VMware Virtualisation Security with IBM Security Solutions

Chee-Nung Wong

What I'll cover

- New Risks Associated with Server Virtualisation
- Limitations of Traditional Security Controls
- Securing Virtual Environments with IBM Solutions
  - IBM X-Force
  - IBM Security Virtual Server Protection

It’s a virtual world

- 80% of Australian organisations planning or implementing virtualisation
- VMWare is the platform of choice
- Gartner expects exponential growth
  - "There will be more VMs deployed during 2011 than in 2001-2009 combined.” [1]
  - "Virtual Machine sprawl is potentially more dangerous than server sprawl”
    such ease of deployment!

1. Gartner: Server Virtualization: From Virtual Machines to Clouds
http://www.gartner.com/it/content/1462900/1462925/december_14_server_virtualization_tbittman.pdf (Dec 2010)

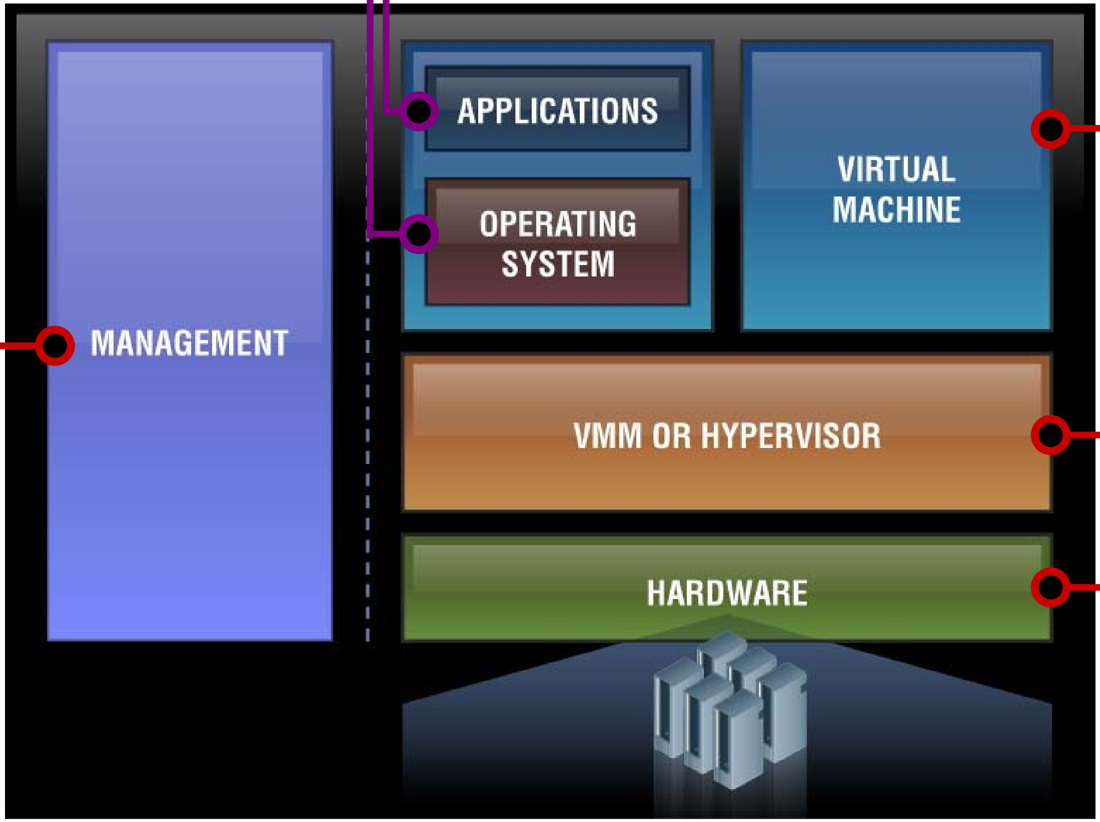
Security Challenges with Virtualisation: New Risks

