



# The Phantom Menace - Security

David M Lynch MBA  
dmlynch@embotics.com

**INTEROP<sup>®</sup>**

BUSINESS. TECHNOLOGY.  
ONE WEEK. ONE PLACE.

# The Phantom Menace: - Security

“As enterprises rush to virtualize they need to be aware of the new security considerations and challenges introduced by virtualization. The use of virtualization creates a number of security issues related to the tracking and patching of VMs and hosts. The use of Virtual Appliances introduces new system variants that have to be secured and maintained. Now that VMs can exist in many formats and multiple states, the task of securing them can get much more complicated. Mothballed VMs may reintroduce viruses and worms that were previously considered eradicated in the enterprise. The easy access to free host software, combined with the growing number of virtual machines and the public availability of virtual appliances will challenge enterprises trying to protect & secure their environments. This session will focus on security challenges introduced by virtualization and offer some advice and tips on how to deal with them.”

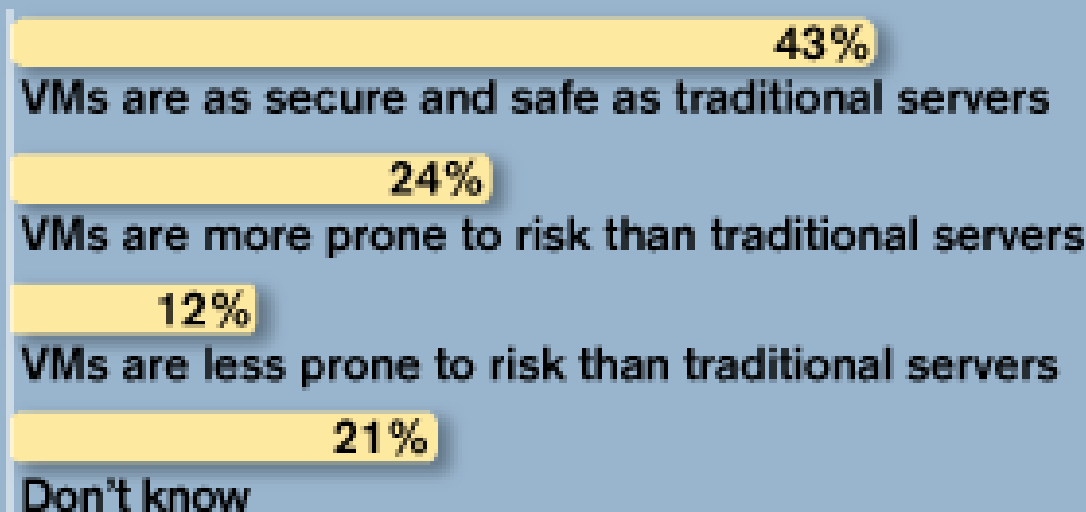
# Agenda

- Which is it.. A Phantom or a Menace?
- Just how risk-exposed are we?
- Control in a Virtual world
- New Technologies
- Advice and Tips

# Is there a security problem?

## Safe And Sound (Maybe)

In your opinion, how do virtual servers compare with traditional server environments for information protection and security?



