



IT Virtualisation – New challenges for IT Security Management

Christian Fahlke

**Channel Leader
IBM Internet Security Systems
Central-, Eastern Europe, Middle East& Africa**

Welcome to the **smart planet...** *and a smarter infrastructure*



The real security problem

New Methods and Motives:

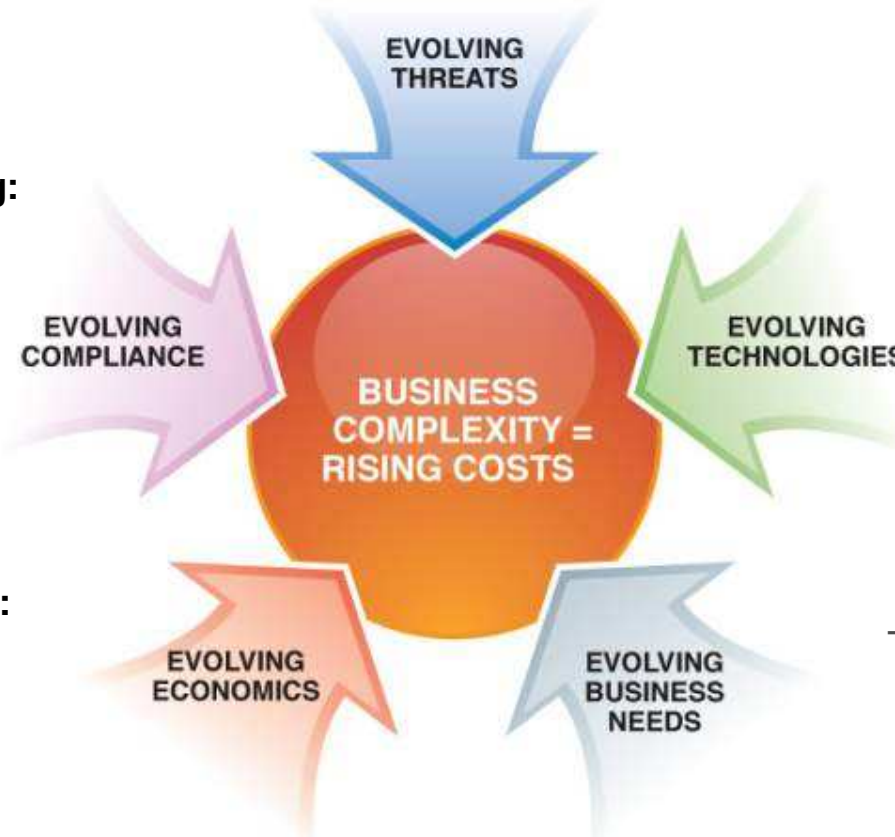
Adding to the complexity and sheer number of risks

Compliance Spending:

Investing in more point products to solve more point problems

IT Innovation:

Requiring new ways to secure the new ways we collaborate



The Global Economy:

Driving new security support requirements

Flexibility in Business Methods:

To improve operations and serve customers

Complexity remains the biggest security challenge!*

Integration is key to managing the cost and complexity of the evolving landscape

*InformationWeek 2008 Security Survey

IBM Security Solutions –why do our customers invest into virtualisation

Reduce Costs



Mitigate Risks



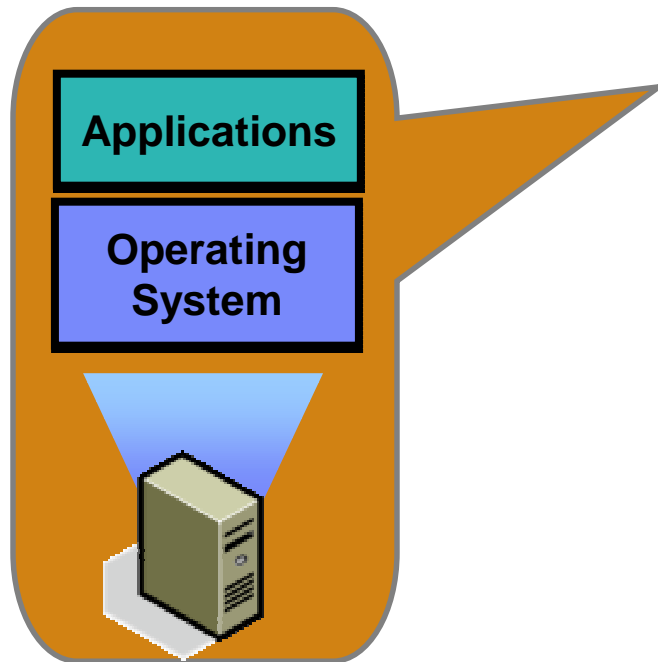
Increase Productivity



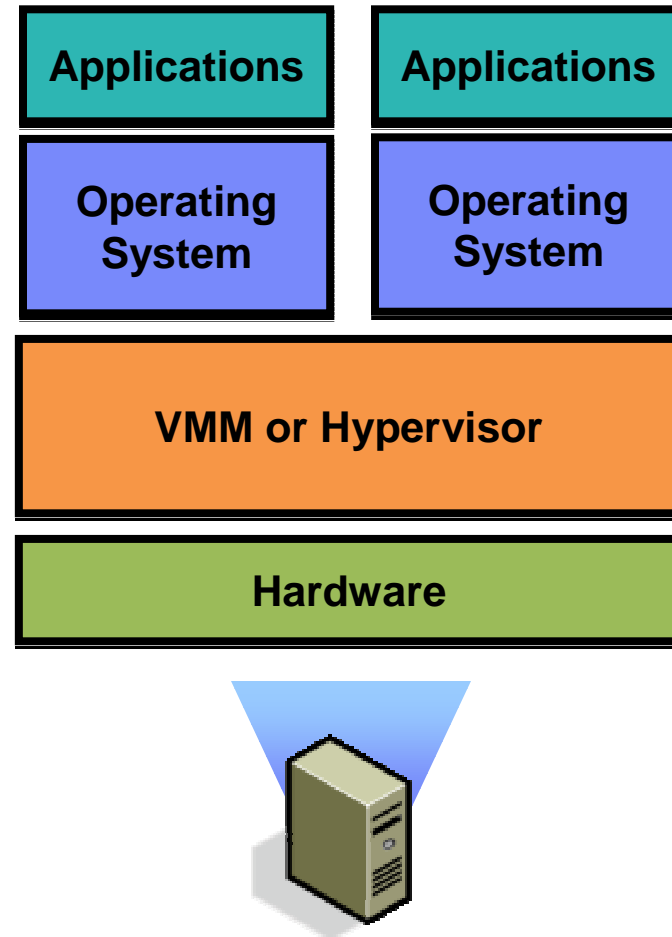
- Provide immediate savings and lower total cost of ownership
- Ensure business continuity
- Enable innovation

Basics: Virtualization Architecture

Before Virtualization



After Virtualization



What does Virtualization Change?

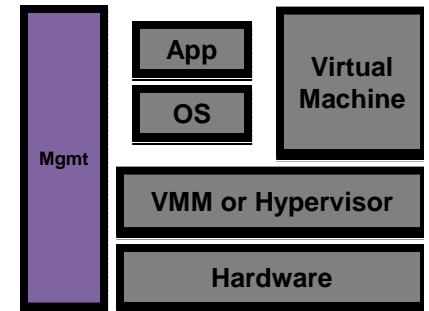
- **Everything**
 - Dynamic, fluid data-center
 - Resource pools
 - Commoditization of everything
 - Increased efficiency
- **Nothing**
 - Virtual IT is still IT
 - Security, sprawl, management, complexity, heterogeneity



Security and Risk Implications

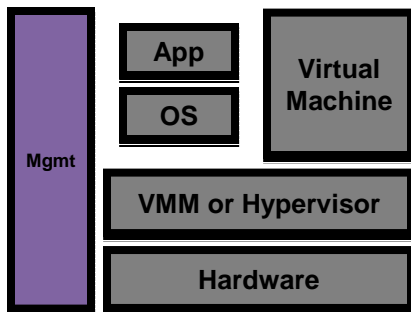
Virtualization and Enterprise Security

- **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
 - Compromise of Virtual Console/Management
 - Provision my own evil guest(s)
 - Adjust resource quotas
 - Shut OFF guest(s)
 - Compromise of the VMM/Hypervisor
 - IsGameOver()