● 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
- Insider threat



- Virtual server sprawl
- Dynamic state
- Dynamic relocation

- Resource sharing
- Single point of failure
- Loss of visibility

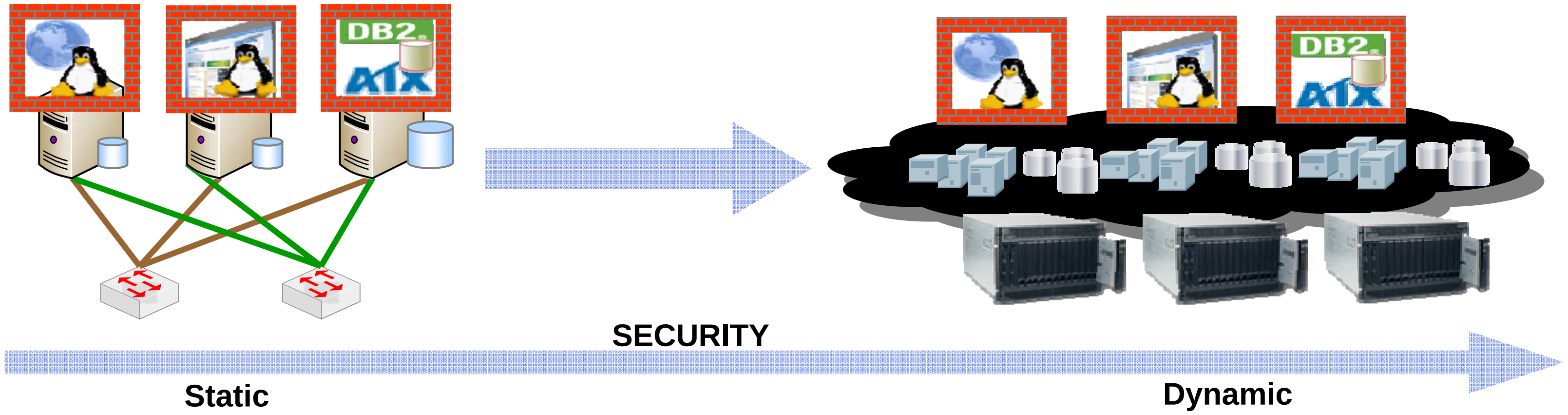
- Stealth rootkits

MORE COMPONENTS = MORE EXPOSURE

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

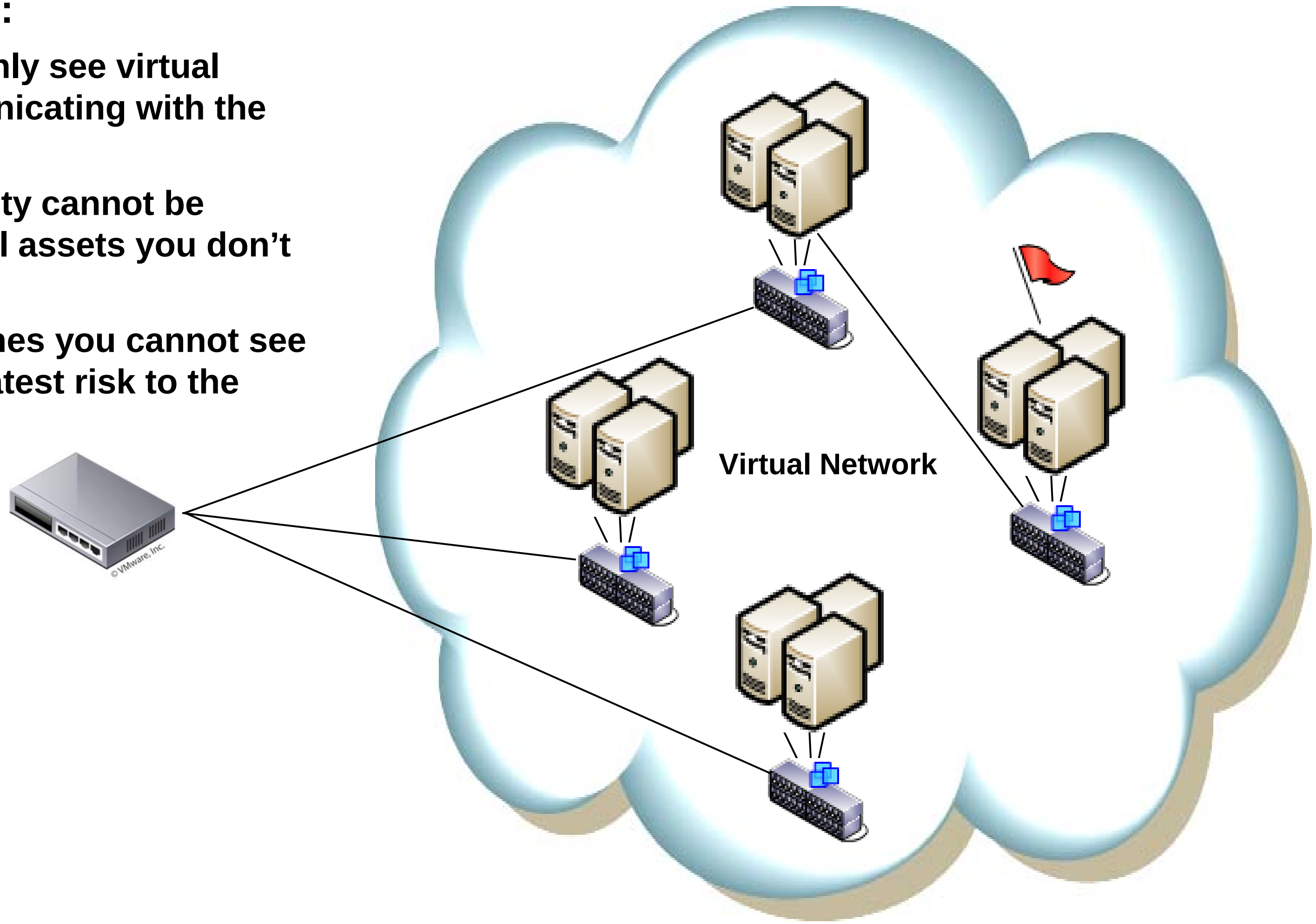
Virtualised	
Network IPS	Should protect against threats at perimeter and between VMs
Server Protection	Securing each VM as if it were a physical server adds time, cost and footprint
System Patching	Needs to protect against vulnerabilities that result from VM state changes
Security Policies	Policies must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



