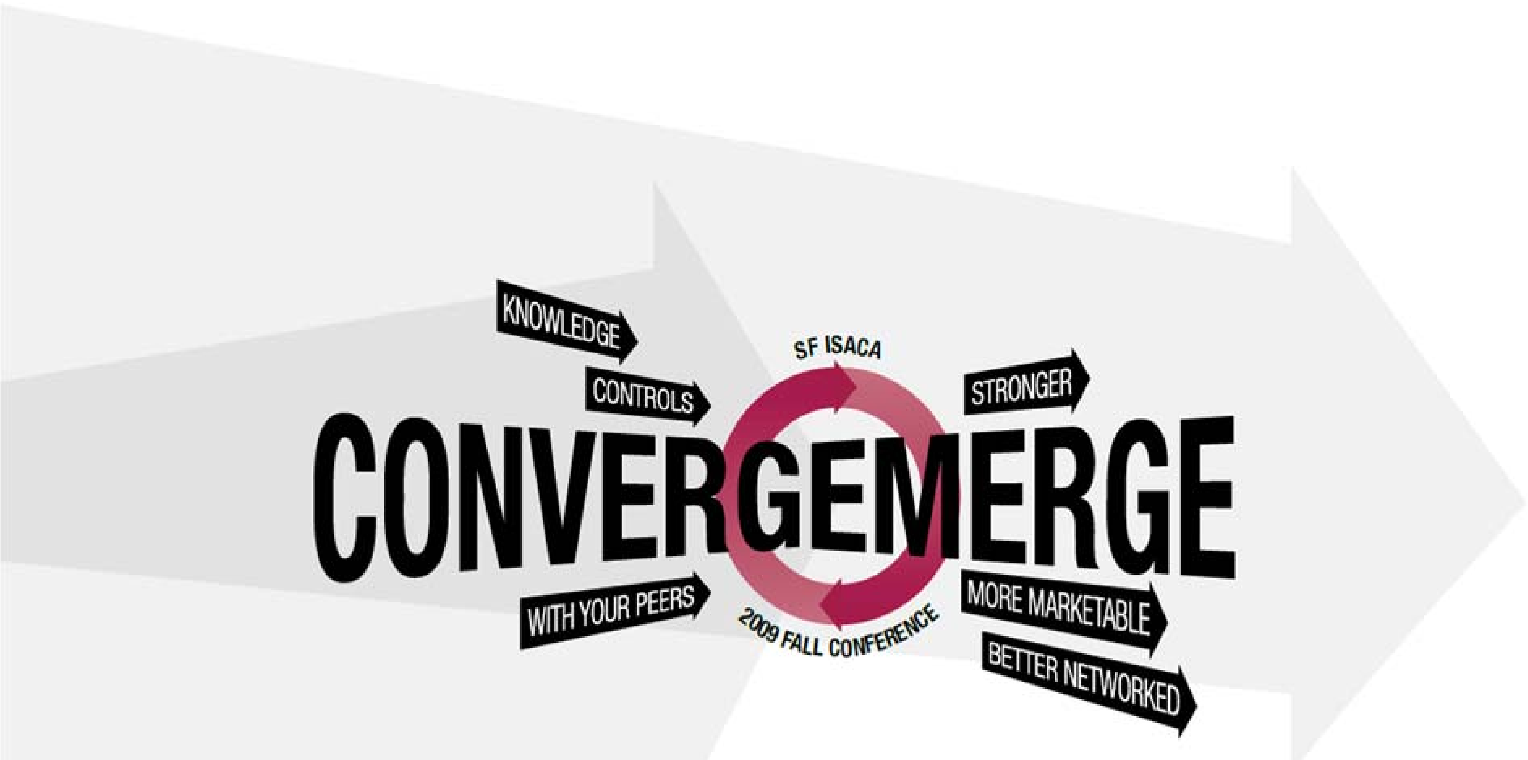
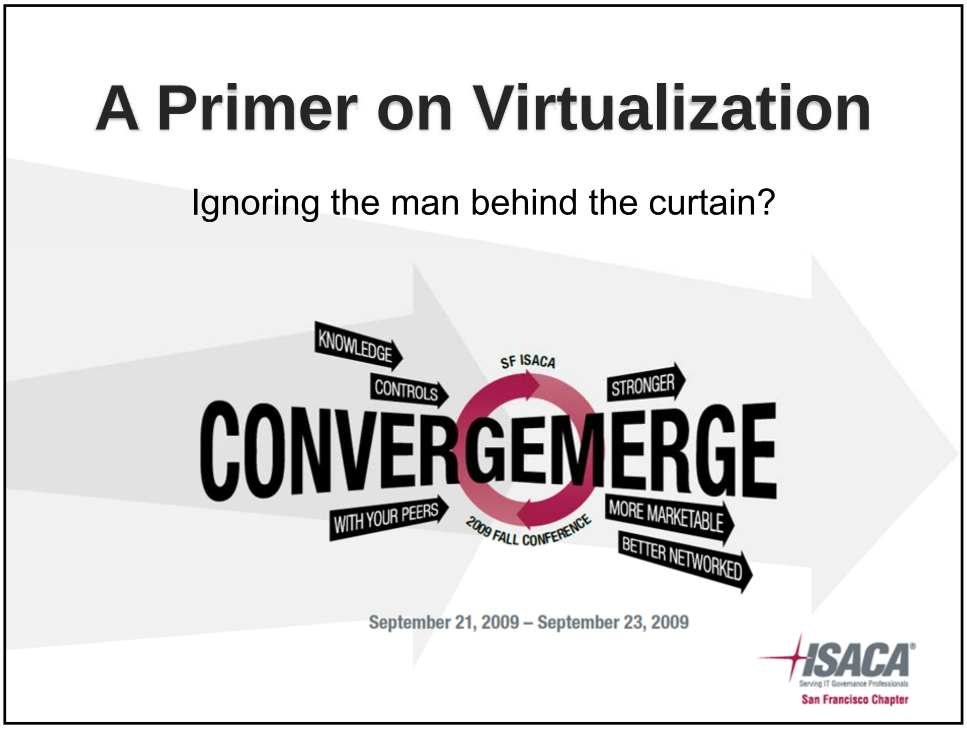
S32 - A Primer on Virtualization

