



# Securing Virtualised Environments

Craig Lawson

## PulseANZ2010

Meet the people who can help  
advance your infrastructure





## Agenda

- Introduction to Virtualization
- 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



# Introduction to Virtualisation



## Basics: Disruptive Innovation

Virtualization is a **Disruptive Innovation**

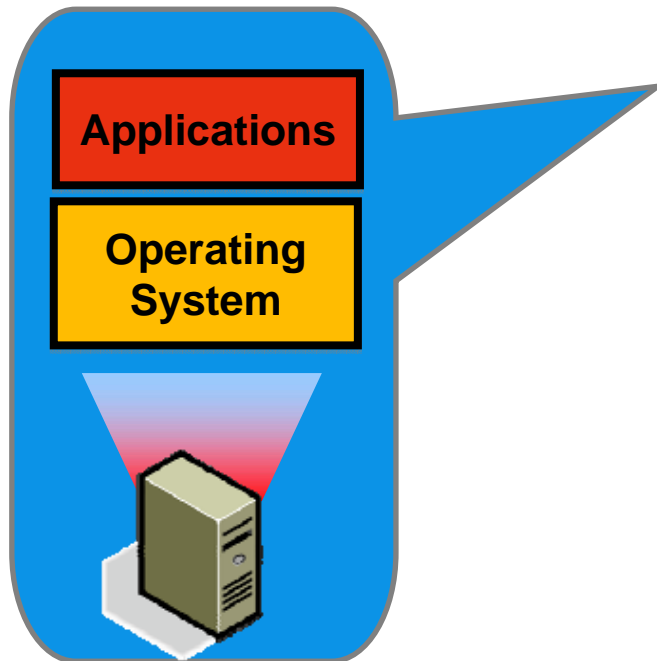
Virtualization:

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.

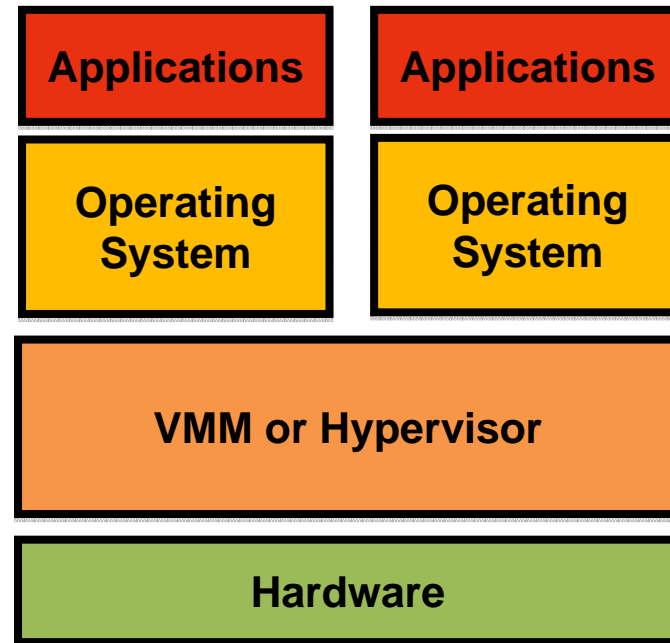


# Basics: Virtualization Architecture

Before Virtualization

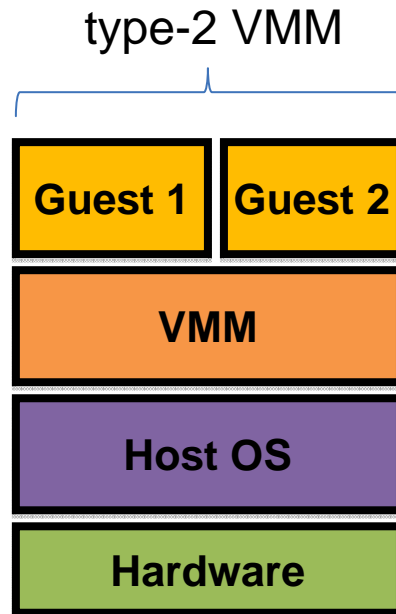


After Virtualization



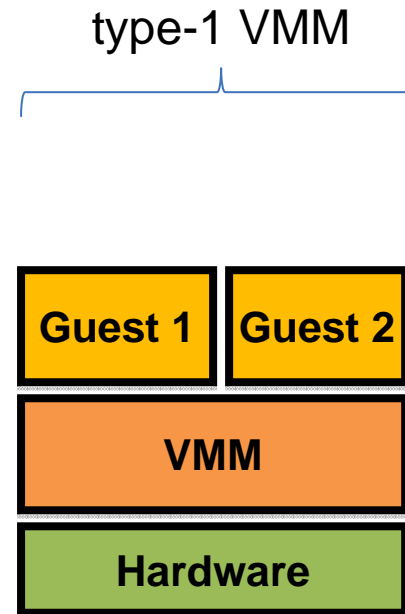


# Basics: Virtualization Types



Examples:

KVM (Linux)  
VMware Workstation  
VMware Server  
Microsoft Virtual PC



Examples:

Xen  
VMware ESX  
IBM pHype / LPARs  
Microsoft Hyper-V



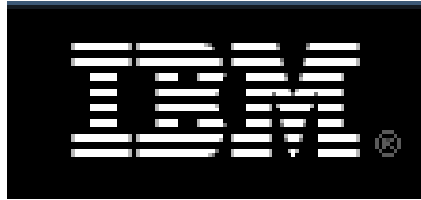
## What does Virtualization Change?

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





## Major Players



- Founded in 1998
- Division of EMC



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



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



- Virtual server, acquired VirtualPC in 2003 from Connectix
- Hyper-V



- Based on open-source Xen hypervisor





# Security and Risk Implications



## 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

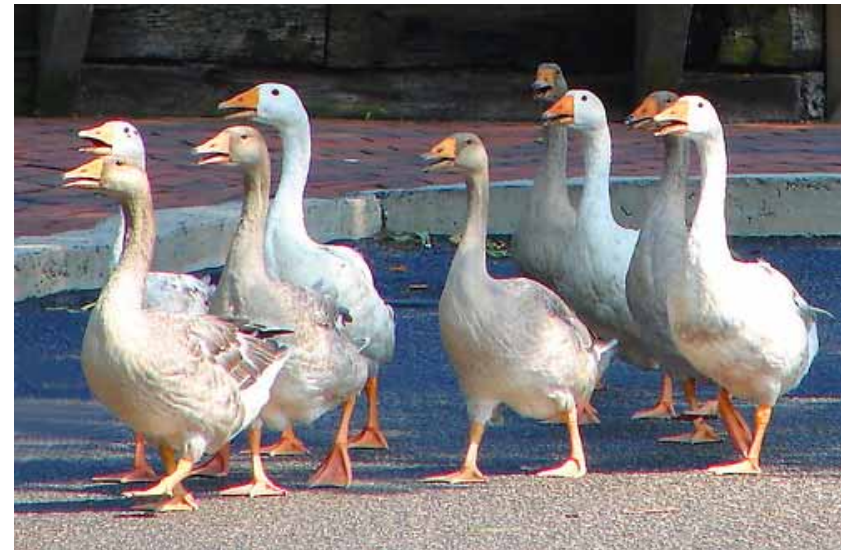
- New Swath of **Availability** Attacks
  - Owning a single guest
  - Breaking out of the guest
  - Guest theft
  - Compromise of Virtual Console/Management
    - Provision my own evil guest(s)
    - Adjust resource quotas
    - Shut OFF guest(s)
  - Compromise of the VMM/Hypervisor
    - IsGameOver()