Limitations of Existing Controls and Processes

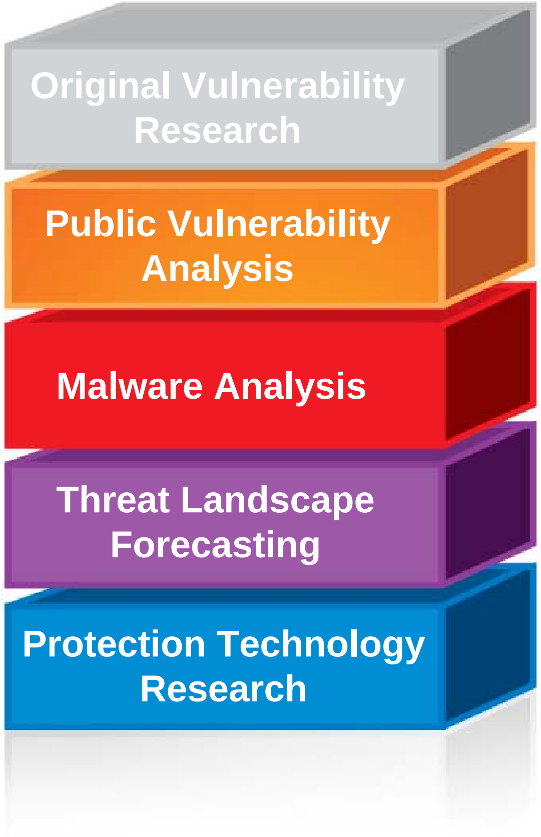
Impact on Security:

- **Discovery tools only see virtual machines communicating with the physical network**
- **Host-based security cannot be deployed to virtual assets you don't know about**
- **The virtual machines you cannot see represent the greatest risk to the environment**



The X-Force team Drives IBM ISS Security Innovation

Research → **Technology** → **Solutions**


Original Vulnerability Research
Public Vulnerability Analysis
Malware Analysis
Threat Landscape Forecasting
Protection Technology Research

