



**Fabio Panada**

Client Technical Professional Leader Tivoli ISS -  
South West Europe

Virtualizzazione e Cloud  
Computing: nuove sfide per  
la gestione della sicurezza

**Security Day 2010**

## State of security on the Smarter Planet

The planet is becoming more...

-  **INSTRUMENTED,**
-  **INTERCONNECTED and**
-  **INTELLIGENT**

New possibilities.  
New complexities.  
**New risks.**



**“We have seen more change in the last 10 years than in the previous 90.”**

*Ad J. Scheepbouwer,  
CEO, KPN Telecom*

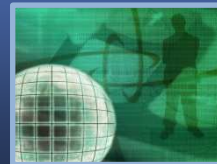
Critical Infrastructure Protection



Privacy and Identity



New and Emerging Threats



Cloud Security



## Cloud computing is...

A user experience *and* a business model

- **Applications**
  - **Data**
  - **IT resources**
- ... provided as services over the network

An infrastructure

- **Provision**
  - **Deploy**
  - **Operate**
- ... virtualized computing resources over an intranet or the Internet

An acquisition and delivery model

- **Acquire computing services through the network**
- **Improve business performance**
- **Control costs**

A way to reduce IT complexity and accelerate business value



## Cloud computing is...

- ...an enterprise architecture
- ...consolidated onto servers
- ...with virtualized resources rapidly provisioning standardized services
- ...over a public or private network
- ...leading to cost savings and business innovation



## What is Cloud Security?

Confidentiality, integrity, availability  
of business-critical IT assets

Stored or processed on a cloud computing platform



**There is nothing new under the sun  
but there are lots of old things we don't know.**

*Ambrose Bierce, The Devil's Dictionary*





## Security remains the top concern for cloud adoption

**80%**

Of enterprises consider security the #1 inhibitor to cloud adoptions

*"How can we be assured that our data will not be leaked and that the vendors have the technology and the governance to control its employees from stealing data?"*

**48%**

Of enterprises are concerned about the reliability of clouds

*"Security is the biggest concern. I don't worry much about the other "-ities" – reliability, availability, etc."*

**33%**

Of respondents are concerned with cloud interfering with their ability to comply with regulations

*"I prefer internal cloud to IaaS. When the service is kept internally, I am more comfortable with the security that it offers."*

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)



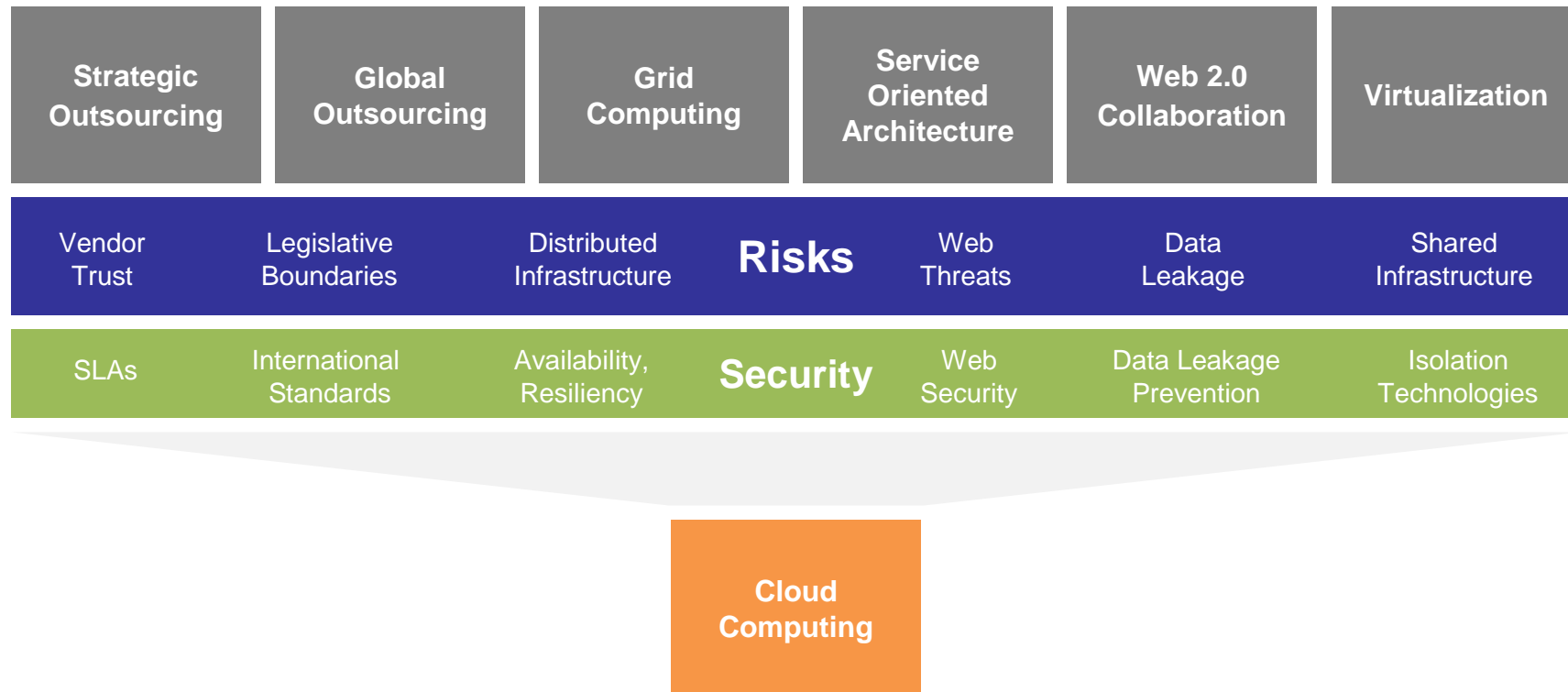
## Recent Analyst Reports Confirm **General Concerns** – But also Highlight Security as a **Potential Market Differentiator**

