

VIRTUALIZATION

Floor Wax, Dessert Topping & the End Of Network Security As We Know It?

Christofer Hoff

Chief Security Architect, Unisys

April 24th, 2008

That Which Does Not Kill Us, Only Makes Us Buy More Firewalls...

Agenda

- ▶ Virtualization: Floor Wax & Dessert Topping
- ▶ Virtualization Risk In Context
- ▶ The VirtSec Technology Landscape
- ▶ Rational Solutions and Guidance



VIRTUALIZATION



Virtualization: Floor Wax & Dessert Topping



- ▶ Virtualization is often technically defined as:
 - “ ...an abstraction layer that decouples the physical hardware from the operating system to deliver greater resource utilization and flexibility* ”
- ▶ But it's really about two things:
 - ▶ Time
 - ▶ Money

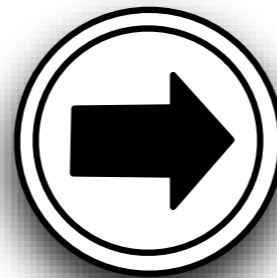


*Yay. I know how to use Wikipedia

Virtualization Is About More Than Just Consolidating Servers

- ▶ Clients
- ▶ Networks
- ▶ Storage
- ▶ Operating Systems
- ▶ Applications
- ▶ Information

- ▶ Security
- ▶ Resilience
- ▶ Agility
- ▶ Operational Efficiency



Resources

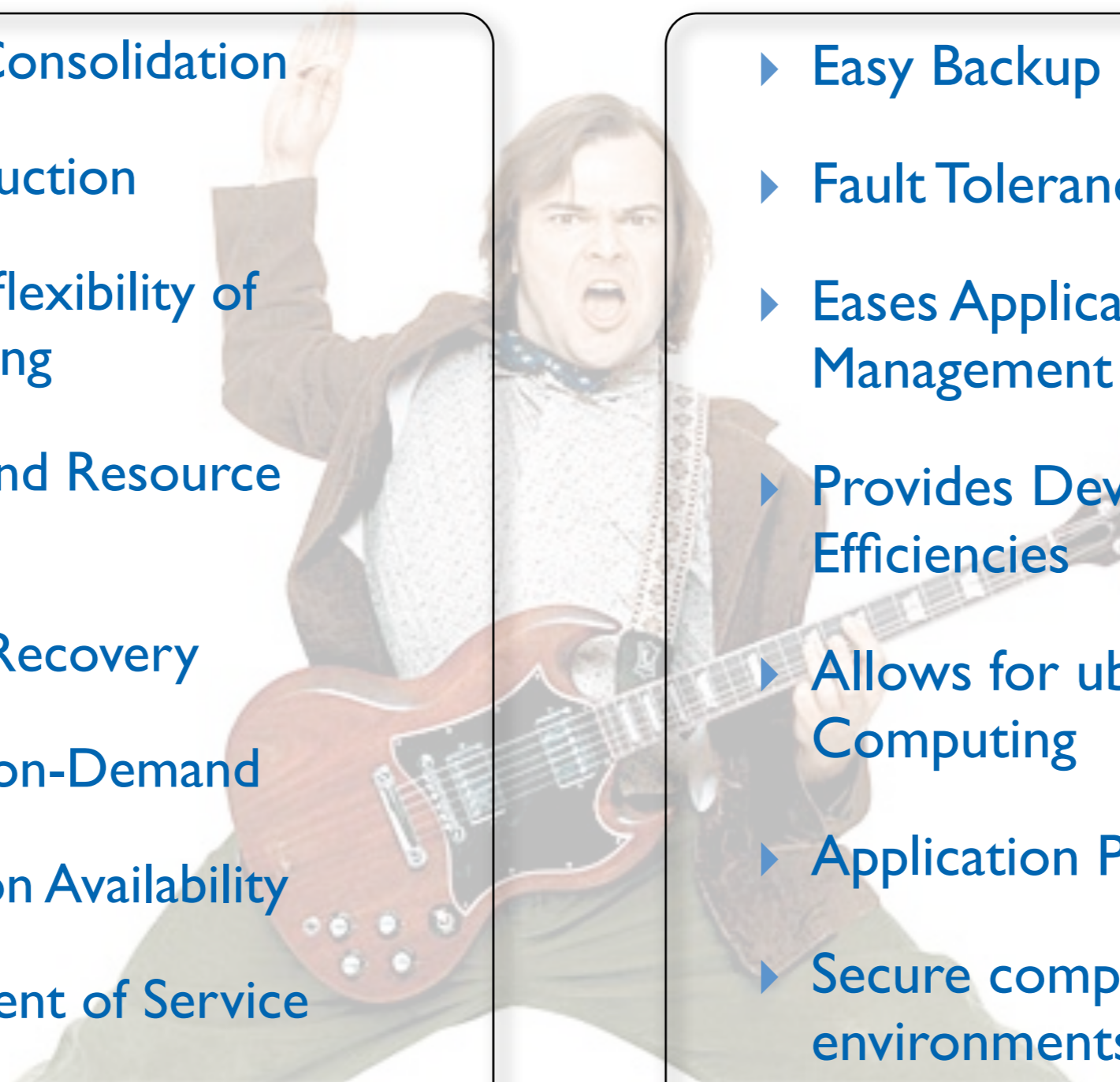
Provisioning
Re-purposing
Governance
Orchestration
Chargeback

Platforms

w00t! Virtualization Rocks!

- ▶ Physical Consolidation
- ▶ Cost Reduction
- ▶ Ease and flexibility of Provisioning
- ▶ On-demand Resource Pooling
- ▶ Disaster Recovery
- ▶ Capacity on-Demand
- ▶ Application Availability
- ▶ Management of Service Levels

- ▶ Easy Backup
- ▶ Fault Tolerance
- ▶ Eases Application Lifecycle Management
- ▶ Provides Development Efficiencies
- ▶ Allows for ubiquitous Computing
- ▶ Application Portability
- ▶ Secure computing environments...



Mama Says “Virtualization Is Da Devil!”

Virtualization changes the way resources & networks are:

- ▶ Designed
- ▶ Provisioned
- ▶ Deployed
- ▶ Administered
- ▶ Patched
- ▶ Recovered
- ▶ Assessed
- ▶ Monitored
- ▶ Audited



