IBM

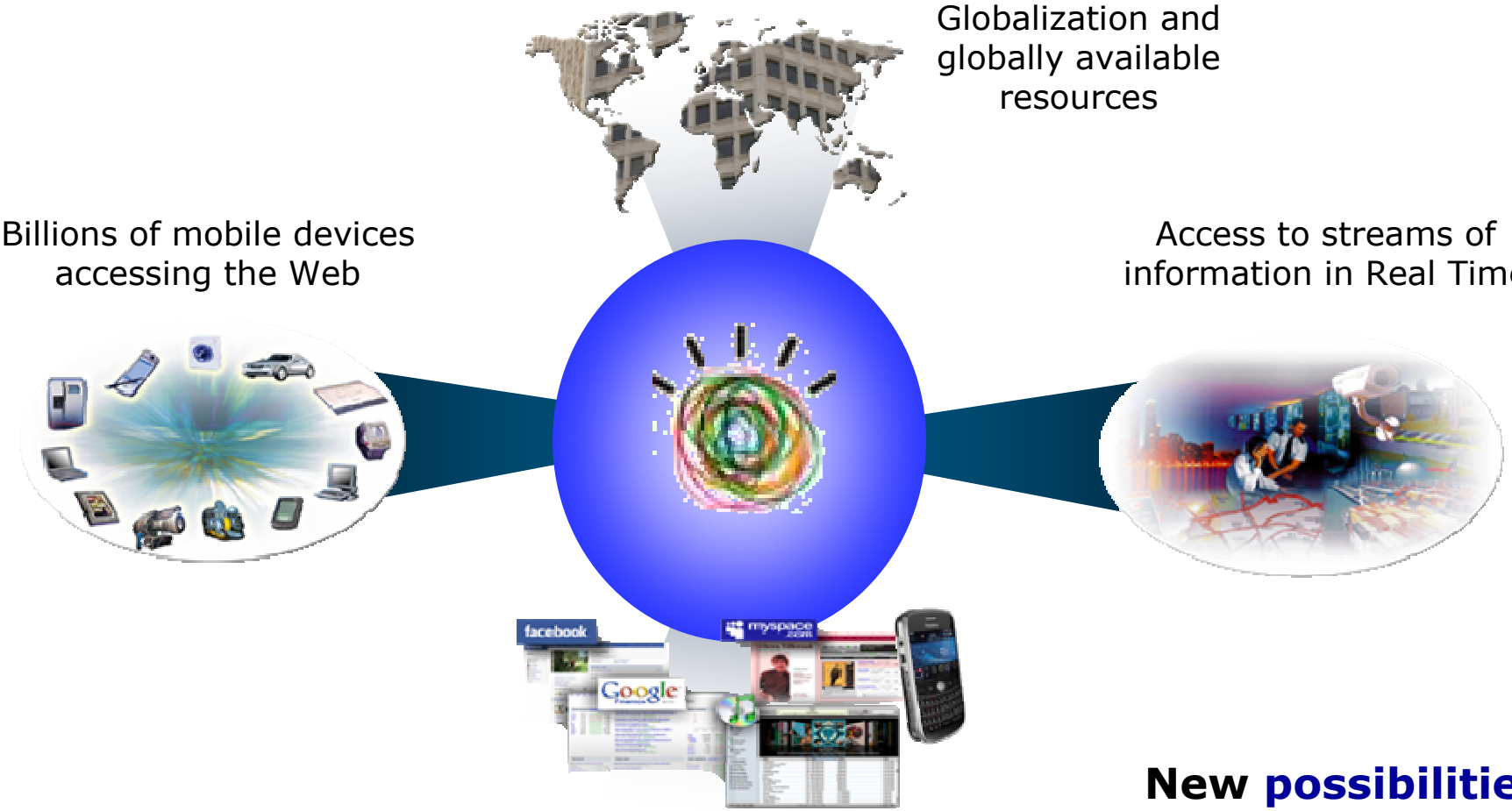
Securing a Virtualized World

Craig Stabler CISSP

15 September 2010

MEET IBM 2010
see differently

Virtualization – an enabler for a Smarter Planet



New possibilities.
New complexities.
New risks.

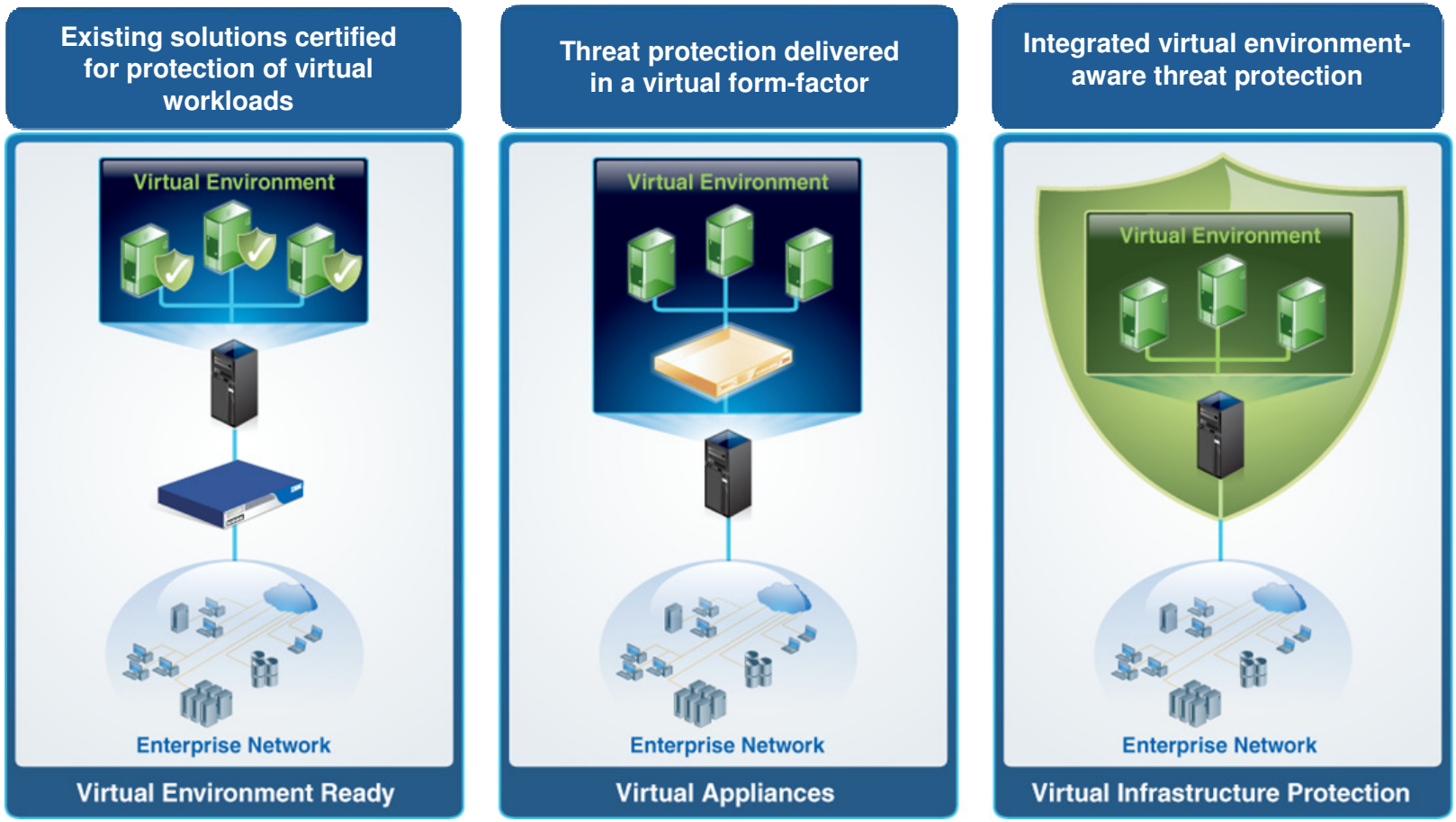
Virtualization - introduces new complexities

- **Virtualization blurs the physical boundaries between systems that are used to separate workloads and those responsible for securing them.**
- **Virtualization enables mobility of systems and flexible deployment and re-deployment of systems. Manually tracking software stacks and configurations of VMs and images becomes increasingly difficult.**