Tom Ray



September 21, 2009 – September 23, 2009

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

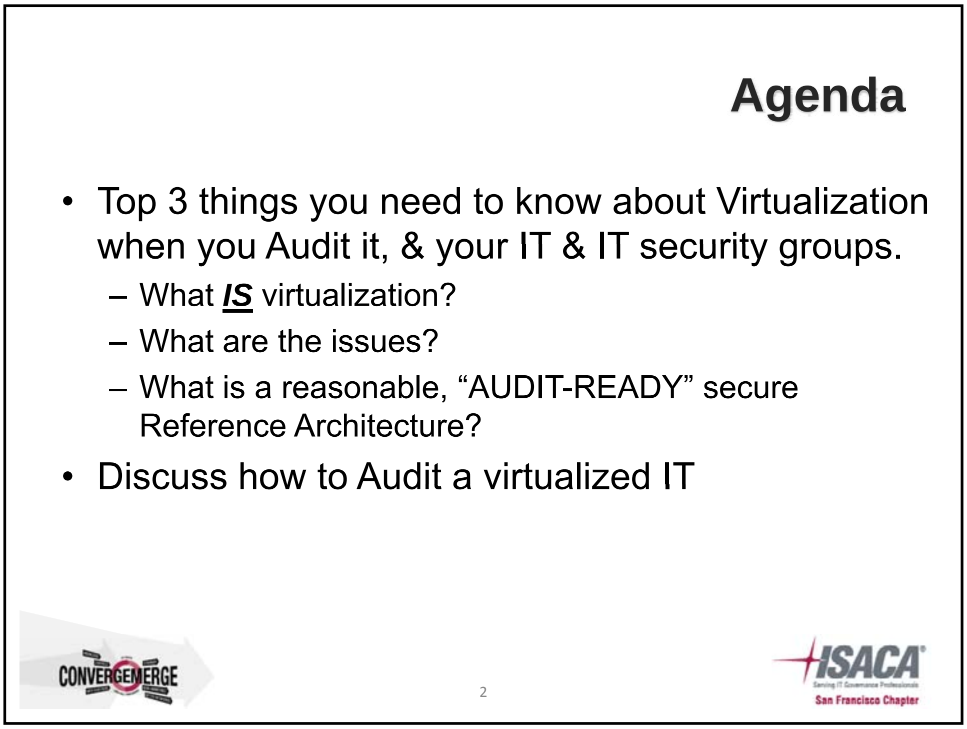


A Primer on Virtualization

Ignoring the man behind the curtain?

KNOWLEDGE
CONTROLS
SF ISACA
STRONGER
CONVERGEMERGE
WITH YOUR PEERS
2009 FALL CONFERENCE
MORE MARKETABLE
BETTER NETWORKED
ISACA
Serving IT Governance Professionals
San Francisco Chapter

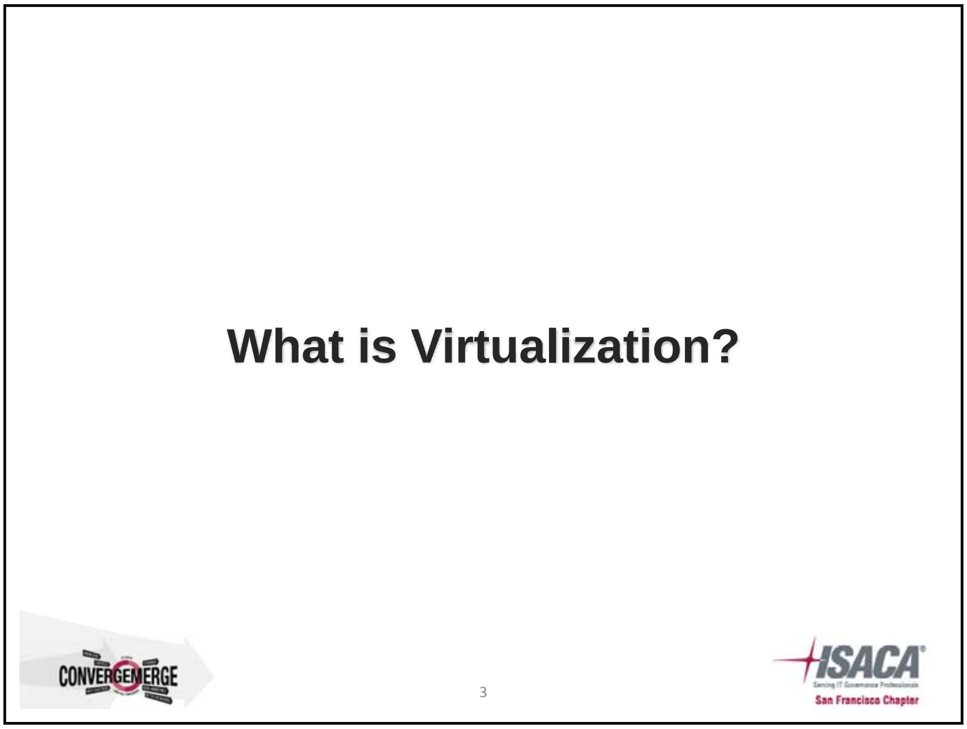
September 21, 2009 – September 23, 2009



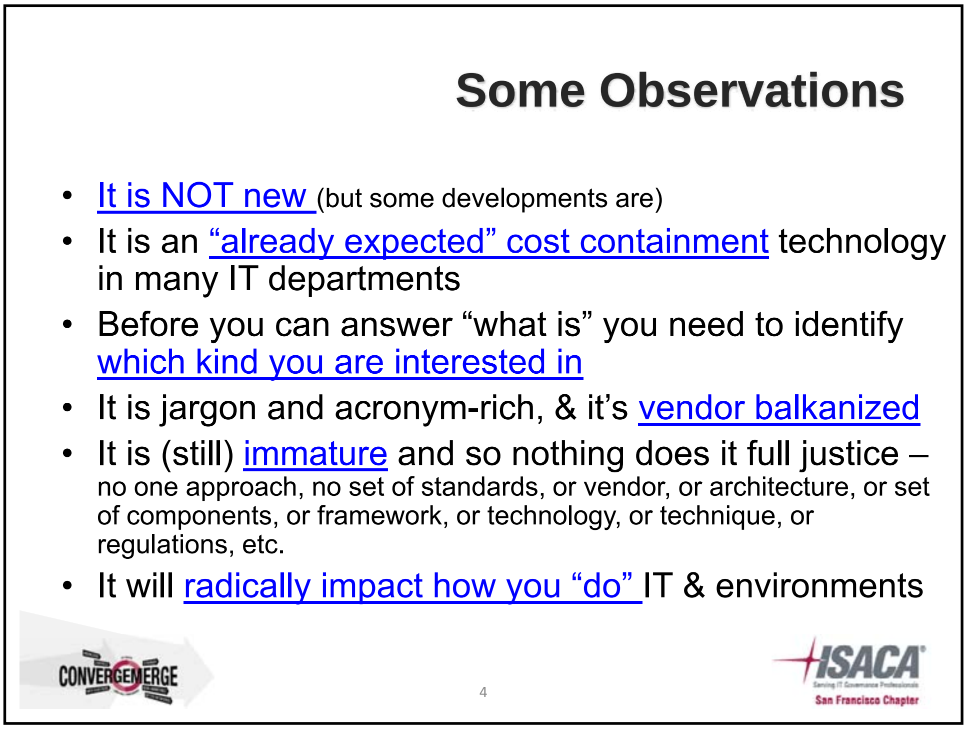
Agenda

- Top 3 things you need to know about Virtualization when you Audit it, & your IT & IT security groups.
  – What ***IS*** virtualization?
  – What are the issues?
  – What is a reasonable, “AUDIT-READY” secure Reference Architecture?
- Discuss how to Audit a virtualized IT