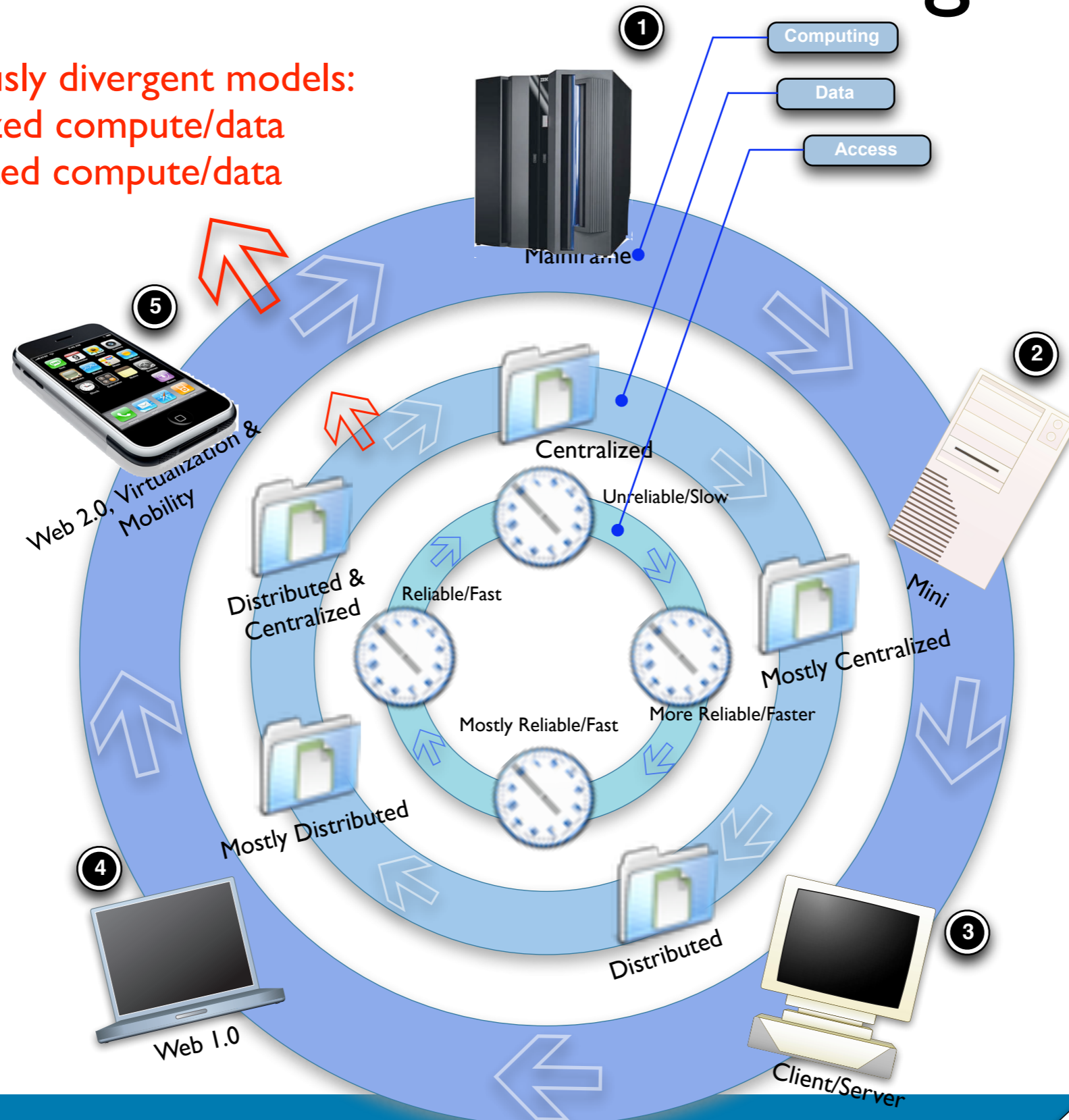
...and how information across its lifecycle is ultimately:

- ▶ Created
- ▶ Stored
- ▶ Controlled
- ▶ Accessed
- ▶ Destroyed
- ▶ Archived, and
- ▶ Secured

Welcome to Groundhog Day!

Simultaneously divergent models:

- ▶ Centralized compute/data
- ▶ Distributed compute/data



So What's the Big Deal?

Virtualization Isn't Exactly New...

Highly Scientific Poll #1

What Fraction of Your Servers Are Virtualized?

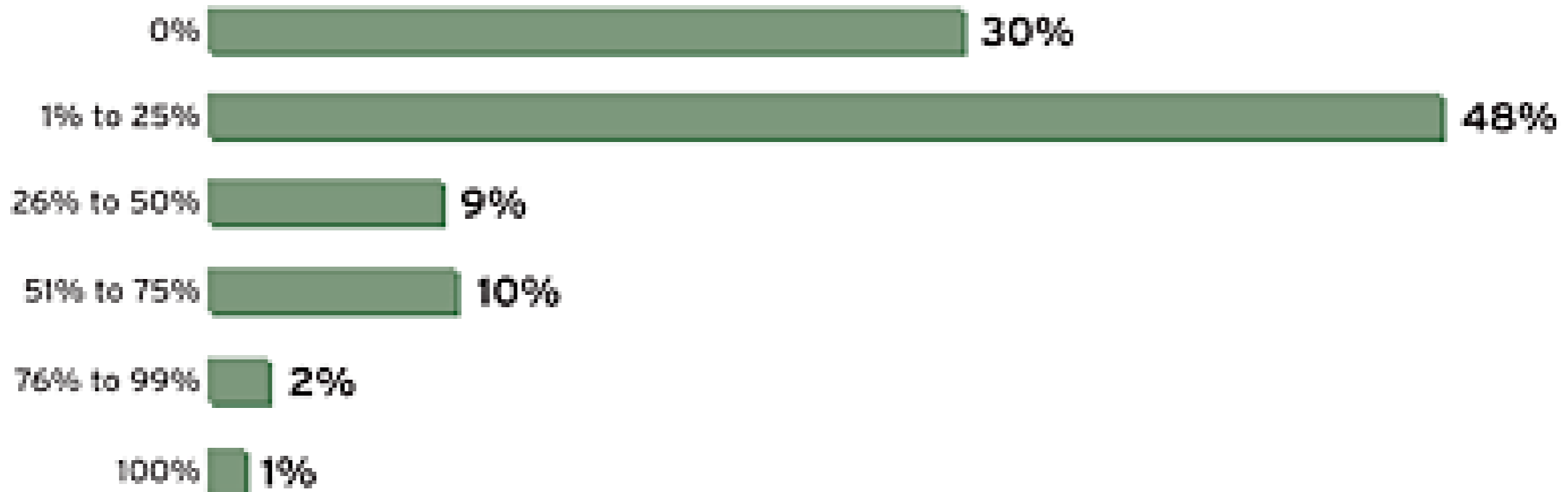
- a. 0%
- b. 1%-25%
- c. 26%-50%
- d. 51% to 75%

Source: Information Week 2007 Analytics Brief : Securing the New Data Center

Survey Says!

VM Volume

What fraction of your servers are virtualized?



Source: InformationWeek Poll

Highly Scientific Poll #2

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

- a. No IT Security/protection in place for virtual servers
- b. A VM-tailored strategy and solution is in place
- c. VM servers comply with company standards defined by conventional server infosec policy
- d. We're working on it!

Source: Information Week 2007 Analytics Brief : Securing the New Data Center

Survey Says!

Security Strategy

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



Source: InformationWeek Poll

Whoops!

The Phantom Menace: Unmanaged VMs and VM “Appliances”

By 2010, unmanaged VMs will be as significant an issue to enterprises as unmanaged devices are in 2007 (0.9 probability).

“Best Practices and Security Considerations for Securing Virtual Machines” G00144828 March 2007

Gartner.