- “Securing your applications or data when they live in a cloud provider’s infrastructure is a complicated issue because you **lack visibility and control** over how things are being done inside someone else’s network.” Forrester, 5/09
- “Large enterprises should generally **avoid placing sensitive information in public clouds**, but **concentrate on building internal cloud and hybrid cloud capabilities in the near term.**” Burton, 7/09
- “Cloud approaches offer a **unique opportunity to shift a substantial burden for keeping up with threats to a provider** for whom security may well be part of the value proposition.” EMA, 2/09
- Gartner’s 7/09 “Hype Curve for Cloud Computing” positions Cloud Security Concerns into the **early phase** (technology trigger, will raise), and gives it a time horizon of **5-10 years**
- “**Highly regulated or sensitive proprietary information should not be stored or processed in an external public cloud-based service** without appropriate visibility into the provider’s technology and processes and/or the use of encryption and other security mechanisms to ensure the appropriate level of information protection.” Gartner 7/09



## Why is security important?

Security enables companies to pursue new, more efficient IT business models.



Cloud Computing is a natural evolution of the evolving IT paradigms listed above.

A variety of **security technologies, processes, procedures, laws, and trust models** are required to secure the cloud. **There is no silver bullet!**

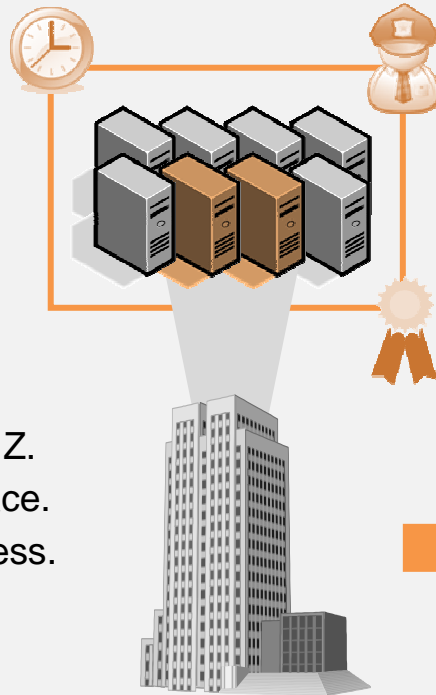




## Cloud Security 101: Simple Example

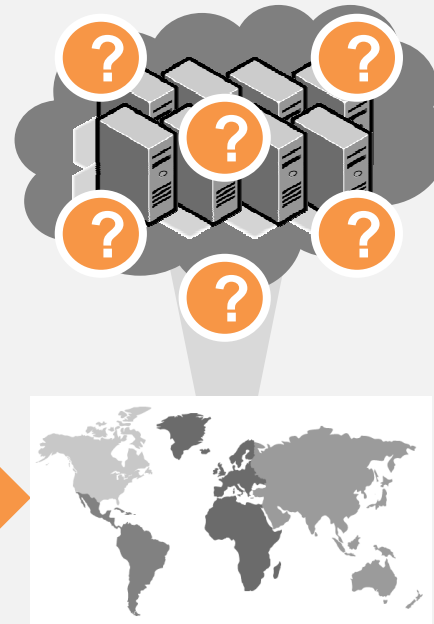
TODAY

TOMORROW



### We Have Control

It's located at X.  
It's stored in server's Y, Z.  
We have backups in place.  
Our admins control access.  
Our uptime is sufficient.  
The auditors are happy.  
Our security team is engaged.



### Who Has Control?

Where is it located?  
Where is it stored?  
Who backs it up?  
Who has access?  
How resilient is it?  
How do auditors observe?  
How does our security team engage?

**Lesson Learned:** We have responded to these questions before...  
clouds demand **fast, responsive, agile** answers.



In the **Cloud**, a single web connection may control...