CONVERGEMERGE
ISACA
Serving IT Governance Professionals
San Francisco Chapter

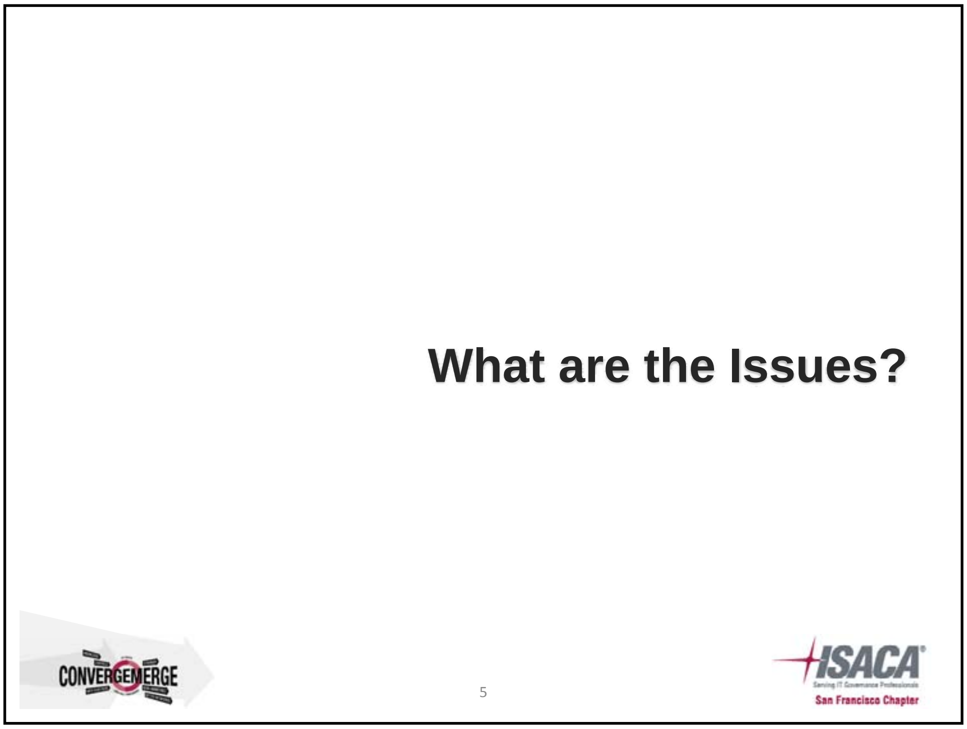


What is Virtualization?

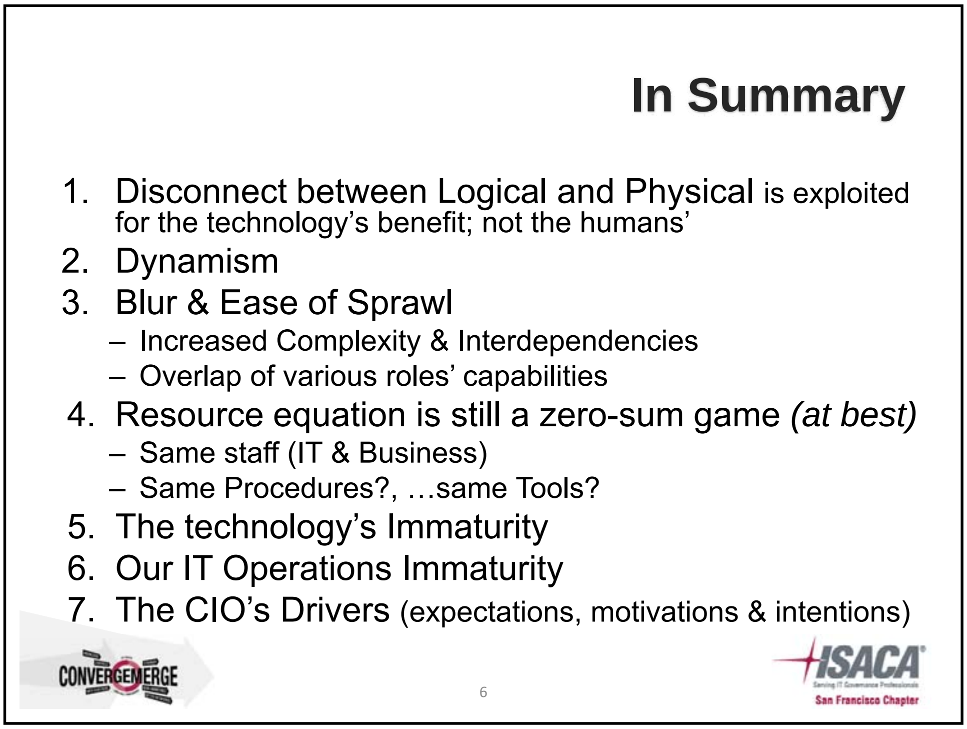


Some Observations

- It is NOT new (but some developments are)
- It is an "already expected" cost containment technology in many IT departments
- Before you can answer "what is" you need to identify which kind you are interested in
- It is jargon and acronym-rich, & it's vendor balkanized
- It is (still) immature and so nothing does it full justice – no one approach, no set of standards, or vendor, or architecture, or set of components, or framework, or technology, or technique, or regulations, etc.
- It will radically impact how you "do" IT & environments

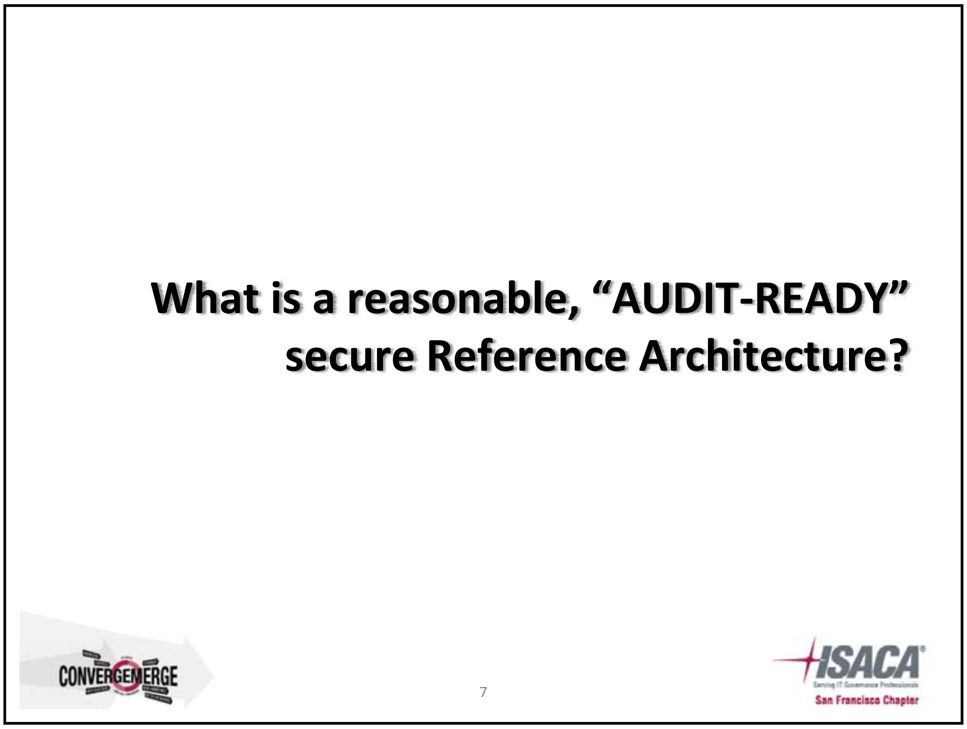


What are the Issues?