Highly Scientific Poll #3

How do virtual servers compare with conventional server environments for information protection and security

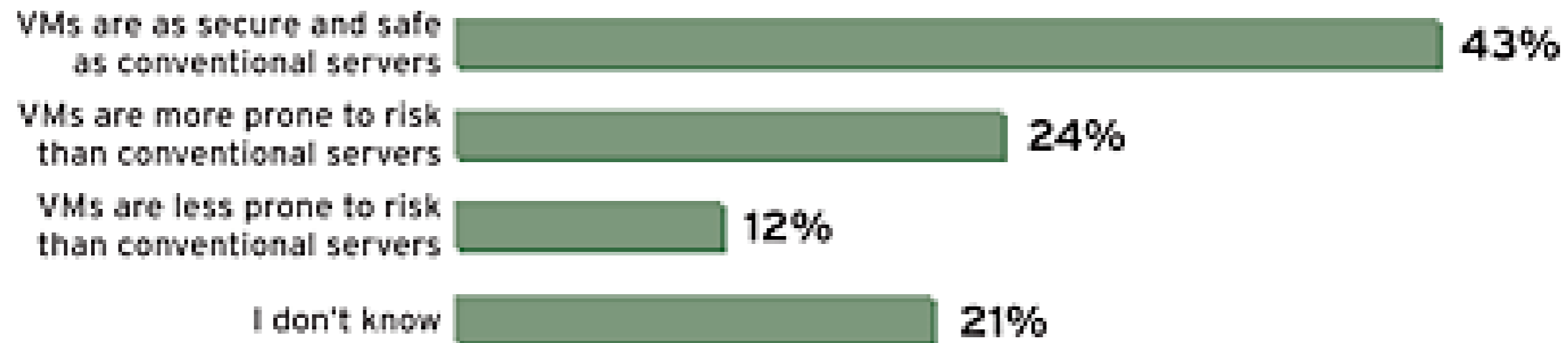
- a. VMs are as secure and safe as conventional servers
- b. VMs are more prone to risk than conventional servers
- c. VMs are less prone to risk than conventional servers

Source: Information Week 2007 Analytics Brief : Securing the New Data Center

Survey Says!

Confidence Level

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



Source: InformationWeek Poll

We Have a Failure To Communicate!

Most Virtual Machines Deployed Will Be Less Secure than Their Physical Counterparts

Through 2009, 60% of production Virtual Machines will be less secure than their physical counterparts (0.8 probability).

“Best Practices and Security Considerations for Securing Virtual Machines” G00144828 March 2007

Gartner.

Computing Megatrends

- ▶ Upgrading from servers to blades
- ▶ Moving from hosts and switches to clusters and fabrics
- ▶ Evolving from hardware/software affinity to virtualized grid/utility computing
- ▶ Transitioning from infrastructure to service layers in “the cloud”

“A hundred years ago, companies stopped producing their own power with steam engines and generators and plugged into the newly built electric grid.” - Nicholas Carr, the Big Switch



Today's Risk Model is Kaput!

- ▶ Virtualization amplifies every issue we have today in network and host-based security strategies
- ▶ Crunchy on the outside and even more gooey in the middle! One moat, lots of castles...
- ▶ Unprepared for new attack surfaces and threat vectors
- ▶ Immature management and security solutions
- ▶ Dynamic & transitive technology mated to static controls & approaches to security = FAIL!
- ▶ Organizational issues & siloes are worse, roles and responsibilities even more blurred
- ▶ Rationalizing how to assess risk in a virtual environment indicates you're not assessing risk in your non-virtualized environment...

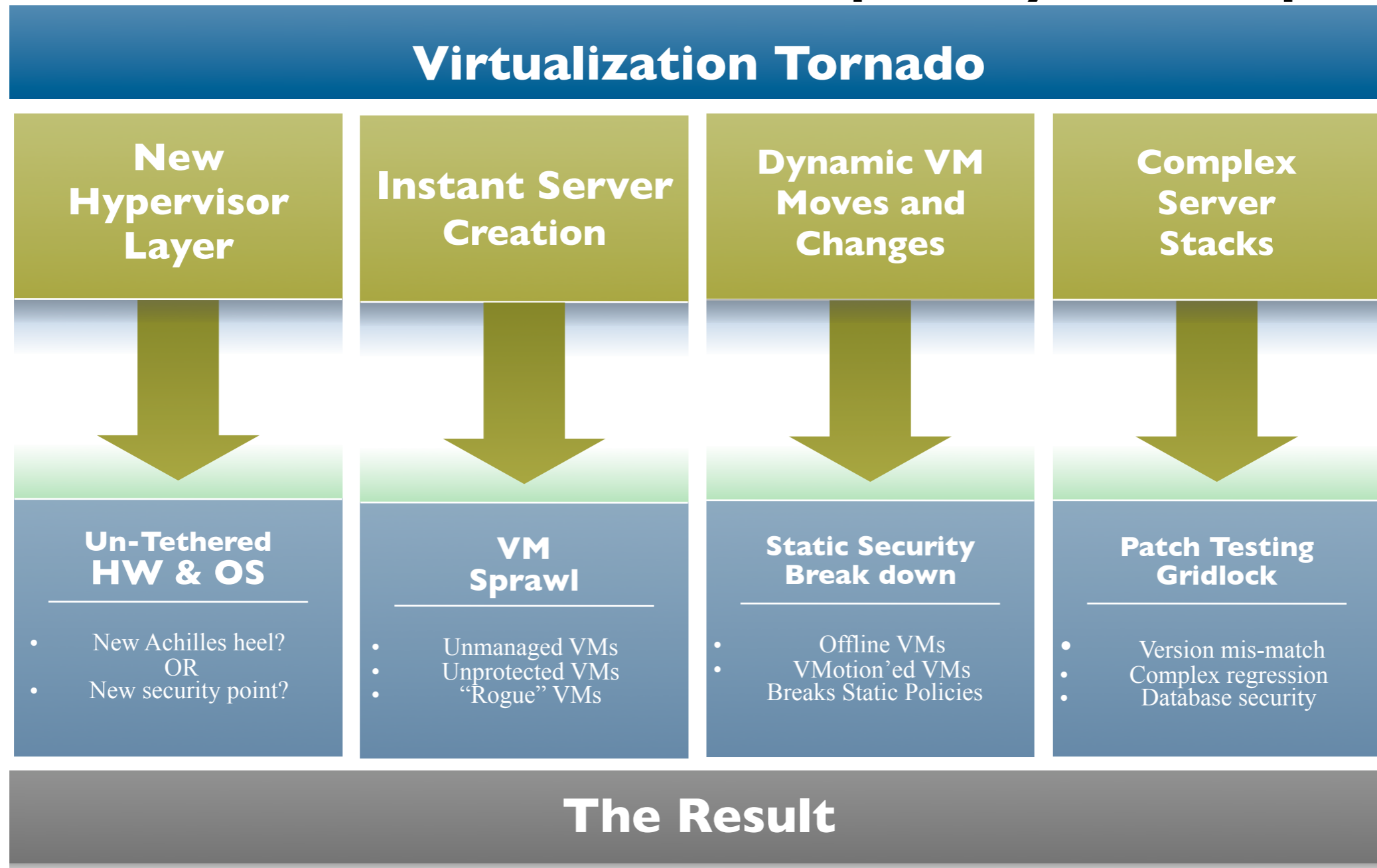


The Virtualization Security Challenge?

- ▶ Today's problems of securing our virtualized environments are not technical, but instead are **organizational and operational**.
- ▶ The technology will ultimately catch up to a point (as it always does,) but how and by whom it is used will be the issue.
- ▶ We have lost not only visibility, but the clearly-defined lines of demarcation garnered from a separation of duties and years of practiced grief we had in the non-virtualized world.
- ▶ Virtualization ultimately further fractures the tenuous relationships between the server, network and security teams.
- ▶ Separate “securing virtualization” from “virtualizing security”
- ▶ We need to focus on the things that really matter now



Virtualization Makes Simplicity Complex?