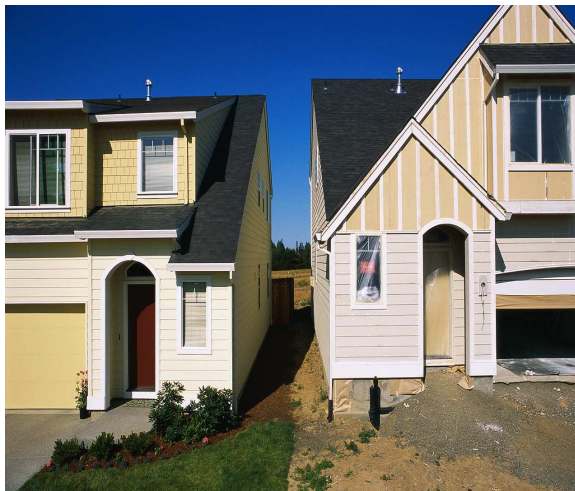


...an **entire data center.**

Virtualization has many benefits but 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**



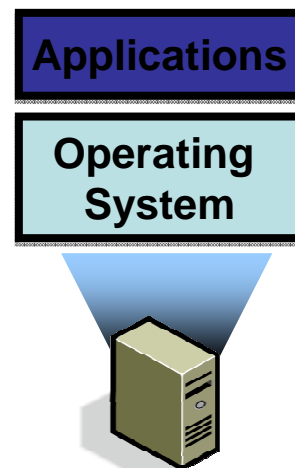
**After Virtualization**



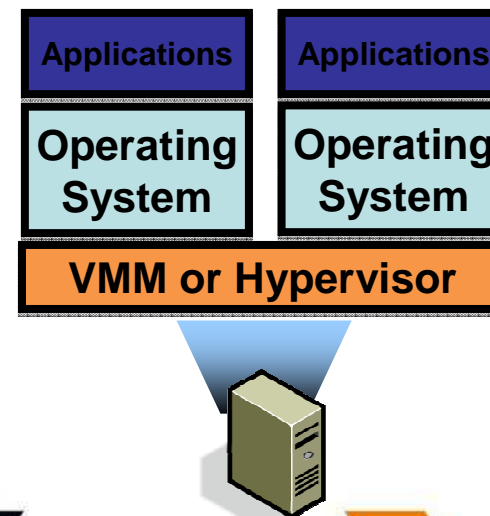
Virtualization has many benefits but introduces new complexities

- 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

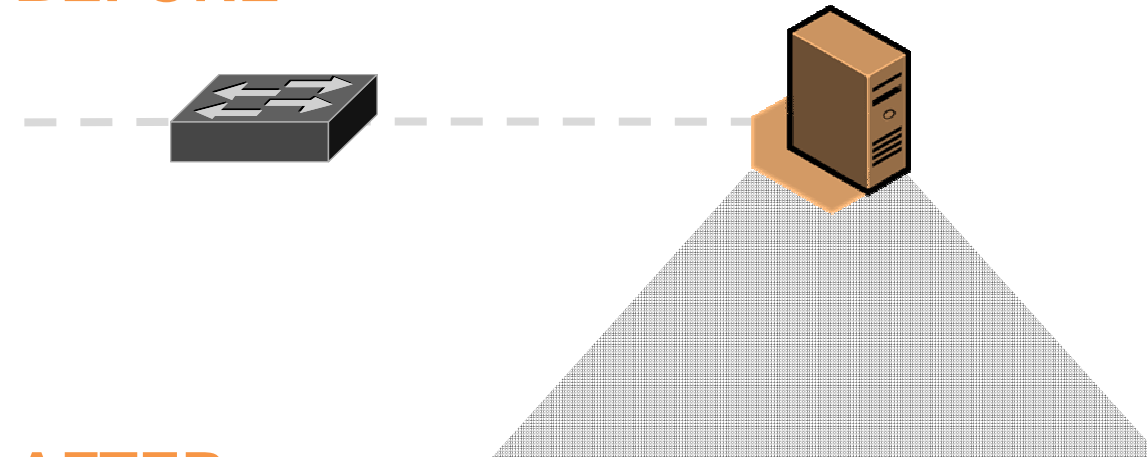


## After Virtualization



## Common security-centric questions with virtualization

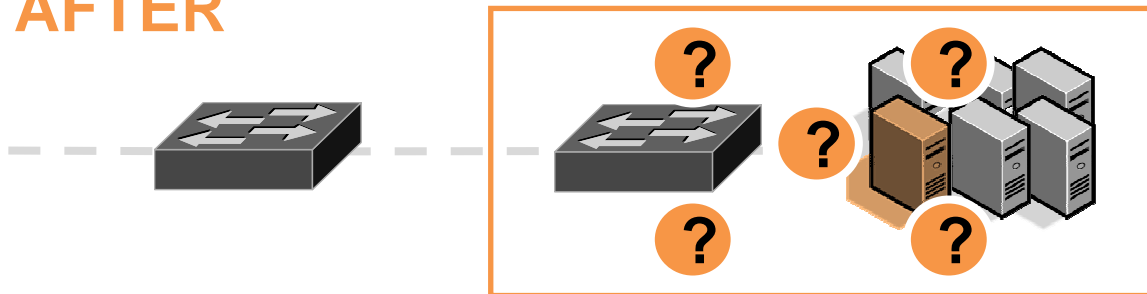
**BEFORE**



### 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.

**AFTER**



### 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?





## Common security-centric concerns with virtualization

	Physical Network	Virtual Security
Network IPS	Block threats & attacks at perimeter and between network segments	Block threats & attacks on virtual network segments
Server Protection	Secure each physical server with multi-layered protection & reporting on a single agent	Securing each VM as if it were a physical server can mean significant time and cost to system admin
System Patching	Patch critical vulnerabilities on each server and network	Dynamic environments lead to unpatched VMs; Difficult to track VM sprawl and keep VMs patched
Security Policies	Set policies specific to critical applications in each network segment & server	Virtualization often drives variety of OS and apps on a single server, so security policies must be more encompassing – web, data, OS coverage, databases, etc.
Integrate Security w/ Virt. Infrastructure	NA	<i>New frontier of risk requires dedicated features to protect the hypervisor &amp; assist in VM management</i>