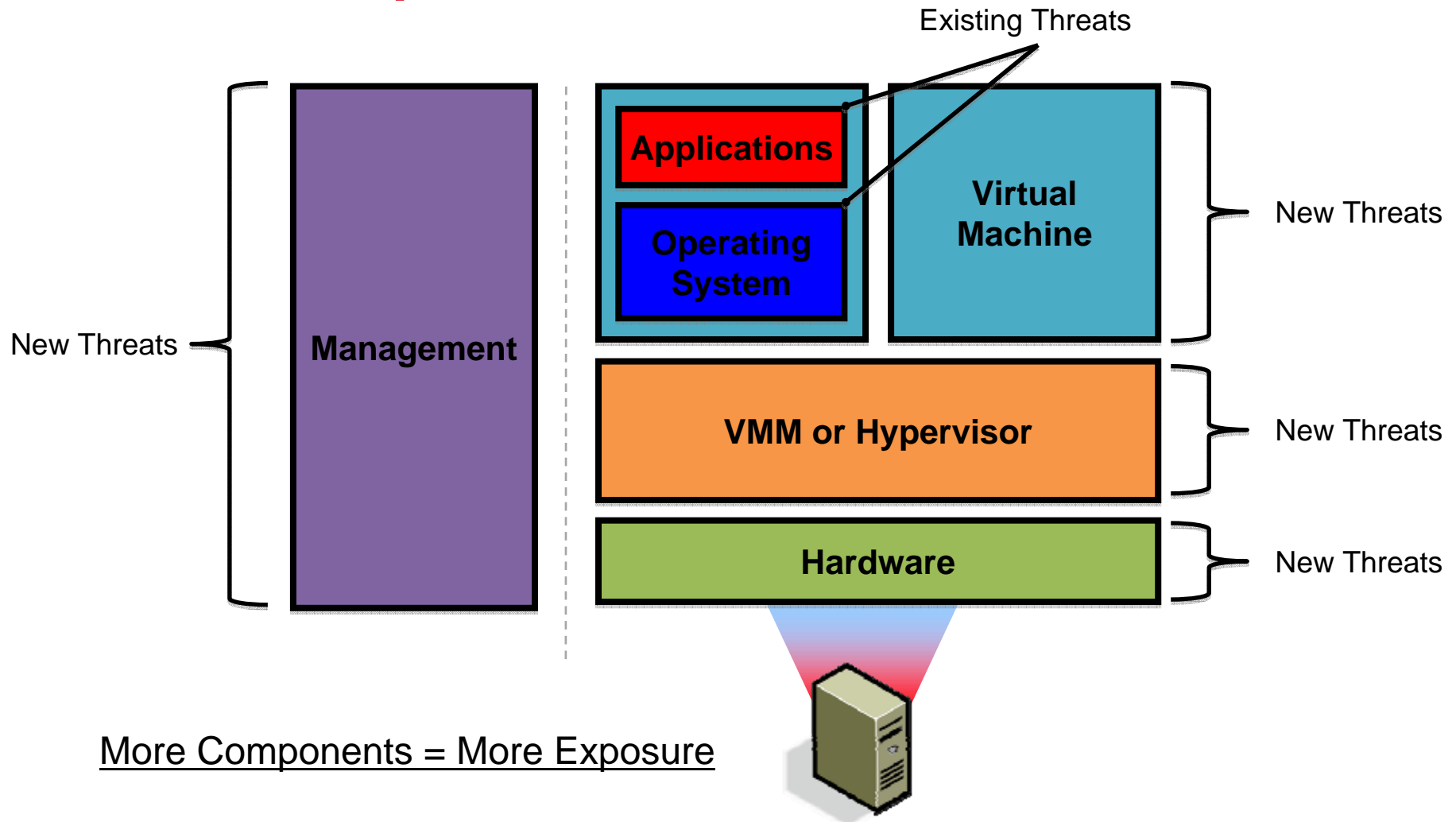
## Threat Landscape (cont.)

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





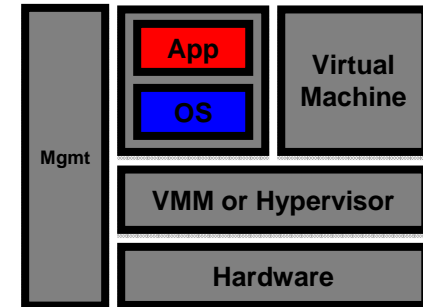
# Points of Exposure





# 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

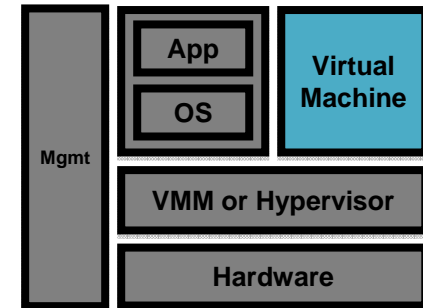






# Virtual Machines

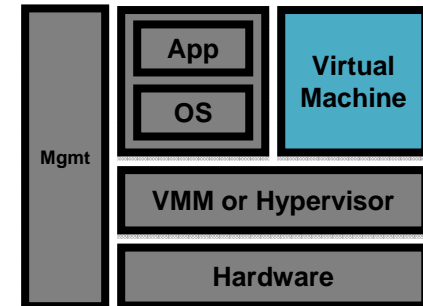
- Compliance and Patching
  - Ability to “Suspend” / “Activate” VMs alters update lifecycle.
- Virtual Sprawl and Identification
  - Difficult to keep track of VMs. Unmanaged, rogue VMs.
- Dynamic Relocation (Live Migration)
  - Are VMs moving to less secure machines, networks, datacenters, etc?
  -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