X-Force Protection Engines

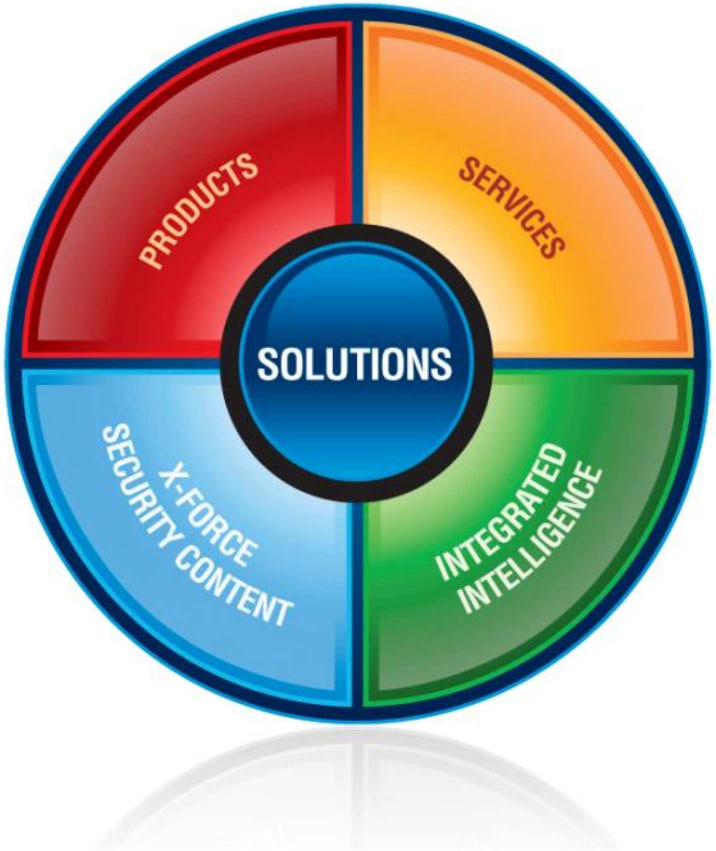
- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

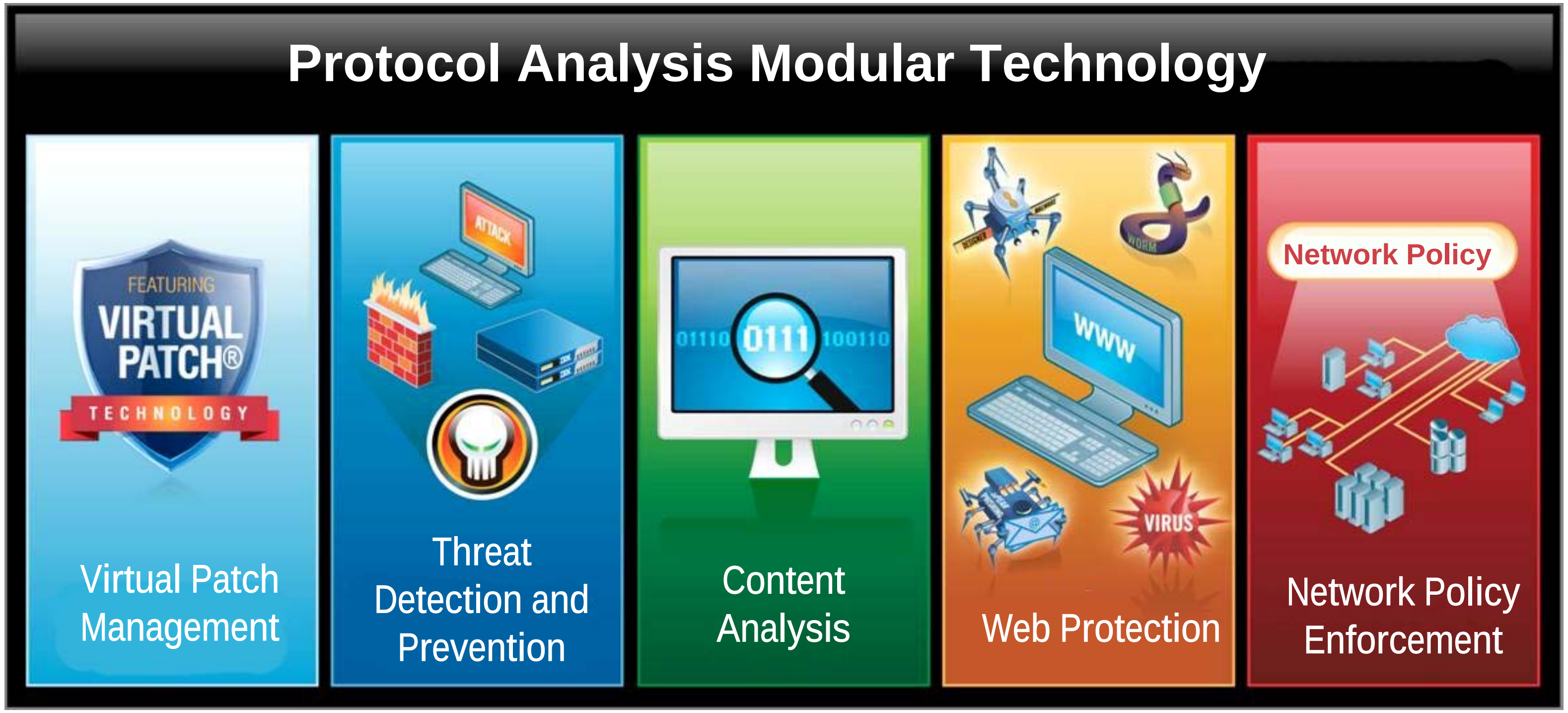
- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing