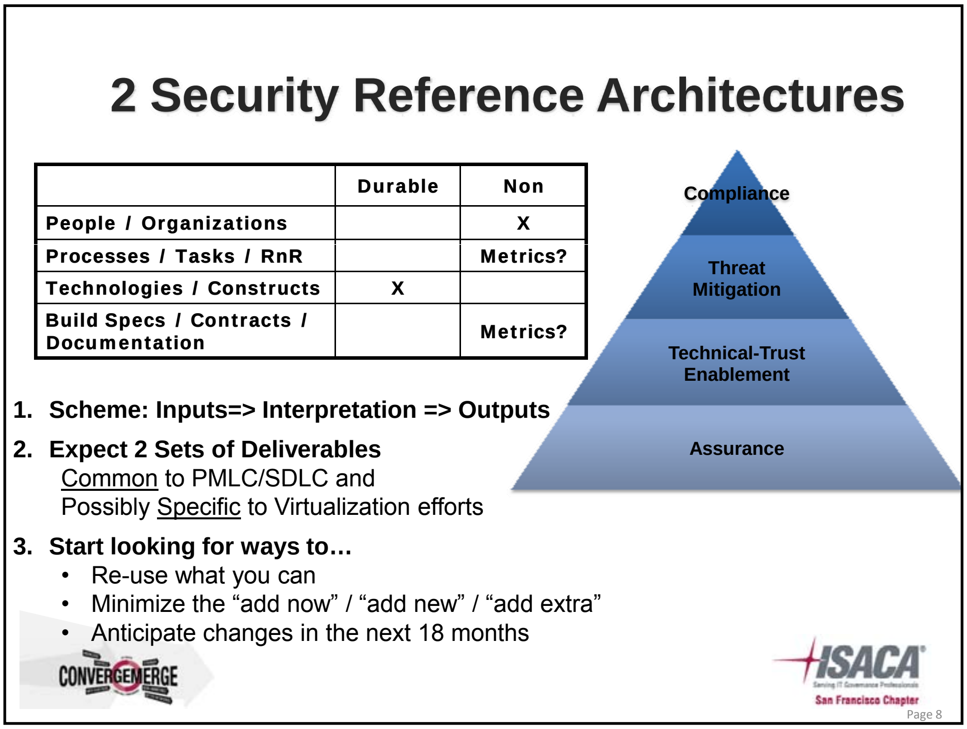


In Summary

1. Disconnect between Logical and Physical is exploited for the technology's benefit; not the humans'
2. Dynamism
3. Blur & Ease of Sprawl
   - Increased Complexity & Interdependencies
   - Overlap of various roles' capabilities
4. Resource equation is still a zero-sum game *(at best)*
   - Same staff (IT & Business)
   - Same Procedures?, …same Tools?
5. The technology's Immaturity
6. Our IT Operations Immaturity
7. The CIO's Drivers (expectations, motivations & intentions)



What is a reasonable, "AUDIT-READY" secure Reference Architecture?



2 Security Reference Architectures

	Durable	Non
People / Organizations		X
Processes / Tasks / RnR		Metrics?
Technologies / Constructs	X	
Build Specs / Contracts / Documentation		Metrics?

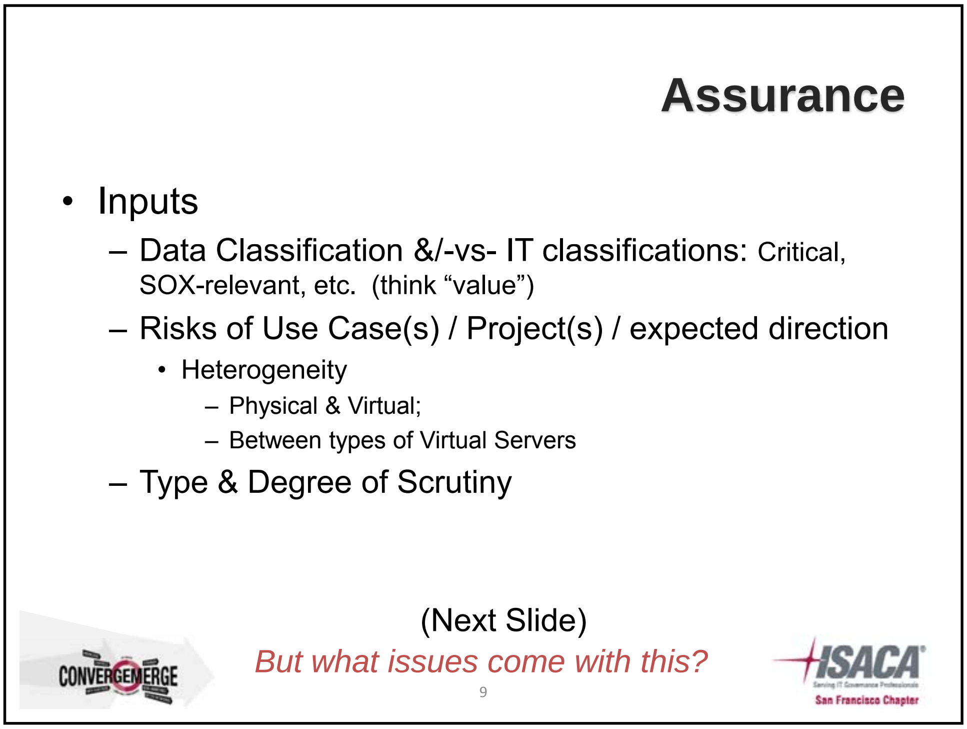
Compliance

Threat Mitigation

Technical-Trust Enablement

Assurance

1. **Scheme: Inputs=> Interpretation => Outputs**
2. **Expect 2 Sets of Deliverables**
   <u>Common</u> to PMLC/SDLC and
   Possibly <u>Specific</u> to Virtualization efforts
3. **Start looking for ways to…**
   - Re-use what you can
   - Minimize the "add now" / "add new" / "add extra"
   - Anticipate changes in the next 18 months