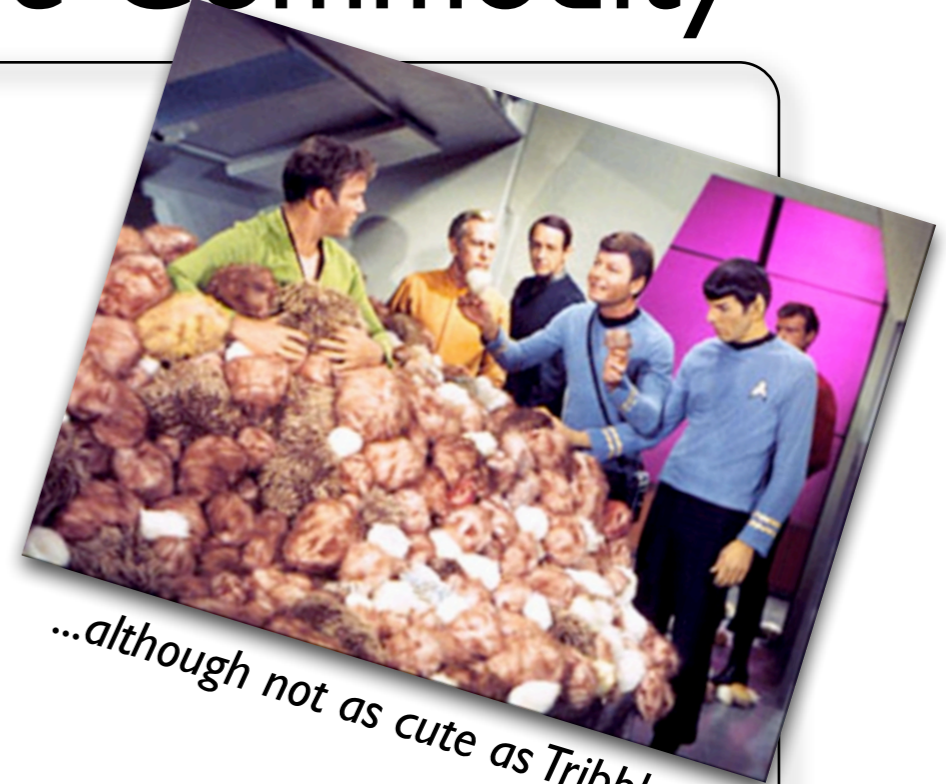


Slide Courtesy of:  BlueLane™

Hypervisors Are a Disruptive Commodity

It seems everybody's got one...

- ▶ VMware
- ▶ Citrix
- ▶ Microsoft
- ▶ Parallels (SWsoft)
- ▶ Oracle
- ▶ Phoenix
- ▶ Sun
- ▶ *nix, Linux
- ▶ Virtual Iron
- ▶ IBM
- ▶ etc...



...although not as cute as Tribbles

...and they're showing up in all sorts of places

- ▶ Servers & Clients, Storage & Networking
- ▶ Hardware (BIOS and Flash) & Software (including OS)
- ▶ A-la-carte or bundled as appliances
- ▶ Mobile Platforms



No One Ring0 To Rule Them All!



CITRIX

Microsoft



Which means:

- ▶ You'll probably end up with 4-5 virtualization platforms spread out across your enterprise

From Monoculture To Overly Diverse?

- ▶ Will our focus shift from managing traditional (guest) OS's to the VMM's?

We Need Some Open Industry Standardization!

- ▶ DMTF Open Virtual Machine Format (OVF)

Context

Why Security Is In Trouble & What We Should Worry About

Let Me Say It Again...

- ▶ Many debates and much ado stems from the inability to distinguish between three fundamental concerns:
 - ▶ Securing Virtualization
 - ▶ Virtualizing Security
 - ▶ Security Through Virtualization
- ▶ It is important to separate the technical, architectural and ideological from the functional, operational and organizational
- ▶ Treating them as a single issue leads to thrashing.



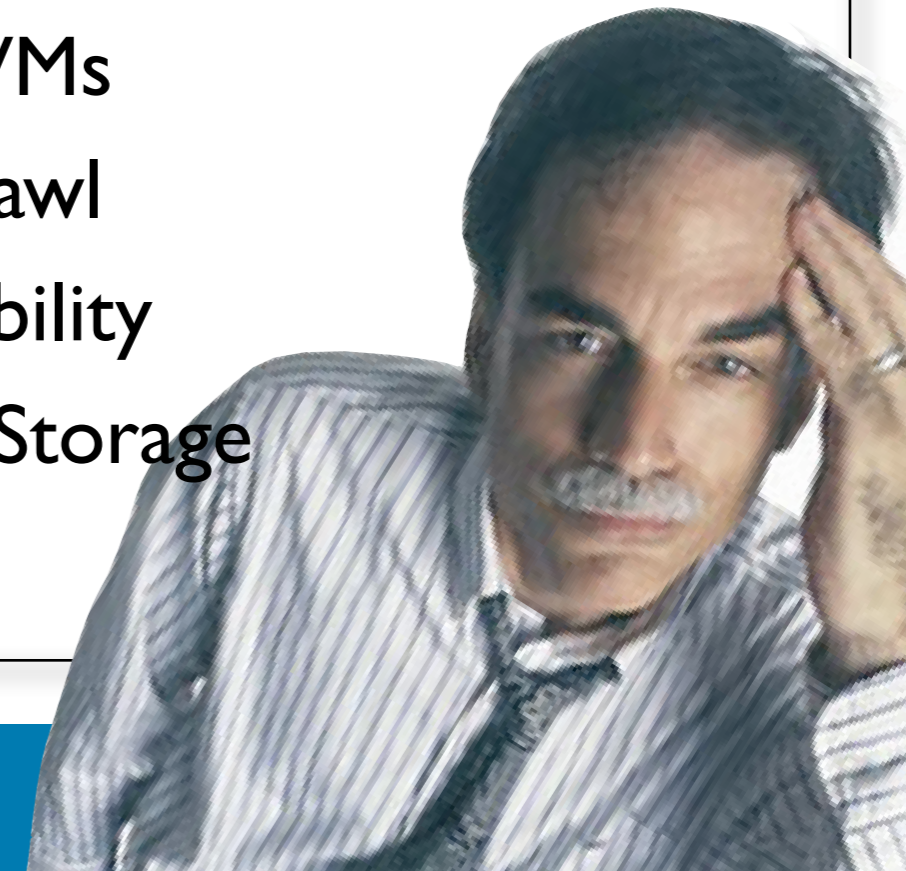
Some Things To Worry About Today

Operational Risks

- ▶ Immature Management & Security Tools
- ▶ Configuration Management
- ▶ Virtual networking
- ▶ Transition & separation of duties
- ▶ Vulnerability Management Lifecycle (on/offline)
- ▶ Inconsistent Security Policies/ Procedures
- ▶ Loss of Visibility
- ▶ Performance, scalability and capacity due to security

▶ Threats & Vectors

- ▶ Guest-hopping & Jailbreak attacks
- ▶ Vulnerabilities in Hypervisors
- ▶ Attacking the management stacks
- ▶ Theft of an intact VM
- ▶ Rogue VMs
- ▶ VM Sprawl
- ▶ VM Mobility
- ▶ Shared Storage



More Stuff To Worry About Today*

Virtualized Security Screws the Capacity Planning Pooch (Conquest)

- ▶ Performance overhead of in-line security VA/VMs & API's is really hard to understand; here comes the UberNic™

The Network is the computer...oh, crap. Never mind, it's broken (Death)

- ▶ Attempting to replicate complex physical networking topologies in virtual switches today will fail

Episode 7: Revenge of the UTM (War)

- ▶ The notion that we will deploy a single vendor/monolithic security VA in each host is silly; let the best-in-breed vs. good-enough battle wage!

