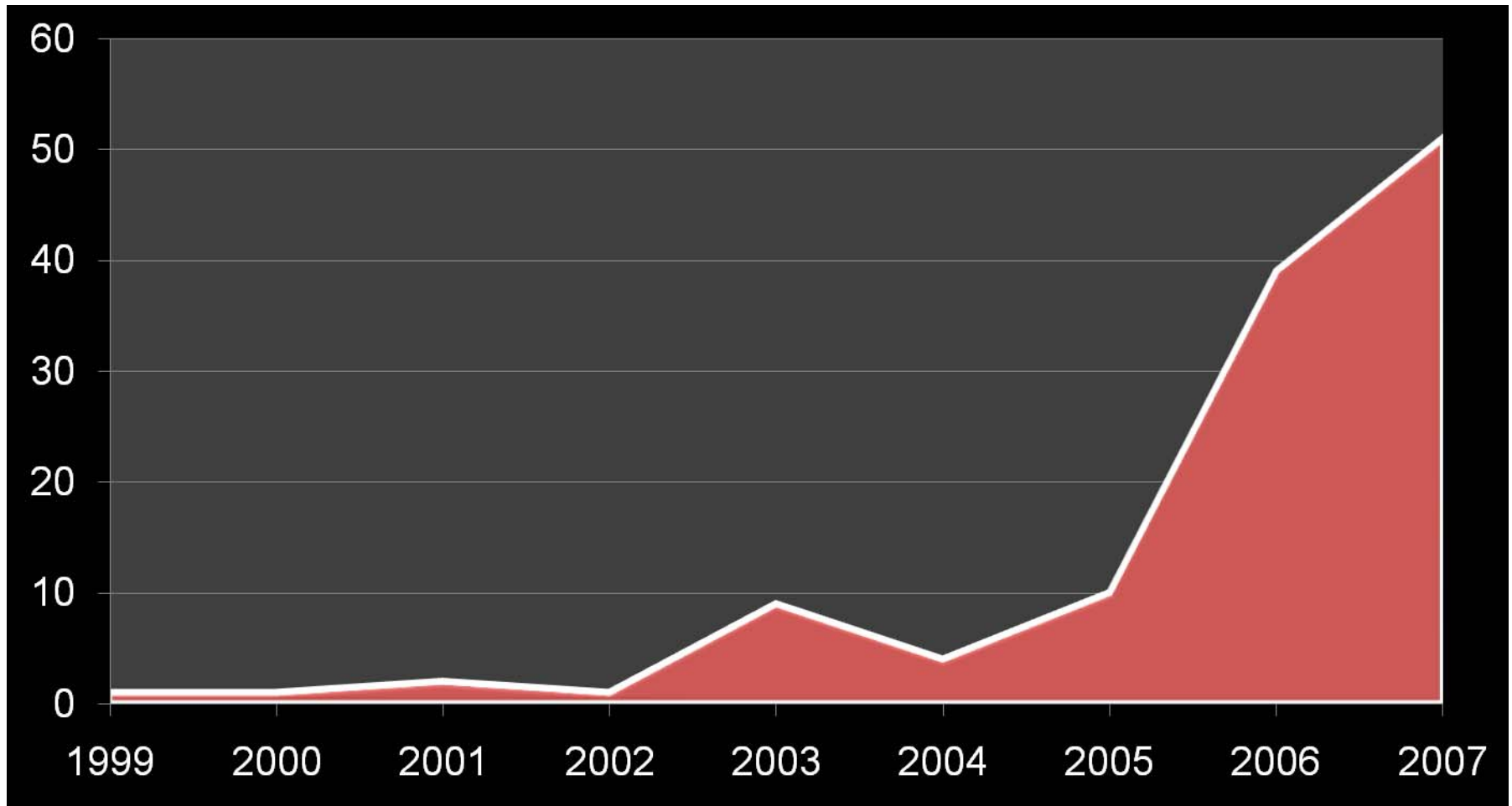


- Operational Threats:

- Managing risk requires new technology, skills and expertise.
- We now also factor the extremely dynamic nature of virtualization into our evaluation of overall risk.