Protocol Analysis Module (PAM) clearly differentiates our IBM Internet Security Systems™ from others.

The Protocol Analysis Module (PAM)

PAM is the engine behind the preemptive protection afforded by many of the solutions of the IBM Proventia product family. PAM is comprised of five key technologies.

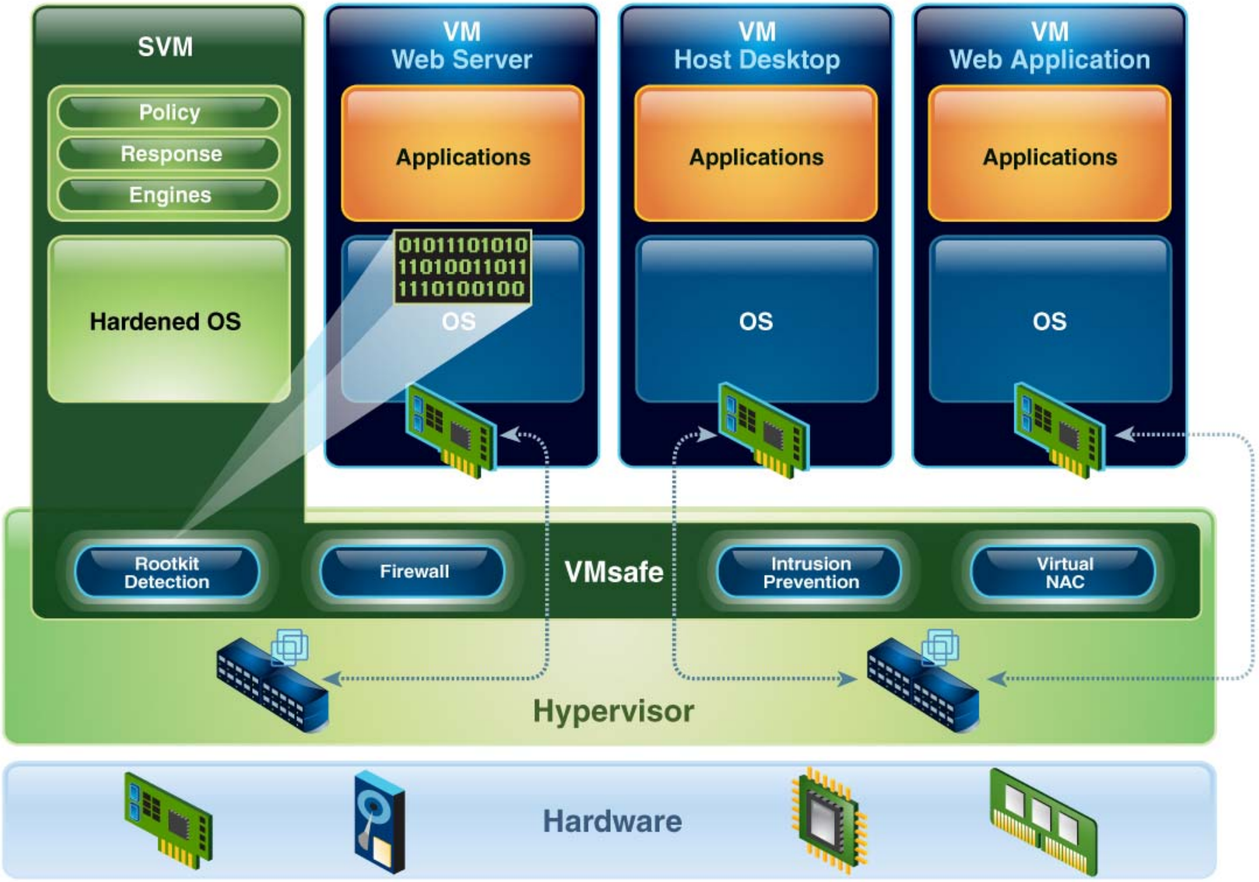


IBM Solution For Virtual Server Protection

Introducing IBM Virtual Server Protection for VMware

Integrated threat protection for VMware vSphere 4

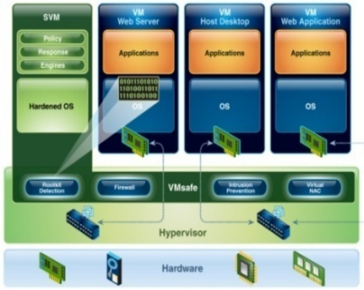
Helps customers to be more secure, compliant and cost-effective by delivering integrated and optimised security for virtual data centers.



- 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

Three reasons you need virtualisation infrastructure protection

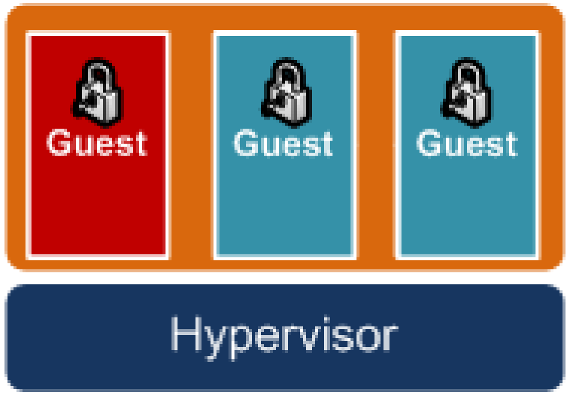
Need	How IBM Virtual Server Protection for VMware® helps
Mitigate new risks and complexities introduced by Virtualisation	Provides dynamic protection for every layer of the virtual infrastructure