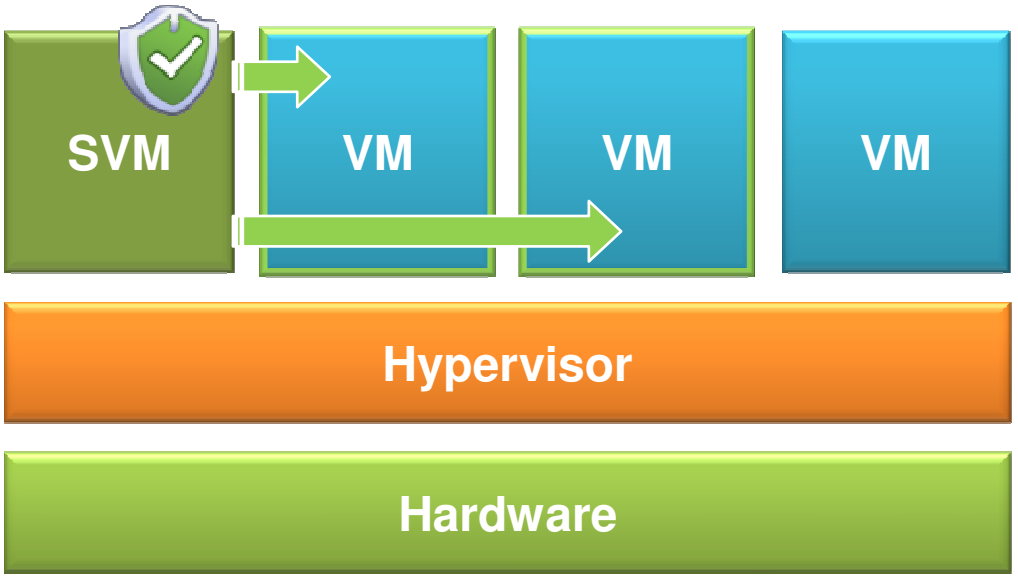
Before Virtualization

After Virtualization

IBM Virtualization Security



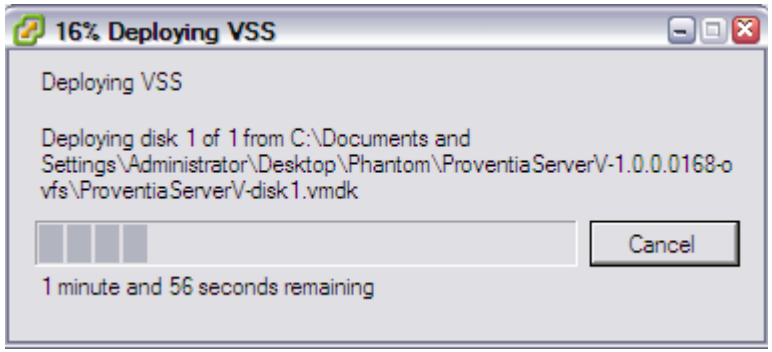
Introducing IBM Virtual Server Protection for VMware



- Integrated security leveraging the hypervisor
- On-demand, centralized protection
- Selective network intrusion and host malware protection

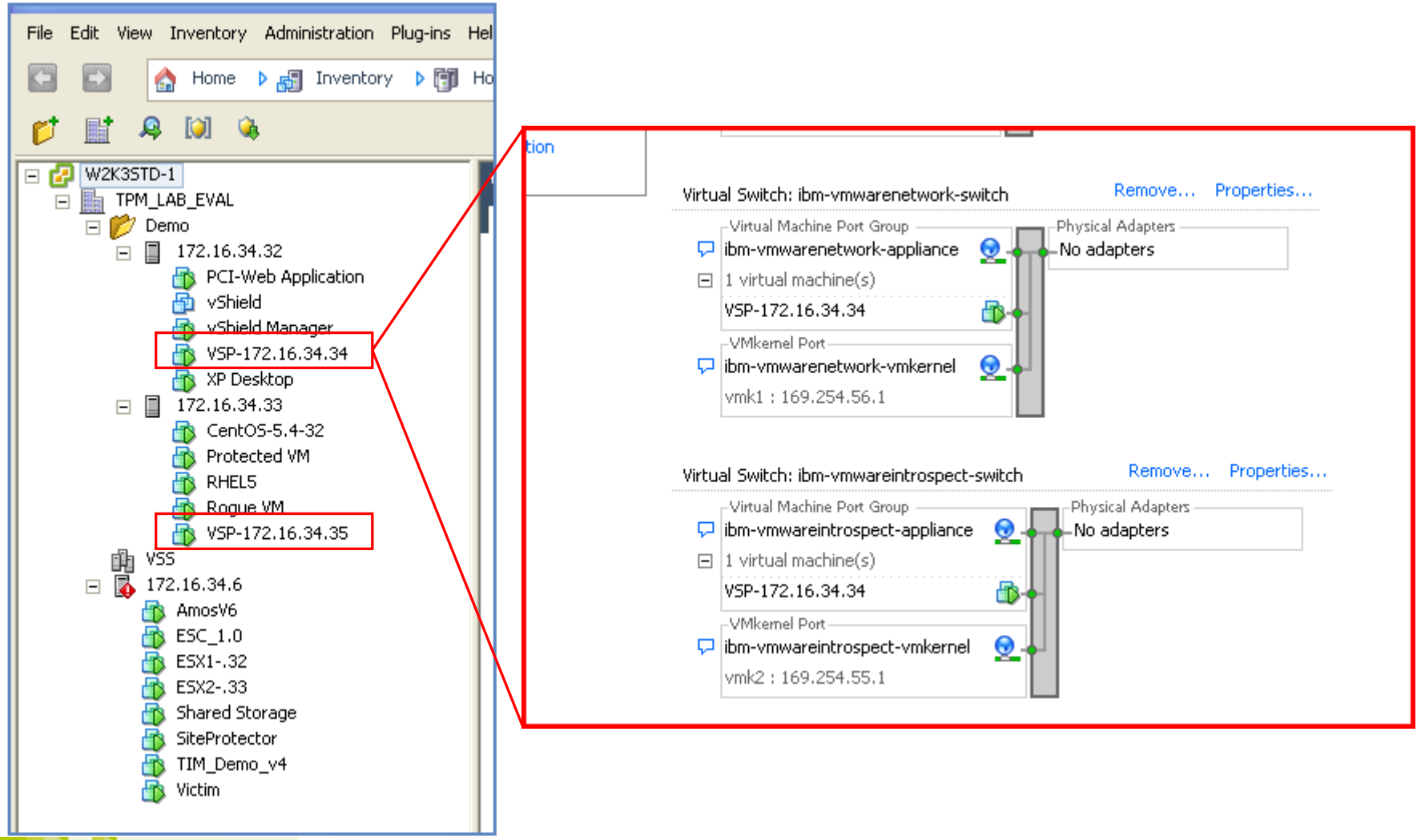
Packaging

- Delivered as an Open Virtualization Format (OVF) package
  - Virtual machine settings (CPU, memory, hard disk, etc) pre-defined
  - Simple deployment procedure
  - Facilitates automated provisioning



Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
Network adapter 5	VM Network
SCSI controller 0	BusLogic Parallel
Hard disk 1	Virtual Disk