Vulnerabilities by Year

XFDB Search: VMware, Xen, Virtual PC, QEMU, Parallels, etc.



Take-aways: Threat Landscape

- Virtualization introduces significant technological and operational risks. It also changes and/or intensifies old risk.
- Virtualization platforms will become the will become the target of choice of the research/hacker community in the years to come.
- The popularity, complexity, and immaturity of x86 virtualization make it very likely that new hypervisor-compromising malware, attacks on management infrastructure, and other malicious activity will make headlines very soon.

- PART V

Operational and Organizational Implications

Operational & Organizational

“The real problem of security in a virtualized world is not technical, it is organizational and operational.

With the consolidation of applications, operating systems, storage, information, security and networking -- all virtualized into a single platform rather than being discretely owned, managed and supported by (reasonably) operationally-mature teams -- **the biggest threat we face in virtualization is now we have lost not only visibility, but the clearly-defined lines of demarcation garnered from a separation of duties we had in the non-virtualized world.”**

Chris Hoff

The Challenge of Virtualization Security: Organizational and Operational, NOT Technical

<http://rationalsecurity.typepad.com/blog/2008/03/the-challenge-o.html>

INTEROP[®]



Organizational Ownership?

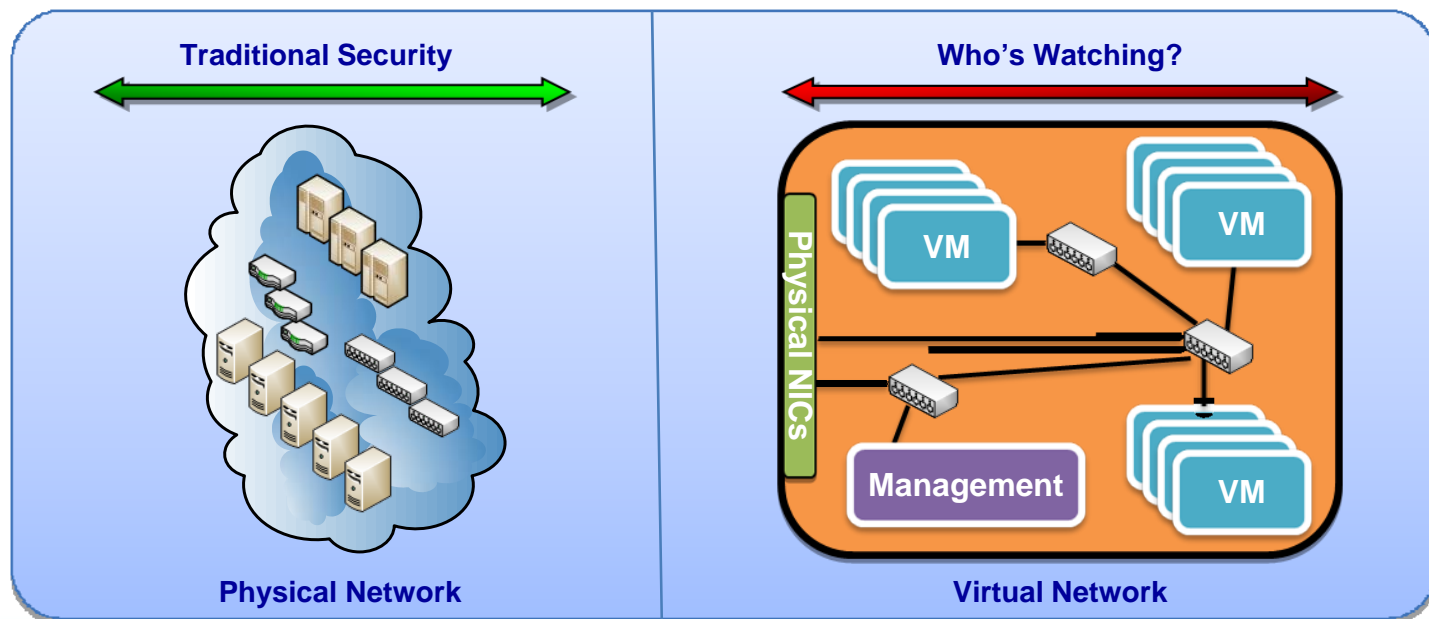
- Who owns the Virtual [Fill in the Blank] ?

