TREND MICRO

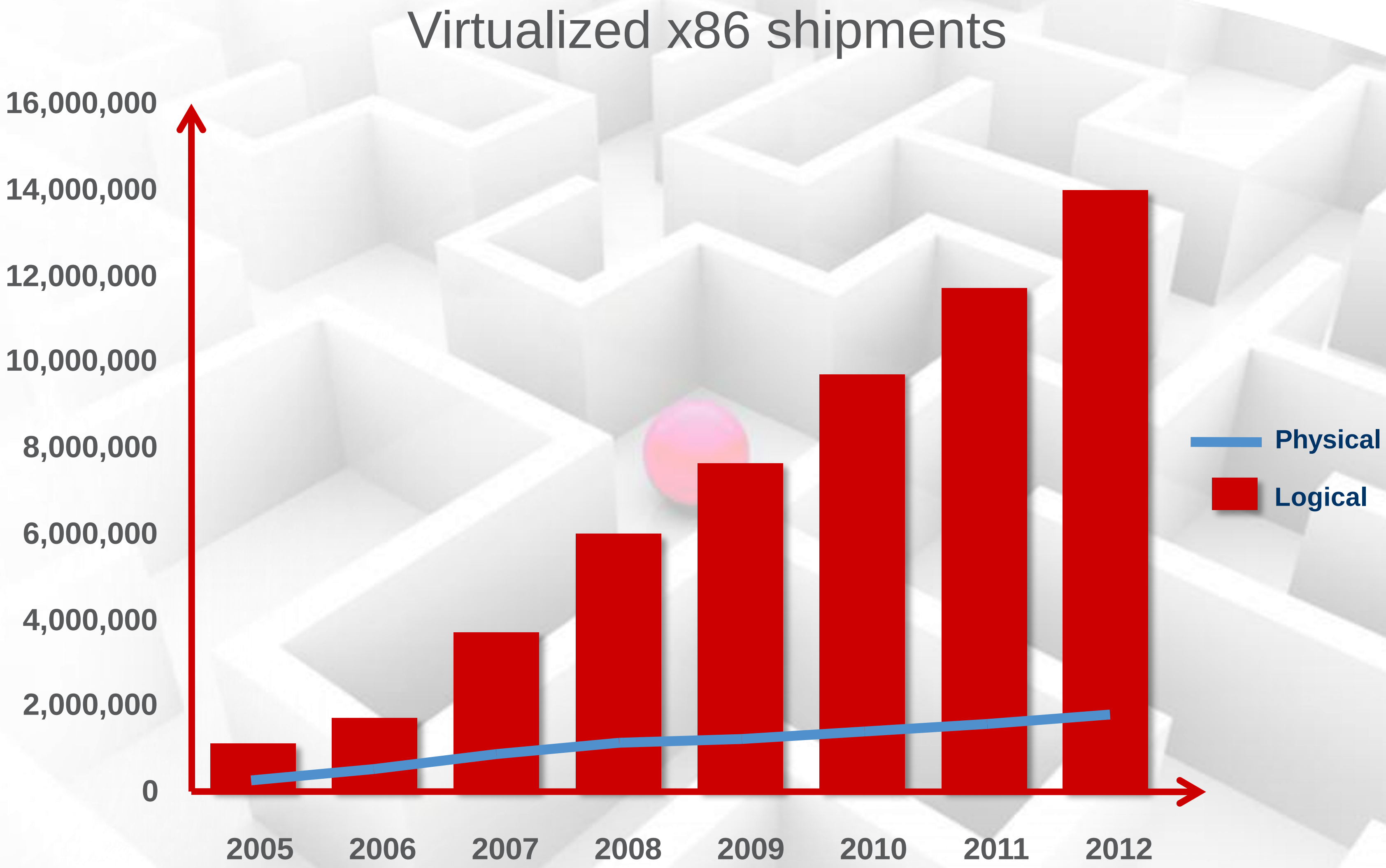
Securing Your Web World

# Securing Your Virtual World

Harri Kaikkonen

Channel Manager

# Virtualisation On The Rise

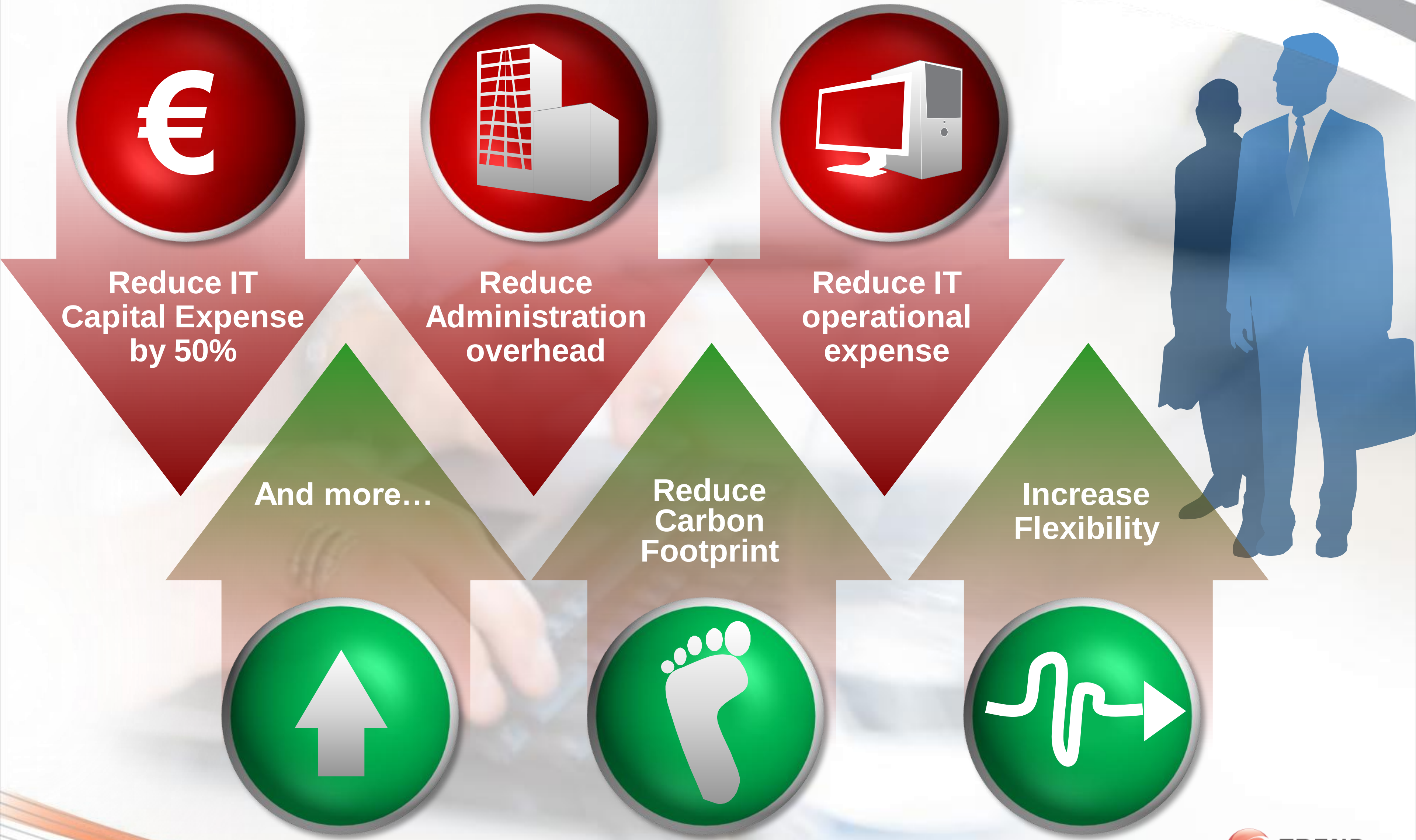


Source: IDC 2009

# Agenda

- The Challenge of Virtual Security
- The Host Defends Itself
- Data is Secure and Controlled in the Public Cloud
- Securing the Computing Chain