VMsafe-Integrated Virtual Appliance



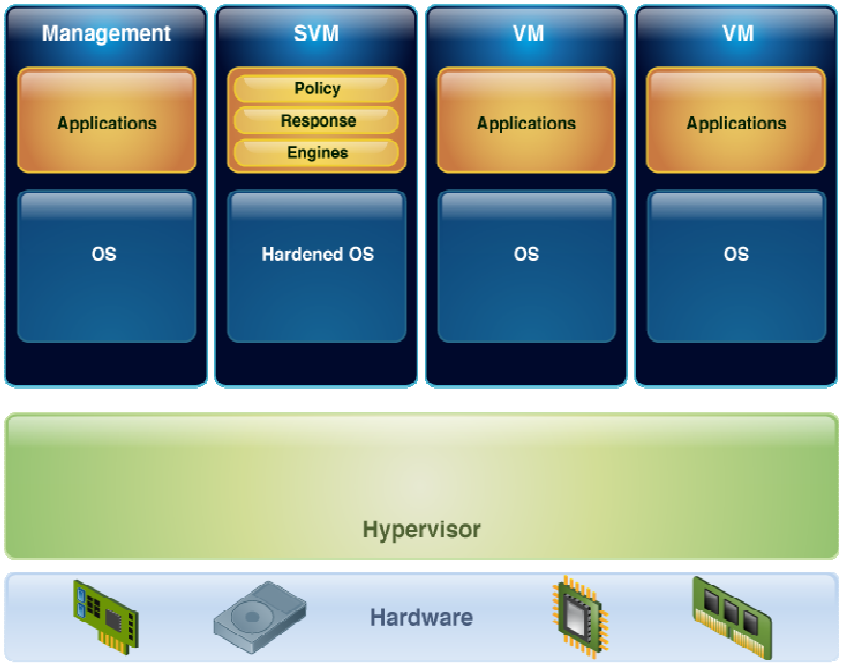
Virtualization – before and after

IBM

Before Virtualization

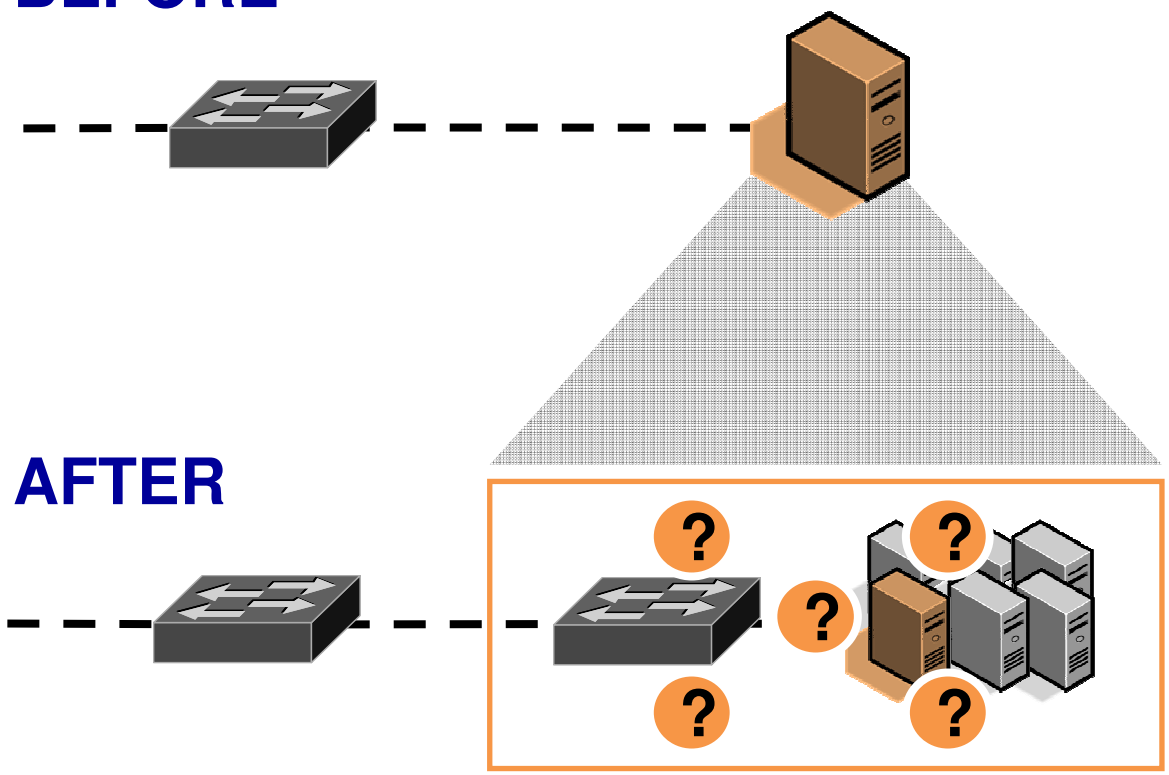
- 1:1 ratio of OSs and applications per server

After Virtualization



- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

Common security-centric questions



Equipment is Physical

- Wires and cables.
- Routers and switches.
- Servers on racks.
- Storage arrays and disks.
- Memory and CPUs.
- Machines stay put.
- Security is in place.

Equipment is Virtual

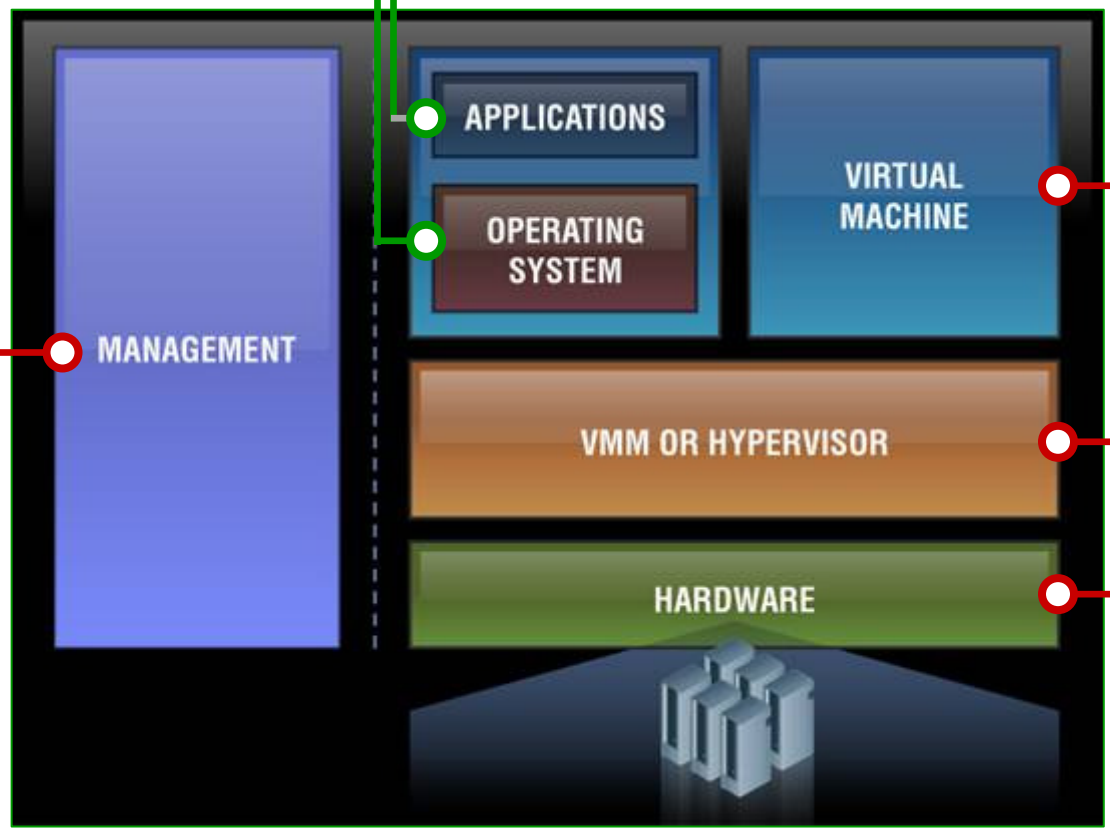
- How do we watch the network?
- Where are VMs located?.
- Are they moving around?
- What's our change control policy
- Are VMs patched?
- Is the hypervisor secure?
- Who's responsible for security?

Threats – old and new

IBM

- 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 sprawl

Dynamic relocation

VM stealing

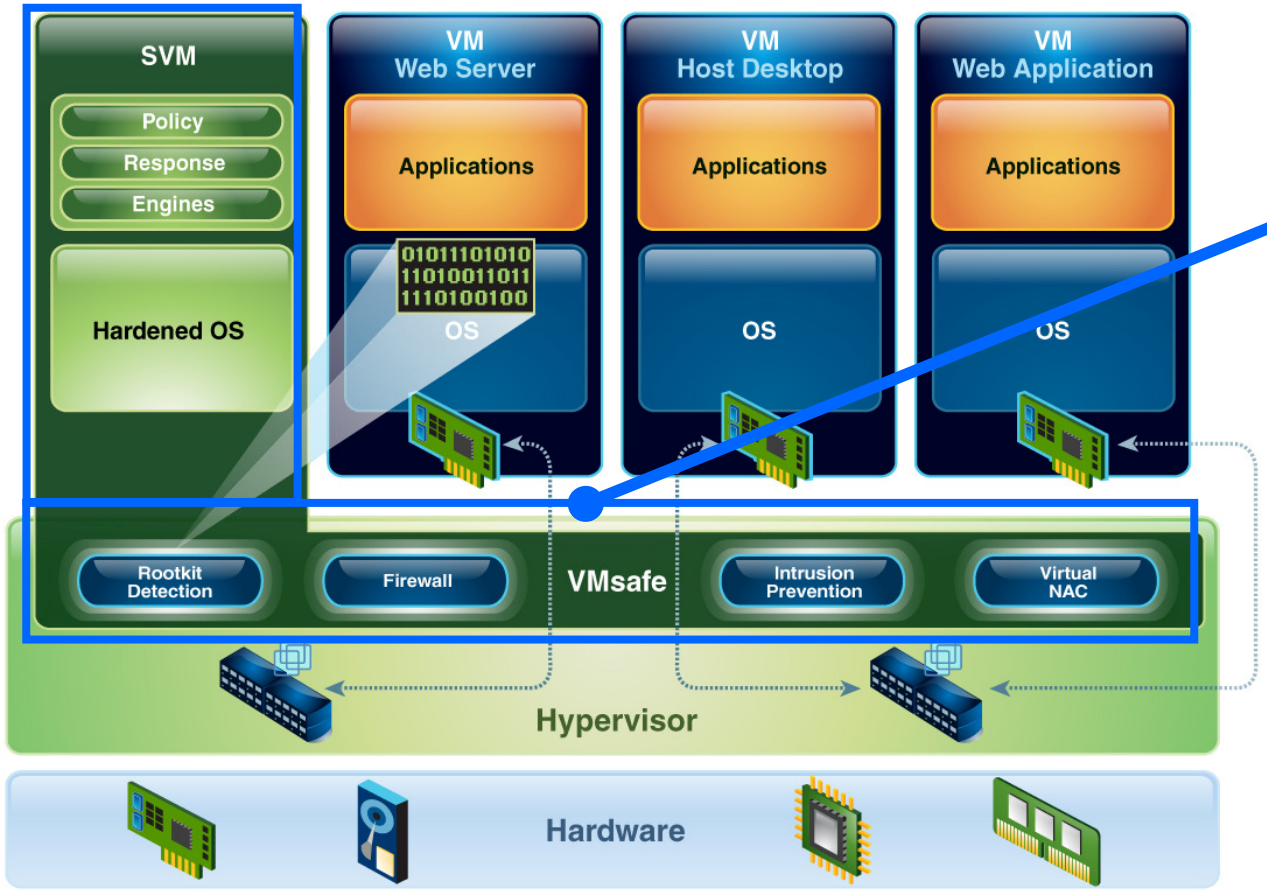
Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