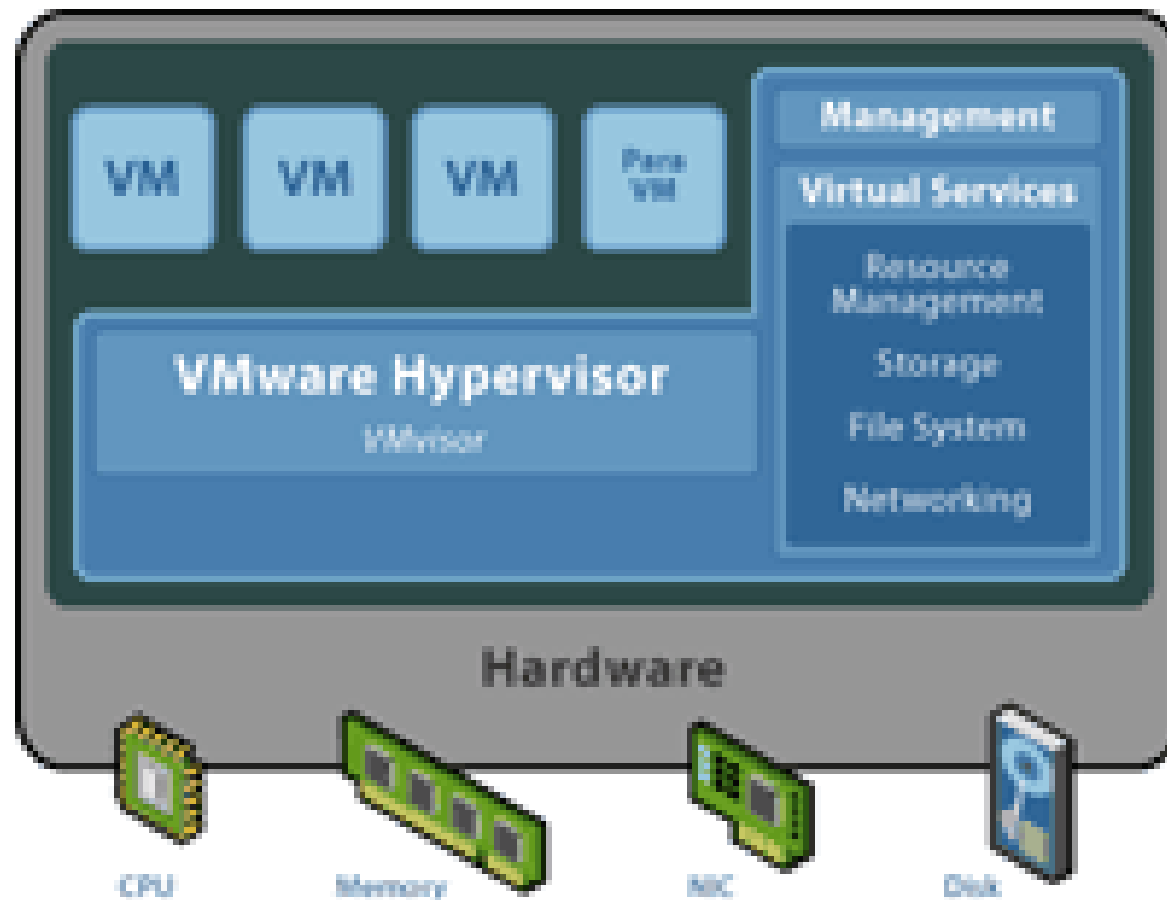
% of respondents

Data: InformationWeek online poll of 384 readers

# State of the Market

- Broad customer adoption – especially in the top end (F100/F1000) (+/- 40% of worldwide organizations with more than 500 employees).
- Installed base expected to continue to grow by 20%, over the next 18 months.

# Architecture



# New security issues

- Another Operating System in the Datacenter
- New attacks could target the virtualization layer
- New attacks could target newer hardware running older operating systems
- Communication within a hypervisor is essentially a “private Lan”
- Guest to Guest attacks
- Virtual Appliance Software delivery
- Server Mobility



# Another Operating System

- Maturity of the hypervisor
- Breaking out of a guest OS into the hypervisor
- Hypervisor root kit installation

# A “private” Lan

- Guest to guest attacks
- Traffic in the open
- Denial of service through VM "overloading"