## Can Virtualization *HELP* Mitigate These Risks?

- **Transparency**

- No reconfiguration of the virtual network
- No heavy presence in the guest OS

- **Security consolidation**

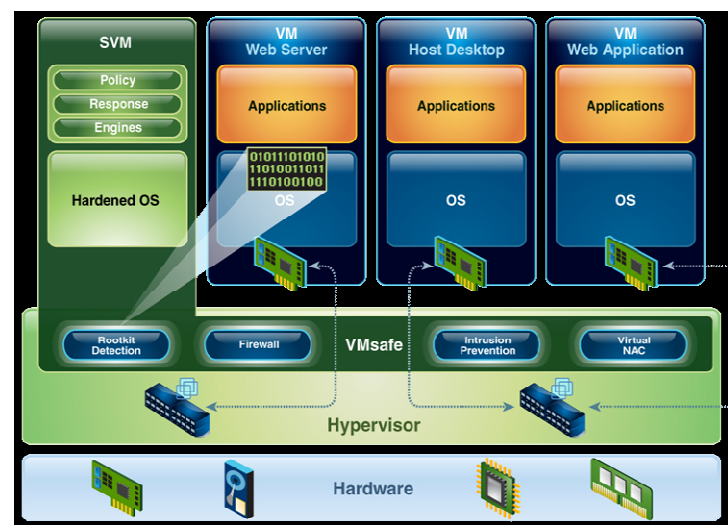
- 1:many protection-to-VM ratio
- Reduced attack surface in the guest OS

- **Automation**

- Privileged presence gives SVM holistic view of the virtual network
- Protection automatically applied as VM comes online

- **Efficiency**

- Eliminates redundant processing tasks
- Protection for any guest OS



## Current best practices for securing virtualization through compliance-oriented internal controls

1. Harden platforms to reduce the risk unauthorized access
2. Configuration and change management processes should be extended to encompass the virtual infrastructure
  - Can add cost and complexity for system administrator to continuously reconfigure in a dynamic environment
  - Ensure patch management practices extend to virtualization
3. Maintain separate administrative access control although server, network and security infrastructure is now consolidated
4. Provide Virtual machine and virtual network security segmentation
5. Maintain virtual audit logging

Source: RSA Security Brief: Security Compliance in a Virtual World

[http://www.rsa.com/solutions/technology/secure/wp/10393\\_VIRT\\_BRF\\_0809.pdf](http://www.rsa.com/solutions/technology/secure/wp/10393_VIRT_BRF_0809.pdf)



## Challenges with Current Technology

- **Intrusiveness of existing solutions**
  - Reconfiguration of virtual network
  - Presence in the guest OS
- **Visibility and control gaps**
  - Virtual servers not connected to the physical network are invisible and unprotected
- **Lacks automation and transparency**
  - Static security controls are too rigid
  - Mobility
- **Resource overhead**
  - Network traffic analysis in each guest OS is redundant, consuming more CPU cycles



## Virtualizing Security vs. Securing Virtualization

### Virtualizing Security

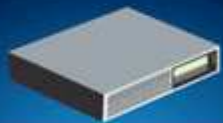
- Existing Solutions
- Virtual Appliances

### Securing Virtualization

- Integrated Security
- Future Protection

#### Network Appliance

Protection for virtual environment via the physical interface to virtual environment



#### Virtual Appliance (Physical Network)

Protect physical assets with security running on VMs



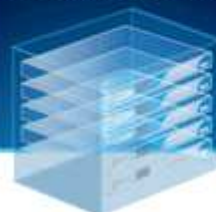
#### Host IPS

Host protection deployed on each VM



#### Virtual Appliance (Virtual Network Segments)

Protect virtual networks and VMs



#### Virtual Infrastructure Protection

Security integrated with the Hypervisor

Hypervisor

#### Future Generation

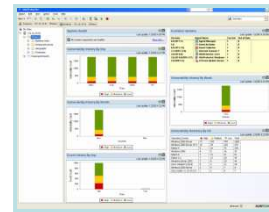
Innovative new security products, protection engines and services