Virtual NICs & Virtual Hardware are targets

IBM Security Virtual Server Protection for VMware



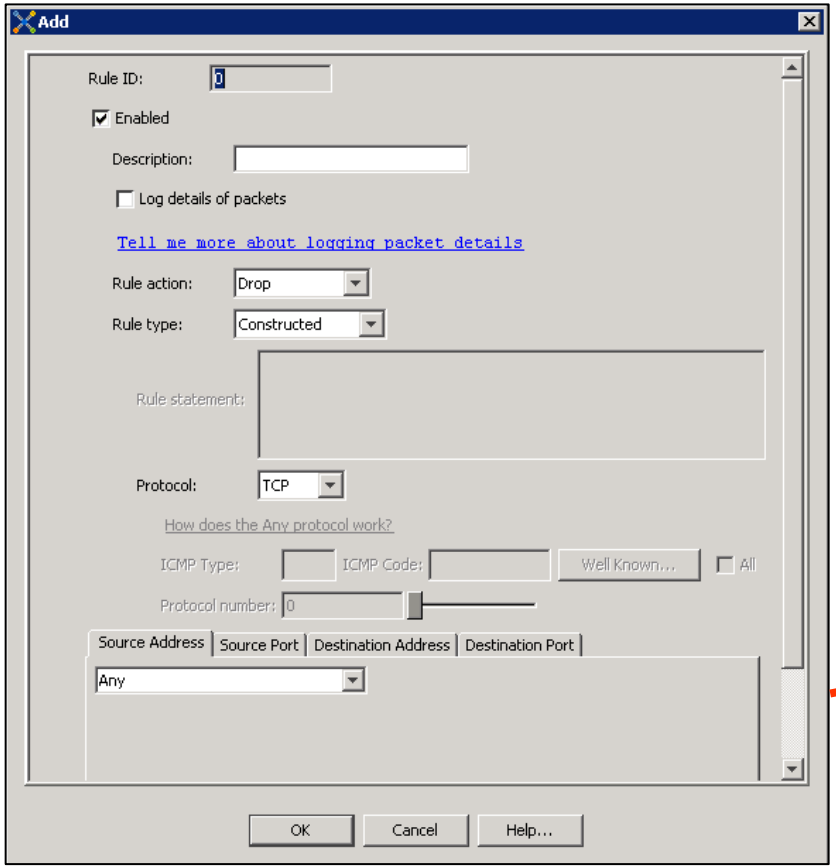
IBM Virtual Server Security for VMware

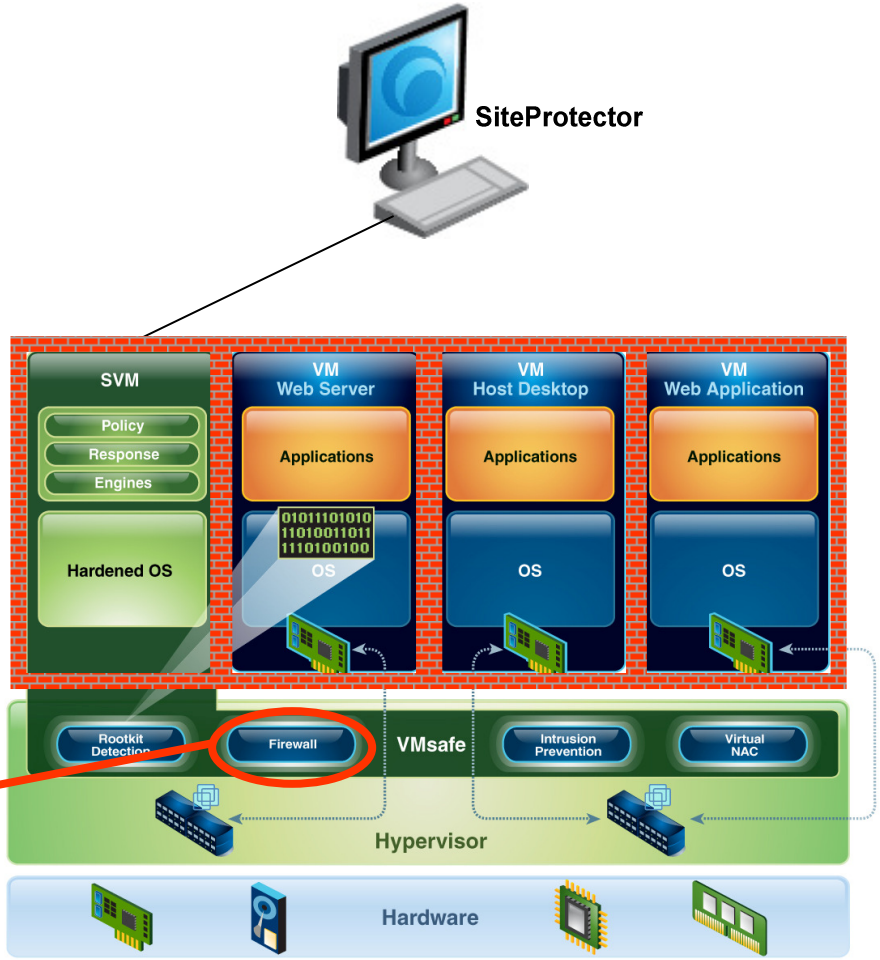
- VMsafe Integration
- Firewall and Intrusion Prevention
- Rootkit Detection/Prevention
- Inter-VM Traffic Analysis
- Automated Protection for Mobile VMs (VMotion)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Infrastructure Auditing (Privileged User)
- Virtual Network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

IBM Security Virtual Server Protection

Firewall

- Enforces dynamic security wherever VMs are deployed

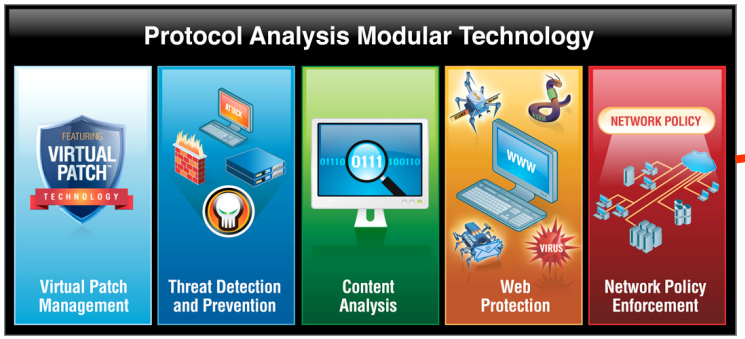


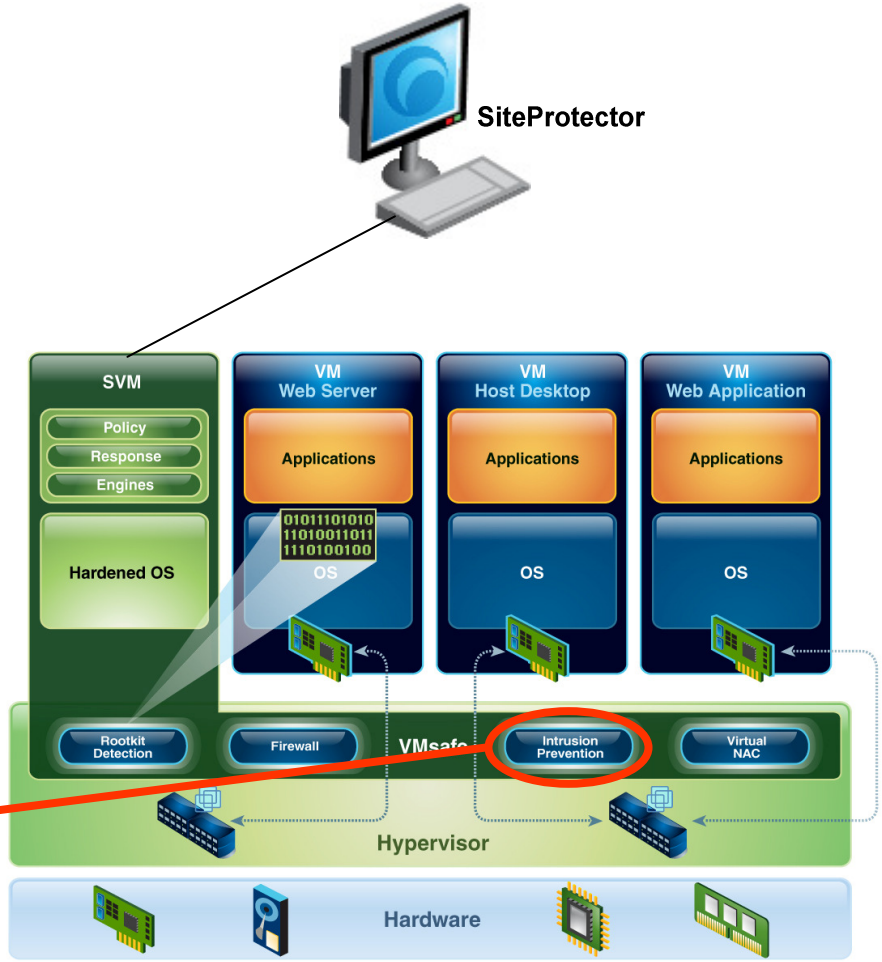


IBM Security Virtual Server Protection

Intrusion Prevention System (IPS)

- Vulnerability-centric, protocol-aware analysis and protection
- Abstraction from underlying network configuration
- Automated protection for new VMs
- Network-level workload segmentation
- Privileged-level protection of OS kernel structures