Maintain compliance standards and regulations	Helps meet regulatory compliance by providing security and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

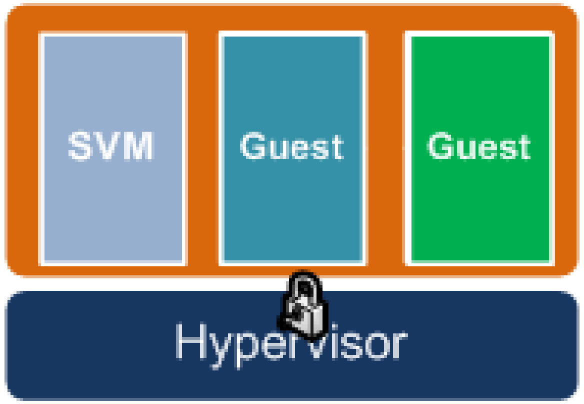


Host-based vs. Integrated Virtual Server Protection

Host-Based Agent	
Isolation	Firewall functions only in the context of the VM
Attack Prevention	Requires agent to be present
VM State	Security is impacted by VM state change
Security Policies	Policy is enforced only within the VM

Virtual Server Protection	
Isolation	Firewall enforces virtual network-wide policy
Attack Prevention	Secures all virtual machines automatically
VM State	Security is not impacted by VM state change
Security Policies	Policy is enforced outside of the VM and irrespective of the VMs location





Summary

- Virtualisation does impact security posture
- New products adapted for virtual environments are available
- Consider your wider network security strategy

Thank you
and questions!

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.

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.