# The Benefits of Virtualisation



Reduce IT Capital Expense by 50%

Reduce Administration overhead

Reduce IT operational expense

And more…

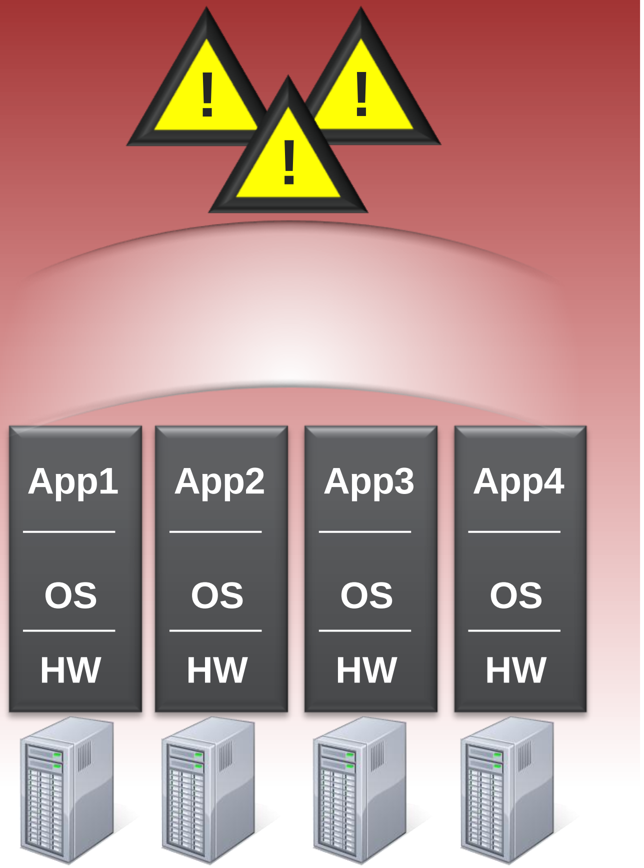
Reduce Carbon Footprint

Increase Flexibility

# Virtualisation Creates Security Challenges

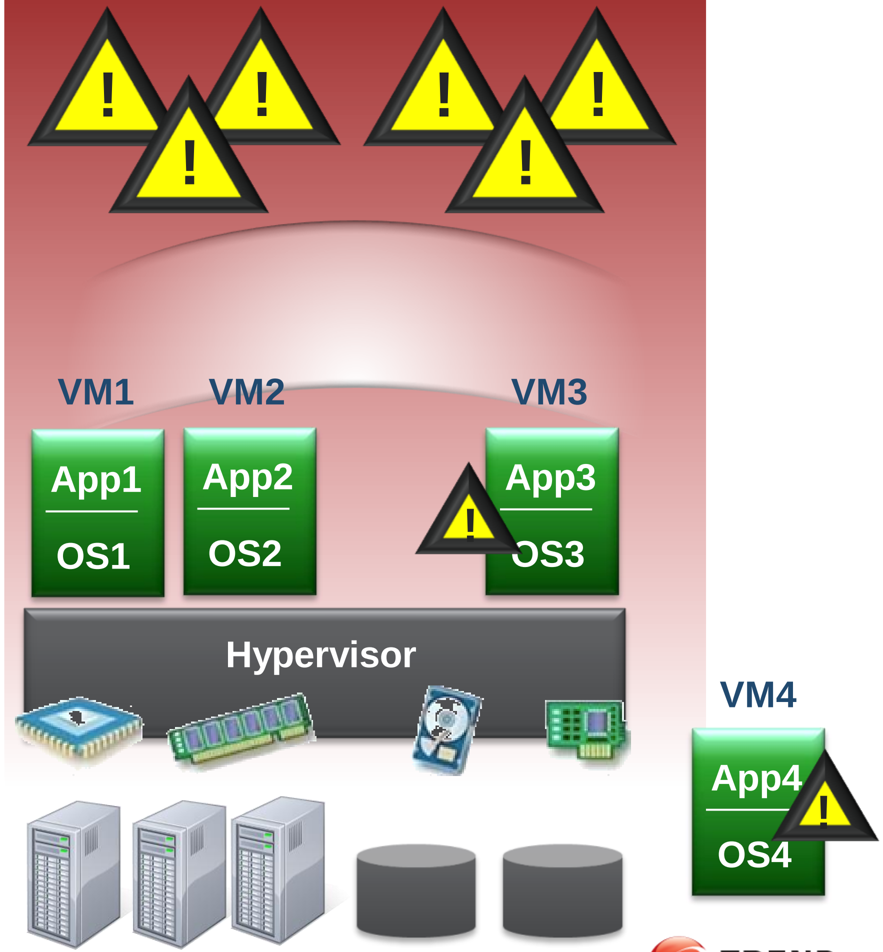
## Old Model

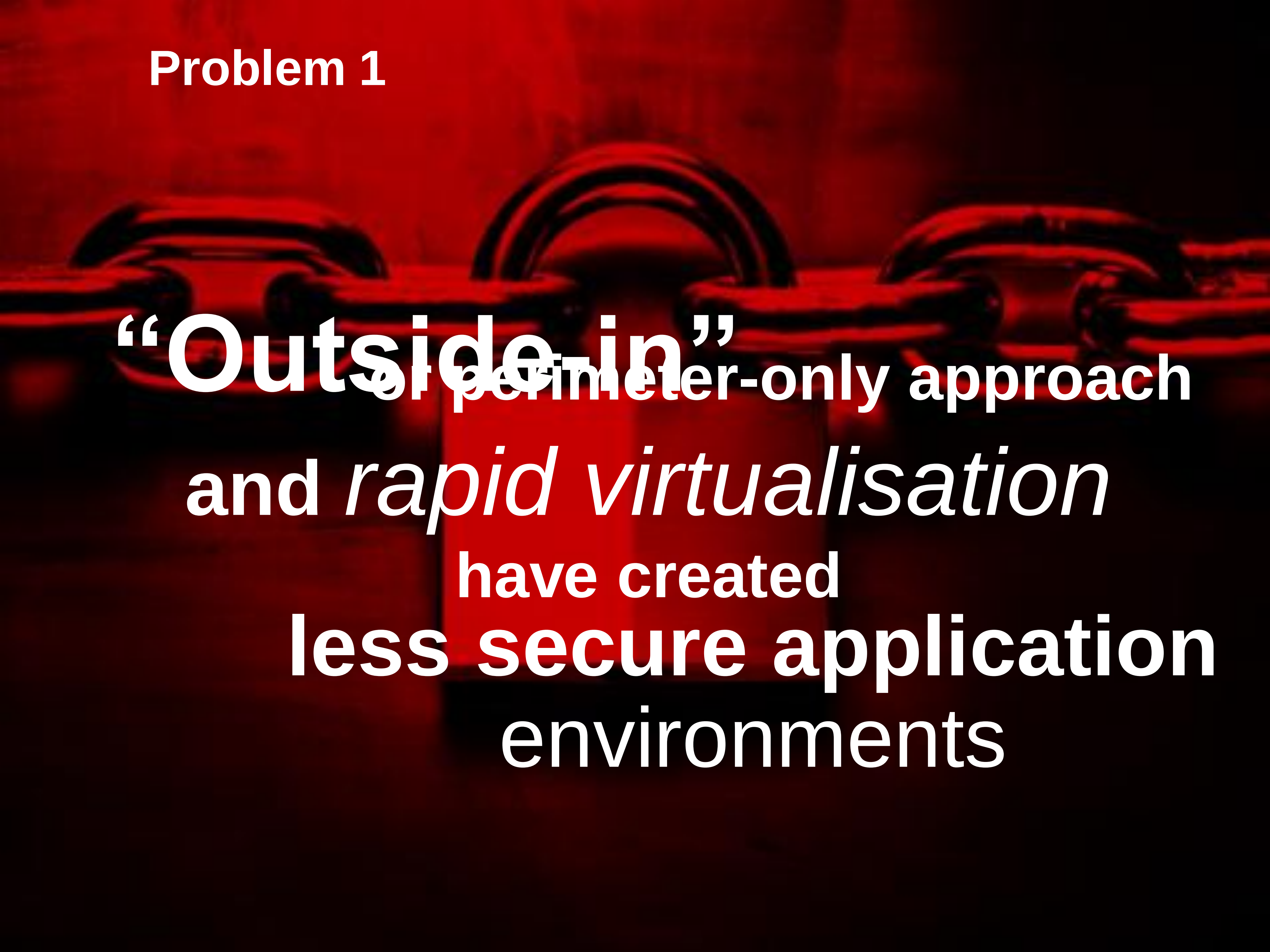
Infrastructure security protects applications & servers



## New Model

Virtual servers and apps move, change…
IPS needs reconfiguration…
so does firewall……where is file OS ?…





## Problem 1

**“Outside-in” or perimeter-only approach**

**and** *rapid virtualisation*

**have created**

**less secure application**

environments