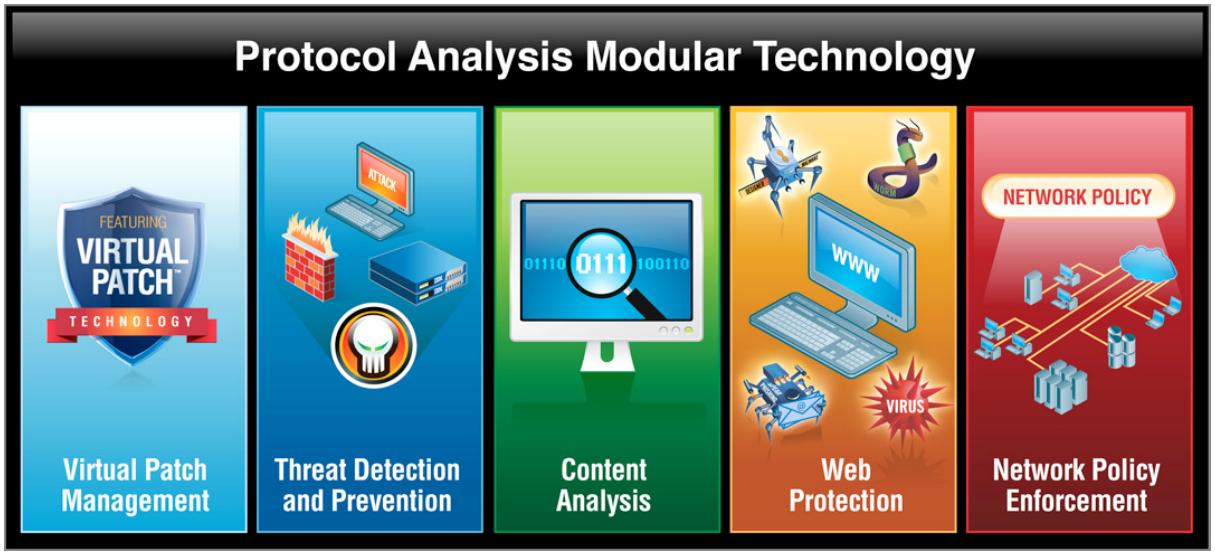




Manage risk in a complex world

IBM Security Virtual Server Protection

IPS - Protocol Analysis Module (PAM)



- Performs deep packet inspection
- Performs deep protocol and content analysis
- Detects protocol and content anomalies
- Simulates the protocol/content stacks in vulnerable systems
- Normalizes at each protocol and content layer

Provides the ability to add new security functionality within the existing solution

IBM Security Virtual Server Protection

VM Rootkit Detection

- Rootkit detection engine that uses memory introspection to identify modifications to key guest OS kernel data structures by malware

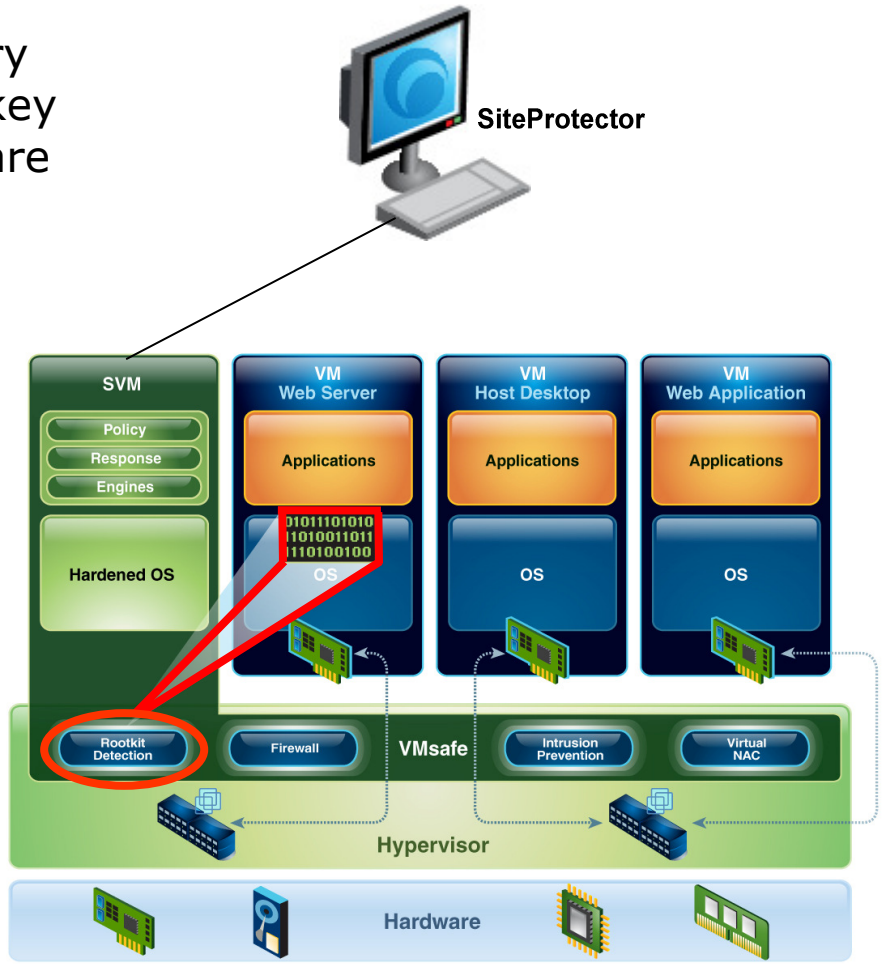
Time *	Tag Name	Event Count	Status
2010-02-09 18:45:0...	SSDT Modification Detected-arktest	1	Detecte...
2010-02-09 07:52:5...	HTTP_GET_XP_Cmdshell	1	Attack f...
2010-02-09 07:52:4...	HTTP_GET_XP_Cmdshell	1	Attack f...
2010-02-09 07:52:4...			
2010-02-09 07:28:0...			
2010-02-09 07:28:0...			
2010-02-09 07:27:5...			
2010-02-09 07:27:4...			
2010-02-09 07:22:0...			

Event Details 1/1

Event Details Name	Event Details Value
Date/Time	2010-02-09 18:45:05 EST
Tag Name	SSDT Modification Detected-arktest
Alert Name	SSDT Modification Detected-arktest
Severity	High
Observance Type	AntiRootkit
Combined Event Count	1
Cleared Flag	☐
Target IP Address	172.16.34.34

Event Attribute Value Pairs

Attribute Name	Attribute Value
:ARK-ActionPerformed	Monitor
:ARK-AffectedEntity	SSDT
:ARK-DriverName	\??\C:\temp\arktest\x86\arktest.sys
:ARK-EntryNumber	37
:ARK-EventID	2
:ARK-guestOS	Microsoft Windows XP (32-bit)
:ARK-HashType	SHA256
:ARK-HashValue	1ed5bf83782ff7250d43def3d93318f1925f248aa fbf8f91994e38bf91c1045
:ARK-moduleOwner	Microsoft
:ARK-VirtualMachineName	XP Desktop
:ARK-VirtualMachineUUID	42032917-d90a-c5d0-065c-913c3a80ae90