## Virtual Machines (cont.)

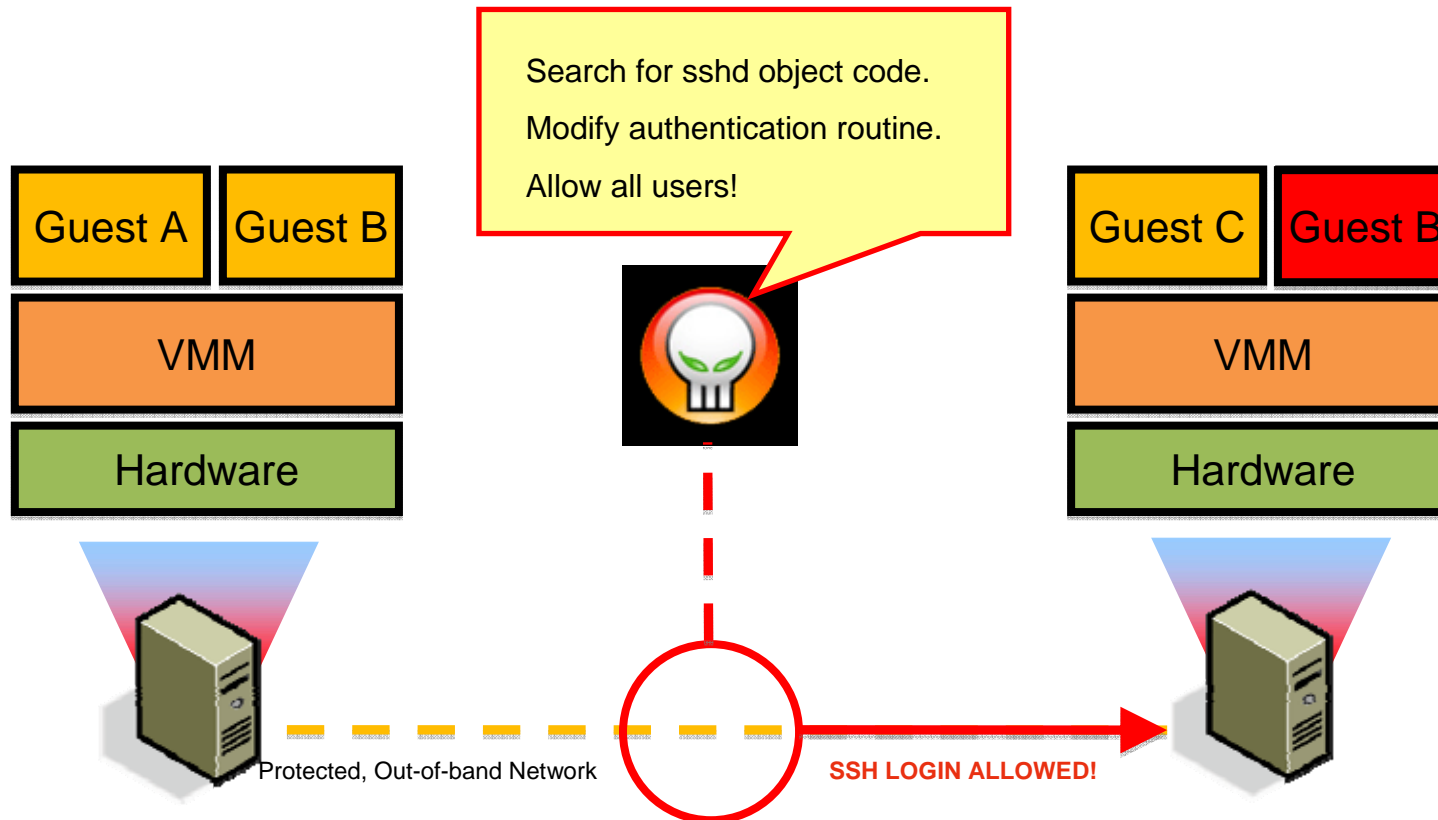
- Replay Attacks and Data Retention
  - VM replay may foster advanced cryptographic attacks.
  - Is sensitive data being cached in unknown areas for replay purposes?
- Virtual Machine Stealing
  - VMs are just files, its trivial to steal a full system or groups of systems.







# Exploiting Live Migration: Xensploit

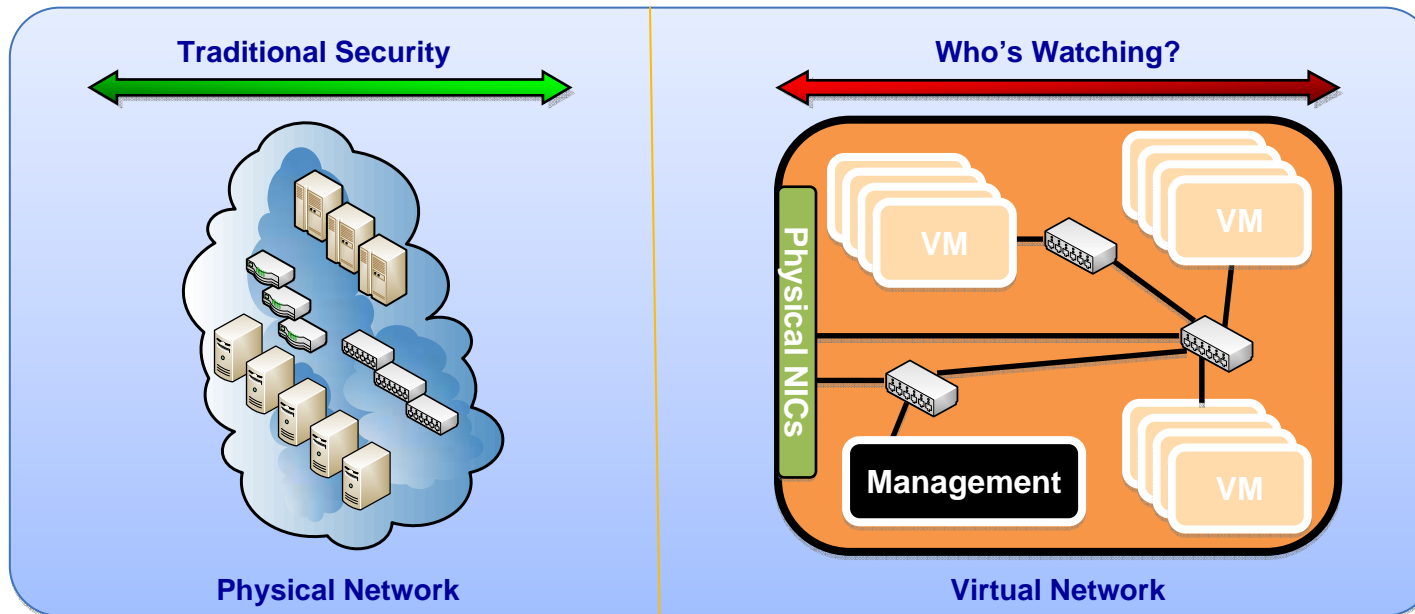
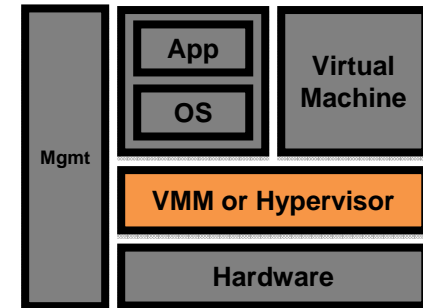


By default, live migration traffic is sent in plain text across the network.  
A man-in-the-middle attack can be used to own endpoints in limitless ways.



# Virtual Machine Manager / Hypervisor

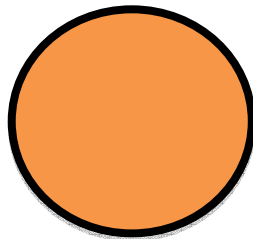
- Single Point-of-Failure/Attack
- Mandatory Access Control / Resource Sharing
  - Can we guarantee isolation, sharing and communication?
- Inter-VM Traffic Analysis:





## 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.



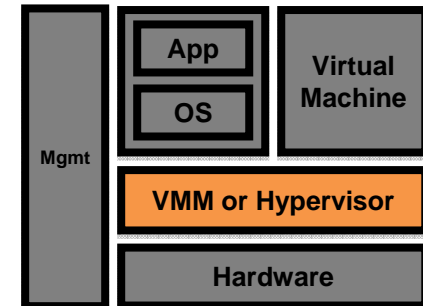
VMware ESX 3  
~2GB Surface Area  
Lines of Code: Millions



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

- Hypervisor Services

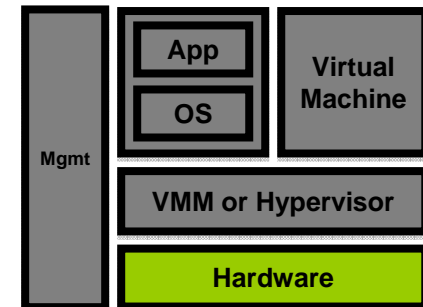
- Network – DHCP, vSwitching, general packet processing
- Communication – Inter-domain communication APIs (VMCI, XenSocket)
- Other Services – Security (VMsafe), Disaster Recovery (vMotion), etc.