# Where is Our Company Data?

"I can replace my device, but not my data"

"I have data in multiple places"

"I use company applications, but I put my data anywhere"

Company Data

Information store 1 Laptop

INFECTED

Information store 2: Mobile phone/PDA

STOLEN

Information store 3: Internet-based app – Gmail, Peoplesoft

DOWN, HACKED

## Problem 2

**Data protection** is the most strategic concern

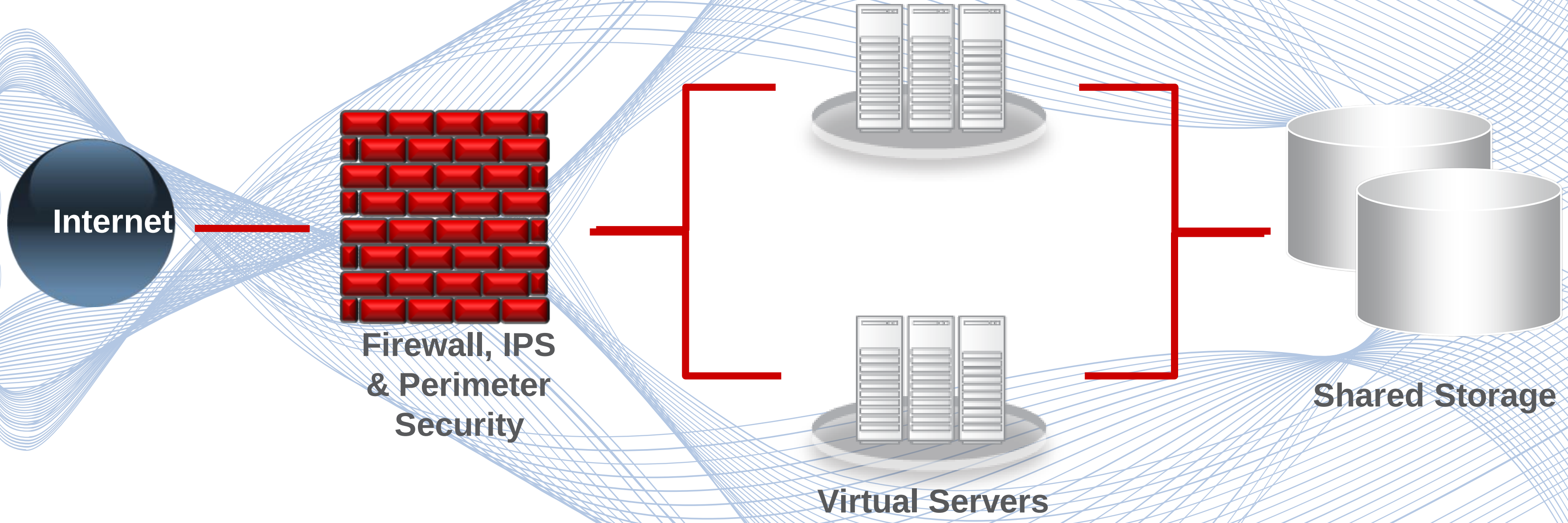
but data is *mobile*,

**distributed,**

and unprotected

# Solution: The Host Defends Itself

# Private Virtualized Datacenter

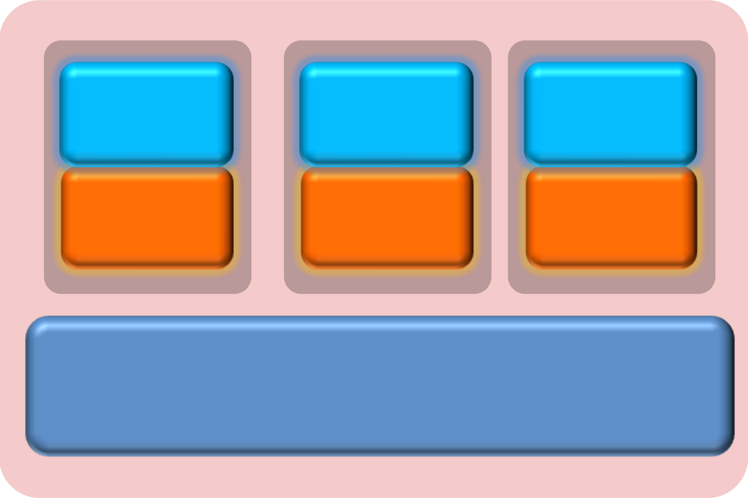


# VMs Need Specialized Protection

Same threats in virtualized servers as physical.