IBM Security Virtual Server Protection

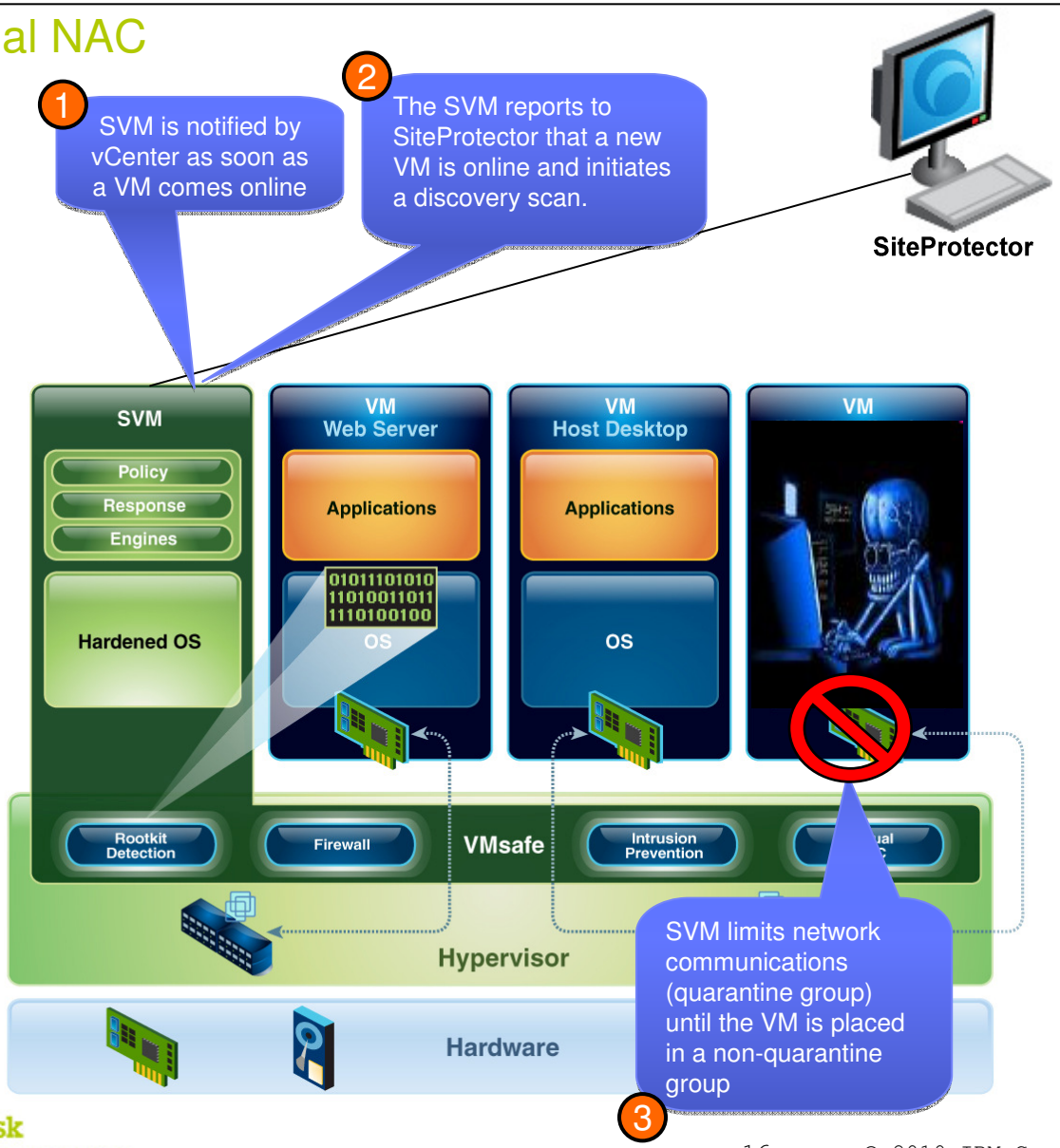
Automated Discovery / Virtual NAC

Features

- Virtual Network Access Control (VNAC)
- Automated discovery
- Virtual Infrastructure auditing integration

Benefits

- Rogue VM protection
- Virtual Infrastructure monitoring
- Virtual network awareness
- Quarantine or limit network access until VM security posture has been validated

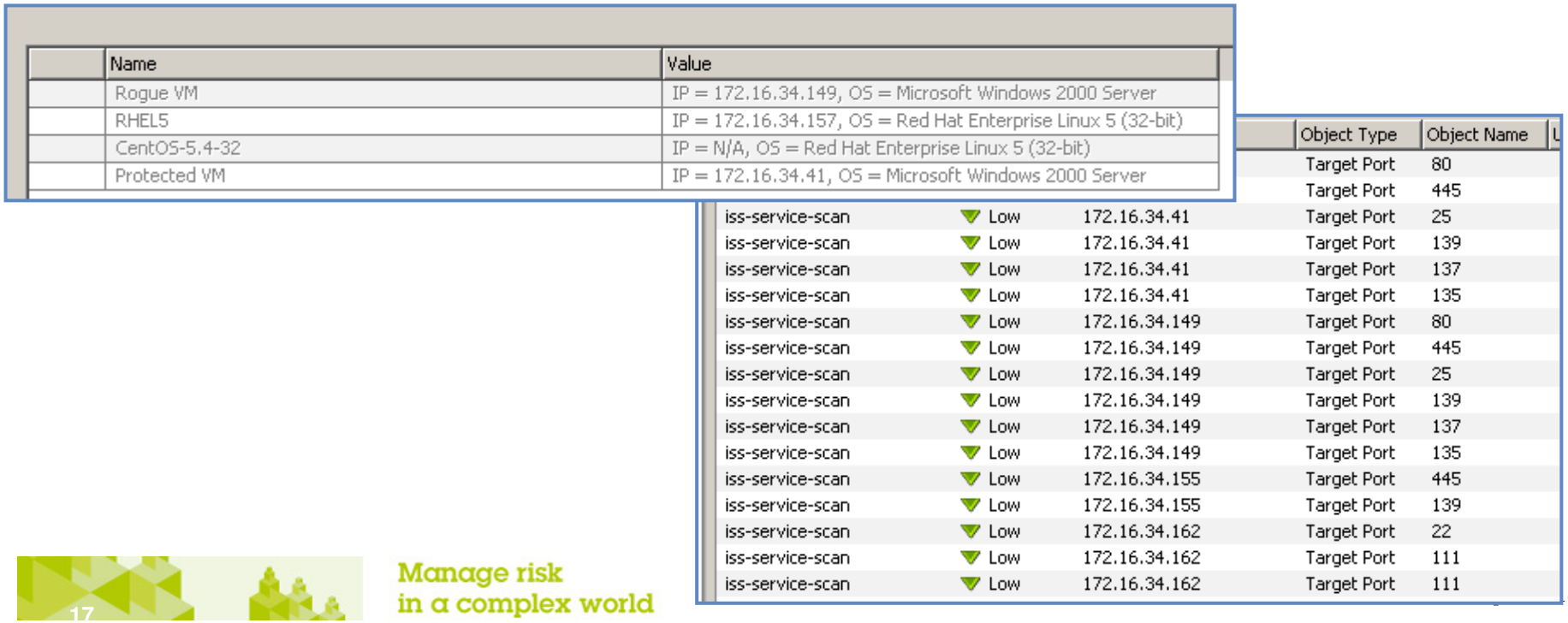


IBM Security Virtual Server Protection

Discovery

- **Use Case -** Discover new virtual machines as they come online.

- **Functionality**
  - Discovery engine that identifies operating system (using NMAP fingerprint database) and listening TCP & UDP ports.
  - Scheduled scanning to keep asset information current.



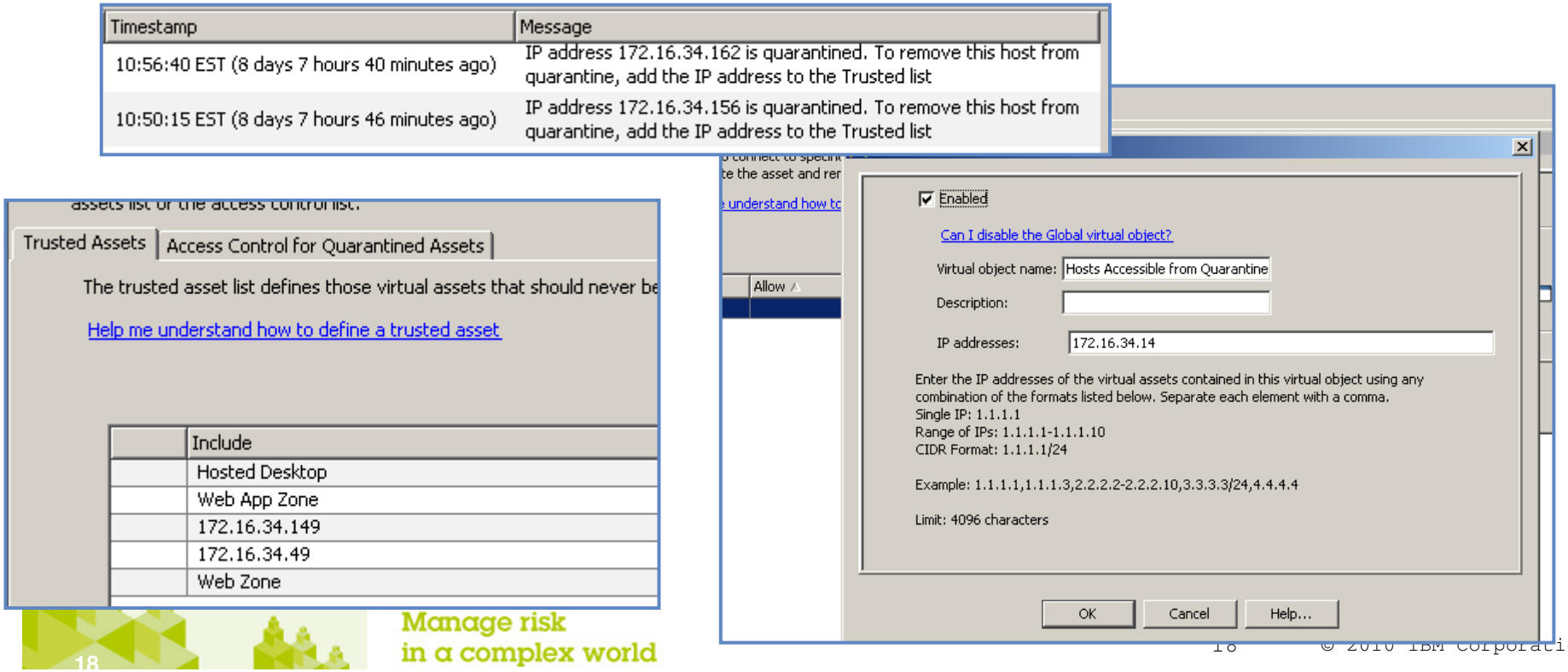
Name	Value
Rogue VM	IP = 172.16.34.149, OS = Microsoft Windows 2000 Server
RHEL5	IP = 172.16.34.157, OS = Red Hat Enterprise Linux 5 (32-bit)
CentOS-5.4-32	IP = N/A, OS = Red Hat Enterprise Linux 5 (32-bit)
Protected VM	IP = 172.16.34.41, OS = Microsoft Windows 2000 Server