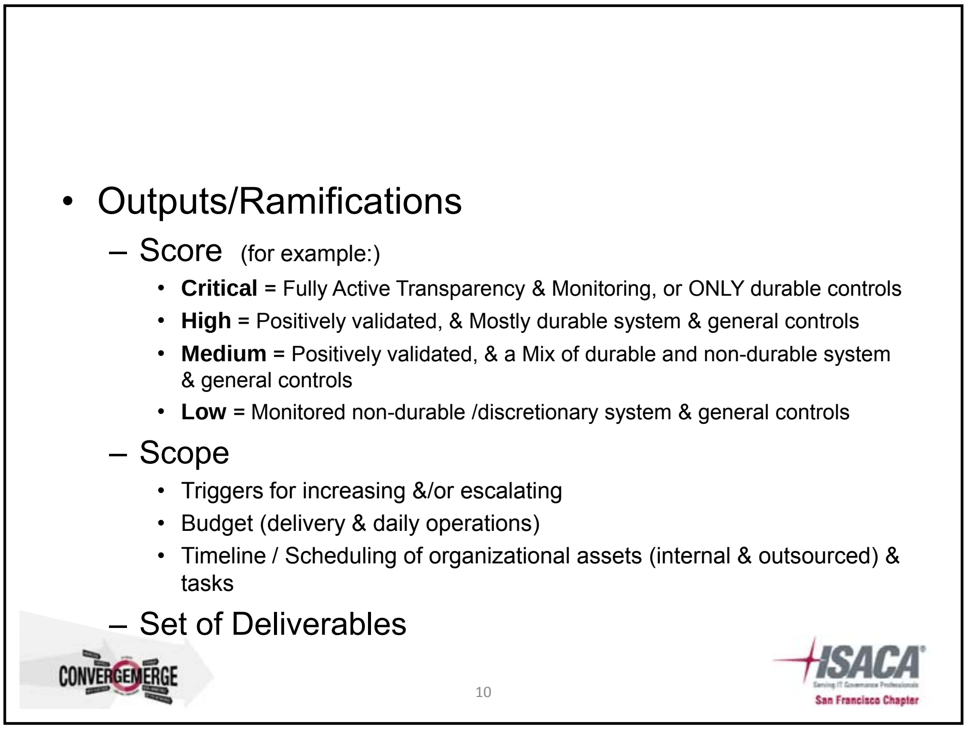


Assurance

- Inputs
  - Data Classification &/-vs- IT classifications: Critical, SOX-relevant, etc. (think “value”)
  - Risks of Use Case(s) / Project(s) / expected direction
    - Heterogeneity
      - Physical & Virtual;
      - Between types of Virtual Servers
  - Type & Degree of Scrutiny

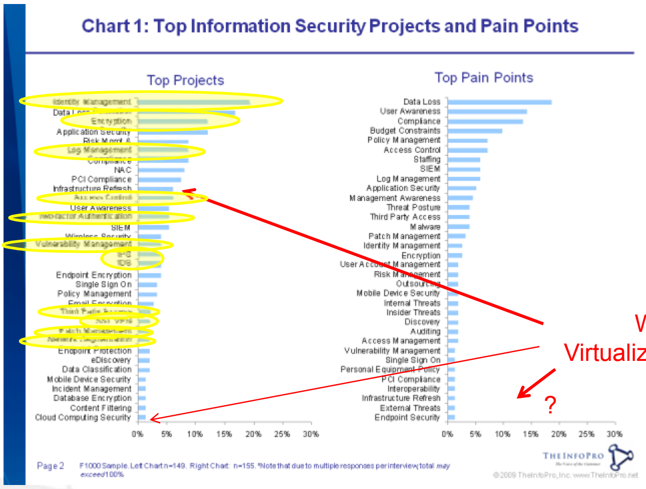
(Next Slide)

But what issues come with this?



- Outputs/Ramifications
  - Score (for example:)
    - **Critical** = Fully Active Transparency & Monitoring, or ONLY durable controls
    - **High** = Positively validated, & Mostly durable system & general controls
    - **Medium** = Positively validated, & a Mix of durable and non-durable system & general controls
    - **Low** = Monitored non-durable /discretionary system & general controls
  - Scope
    - Triggers for increasing &/or escalating
    - Budget (delivery & daily operations)
    - Timeline / Scheduling of organizational assets (internal & outsourced) & tasks
  - Set of Deliverables

Budget & Priority



F1000 Sample. Left Chart n=149. Right Chart: n=155. *Note that due to multiple responses per interview, total may exceed 100%

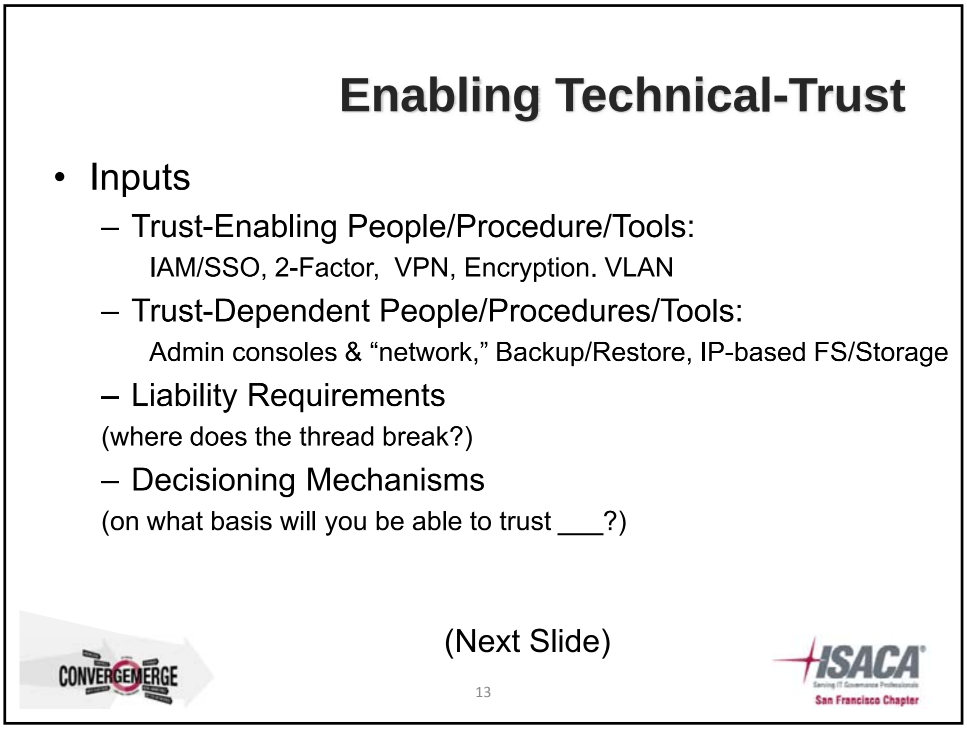
©2009 TheInfoPro, Inc. www.TheInfoPro.net

Where is Virtualization Security?

?