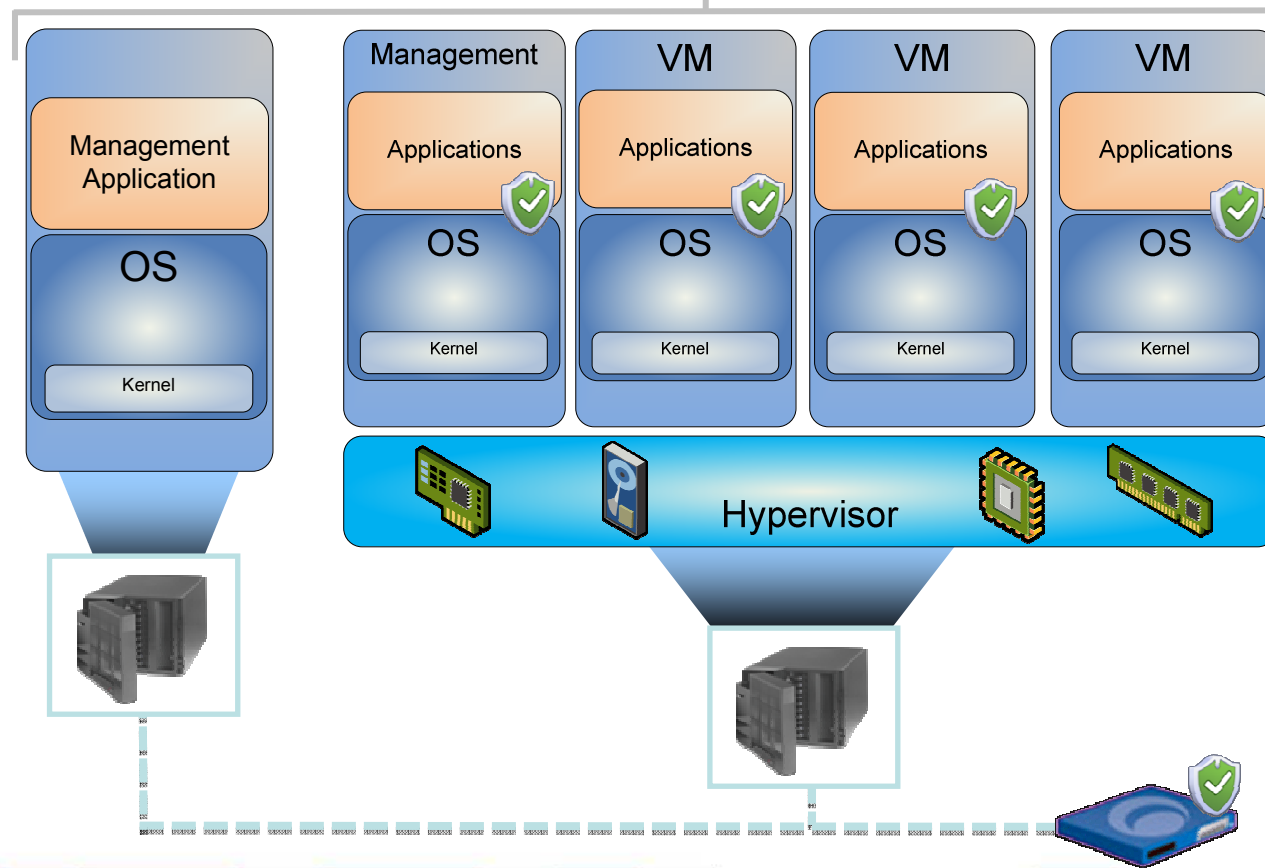


## Virtualization - Present Solution

Leveraging existing solutions to protect virtual environments



SiteProtector  
Centralized  
Management



## Virtualizing Security... Proventia Virtualized Network IPS - VIPS

- Virtual appliance (software) running as VMware image
- Full-featured Proventia IPS Firmware
- High performance traffic inspection
- Enables clients to accelerate datacenter virtualization, addresses security and compliance requirements
- Additional upgrade path for RealSecure Network Sensor customers
- Provides flexible deployment options such as running on ruggedized hardware
- World class, vulnerability-based protection powered by X-force research
- Intrusion prevention and network protection for traffic between vSwitches
- Integrate and manage virtual security with traditional network security