# 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?





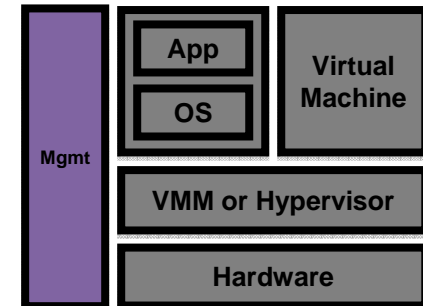
# Management Infrastructure

- Software Threats:

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

- Operational Threats:

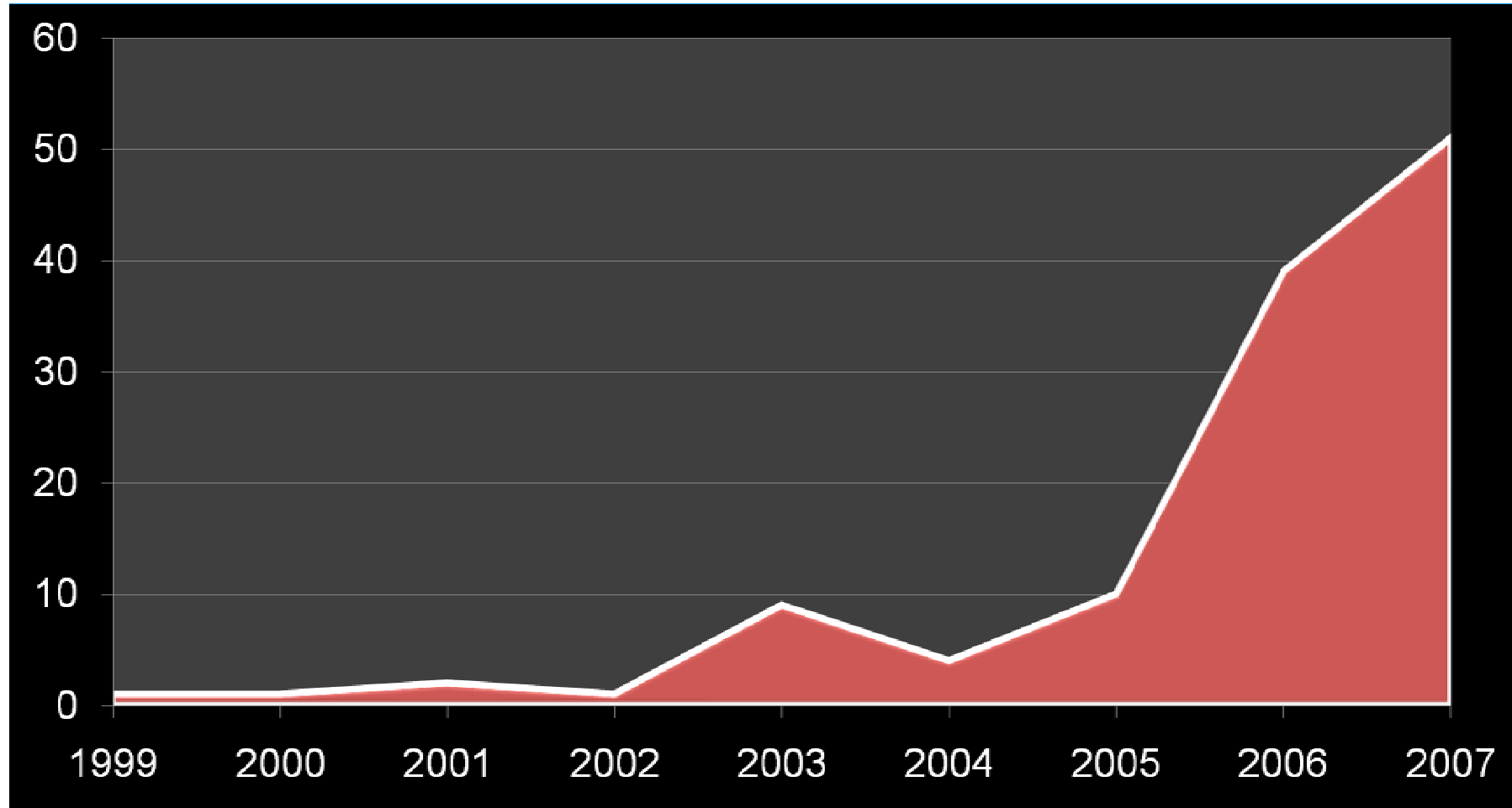
- Managing risk requires new technology, skills and expertise.
- We now also factor the extremely dynamic nature of virtualization into our evaluation of overall risk.





# Vulnerabilities by Year

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





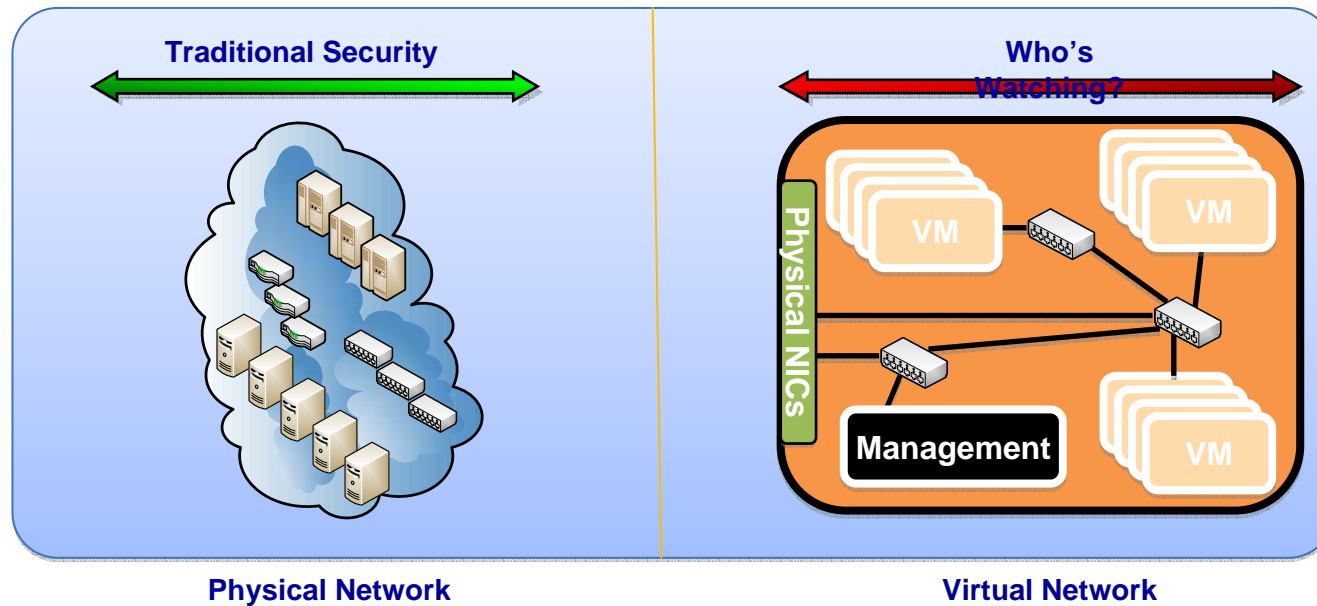
# Operational and Organizational Implications