Deliverables

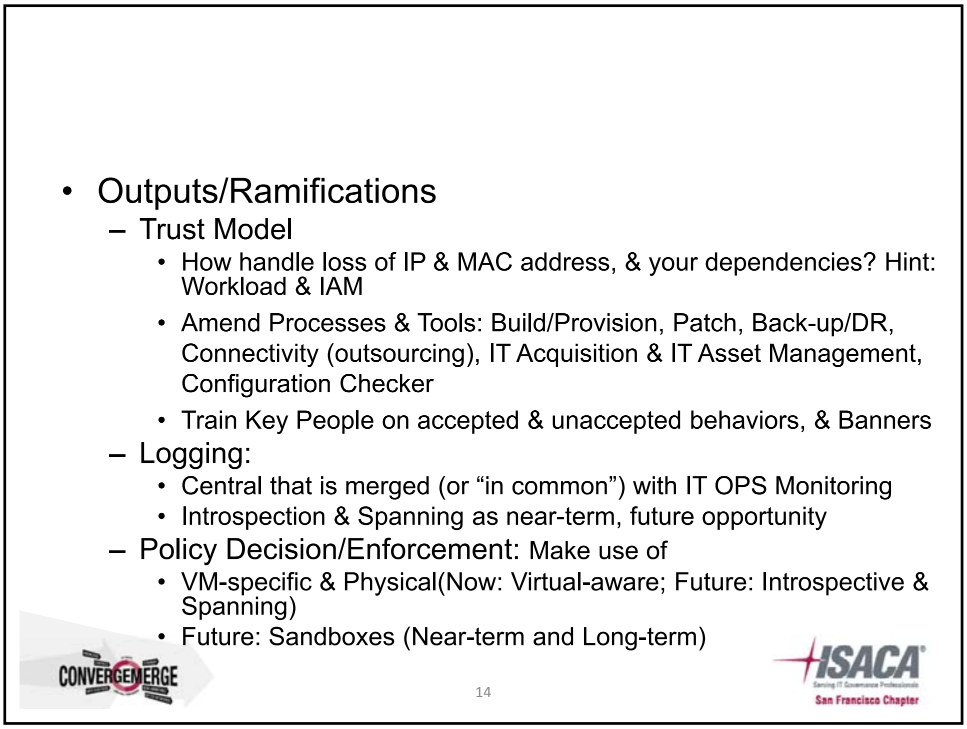
- Risk Assessment Report
  - Score
  - Scope
- Baseline / Certifications of Virtualized Implementations and of (impact on) enterprise
- Set of other "standard" Documentation expectations
  - Roles & Responsibilities Matrix
  - Design Diagram(s) (aka "architecture")
  - Secure Configuration Standard (one per hypervisor/VMM)
  - IT Operations Runbooks (&/or PPS&G)
  - Contract Change Orders & Provisions (T&Cs, SLAs, Pricing structures/ Costs (BAU+, BAU basis), Governance, T/S, Procedures Manuals)
  - System Security Build Specification (& Connectivity Agreements)
  - IT Integration/Interoperability Standard(s)



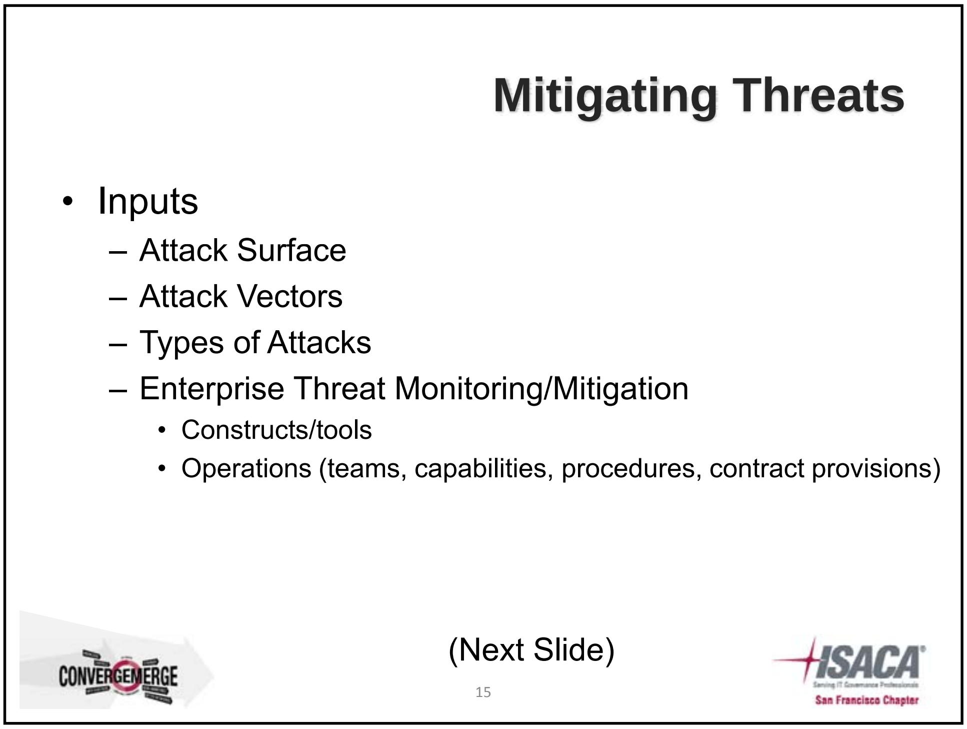
Enabling Technical-Trust

- Inputs
  - Trust-Enabling People/Procedure/Tools:
    IAM/SSO, 2-Factor, VPN, Encryption. VLAN
  - Trust-Dependent People/Procedures/Tools:
    Admin consoles & “network,” Backup/Restore, IP-based FS/Storage
  - Liability Requirements
  (where does the thread break?)
  - Decisioning Mechanisms
  (on what basis will you be able to trust ___?)

(Next Slide)



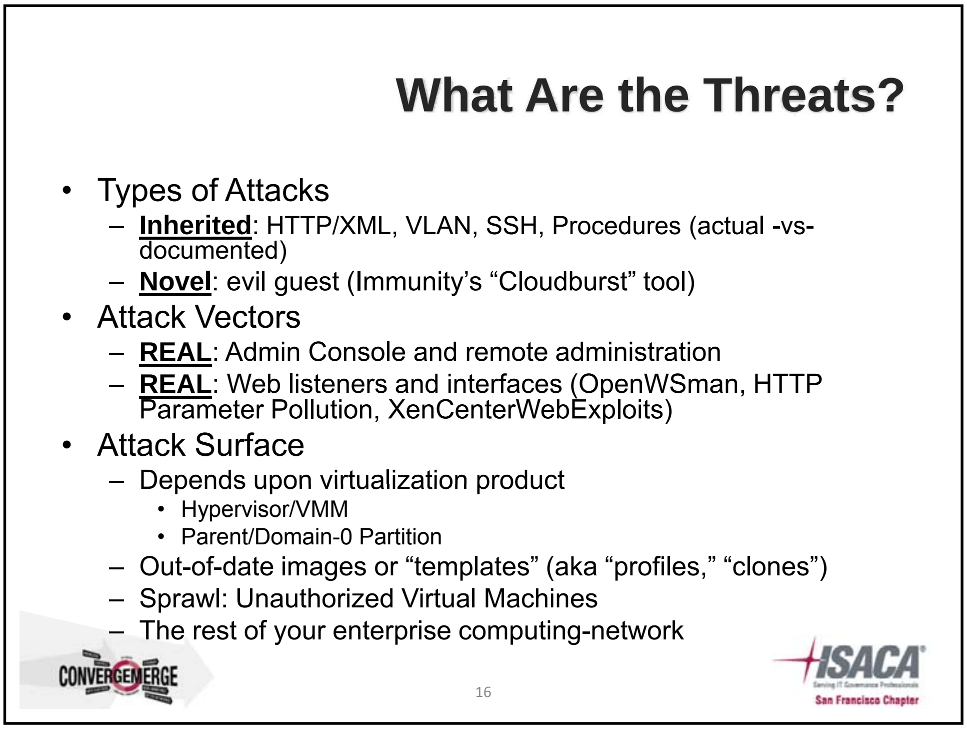
- Outputs/Ramifications
  - Trust Model
    - How handle loss of IP & MAC address, & your dependencies? Hint: Workload & IAM
    - Amend Processes & Tools: Build/Provision, Patch, Back-up/DR, Connectivity (outsourcing), IT Acquisition & IT Asset Management, Configuration Checker
    - Train Key People on accepted & unaccepted behaviors, & Banners
  - Logging:
    - Central that is merged (or “in common”) with IT OPS Monitoring
    - Introspection & Spanning as near-term, future opportunity
  - Policy Decision/Enforcement: Make use of
    - VM-specific & Physical(Now: Virtual-aware; Future: Introspective & Spanning)
    - Future: Sandboxes (Near-term and Long-term)