### Virtual Security Appliances



– Pat O'Day – CTO, Bluelock



## ...and Securing virtualization

### Next Generation Virtualization Security:

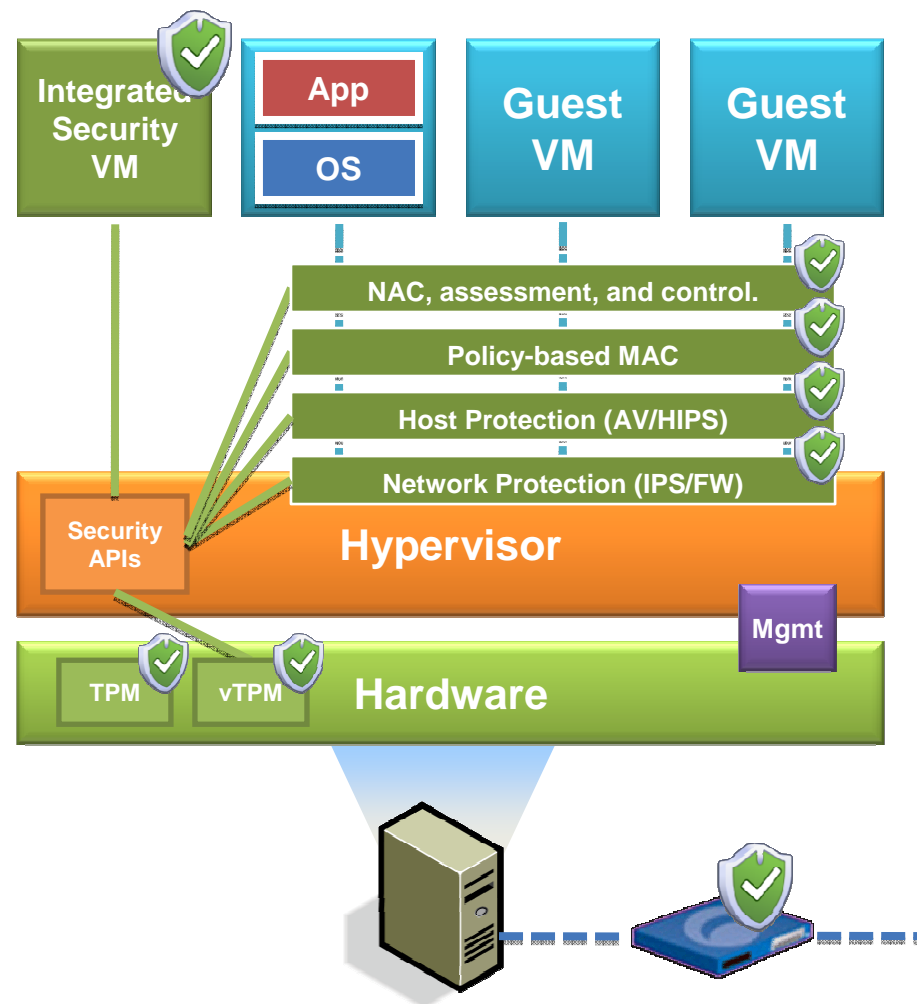
- Apply defense-in-depth.
- Shrink the management stack.
- Install Security VM on each machine.
- Integrate Security VM with VMM.

### Security VM Features:

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

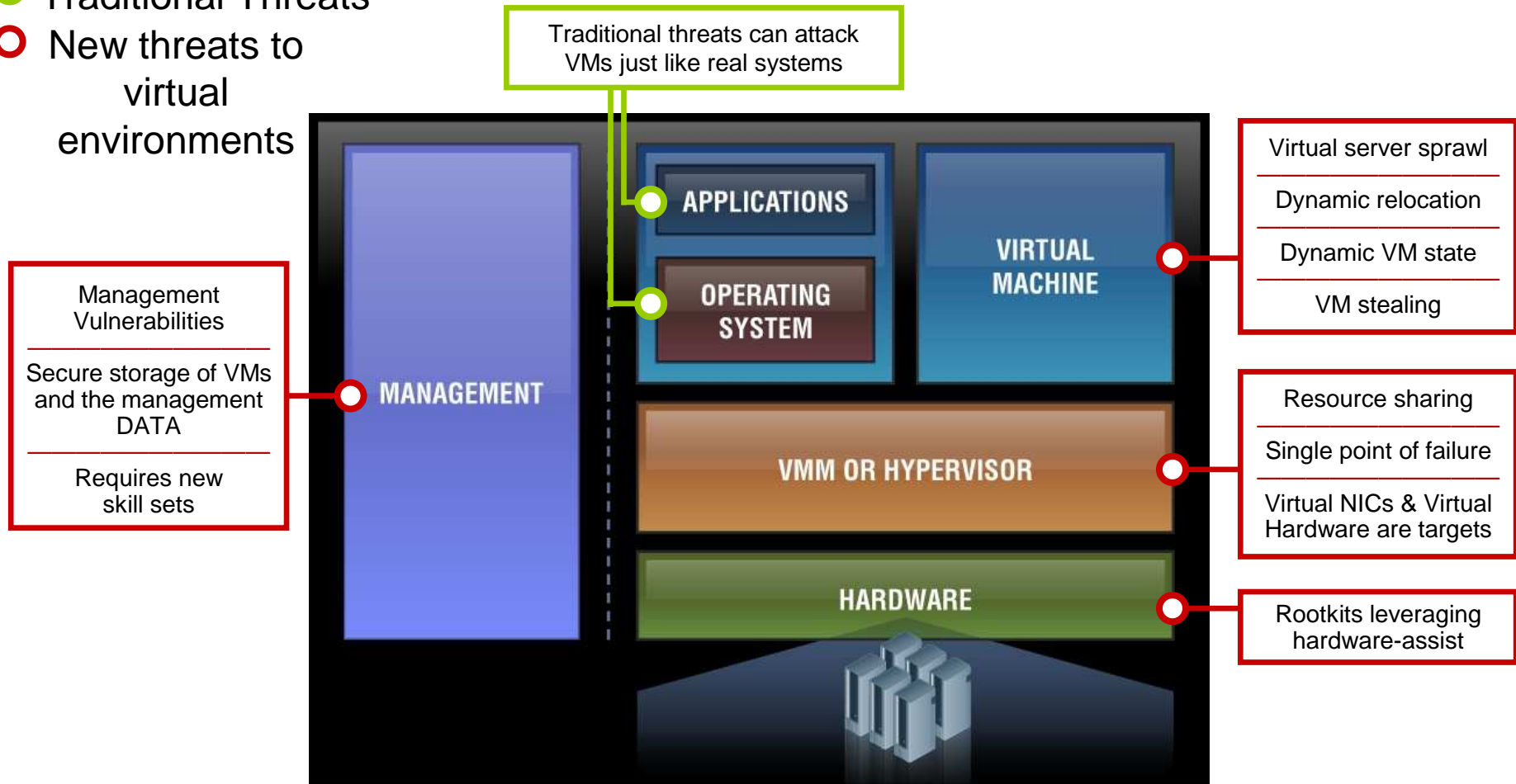
### Additional Security:

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



## Managing the Risks of Virtualization

- Traditional Threats
- New threats to virtual environments



MORE COMPONENTS = MORE EXPOSURE



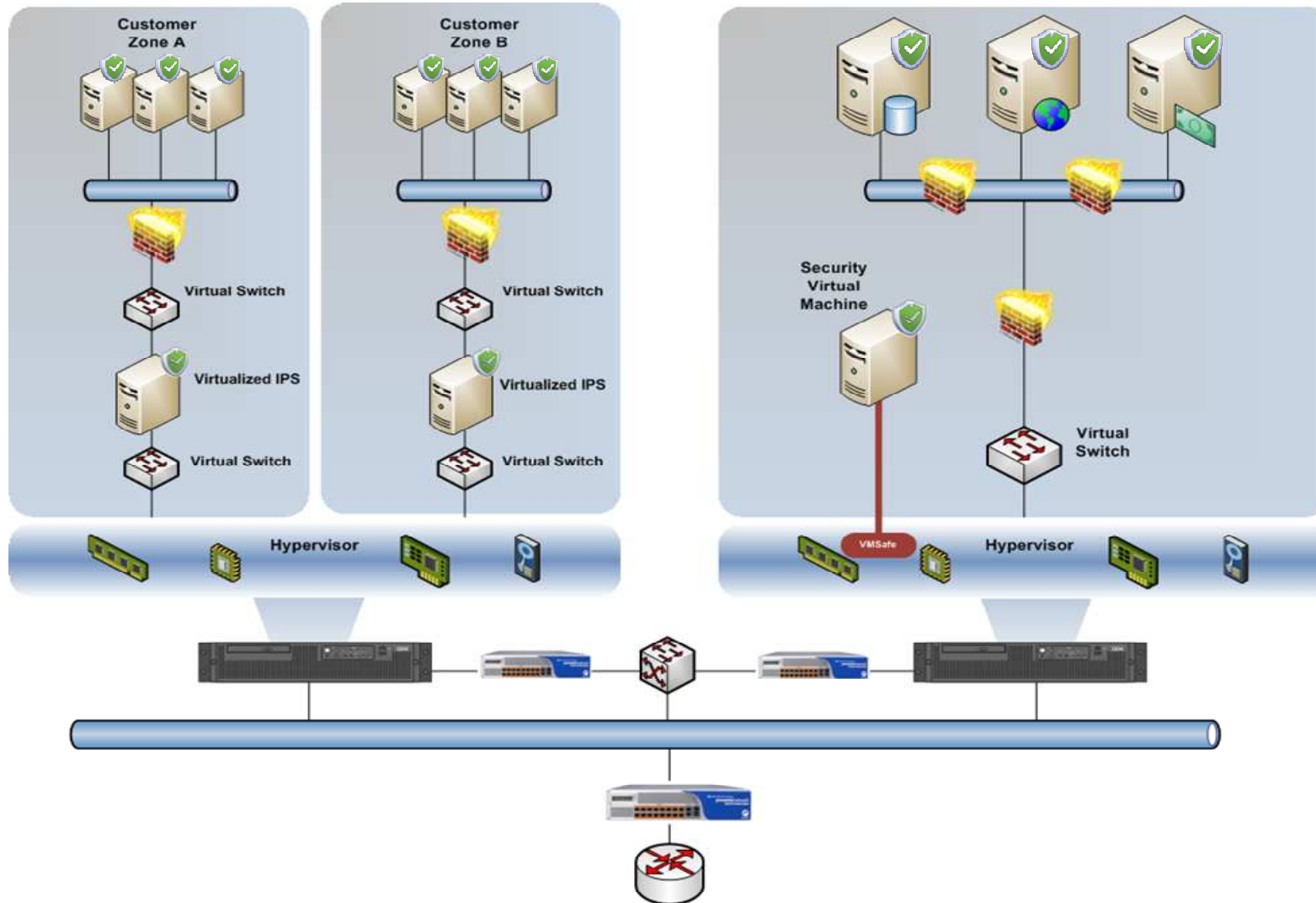
## IBM Virtual Server Security Features

- Intrusion Prevention and Firewall
  - Enforces dynamic security wherever VMs are deployed
  - Applies one Security Virtual Machine (SVM) per physical server
  - Privileged presence gives SVM a holistic view of the virtual network
  - Enables IBM Virtual Patch® technology to protect vulnerabilities on virtual servers regardless of patch strategy
  