			Object Type	Object Name
iss-service-scan	Low	172.16.34.41	Target Port	80
iss-service-scan	Low	172.16.34.41	Target Port	445
iss-service-scan	Low	172.16.34.41	Target Port	25
iss-service-scan	Low	172.16.34.41	Target Port	139
iss-service-scan	Low	172.16.34.41	Target Port	137
iss-service-scan	Low	172.16.34.41	Target Port	135
iss-service-scan	Low	172.16.34.149	Target Port	80
iss-service-scan	Low	172.16.34.149	Target Port	445
iss-service-scan	Low	172.16.34.149	Target Port	25
iss-service-scan	Low	172.16.34.149	Target Port	139
iss-service-scan	Low	172.16.34.149	Target Port	137
iss-service-scan	Low	172.16.34.149	Target Port	135
iss-service-scan	Low	172.16.34.155	Target Port	445
iss-service-scan	Low	172.16.34.155	Target Port	139
iss-service-scan	Low	172.16.34.162	Target Port	22
iss-service-scan	Low	172.16.34.162	Target Port	111
iss-service-scan	Low	172.16.34.162	Target Port	111

IBM Security Virtual Server Protection

vNAC configuration

- **Use Case –** Mitigate risk introduced by virtual server sprawl by quarantining untrusted virtual machines until security posture has been assessed.
- **Functionality**
  - Quarantine capability that limits communications to and from the untrusted virtual machine.

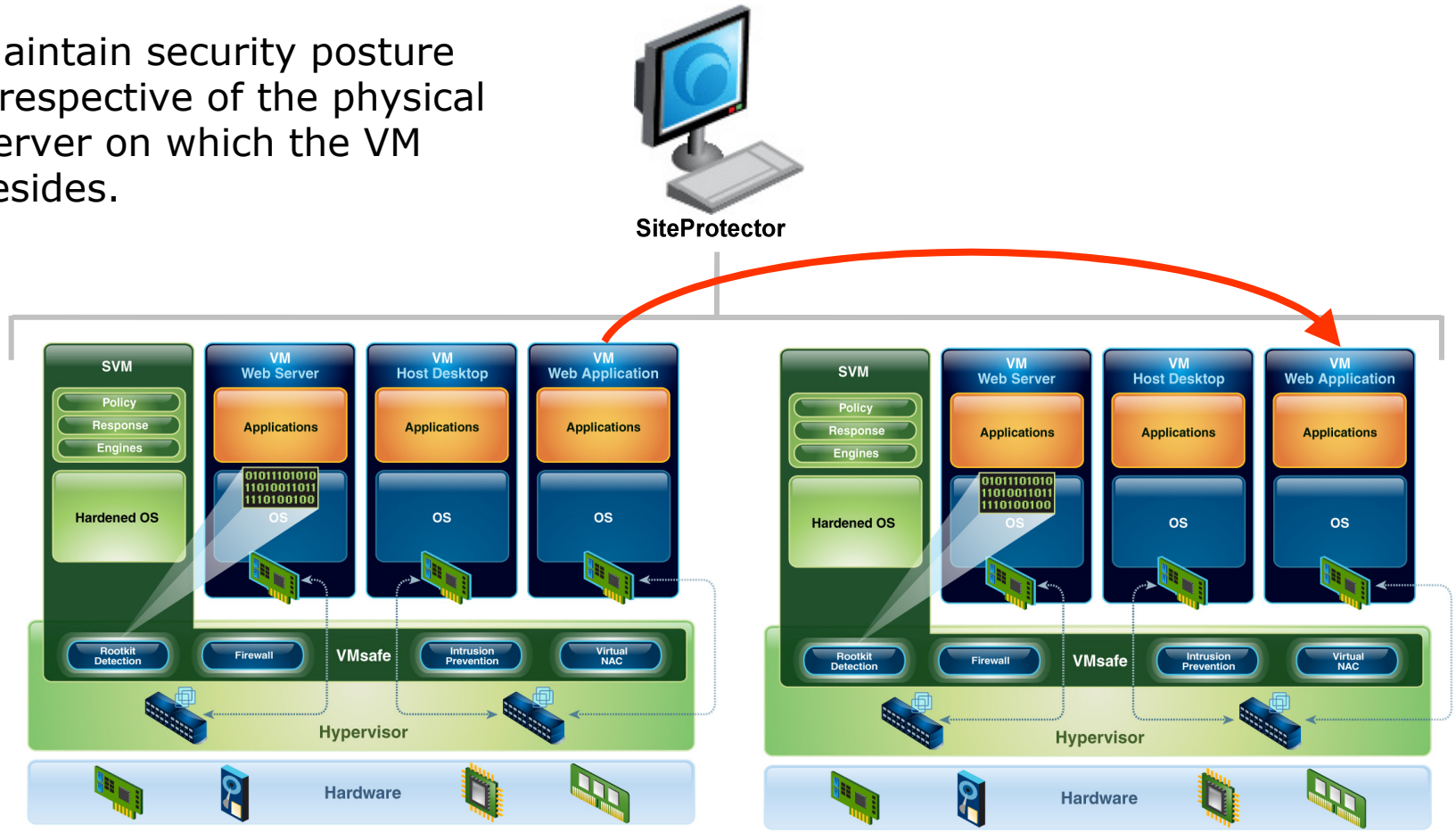


Manage risk in a complex world

IBM Security Virtual Server Protection

Mobility (vMotion)

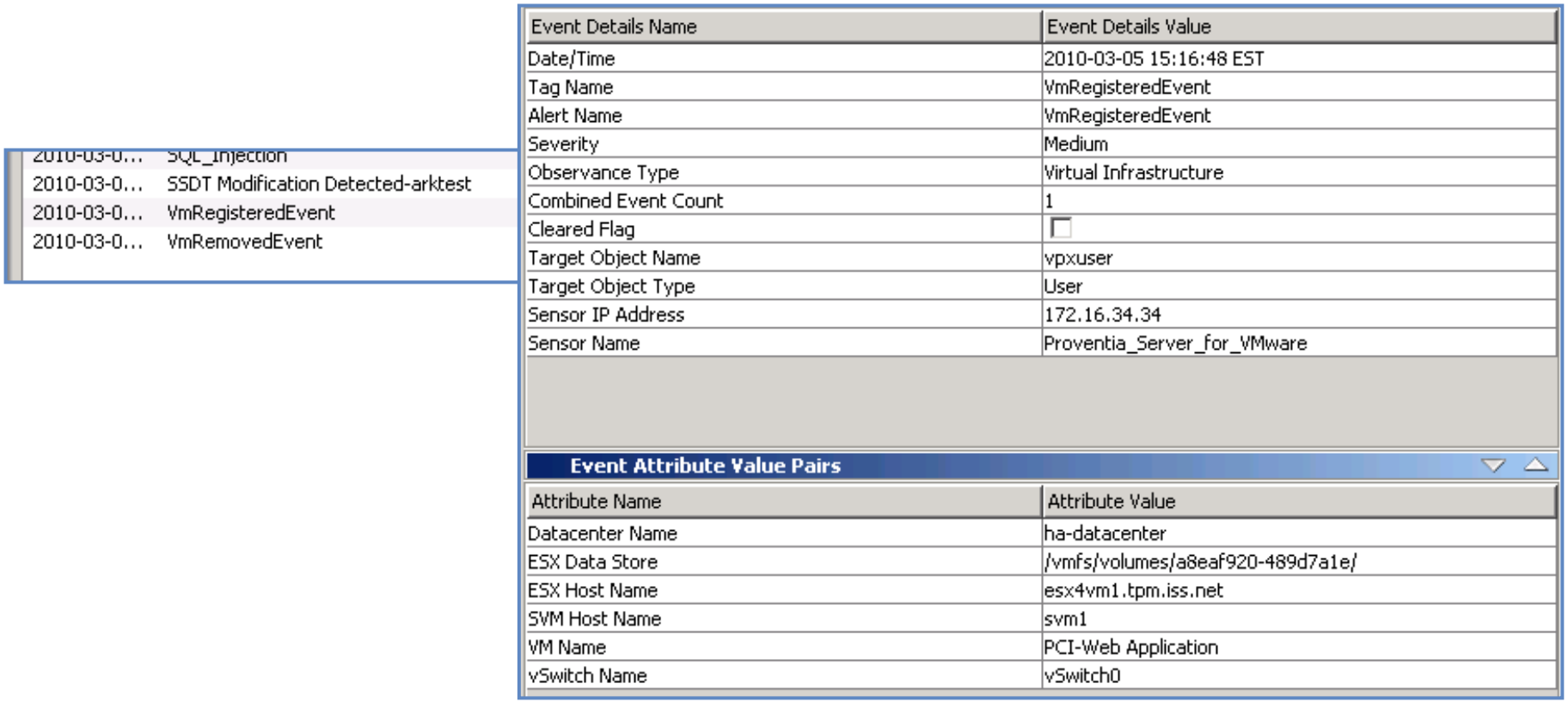
Maintain security posture irrespective of the physical server on which the VM resides.