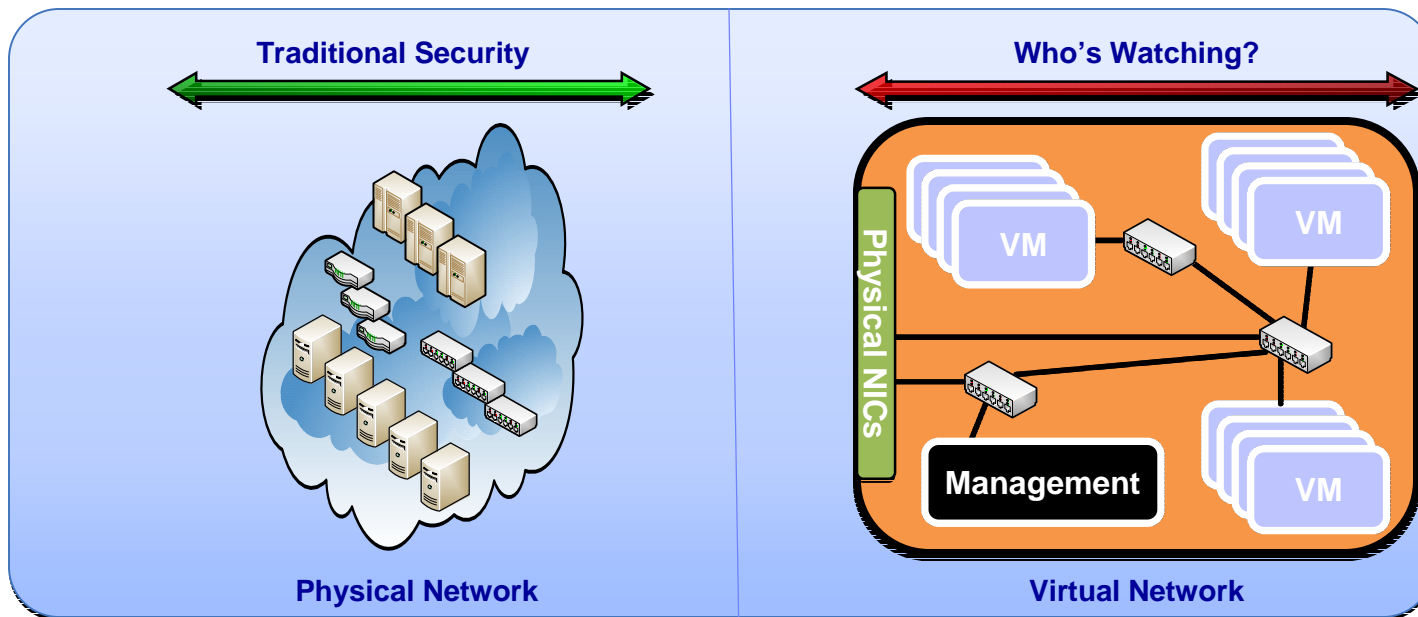


Operational and Organizational Implications



Organizational Ownership?

- Who owns the Virtual [Fill in the Blank] ?
 - Network Admin
 - Server Admin
 - Application Owners
 - Data Custodians



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



“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?

The IBM Security Framework

From Reactive Security to a Risk-Aware Enterprise



Securing Virtualization: Tomorrow

Next Generation Virtualization Security:

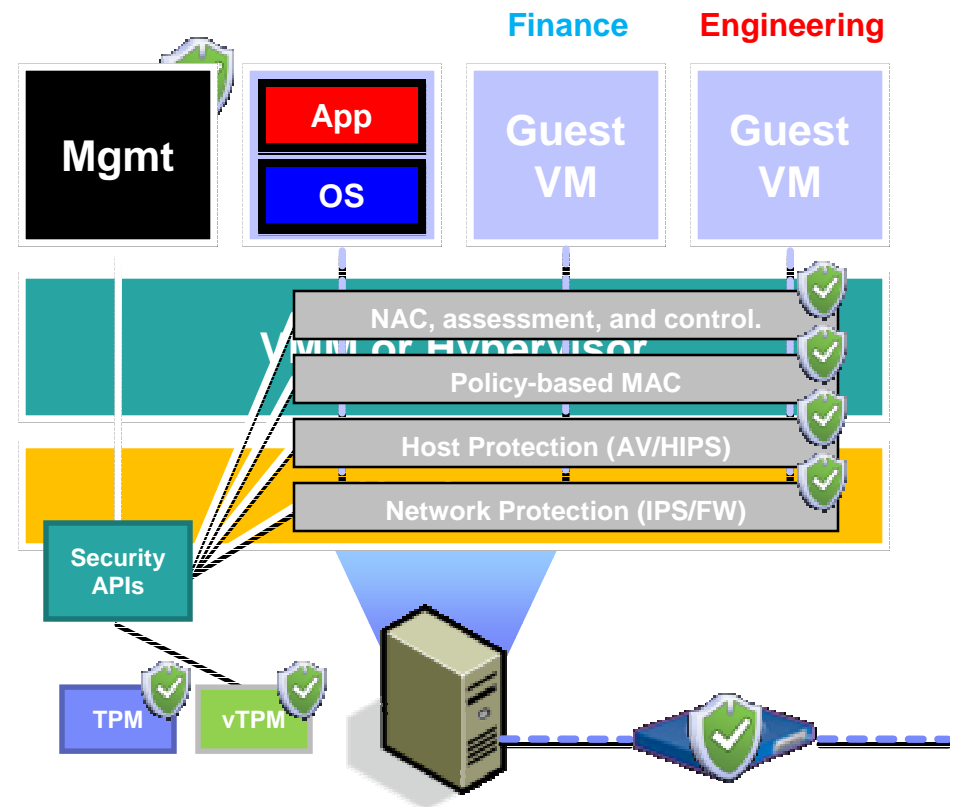
- Apply defense-in-depth.
- Shrink the management stack.
- Install Security VM on each machine.
- Integrate Security VM with VMM.

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)



The IBM logo is displayed in white, bold, sans-serif capital letters in the top left corner of the slide. The background of the slide is a dark blue gradient with a faint, large-scale pattern of interlocking puzzle pieces. One puzzle piece in the center is highlighted in a lighter, textured brownish-grey color.

IBM

Christian Fahlke – Channel Leader
IBM Internet Security Systems

Central-, Eastern Europe, Middle East & Africa
fahl@ch.ibm.com

Thank you