Spinning VM straw into budgetary Gold (Famine)

- ▶ Virtualizing security will not save you money; it will cost you more!



**The Four Horsemen Of the Virtualization Apocalypse*

Hoff's Virtualization Security Public Service Announcement



Headlines & Hand Grenades: Virtual Malware

What are the real risks associated with virtualization-aware malware & hardware rootkits?

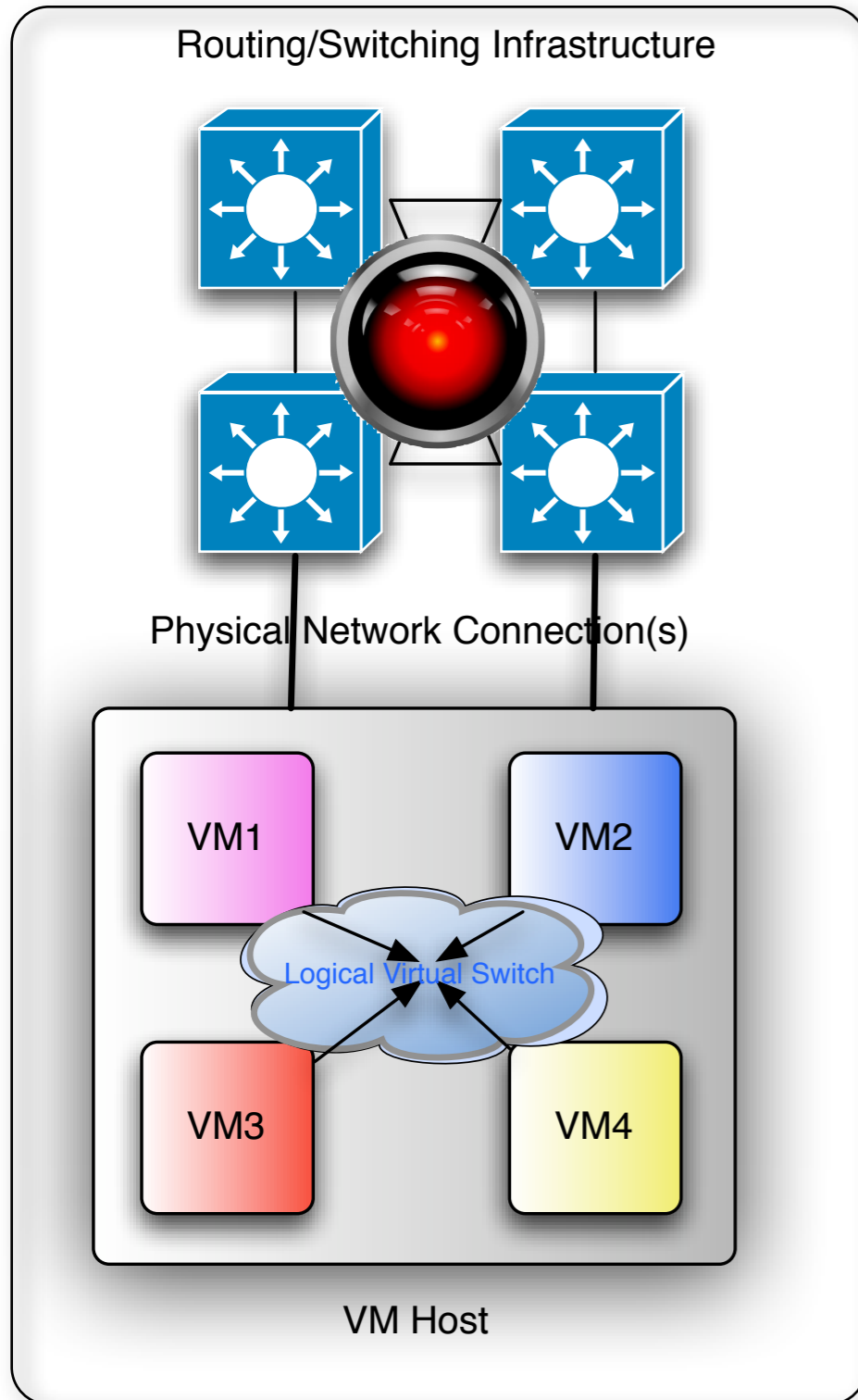
- ▶ This research is important, but how it's presented is also*
- ▶ Current “exploits” and PoC are research-based and not in the wild
- ▶ Many of the overly-sensationalized examples are products of mis-configuration, others require operating scenarios that do not reflect the realities of deployment
- ▶ Hand-wringing about the sizzle when the steak should be the focus is distracting; if you don't have the basics down, this is the least of your worries

** Debating “possibility” versus “probability” is always fun at parties*

Solutions

How Can We Approach Securing Our Virtualized Environments Today?

Please Self-defend the Network, HAL...



- Virtualization breaks our existing model of “network” security
- Visibility, capacity, efficacy and resilience are all up for grabs
- How does the “network” supposedly self-defend when it’s not even used?
- A whole slew of “new” solutions is emerging, but it’s hard to separate the snake oil...