# 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 of Ownership

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





## New Operational Challenges

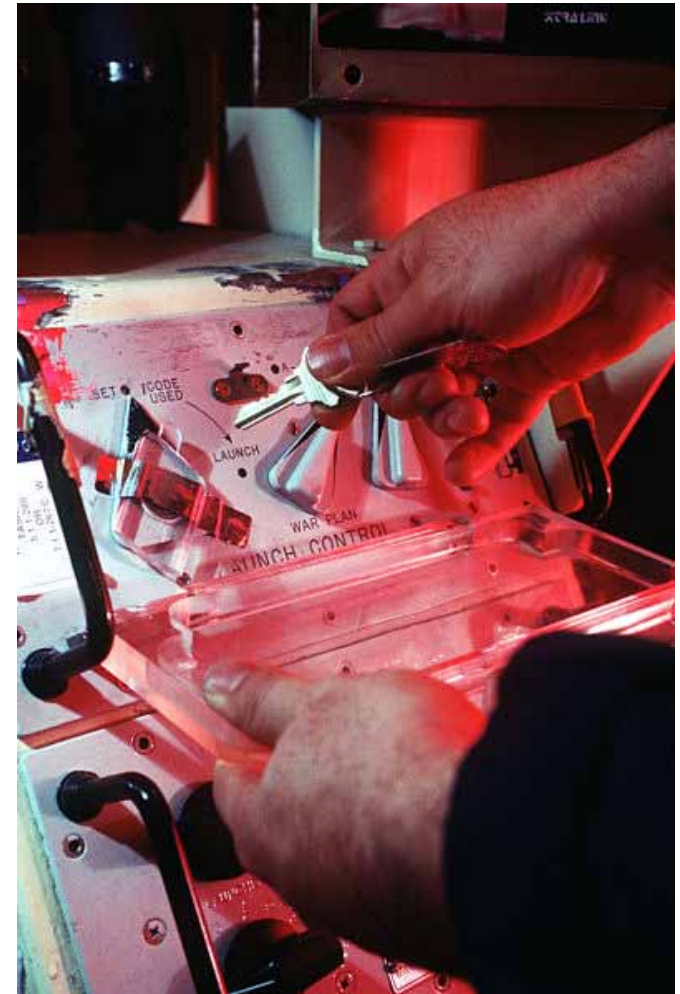
- Find the Server...
  - Live Migration makes servers harder to track
- Configuration/Patch Management
  - Pause/Offline features impact:
    - Audits
    - Scanning
    - Patching
  - Boot Prone?
- Image Management
  - Storage
  - Version Control





## 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?





# Common Mistakes



## Elective Risk

- Understand the inherent differences in Type 2 vs Type 1 Virtualization for Production
- 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

- Anticipate Future Regulatory Granularity
  - Right now Virtualization is ahead of 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?







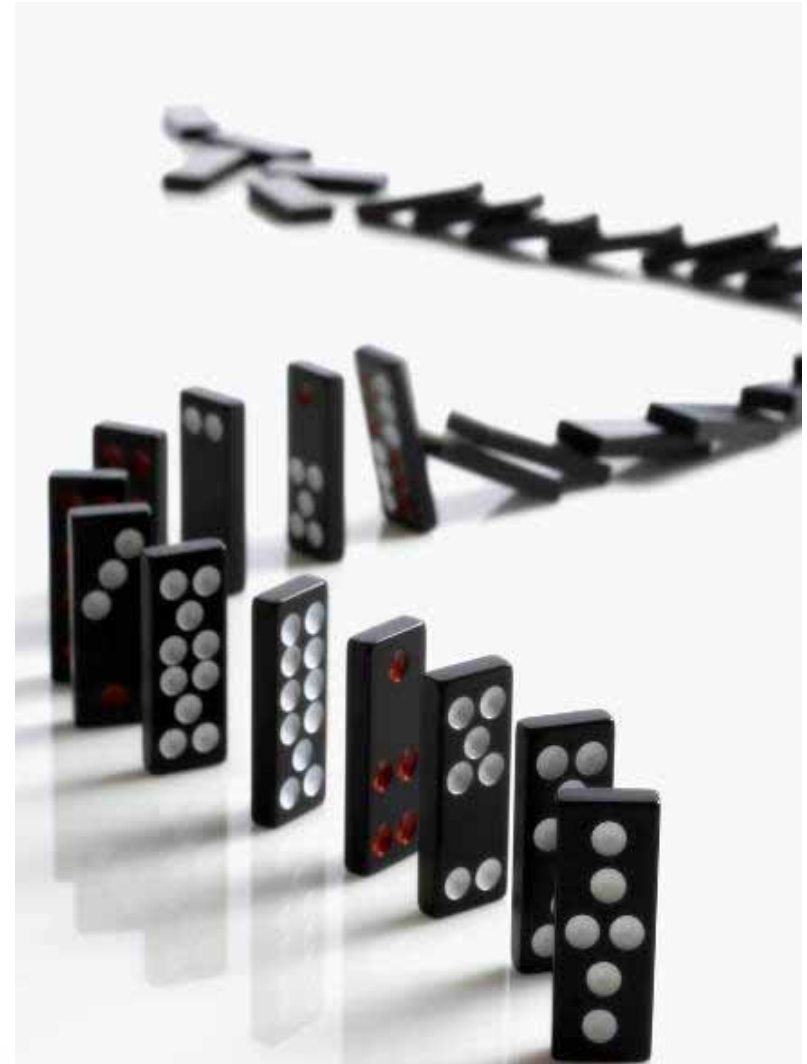
## Failure to Involve Security

- 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





## “Silver Bullet” Virtual Appliances

- Today’s Virtual Security Appliances are very nascent
  - Coverage is limited
  - 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 Virtual Platforms release their Security APIs and as Security Vendors leverage them



**What Can I Do?**



# 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





# Traditional Security in the Virtual Environment

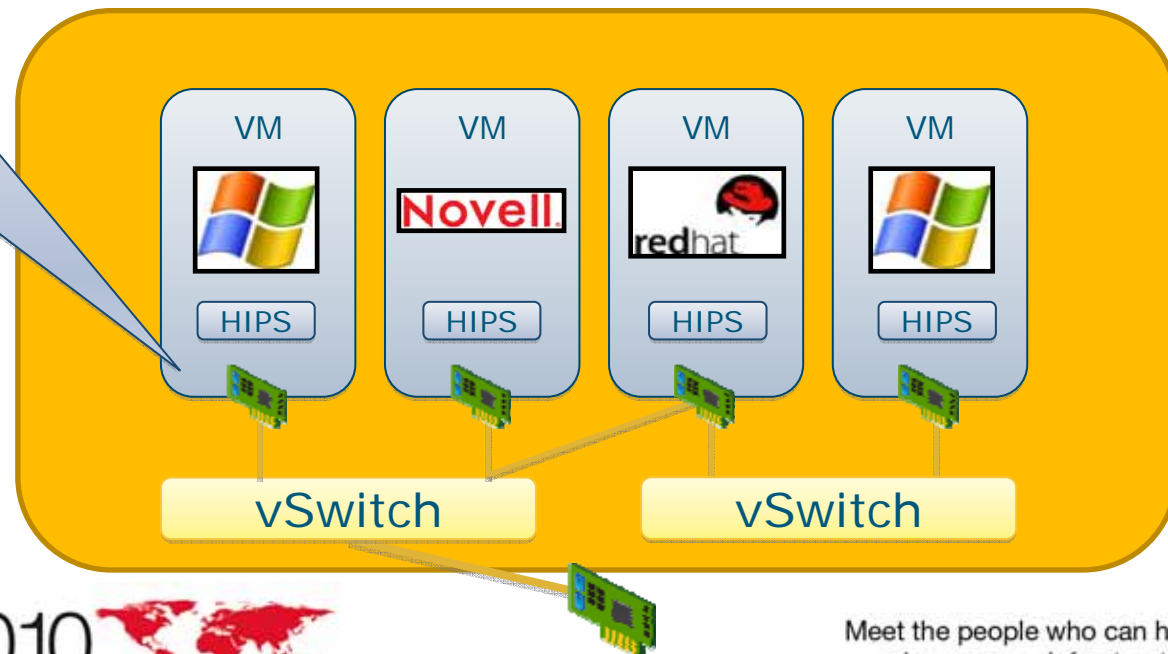
	Seems Secure .....	Not Secure Enough
Network IPS	Only blocks threats and attacks at the perimeter	Should protect against threats at perimeter and between VMs
Server Protection	Secures each physical server with protection and reporting for a single agent	Securing each VM as if it were a physical server adds time, cost and footprint
System Patching	Patches critical vulnerabilities on individual servers	Needs to protect against vulnerabilities that result from VM state changes
Security Policies	Policies are specific to critical applications in each network segment and server	Policies must be able to move with the VMs