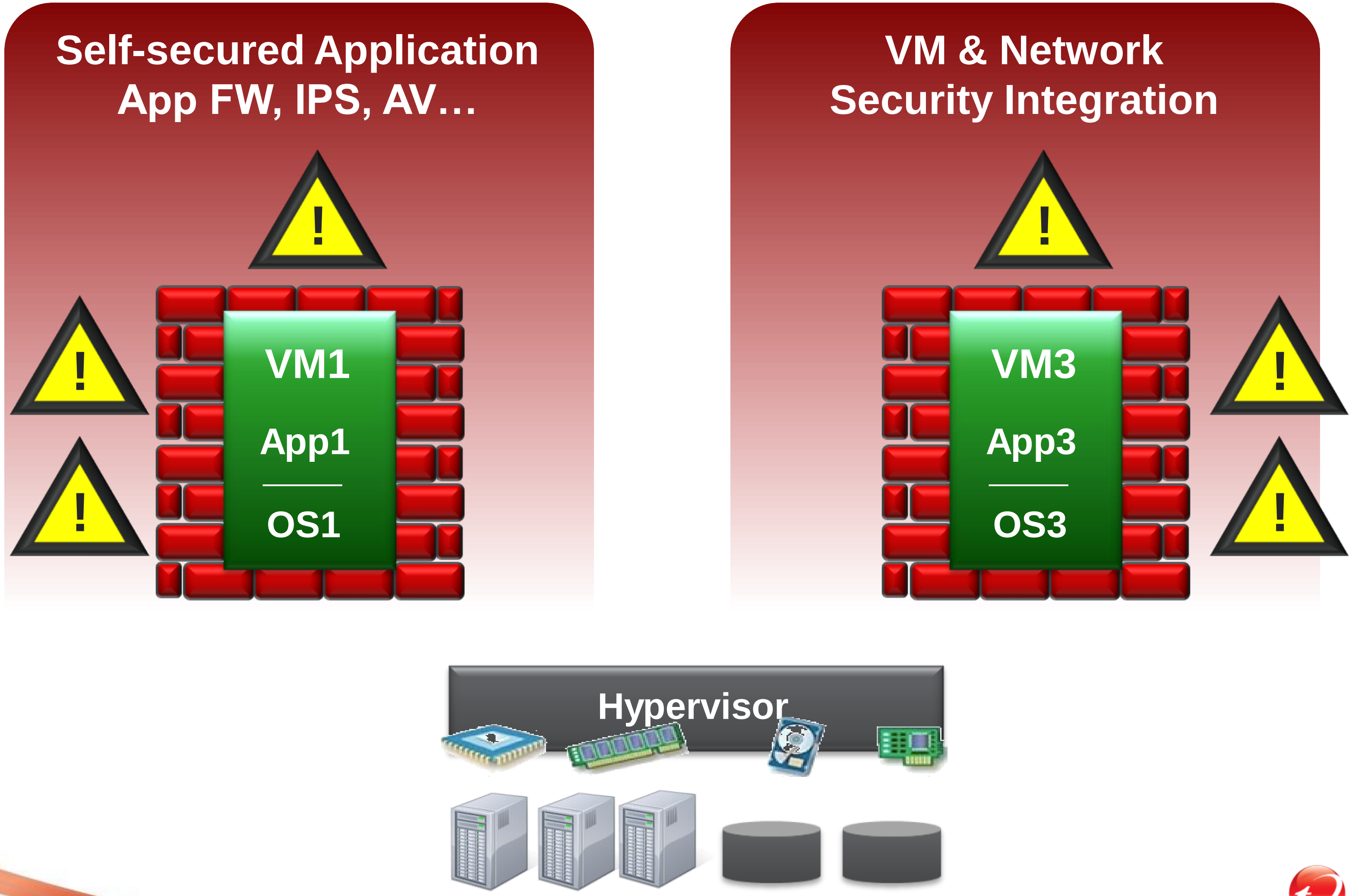
## New Challenges

1. Dormant VMs
2. Resource contention
3. VM Sprawl
4. Inter-VM traffic
5. vMotion



# Vision for the New Datacenter Security Model

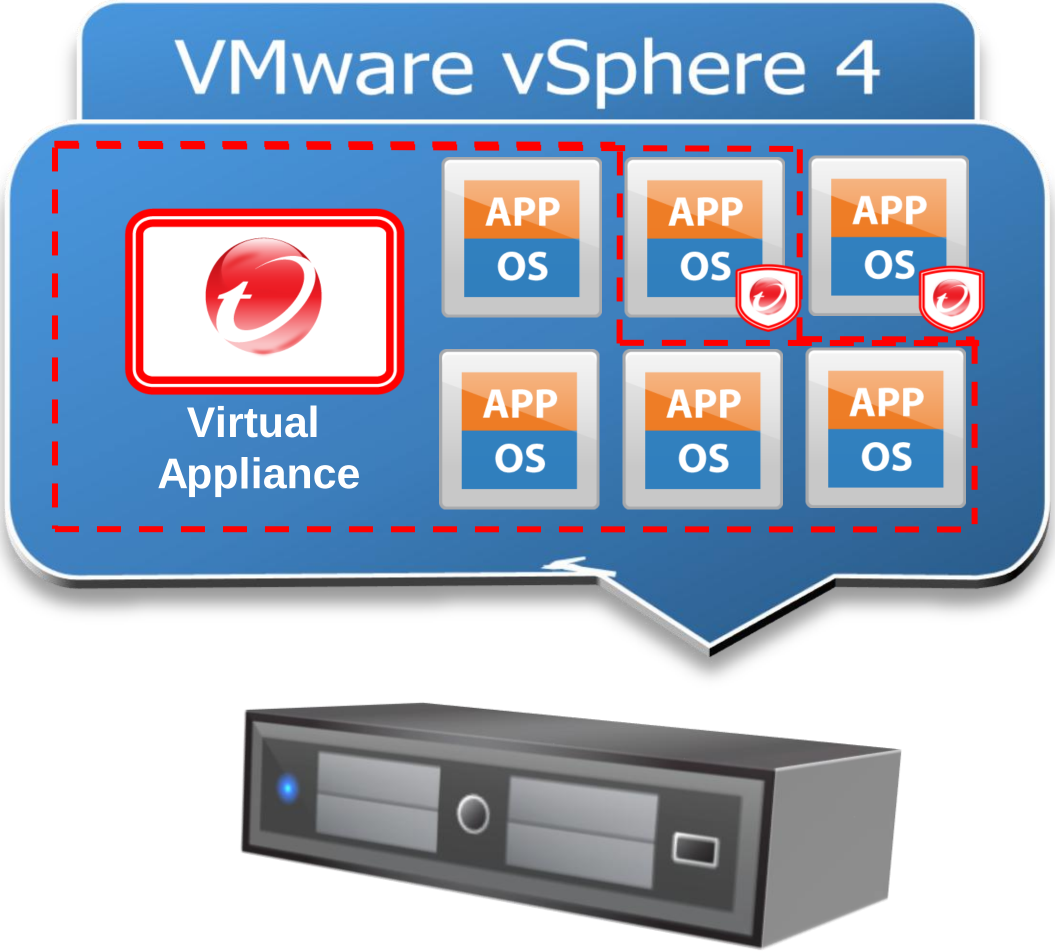
## “The virtual host must protect itself”