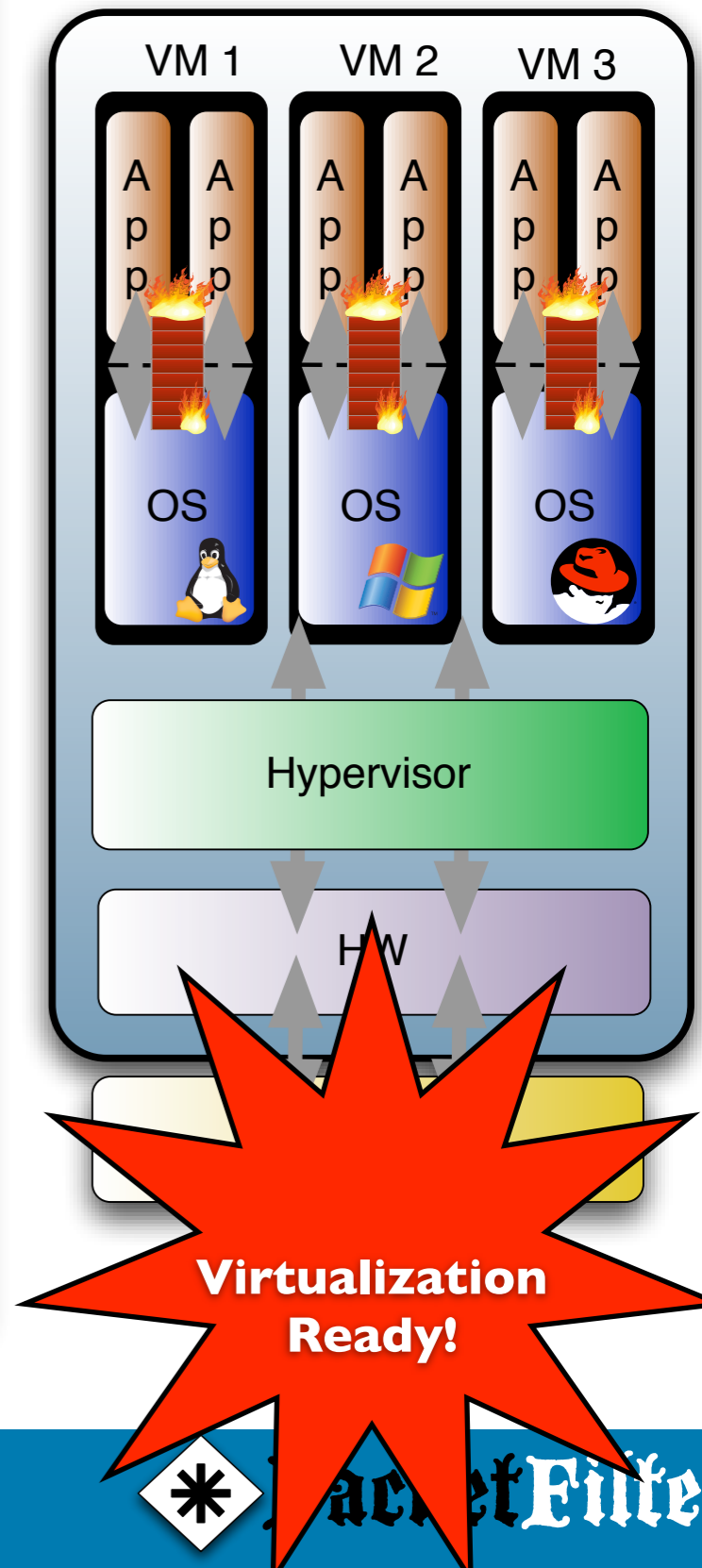
Security Software in the VM

Pros

- Security Software installed on each VM which we know how to do
- Same management functionality as today
- Preserves most functional separation of duties
- Preserves your vendor relationships of today

Cons

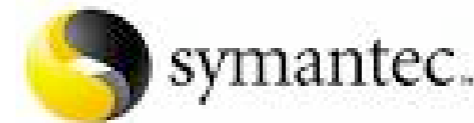
- Protects only that VM
- Limited visibility
- Unaware that the VM is virtualized
- Does not reduce security costs
- Vendor Support Issues
- Consumes Host Resources



Example: All The Usual Suspects...

▶ Most anything you run today in your conventional environments will work here...

- ▶ Firewalls
- ▶ HIDS
- ▶ HIPS
- ▶ Anti-virus
- ▶ NAC
- ▶ Endpoint Assurance
- ▶ Patch Management
- ▶ Inventory
- ▶ Configuration Audit & Control
- ▶ ...



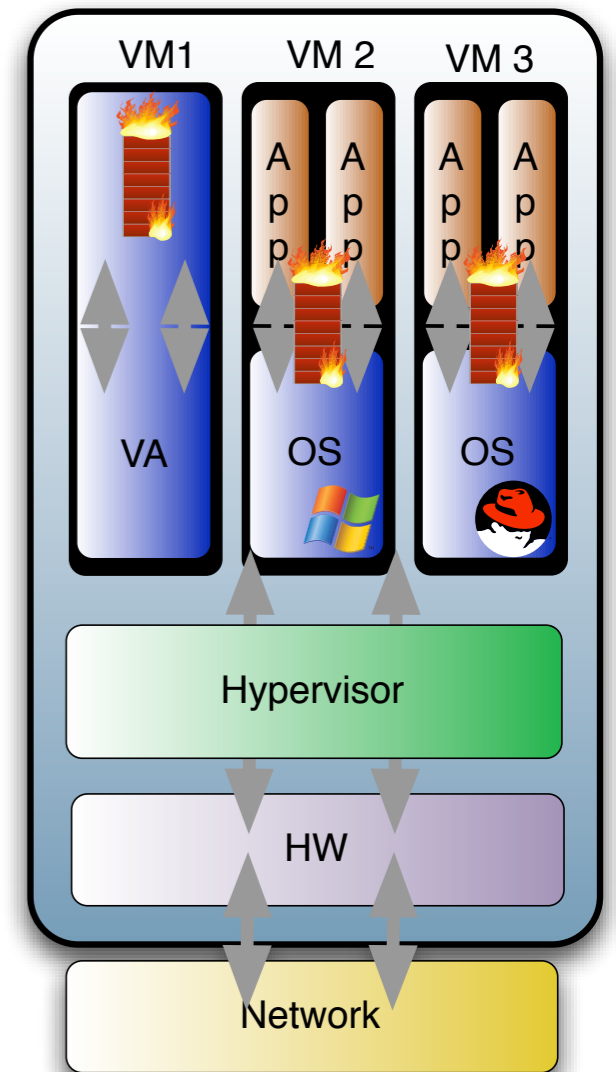
Virtualized Security as Virtual Appliance/VM

Pros

- Security software installed in a VM as a virtual appliance
- Paired with software installed in VMs per previous model
- Allows virtualization of security across Host
- Potentially better Intra-VM visibility
- Easy to deploy

Cons

- Consumes Host Resources
- Requires careful virtual networking configuration
- HA/Resilience an issue
- Beware of False Advertising!



ALTOR
networks

BlueLane

catbird

Montego Networks
Secure Switching for Virtual Environments

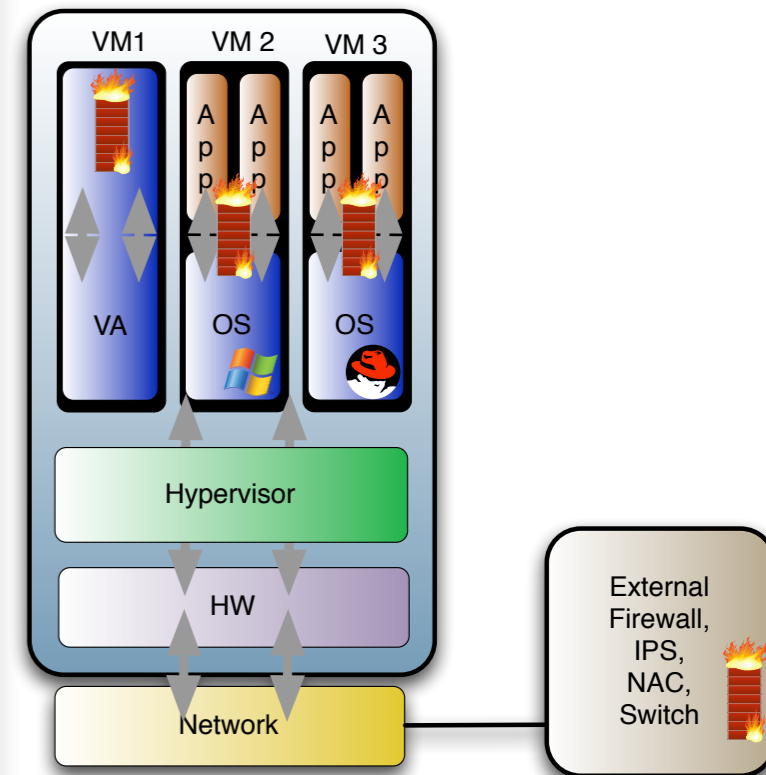
Virtualized Security Interacting with Security Fabric

Pros

- Same as previous models but adds integration with external security devices
- Better performance with offloading
- Ability to tie into non-virtualized security fabric
- Consistent policies across physical/virtual boundaries

Cons

- Tend to be proprietary
- Vendor lock-in
- Effectiveness debatable given existing vSwitch features/limitations
- Depending on capabilities, may end up playing traffic ping pong
- Expensive