Network Admin

Server Admin

Application Owners

Data Custodians



Organizational Ownership?

- Traditional disciplines and functions still require competence
- Separation/Segregation of Duties remains critically important
- Care and Feeding of the Virtual Infrastructure will also be required
 - Are you likely to have a mix of Physical and Virtual Servers?
 - Are you likely to have a heterogeneous mix of Virtual platforms?

Politics

- “Turf Wars” and “Land Grabs” are possible
- “Hot Potato” is also possible
- “Finger Pointing” is probable



New Operational Challenges

- Find the Server...
 - Live Migration makes servers harder to track
- Configuration/Patch Management
 - Pause/Offline features impact:
 - Audits
 - Scanning
 - Patching
 - Boot Prone?
- Image Management
 - Storage
 - Version Control



Operational Controls

- Discipline, Discipline, Discipline
- What are your policies for use of Virtualization?
 - Which Servers can be clustered?
 - Which Servers cannot be clustered?
- What are your controls for provisioning?
 - Easy to slip into Virtual Sprawl
 - Two Key System?

•PART VI

Common Mistakes

Elective Risk

- Never use Type 2 Server Virtualization for Production
 - True Story...
- These “Free” versions of the platform are meant for Testing
- Type-2 VMM specific vulnerabilities

Failure to Establish Policy

Before it gets away from you...

- Establish Clear Use Guidelines
- Establish Clear Roles & Responsibilities
- Establish Controls for Provisioning
- Establish Intelligent Image Management
- Establish Security Guidelines
- Establish Compliance Requirements