Self-secured Application
App FW, IPS, AV…

VM & Network
Security Integration

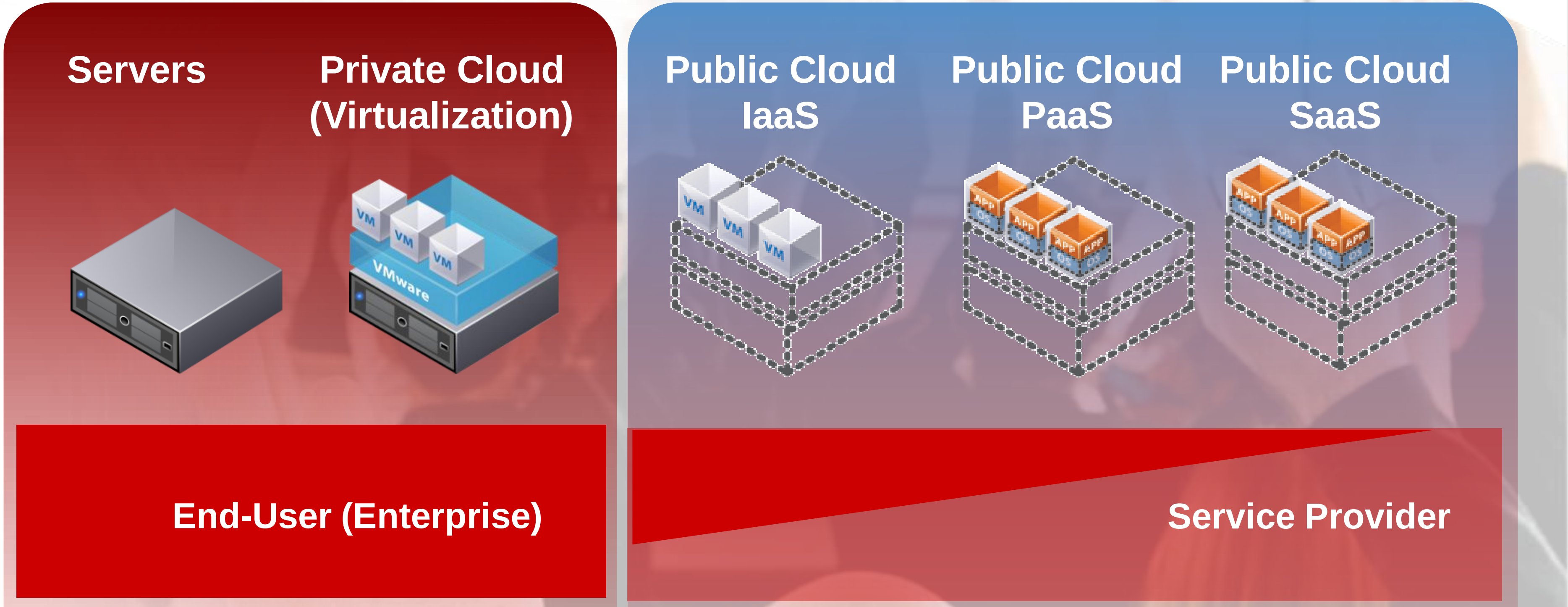
# Virtualisation Security Advances



- Protect the VM by inspection of virtual components
- Unprecedented security for the app & data inside the VM
- Complete integration with, and awareness of, vMotion,Storage VMotion, HA, etc

# Solution: Data is Secure and Controlled in the Public Cloud

# Who Has Control?



Servers

Private Cloud (Virtualization)

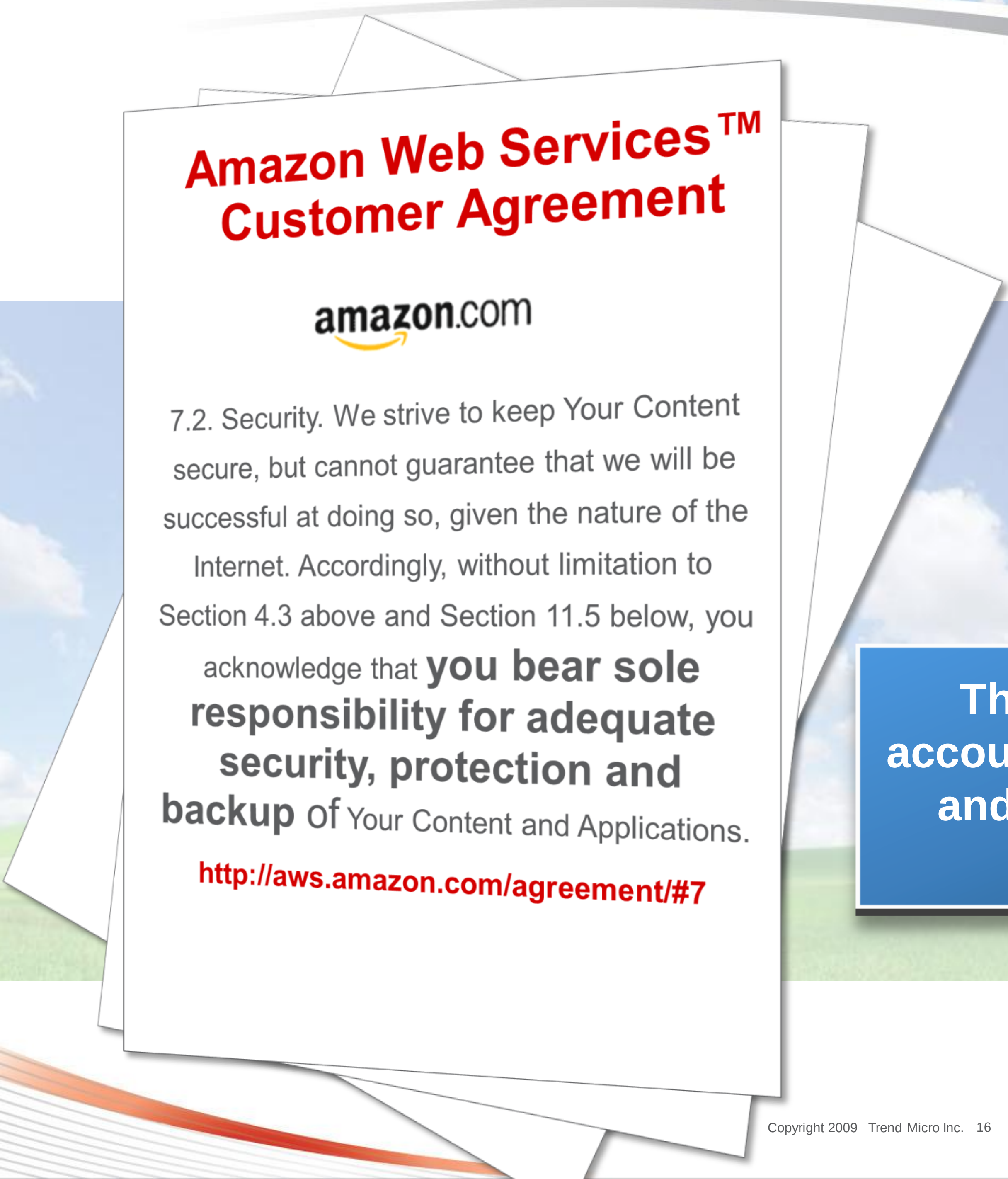
Public Cloud IaaS

Public Cloud PaaS

Public Cloud SaaS

End-User (Enterprise)