Mitigating Threats

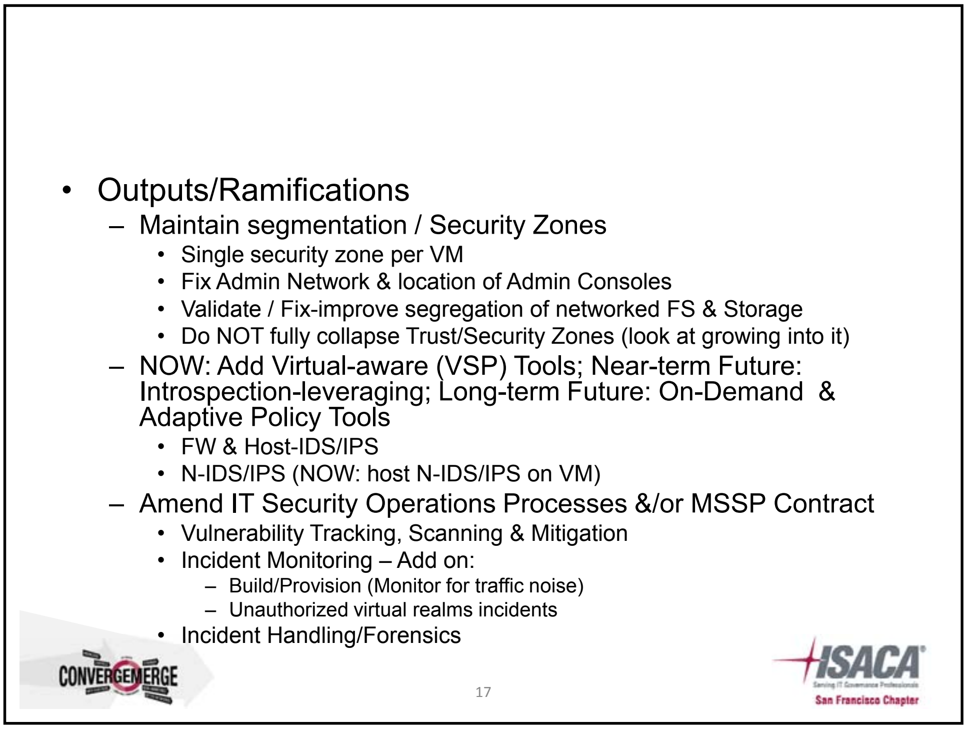
- Inputs
  - Attack Surface
  - Attack Vectors
  - Types of Attacks
  - Enterprise Threat Monitoring/Mitigation
    - Constructs/tools
    - Operations (teams, capabilities, procedures, contract provisions)

(Next Slide)

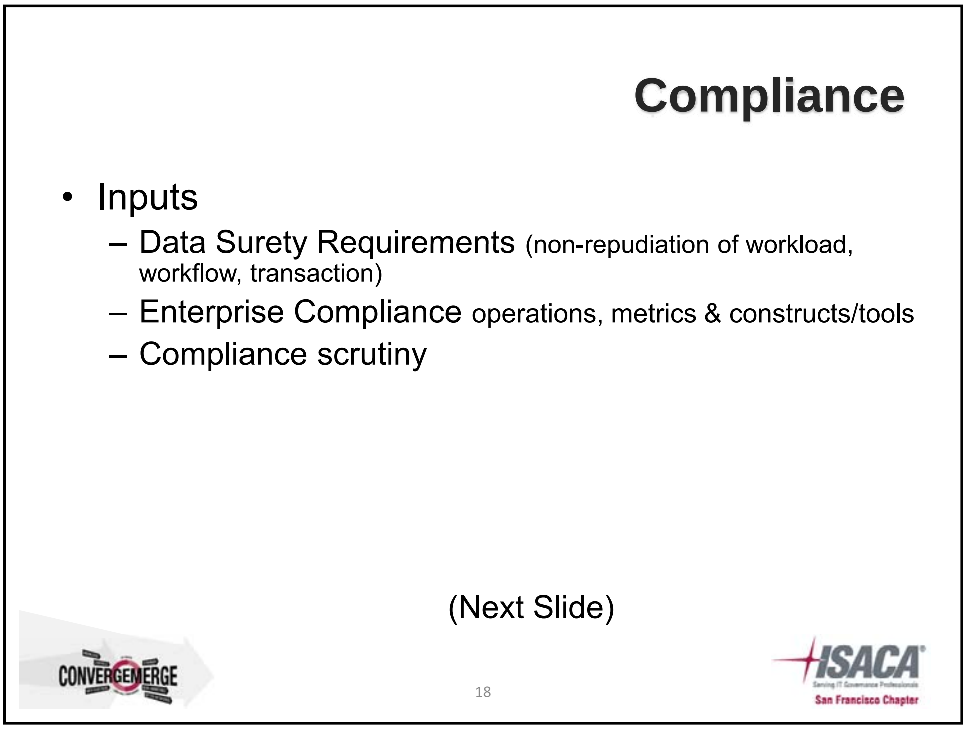


What Are the Threats?

- Types of Attacks
  - **Inherited**: HTTP/XML, VLAN, SSH, Procedures (actual -vs- documented)
  - **Novel**: evil guest (Immunity’s “Cloudburst” tool)
- Attack Vectors
  - **REAL**: Admin Console and remote administration
  - **REAL**: Web listeners and interfaces (OpenWSman, HTTP Parameter Pollution, XenCenterWebExploits)
- Attack Surface
  - Depends upon virtualization product
    - Hypervisor/VMM
    - Parent/Domain-0 Partition
  - Out-of-date images or “templates” (aka “profiles,” “clones”)
  - Sprawl: Unauthorized Virtual Machines
  - The rest of your enterprise computing-network