REFLEX
SECURITY

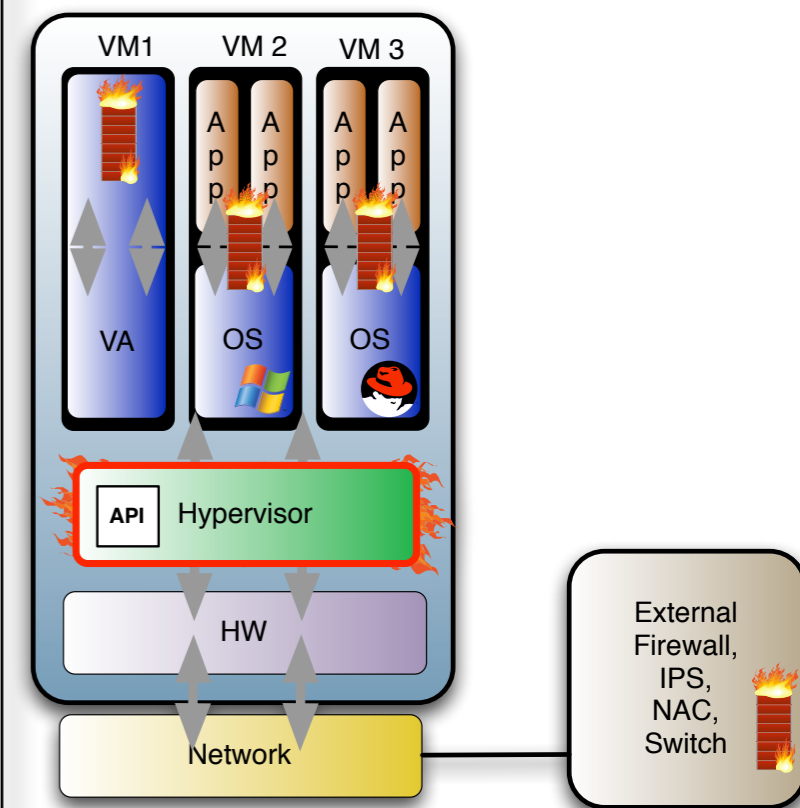
...Adding Abstracted Security via VMM API's

Pros

- Same as previous models but adds/relies upon additional security capabilities exposed via API
- Tighter integration between third party security functions, HV and management toolsets
- Allows longer shelf life of existing solutions

Cons

- Requires re-tooled ISV software & virtualization platforms
- No industry standardization
- Coarse triggers
- Dispositions are limited



Example: VMware's VMsafe

VMware VMsafe

Enables partners to build security solutions in the form of a virtual machine that can access, correlate and modify data to help control and protect:

- **Memory and CPU.** VMsafe provides introspection of virtual machine memory pages and CPU states.
- **Networking.** VMsafe enables filtering of network packets inside hypervisors as well as within the security virtual machine itself.
- **Process execution.** VMsafe provided in-guest, in-process APIs that enable complete monitoring and control of process execution.
- **Storage.** Guest virtual machine disk files can be mounted, manipulated and modified as they persist on storage devices.

Security solutions built with VMware VMsafe will provide customers better granularity, visibility, correlation and scalability in virtual machine deployments.

Great If You Use VMware Infrastructure Solutions...

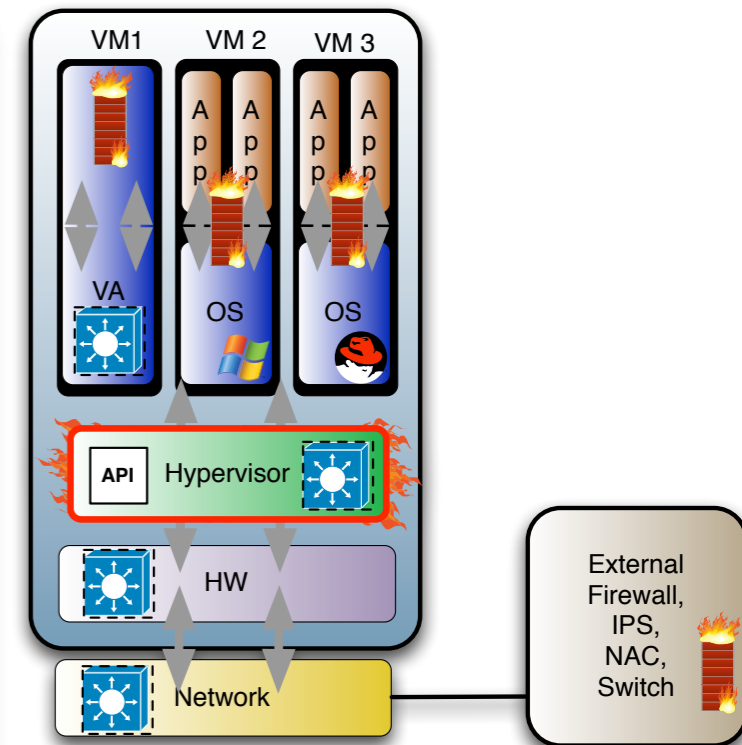
...With Third Party Virtual Switches

Pros

- Same as previous models but now allows for choice/addition of additional virtual switches
- Acts as a policy-driven intelligent disposition director to 3rd party security functions
- Allows integration/replication of external software, fabric capabilities and policy
- Consistency in networking capabilities (load-balancing, QoS, L3-7, etc...)

Cons

- Blurs the line of where the “network” exists Requires extremely careful network configuration
- May reintroduce security issues due to complexity/diversity versus limits of today
- Further complicates the separation of duties
- Potential performance implications
- Vendor lock-in
- Support issues



vSwitches evolving to reside in hardware & software:

- Hypervisor
- VA/VM
- Underlying Virtualization-enabled CPU's
- In “new” breed of NIC cards

Montego Networks
Secure Switching for Virtual Environments

CISCO

NETEFFECT

Watch this space...