Service Provider



## Amazon Web Services™ Customer Agreement

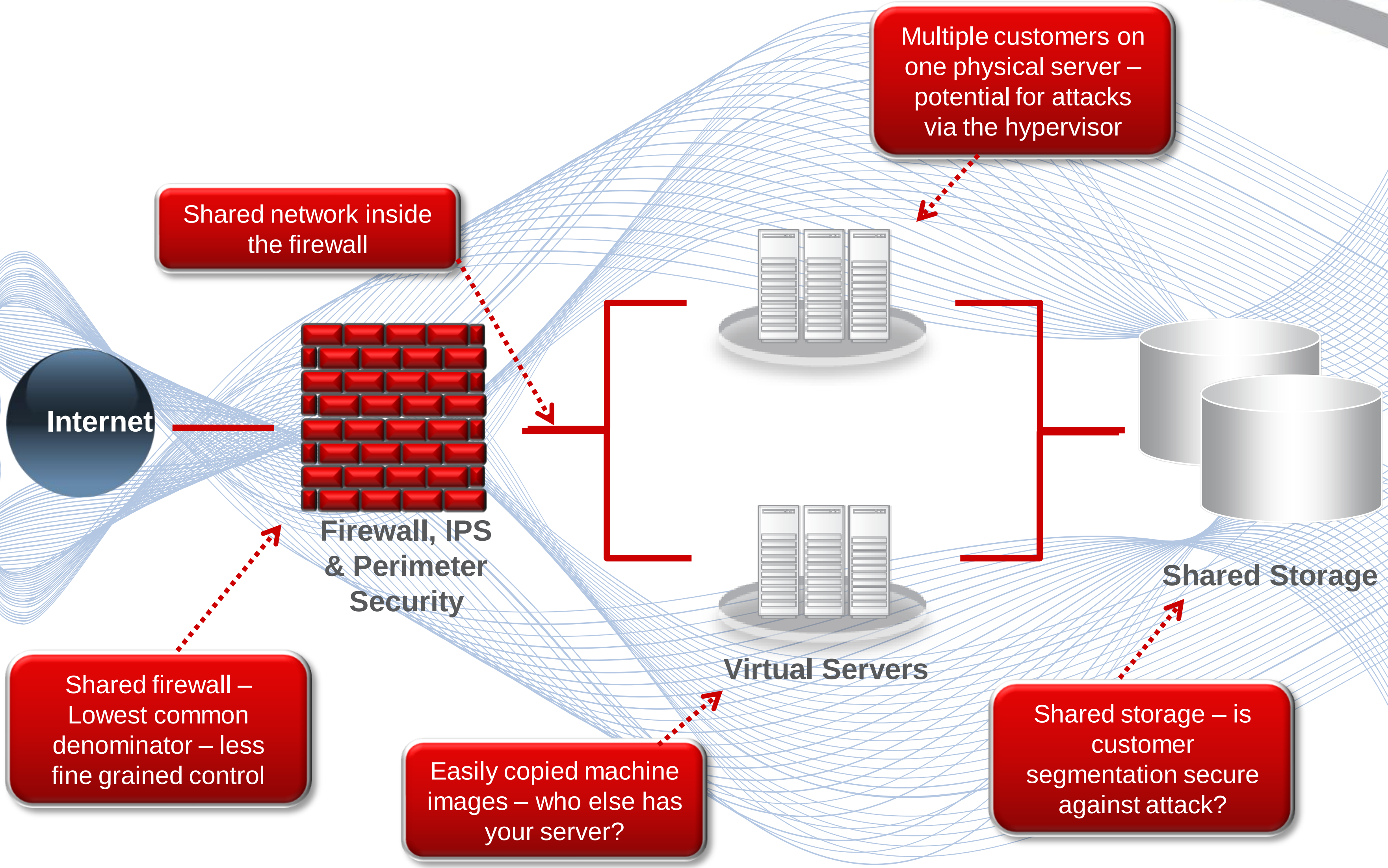
amazon.com

7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that **you bear sole responsibility for adequate security, protection and backup** of Your Content and Applications.

http://aws.amazon.com/agreement/#7

**The cloud user has accountability for security and needs to plan for security.**

# Public Cloud


Multiple customers on one physical server – potential for attacks via the hypervisor
Shared network inside the firewall
Internet
Firewall, IPS & Perimeter Security
Shared Storage
Virtual Servers
Shared firewall – Lowest common denominator – less fine grained control
Easily copied machine images – who else has your server?
Shared storage – is customer segmentation secure against attack?