Failure to Consider Compliance

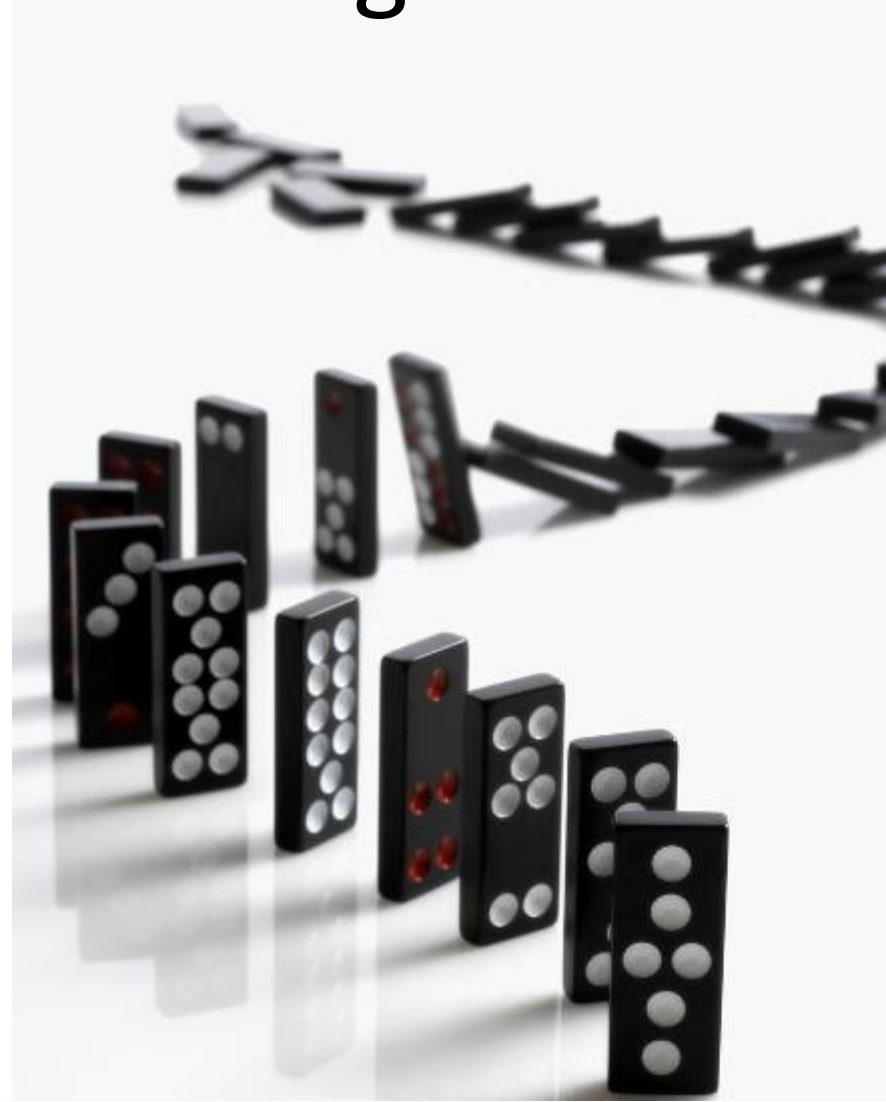
- Will you still be PCI Compliant?
 - Consult your Auditors **Early and Often**
- PCI DSS 2.2.1 states: **“Implement only one primary function per server”**
 - How does your auditor interpret this?
 - What I’ve seen...
- Anticipate Future Regulatory Granularity
 - Right now Virtualization is ahead of Compliance

Failure to Involve Security

- By default, Virtualization reduces your security posture
 - New attack surfaces
 - New operational risks
 - New availability risks
 - Increased complexity that comes with beneficial features
 - E.g. Live Migration
- Security Analysis/Design can inform smart compensating controls and best practices while countermeasures mature

Failure to Control Live Migration

- Cascading Failover Example
 - True Story...
- We often overlook the fluid realities of Live Migration
 - E.g VMotion



Failure to Performance/Capacity Plan

- Virtualization is not devoid of bottlenecks
- Proper Capacity planning is often overlooked
 - This is exacerbated by the Live Migration
 - Bottlenecks often appear far earlier than expected
 - See Hoff's ***"The Four Horsemen Of the Virtualization Security Apocalypse"***
 - <http://rationalsecurity.typepad.com/blog/2008/04/the-four-horsemen.html>
 - <http://rationalsecurity.typepad.com/blog/2008/08/complete-slides.html>

“Silver Bullet” Virtual Appliances

- Today’s Virtual Security Appliances are very nascent
 - Coverage is limited (I will explain)
 - There is NO Silver Bullet
 - Buzz Words and Snake Oil abound
 - Realistic expectations can help reduce over-confidence in these products
- Security will improve as Virt Platforms release their Security APIs and as Security Vendors leverage them

•PART VI

What Can I Do?

Integrated Protection Solutions

- **Virtualization Security has many attributes:**
 - Virtual security services vs. securing the platform vs. [securing VMs](#).
- **Securing VMs requires unique capabilities.**
 - Future solutions should offer the granularity, visibility, correlation and scalability required to properly secure virtual machine deployments.
- **Leverage the hypervisor**
 - Use the VMM to understand/modify VMs and the virtual environment:
 - [Memory and CPU](#): View/Alter VM memory pages and CPU states.
 - [Networking](#): Inspect network packets before they reach the VM.
 - [Process execution](#): Protect and intersect with guest user-level agents.
 - [Storage](#): Mount, manipulate and modify VM storage devices.