Manage risk in a complex world

Virtual Infrastructure Auditing

- **Threat –** Virtual machine state change or migration that mixes trust zones.
- **Functionality**
  - Hooks into VMware management auditing to report events interesting from a security perspective.



2010-03-0...	SQL_Injection
2010-03-0...	SSDT Modification Detected-arktest
2010-03-0...	VmRegisteredEvent
2010-03-0...	VmRemovedEvent

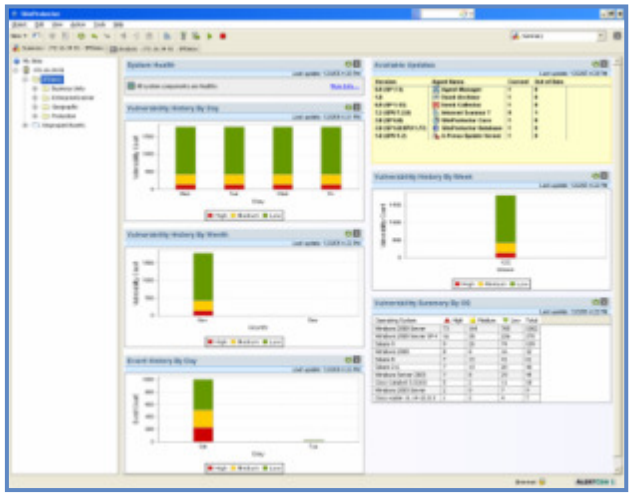
Event Details Name	Event Details Value
Date/Time	2010-03-05 15:16:48 EST
Tag Name	VmRegisteredEvent
Alert Name	VmRegisteredEvent
Severity	Medium
Observance Type	Virtual Infrastructure
Combined Event Count	1
Cleared Flag	☐
Target Object Name	vpxuser
Target Object Type	User
Sensor IP Address	172.16.34.34
Sensor Name	Proventia_Server_for_VMware

Event Attribute Value Pairs

Attribute Name	Attribute Value
Datacenter Name	ha-datacenter
ESX Data Store	/vmfs/volumes/a8eaf920-489d7a1e/
ESX Host Name	esx4vm1.tpm.iss.net
SVM Host Name	svm1
VM Name	PCI-Web Application
vSwitch Name	vSwitch0

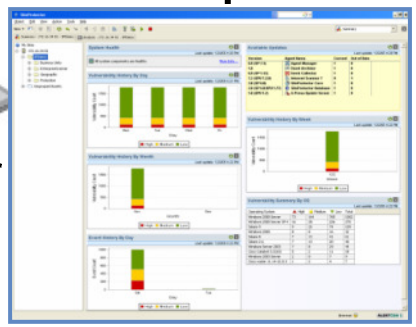
IBM Security Virtual Server Protection

Central Management - SiteProtector

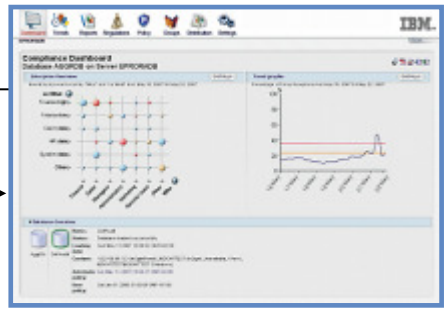


The Bigger Picture - Management

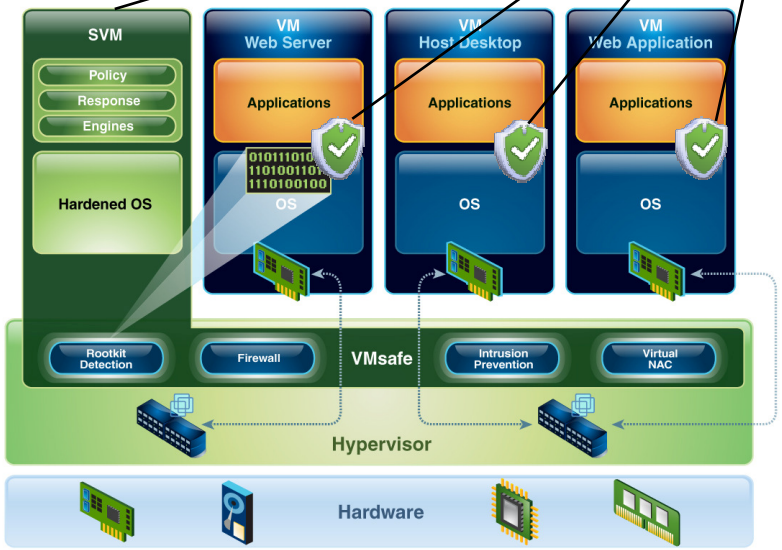
SiteProtector



SiteProtector



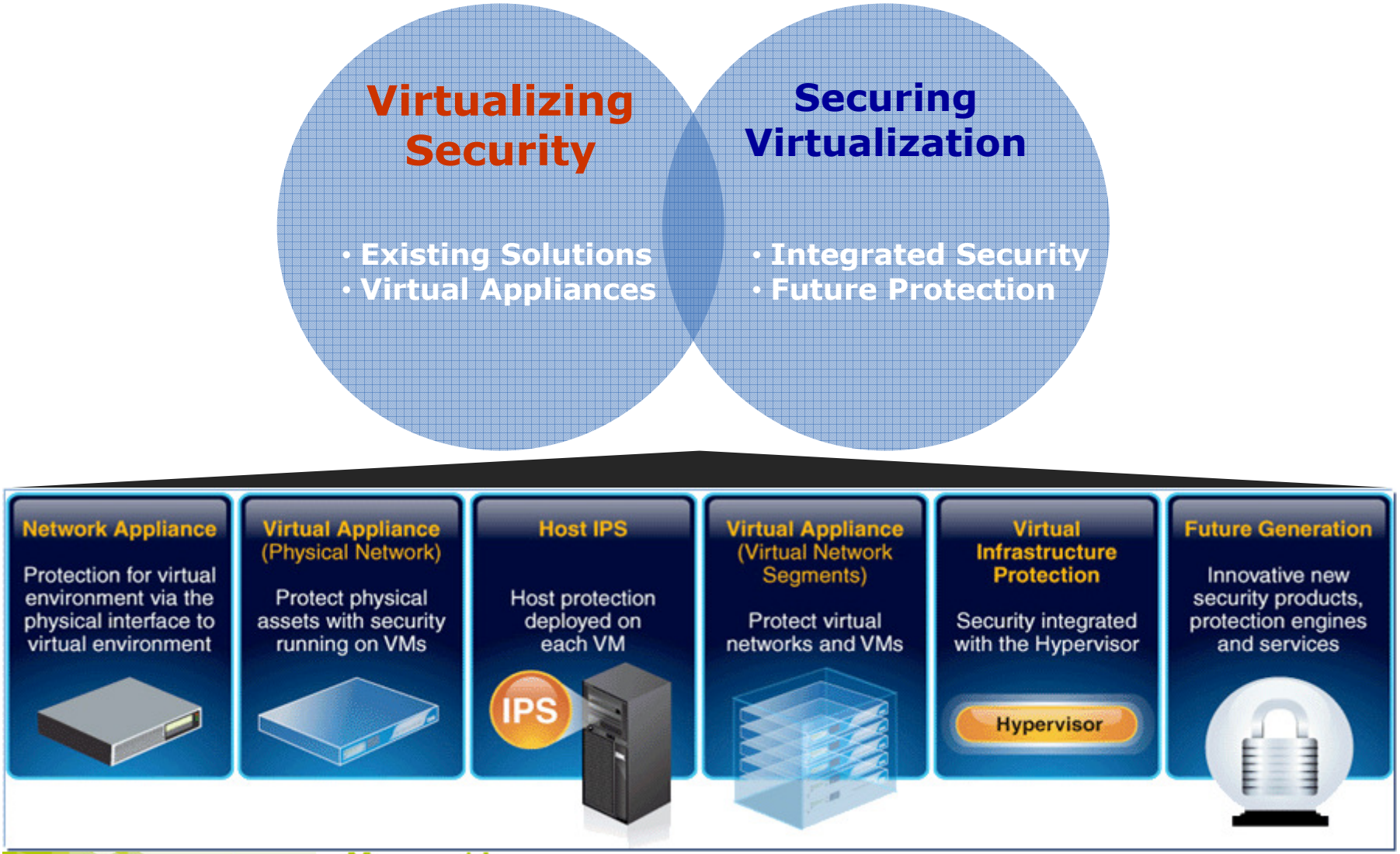
Tivoli Compliance Insight Manager



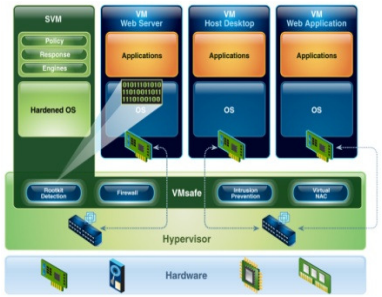
- Host-based intrusion prevention and system monitoring
- Network-based intrusion prevention and network policy enforcement
- Centralized management

Manage risk in a complex world

Virtualizing Security vs. Securing Virtualization



Summary

Need	How IBM Security 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

Contact Details

Craig Stabler CISSP
Security Consultant
IBM Security Solutions
craig.stabler@nl.ibm.com