# Virtual Appliances

- New system variations
- Patching
- Certifying

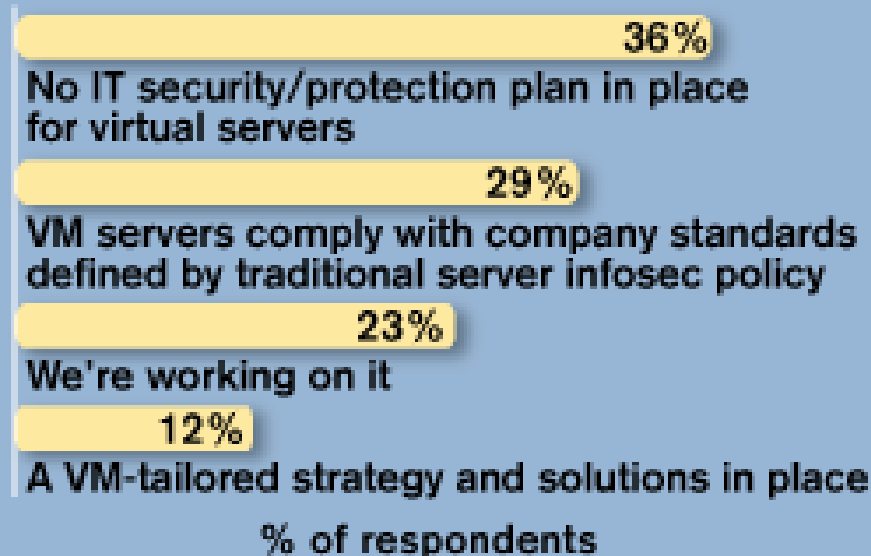
# Mobility

- Mobile VMs compromise “security in layers”
- Using virtualization breaks existing data center management tools
- Traditional security tools may not work well

# How worried are we?

## Not A Perfect Fit

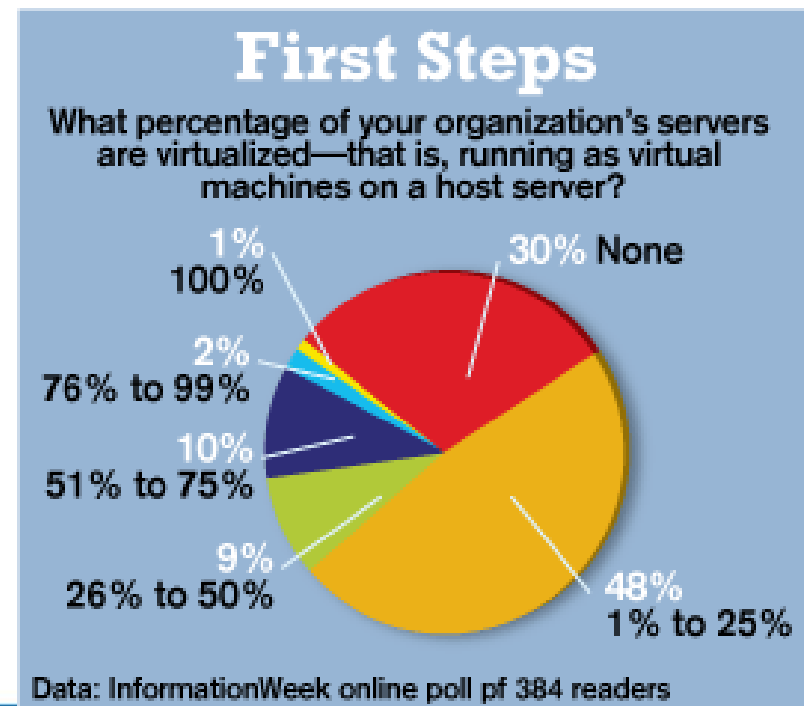
Does your organization have a formal security/information protection strategy for virtualized server environments?



Data: InformationWeek online poll of 384 readers

# Shallow penetration

- Led by departments rather than corporate strategy
- On average only 7% of physical servers are virtualized today (IDC)



# But, it will eventually get everywhere:

“By 2010, Intel projects that 25% of enterprise data center servers will be running in virtualization mode”. Intel - July 2007

“50% of physical servers will be virtualized by 2011”. - (IDC)

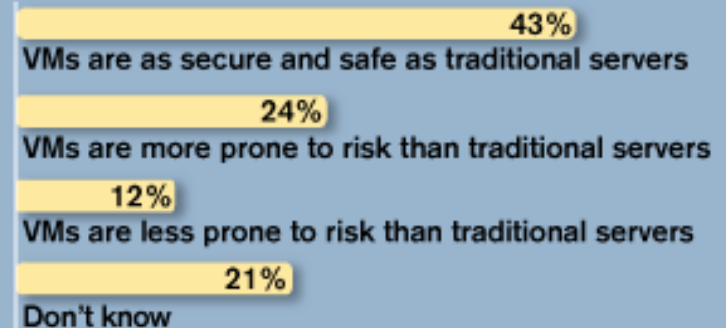
“Virtualization will be part of nearly every aspect of IT by 2015” - Gartner May 2007

# How worried should we be?

- The normal "Arms Race"
  - But attacks will come
  - It's too tempting a target

## Safe And Sound (Maybe)

In your opinion, how do virtual servers compare with traditional server environments for information protection and security?