Integrated Protection Solutions (cont.)

- **Move towards integrated and automated solutions**
 - Move beyond virtual form-factor solutions.
 - Find optimal analysis points to reduce redundancy and overhead.
 - Automate discovery and security provisioning.
- **Minimize footprint and impact on performance/visibility**
 - Include Guest OS presence on necessary components.
- **Transparency throughout fail-over and migration**
 - Solutions must be as dynamic as the virtual environment.
 - security follows virtual machines (e.g. VMotion)
- **Multiple layers (Defense-in-depth)**
 - Risk mitigation solution combines compliance, data security, isolation, access control and threat mitigation.

Securing Virtualization: Today

First Generation Virtualization Security:

- Install security in each guest VM.
- Apply defense-in-depth.
- Lock-Down Management.
- Segment networks with VLANs.
- Use stand-alone security appliances.

Potential Limitations:

- New VMs need security provisioning.
- Redundant security = more resources.
- Management nightmare.
- Inter-VM network traffic analysis.
- Implicit trust in the VMM

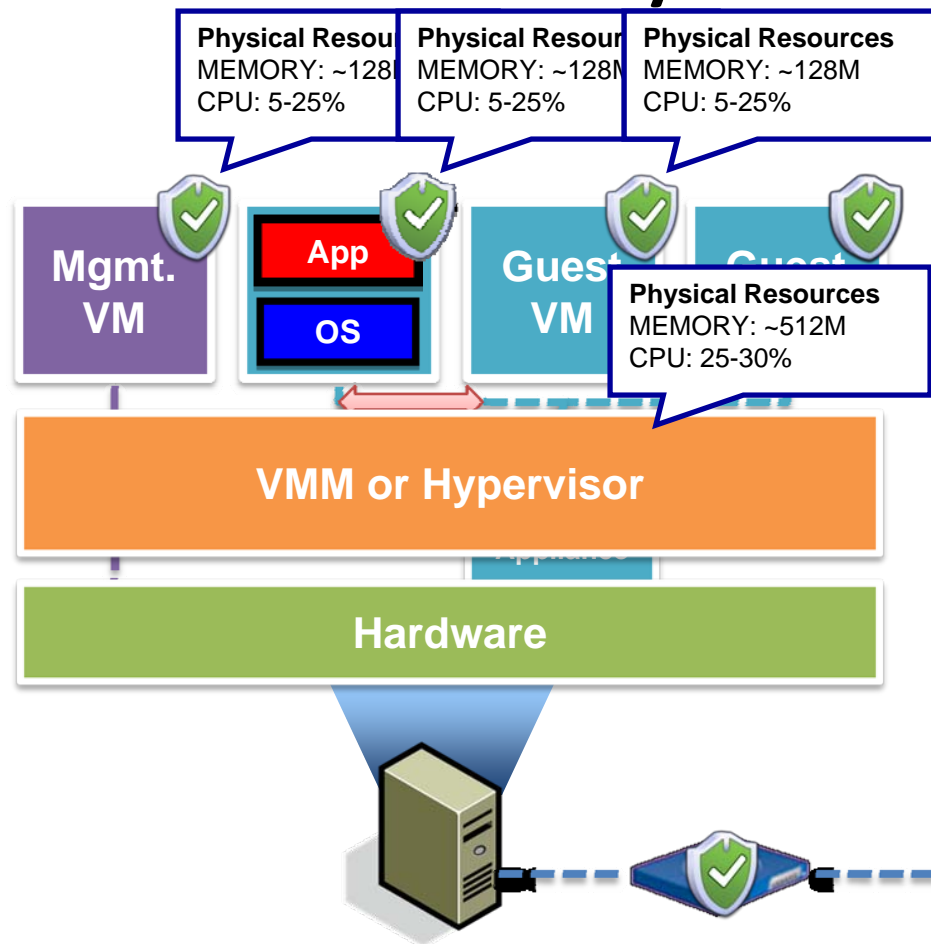


CPU



Memory

We can do better! - Integrate security into the Virtual infrastructure, don't bolt it on.