## Host-Based IPS

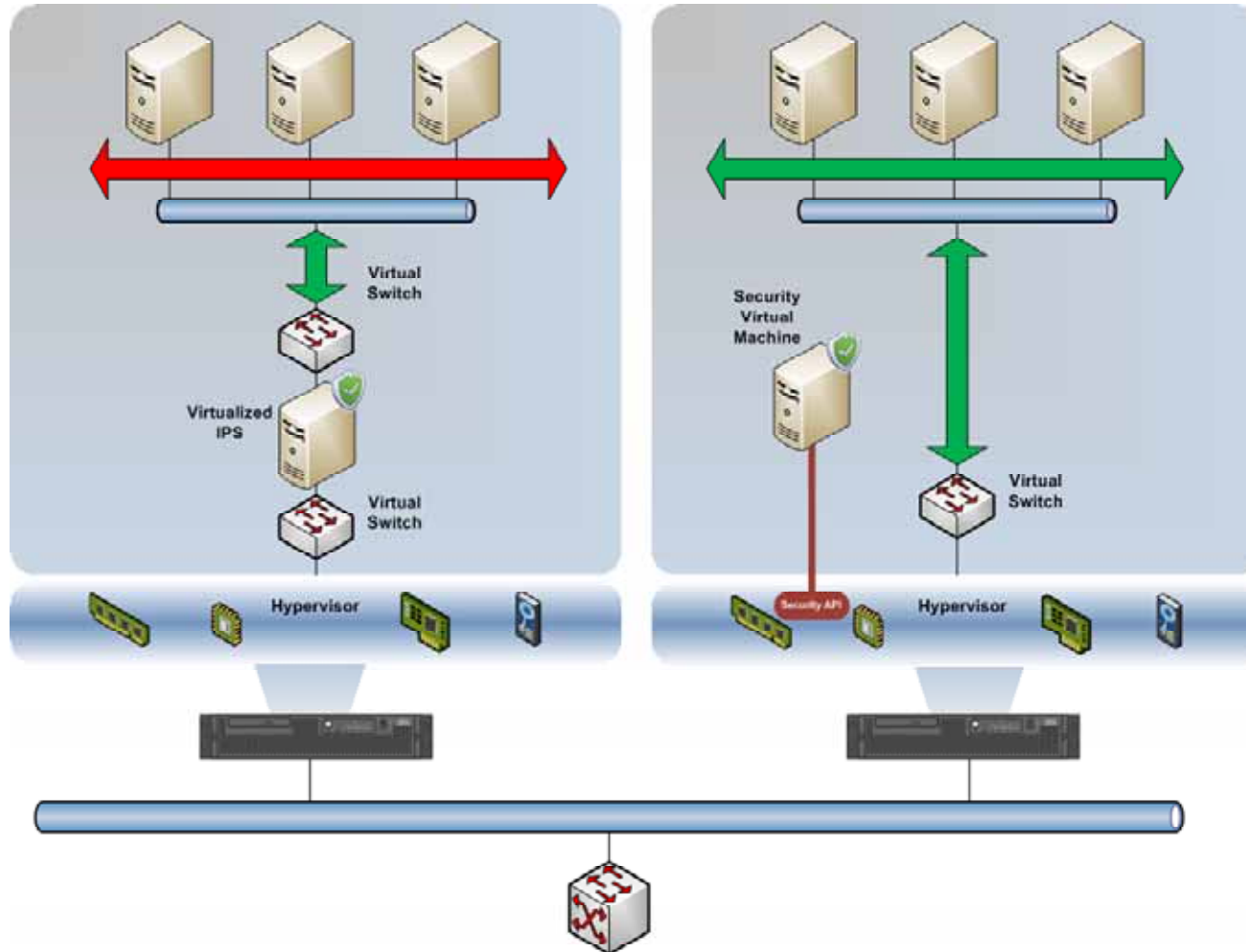
- Captures inter-VM communication...
  - IF host agent is installed
- Larger “total” footprint on a hypervisor

- Firewall
- Intrusion Prevention
- Audit log monitoring
- File integrity monitoring





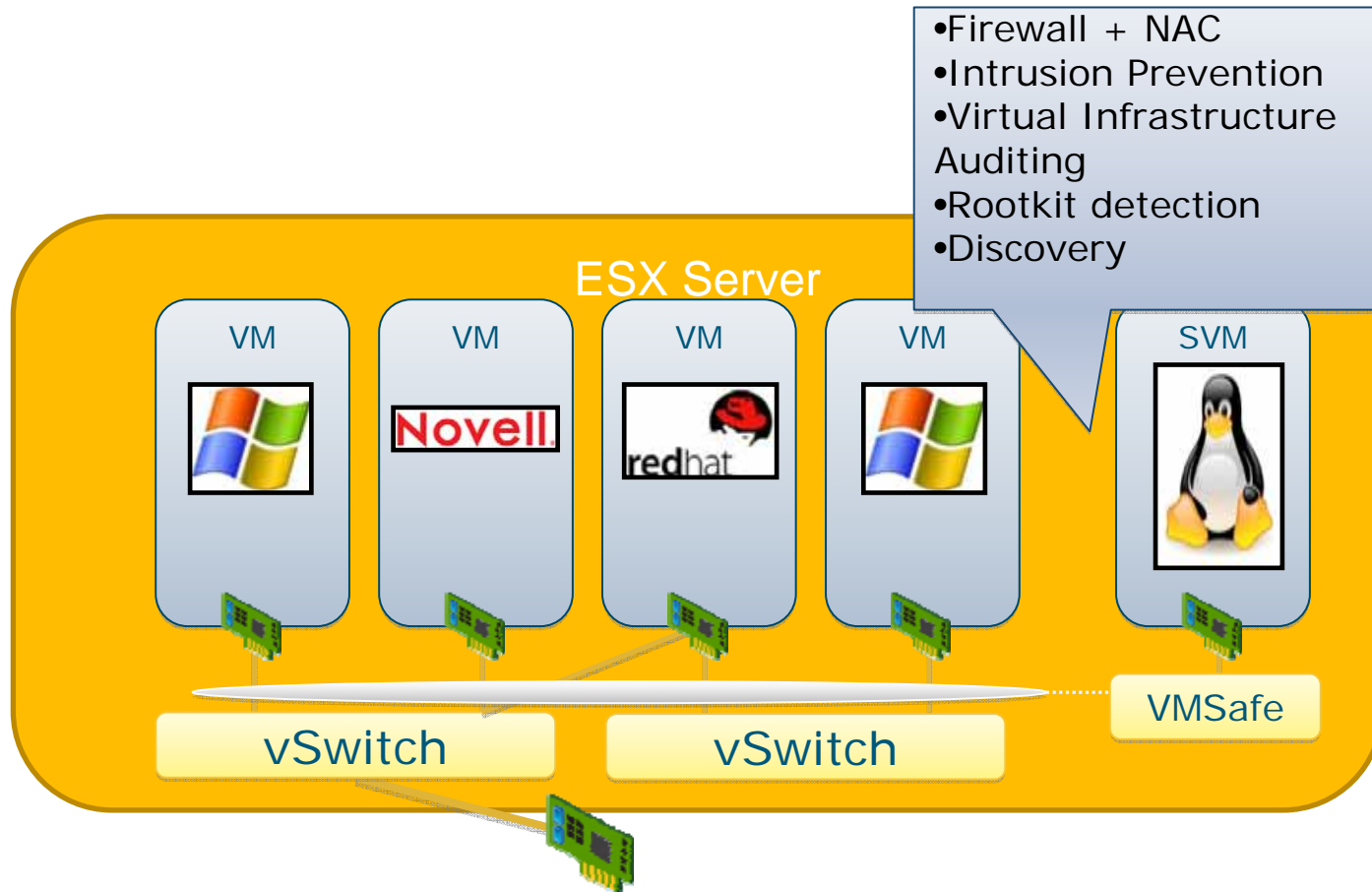
# Virtual IPS vs. Security Virtual Machine