# Breadcrumbs

Leaving a trail behind

Your data left on cloud storage devices after you leave

Is it really deleted or just the link to you cut

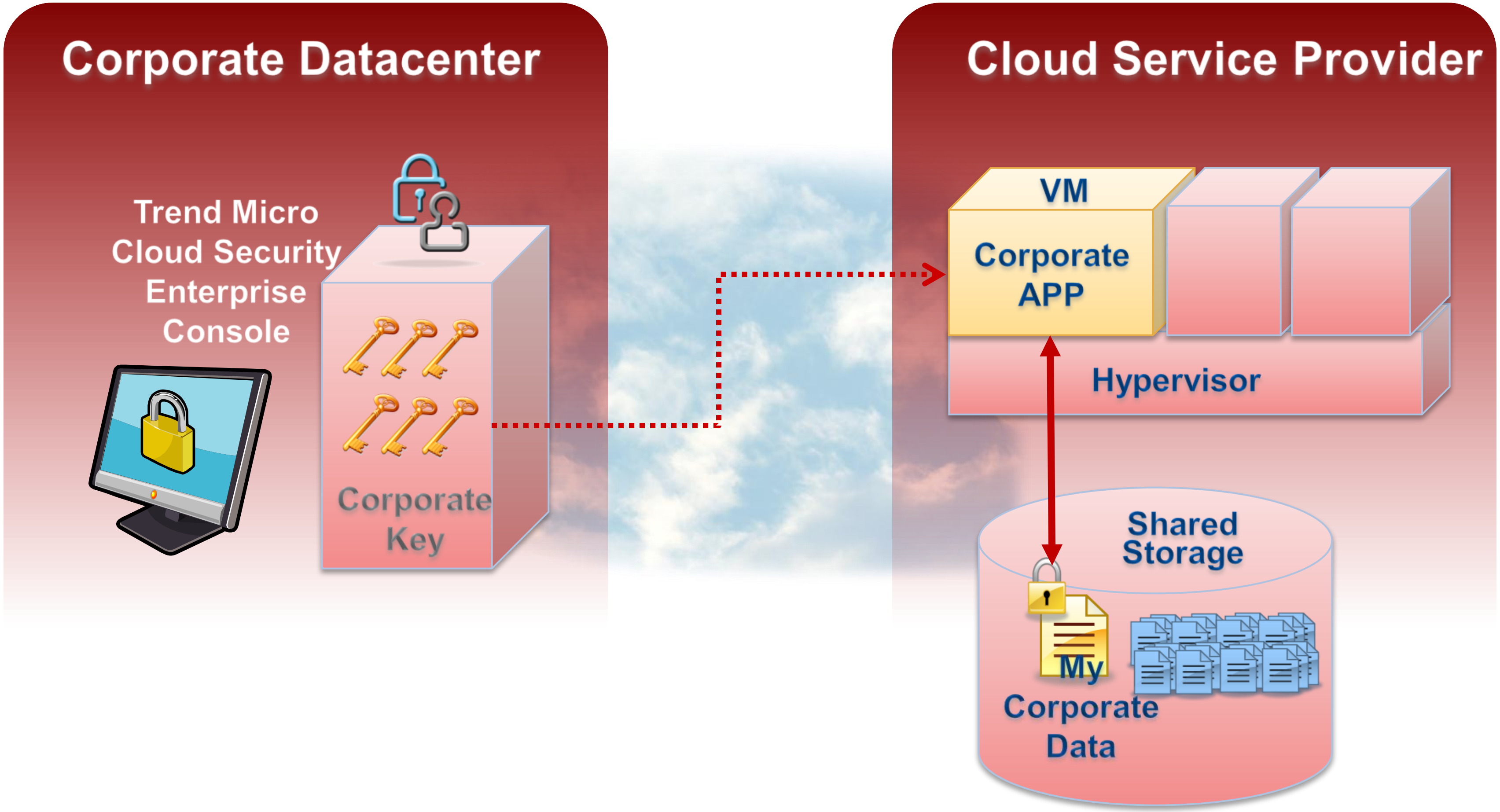
Can you ever be really sure?

How do you erase the cloud?

# Enterprise Solution

## Public Cloud Data Protection

Enterprise Manages Directly



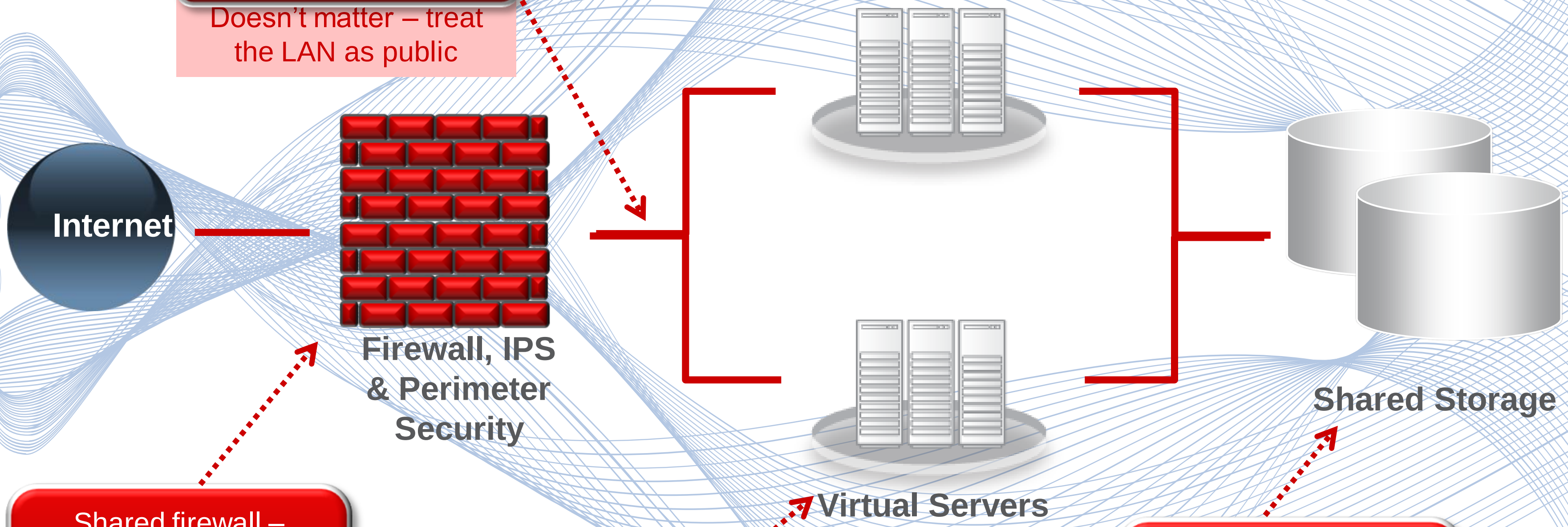
# So what does this mean?

Public Cloud offers key benefits

But also high risk

To benefit fully from this new opportunity we need a new generation of security products designed for the cloud

# Public Cloud – Private Security



Multiple customers on one physical server – potential for attacks via the hypervisor

Doesn't matter – the edge of my virtual is firewalled

Shared network inside the firewall

Doesn't matter – treat the LAN as public

Shared firewall – Lowest common denominator – less fine grained control

Doesn't matter – treat the LAN as public

Easily copied machine images – who else has your server?

Doesn't matter – They can start my server but only I can unlock my data

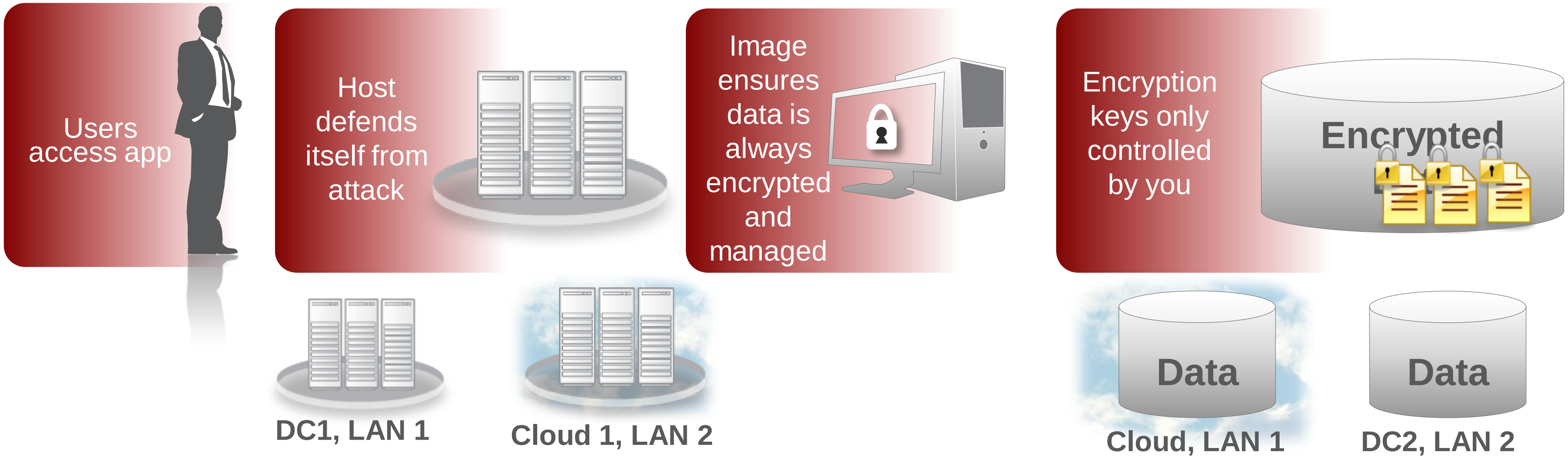
Shared storage – is customer segmentation secure against attack?