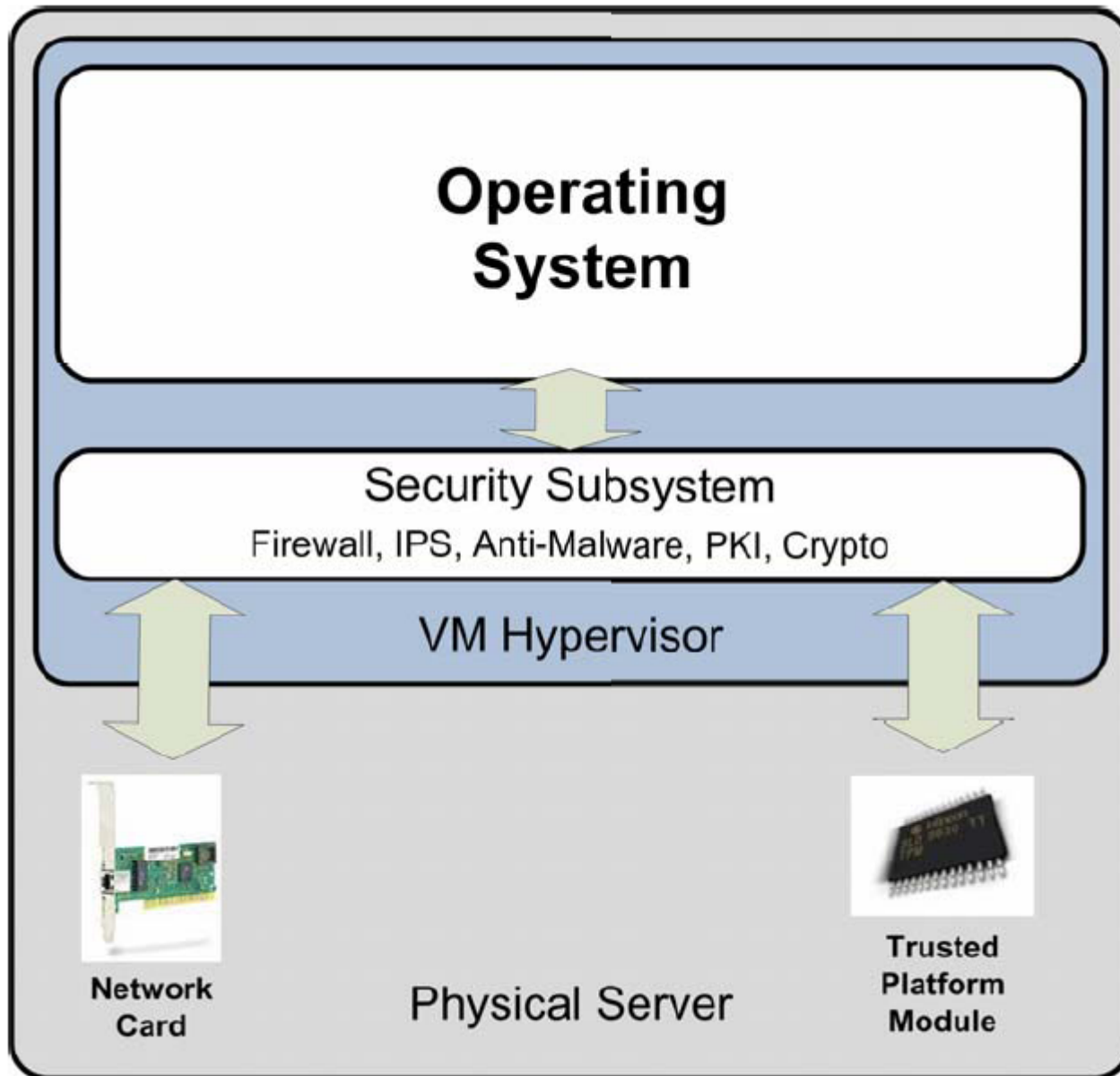


% of respondents

Data: InformationWeek online poll of 384 readers

# New Security Technologies

- Security inside the hypervisor
- Virtual Appliances
- Security as a plug-in to the hypervisor
  - Trusted Platform Module (TPM)
- Control and Management Systems



# Best Practices

- Maintain Security Group Focus
- Track
- Control
- Classify and segment
- Authorize
- Validate
- Protect

---

# Questions?

---

# Security concerns

- Desktop virtualization - A way around NAC