# Integrated Virtual Infrastructure Protection





## Integrated Security Benefits

- Simplified deployment
- Eliminates visibility gaps
  - Inter-VM communication
  - Discovery
  - VM whitelisting/vNAC
- Automated protection
- Advanced security techniques
  - Introspection-based malware detection
- Control of resources allocated to security



## Host Security Footprint Reduction

- Security Virtual Machines take over host-level firewall and IPS/IDS functions from HIPS agent
  - Fewer resources (CPU, memory) consumed
  - Less intrusive (kernel drivers)
  - Guest OS-independent
- More to come...



# Simplified Deployment

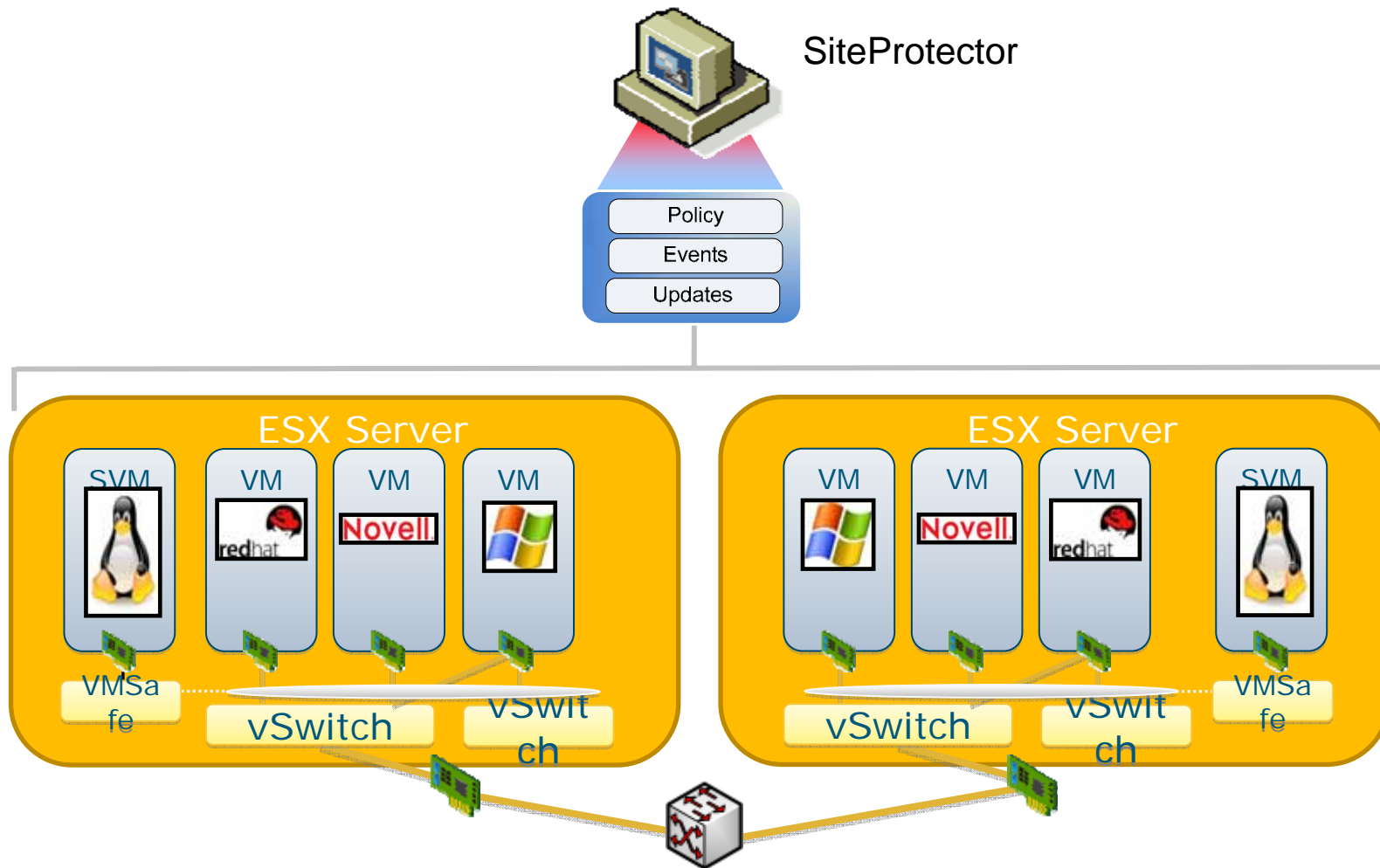
- Virtual appliance form-factor
  - No reconfiguration of virtual network
    - Abstracts underlying network topology
  - Consolidated, locked-down VM dedicated to security
  - OVF format reduces configuration time
  - Compatible with automated image deployment solutions



## Control VM Sprawl

- Identify VMs that are invisible to traditional discovery tools
- Control unauthorized crossing of trust zones
- Ensure VMs that come online do not introduce vulnerabilities
- Quarantine unauthorized VMs
  - VMs that are not considered trusted are given limited network access