- VM lifecycle enforcement
  - Performs automatic VM discovery in order to reduce virtual sprawl
  - Provides virtual access control and assessment by quarantining or limiting network access until VM security posture can be validated
  - Virtual infrastructure auditing
  
- VM Rootkit detection
  - Transparently inspects VMs and detects installation of rootkits
  - Reports on access and usage of the virtual environment





## Deployment Scenarios



# Security Day 2010



Tivoli ISS Provides a complete virtualization Security Portfolio at all layers

## Security Management



### Managed Security

#### Virtual SOC – Managed Security Services

Secure Web-based tool that allows you to easily monitor the security of your systems



### Enterprise Security Management

#### Proventia SiteProtector

## Virtual Machines



### Server Virtual Machines

#### Proventia Server / Server Sensor

Host-based intrusion prevention to protect guest VMs and their OS

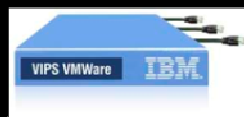


### Desktop Virtual Machines

#### Proventia Desktop

Unified security with increased ease-of-use at a lower overall cost

## Virtual Infrastructure



### Virtual Network Protection

Delivering proven network protection in a virtual form factor



### Virtual Infrastructure Protection

#### Proventia VSS

Integrated security for the entire virtual infrastructure

## Physical Infrastructure



### Physical Network Protection

#### Proventia Network Intrusion Prevention System

Transparent, in-line network appliances block attacks while allowing legitimate traffic



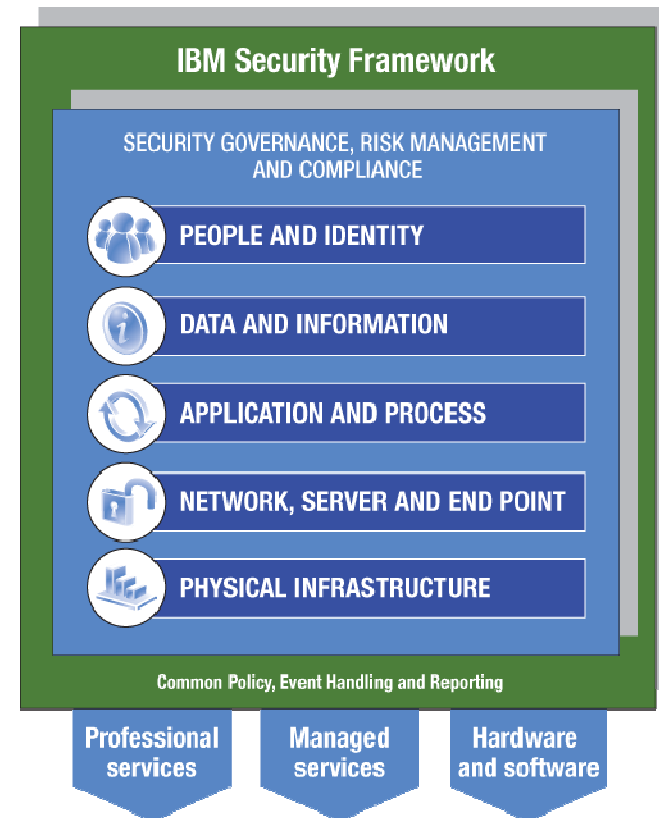
### Unified Threat Management

#### Proventia Network Multi-Function

Single cost-effective appliance for firewall, VPN, IPS, AV URL filtering, and anti-spam

## X-Force R&D -- Unmatched Security Leadership

- The only security vendor in the market with an **end-to-end framework** and solution coverage from both the business and IT security perspectives
- **15,000** researchers, developers and SMEs on security initiatives
- **3,000+** security & risk management patents
- **200+** security customer references and **50+** published case studies
- Managing over **4 Billion** security events per day for over 3,700 clients
- **40+** years of proven success securing the zSeries environment
- **\$1.5 Billion** security spend in 2008



## For more information



### **IBM Cloud Computing**

IBM approaches cloud computing from the inside out, designing a cloud environment or providing cloud-based services for each organizations unique requirements. Find out more at <http://www.ibm.com/ibm/cloud/>



### **IBM Enterprise Security**

IBM business-driven approach to enterprise security helps you to address risk and reduce cost and complexity. Find out more at <http://www-03.ibm.com/security/>



### **IBM Internet Security Systems**

Protect your IT environment from the perimeter to the core with advanced security solutions from IBM Internet Security Systems. Find out more at <http://www.ibm.com/services/security/>



### **X-Force Security Alerts and Advisories**

Only IBM X-Force can deliver preemptive security due to our unwavering commitment to research and development and 24/7 global attack monitoring. Find out more at <http://xforce.iss.net/>







Fabio Panada

[fabio.panada@it.ibm.com](mailto:fabio.panada@it.ibm.com)

Thanks

Security Day 2010