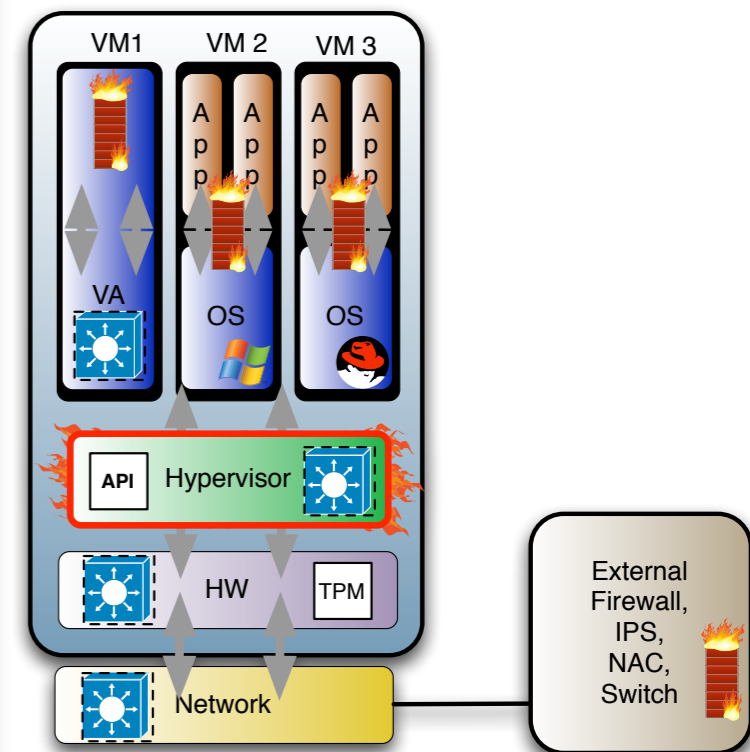
...With a Trusted Platform Module

Pros

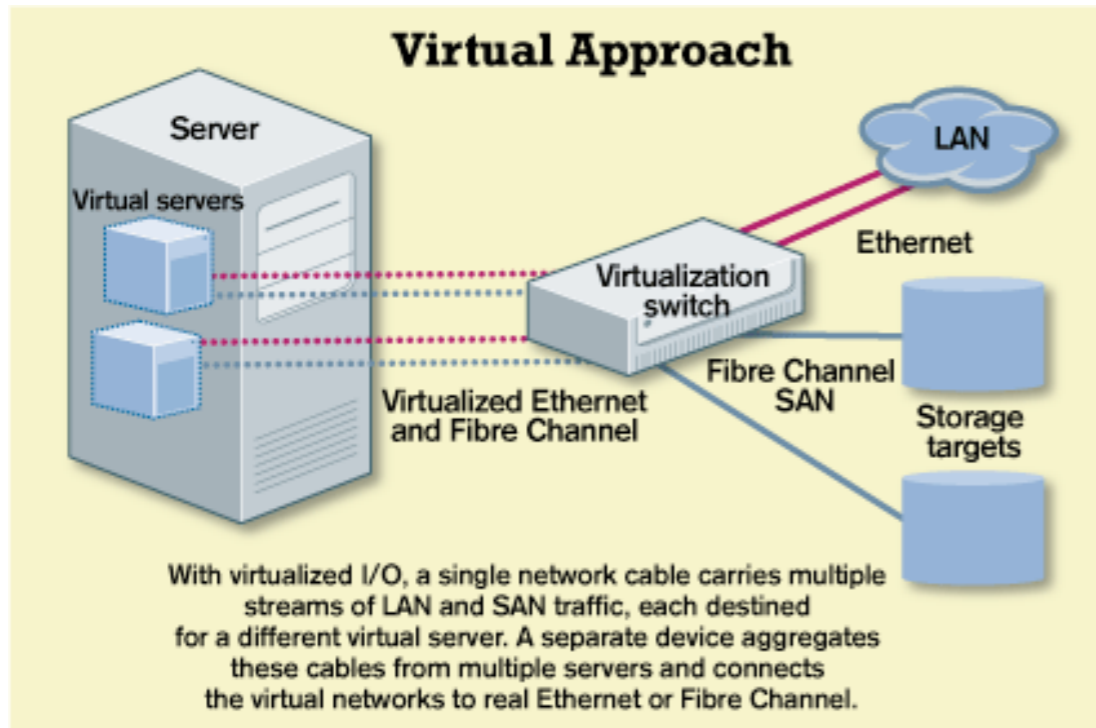
- Same as previous models but relies upon integrated TPM for trust model, assurance & attestation
- Offloading of certain functions to TPM
- More secure VMM, less footprint

Cons

- Requires ubiquity and consistent adoption of TPMs up/down the stack
- Single point of failure?
- Attack Target?



Just To Confuse Things: I/O Virtualization



InformationWeek

I/O Virtualization:

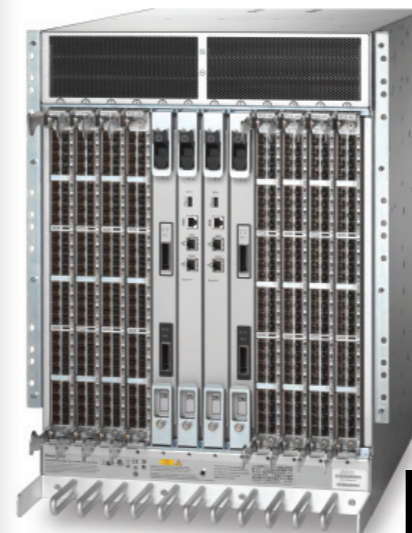
- Single network connection provides virtualized fabric interconnectivity for LAN & SAN
- Ethernet/FC/Infiniband
- Ultimately supporting RDMA



- Cisco 7000 Nexus
- Brocade DXC Backbone
- 3Leaf V-8000 Virtual I/O Server
- Xsigo I/O Director



3LEAF SYSTEMS



Start From the Bottom Up: Risk-Driven Segmentation



Guidelines:

- ▶ Use risk assessment and threat modeling to determine exposure tolerance of both physical and virtual machines
- ▶ Don't cross the streams; mixing high and low risks assets onto a consolidated virtualized platform is likely a bad idea
- ▶ Segment your network based upon risk, asset criticality, function or access requirements
- ▶ Think about zone defense first, then man-to-man.
Group/consolidate assets that require like policy enforcement and can survive potential cascading failures accordingly
- ▶ Integrate host & network protection schemes and tie in telemetry (at best today: SEIM+)
- ▶ Monitor, monitor, monitor

I'm OK, You're OK - 10 Things We Can Do Today

- ▶ Get the organizational and operational issues on the table & deal with them
- ▶ Start to manage risk in the things that matter rather than hand-wringing over things that are possible but not currently probable
- ▶ Follow your virtualization platform provider's and industry guidelines for securing virtualized environments
- ▶ Apply at least the same strategies to your VM's that you use for your non-virtualized environments
- ▶ Segment your network and manage by risk, criticality, function
- ▶ Treat each cluster of VM's as a micro-perimeterized DMZ's sharing the same consistent zone-based compensating controls and policies
- ▶ Monitor and extract really good telemetry and instrumentation
- ▶ Explore new technologies and evaluate their RROI (reduction of risk on investment)
- ▶ Enforce rigorous control over admins with auditing and device management (physical and logical)
- ▶ Push vendors to develop solutions for virtualized environments



The Quest For the Virtualization Security Holy Grail

- ▶ Implement & utilize a trust model in hardware & software (TPM)
- ▶ We need affinity between the VM and protection schemes; security policy is attached to and moves with the VM and is enforced consistently both virtually and physically
- ▶ Centralized VM registration providing VM telemetry that controls spin-up, state and mobility capabilities regardless of vendor (i.e. open standards for VM configuration/policies)
- ▶ Comprehensive discovery, profiling, dynamic configuration & security management of all VM's -- online or offline
- ▶ Intelligent networking capabilities within the virtual switching infrastructure for consistency, visibility and security including integrated virtual network admission control & access Control (vNAC)
- ▶ Rootkit Detection for both hardware and software layers
- ▶ Separate and secure control/data paths
- ▶ Correlation of telemetry between VM Management and security planes
- ▶ Tie in network security functions, host controls and virtualization provisioning & management into a consolidated single pane of glass



Summary Advice for InfoSec Types

- ▶ Virtualization reinforces the need to assess and manage risk and communicate in business terms
- ▶ Just like always, focus on the basics...if you're fretting about virtualization chipset malware and you don't have configuration & change management handled, you're doomed
- ▶ Use the opportunity to bring your developers, sysadmins, the network, & security teams and the auditors closer...even if blunt-force trauma ensues
- ▶ There's no silver bullet, but instead a lot of silver buckshot. Use it all.
- ▶ If you're security sucks now, you'll be comforted by the lack of change when you deploy virtualization!



CGNetworks.com | CGTalk.com Copyright (C) Matt G

CGNetworks.com | CGTalk.com Copyright (C) Matt G

Questions/Comments?

Christofer Hoff

Chief Architect, Security Innovation - Unisys

Christofer.Hoff@Unisys.com (work)

choff@packetfilter.com (not work)

+1.978.631.0302

Blog:

<http://rationalsecurity.typepad.com>

Twitter: Beaker