Securing Virtualization: Tomorrow

Next Generation Virtualization Security:

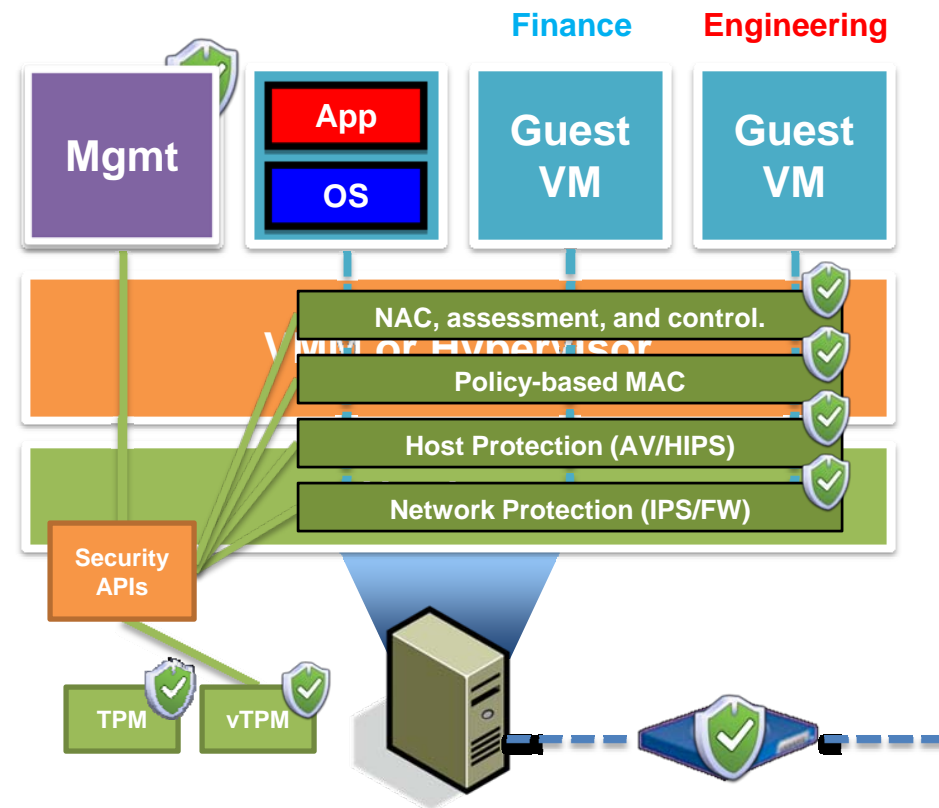
- Apply defense-in-depth.
- Shrink the management stack.
- Install Security VM on each machine.
- Integrate Security VM with VMM.

Security VM Features:

- Centralized network protection.
- Agent-less host protection.
- Policy-based MAC and isolation.
- VM NAC, assessment, and control.

Additional Security:

- Hypervisor attestation (TPM)
- VM attestation (vTPM)



Further Reading

- Chris Hoff's BLOG "Rational Survivability"
 - <http://rationalsecurity.typepad.com/blog/>
 - <http://rationalsecurity.typepad.com/blog/virtualization/index.html>
 - Ongoing Virtualization Thought Leadership
- Neil MacDonald of Gartner
 - Several Excellent Research Notes
- X-Force Threat Research
 - http://www.iss.net/x-force_threat_insight_monthly/index.html
 - <http://blogs.iss.net/>
- Center for Internet Security Benchmarking
 - http://www.cisecurity.org/bench_vm.html

Joshua Corman
Principal Security Strategist
IBM Internet Security Systems
jcorman@us.ibm.com

INTEROP[®]