Doesn't matter – My data is encrypted (no breadcrumbs)

# A New Approach

# A New Model for Security – Securing the Computing Chain

All environments should be considered un-trusted



Users access app

Host defends itself from attack

Image ensures data is always encrypted and managed

Encryption keys only controlled by you

**When this whole chain is secure**

**Components can move**

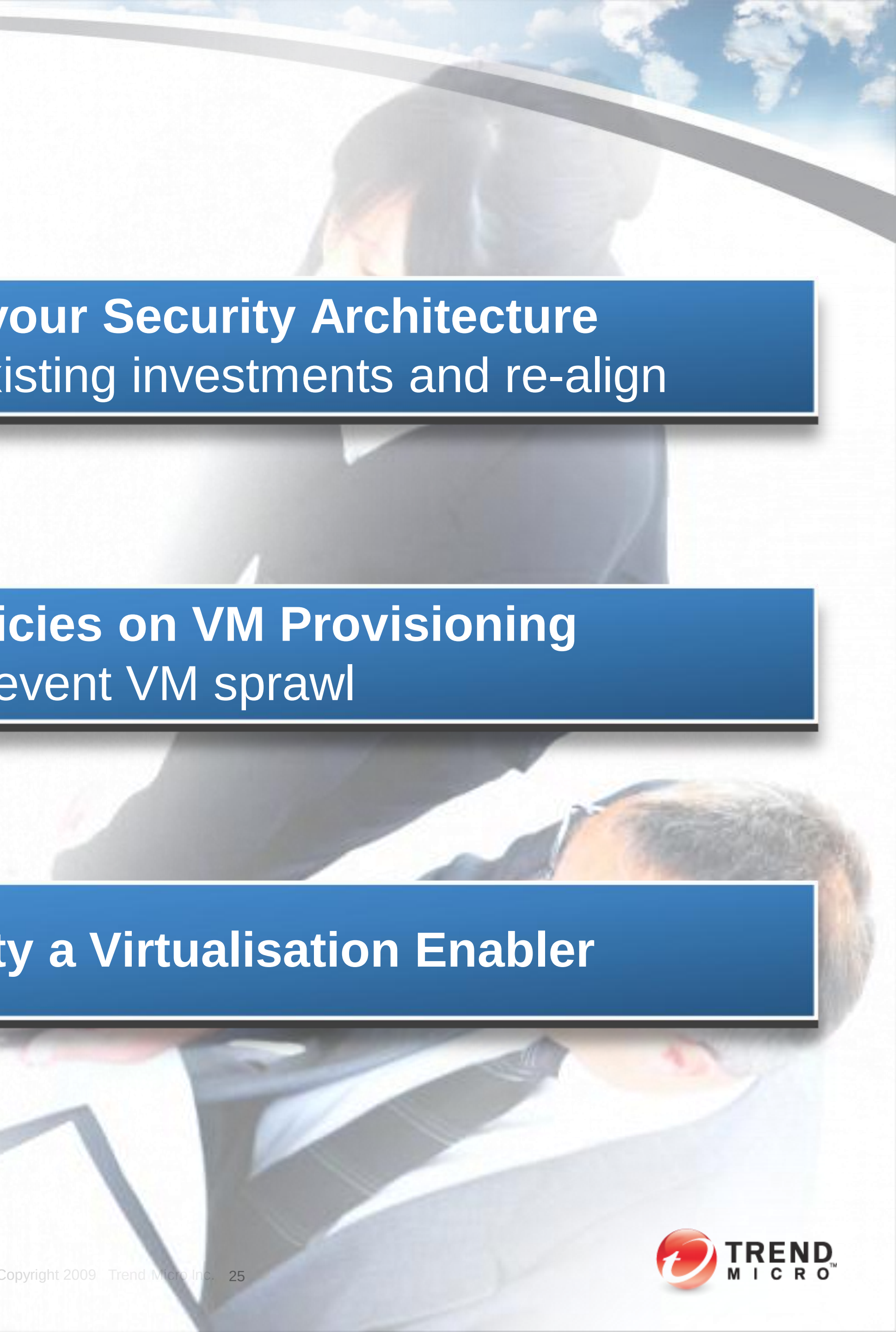
**Service provider “lock” goes away**

**Shared storage ROI goes up**

**Location doesn’t matter**

**Virtual “neighbours” don’t matter**

# Recommendations



1 **Reconsider your Security Architecture**
Consider your existing investments and re-align

2 **Enforce Policies on VM Provisioning**
Prevent VM sprawl

3 **Make Security a Virtualisation Enabler**

# Available from Trend

**TODAY**

Trend Micro Core Protection for VMs

- Anti-malware protection for VMware virtual environments

Trend Micro Deep Security 6

- Firewall, IDS/IPS, Integrity Monitoring & Log Inspection
- Runs in VMs with vCenter integration

**OCT 2009**

Trend Micro Deep Security 7

- Virtual Appliance complements agent-based protection

# Deep Security: Platforms protected

| | |
|---|---|
| Microsoft | • Windows 2000<br>• Windows XP, 2003 (32 & 64 bit)<br>• Vista (32 & 64 bit)<br>• Windows Server 2008 (32 & 64 bit)<br>• HyperV (Guest VM) |
| solaris™ | • 8, 9, 10 on SPARC<br>• 10 on x86 (64 bit)<br>• Solaris 10 partitions |
| Linux | • Red Hat 3<br>• Red Hat 4, 5 (32 & 64 bit)<br>• SuSE 9, 10 |
| VIRTUALIZED BY vmware® | • VMware ESX Server (Guest VM)<br>• Virtual Center integration |
| CITRIX® | • XenServer Guest VM |
| Integrity Monitoring & Log Inspection modules | • HP-UX 11i v2<br>• AIX 5.3 |

TREND MICRO | Securing Your Web World

# Securing Your Virtual World

Harri Kaikkonen

Channel Manager