# Dynamic Environment Protection



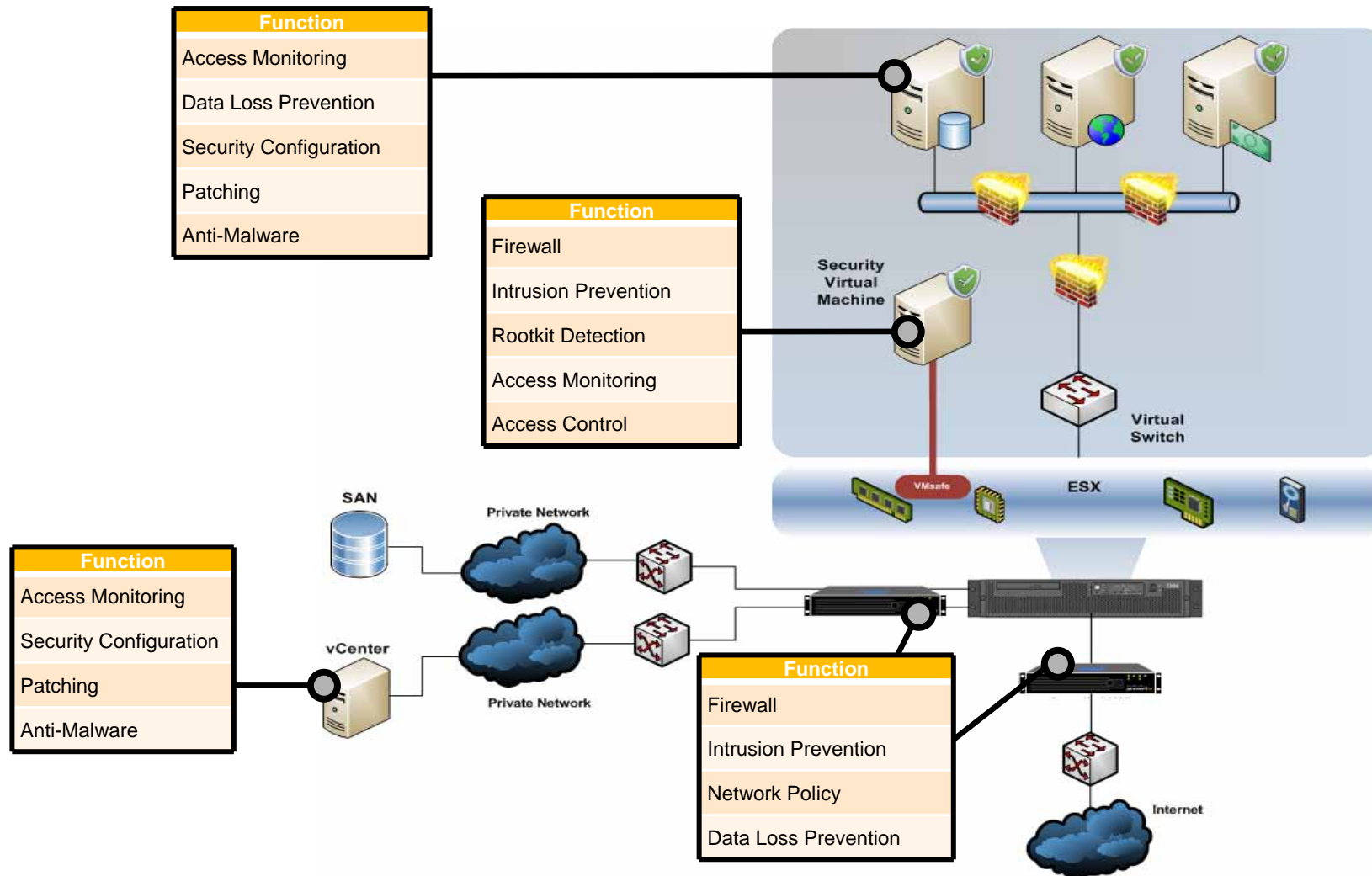


## Is There a Need for Host-Based Agents

- YES!
- Host context required for many security functions
  - Privileged-access control/monitoring
  - File integrity monitoring
  - Encryption
  - Anti-malware
  - Patching
  - Security configuration management



# Defense in Depth

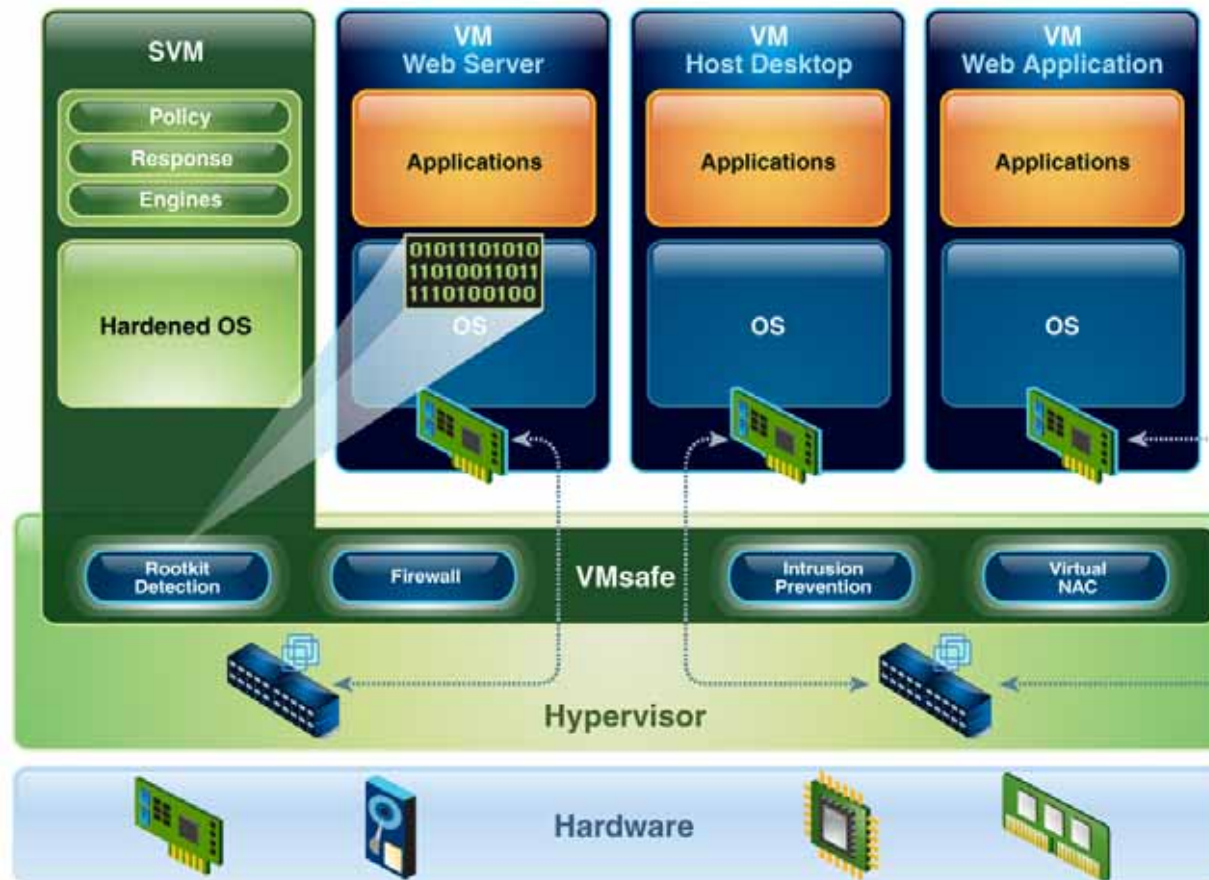






# IBM Virtual Server Protection for VMWare

*Helps customers to be more secure, compliant and cost-effective by delivering integrated and optimized security for virtual data centers.*



- VMSafe Integration that's transparent to guests
- Inter-VM Traffic Analysis
- Fail open
- Firewall and Virtual Network Access Control
- Network Intrusion Prevention
- Rootkit Detection/Prevention
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)



## Summary

- Virtualization does impact security posture
- “Traditional” tools are still relevant
- New products adapted for virtual environments are available
- No single product provides adequate protection



## Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© IBM Corporation 1994-2010. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at <http://www.ibm.com/legal/copytrade.shtml>.