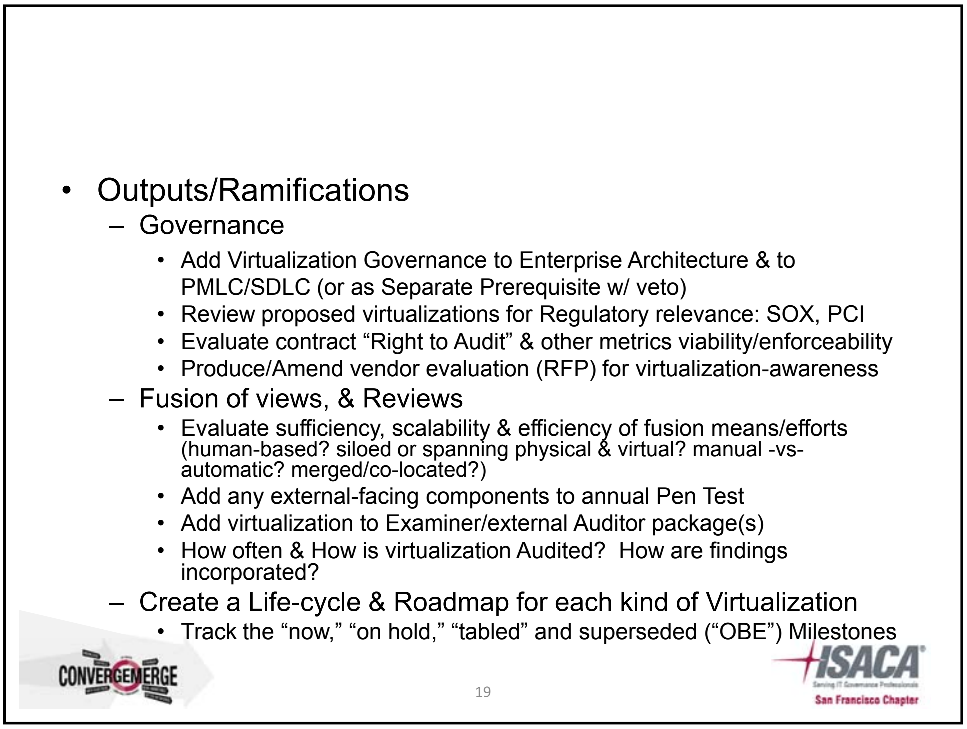
- Outputs/Ramifications
  - Maintain segmentation / Security Zones
    - Single security zone per VM
    - Fix Admin Network & location of Admin Consoles
    - Validate / Fix-improve segregation of networked FS & Storage
    - Do NOT fully collapse Trust/Security Zones (look at growing into it)
  - NOW: Add Virtual-aware (VSP) Tools; Near-term Future: Introspection-leveraging; Long-term Future: On-Demand & Adaptive Policy Tools
    - FW & Host-IDS/IPS
    - N-IDS/IPS (NOW: host N-IDS/IPS on VM)
  - Amend IT Security Operations Processes &/or MSSP Contract
    - Vulnerability Tracking, Scanning & Mitigation
    - Incident Monitoring – Add on:
      - Build/Provision (Monitor for traffic noise)
      - Unauthorized virtual realms incidents
    - Incident Handling/Forensics



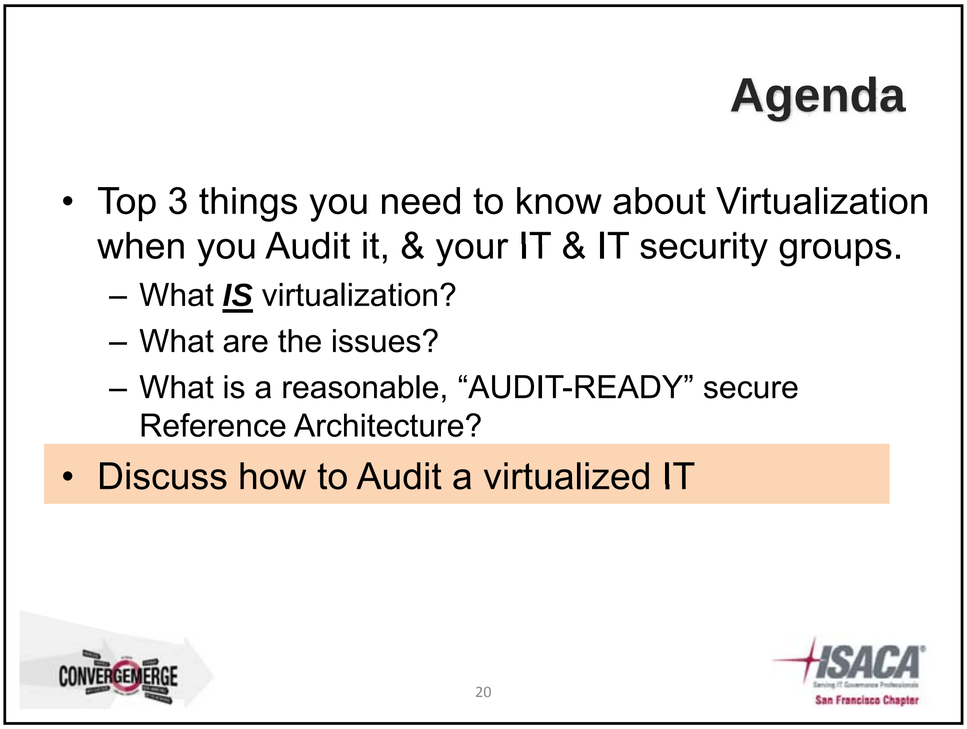
Compliance

- Inputs
  - Data Surety Requirements (non-repudiation of workload, workflow, transaction)
  - Enterprise Compliance operations, metrics & constructs/tools
  - Compliance scrutiny

(Next Slide)

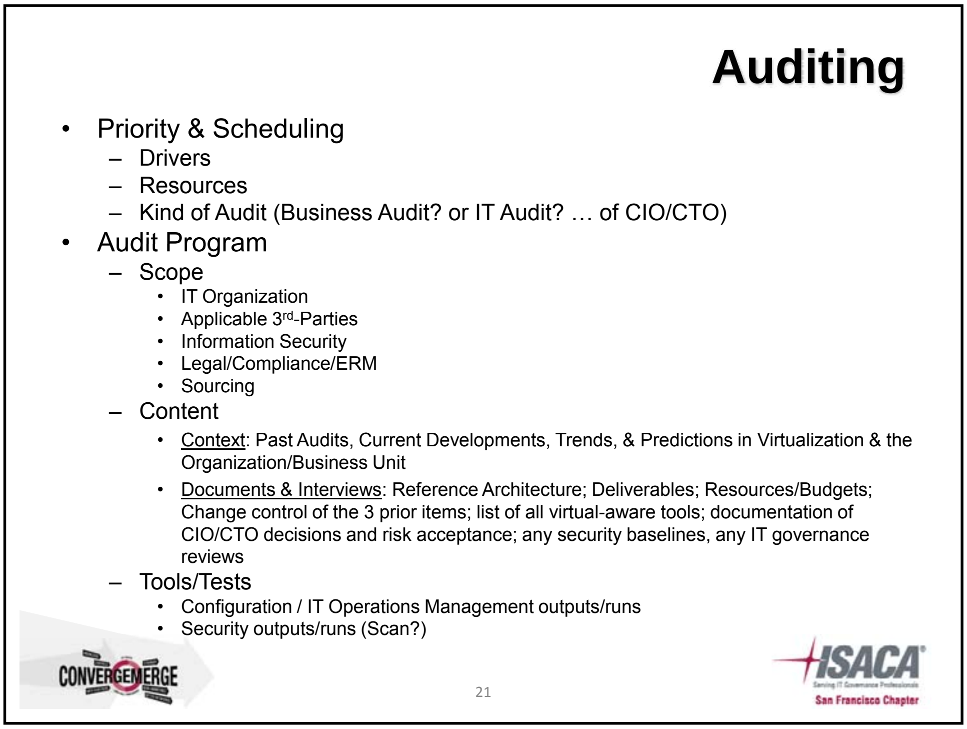


- Outputs/Ramifications
  - Governance
    - Add Virtualization Governance to Enterprise Architecture & to PMLC/SDLC (or as Separate Prerequisite w/ veto)
    - Review proposed virtualizations for Regulatory relevance: SOX, PCI
    - Evaluate contract “Right to Audit” & other metrics viability/enforceability
    - Produce/Amend vendor evaluation (RFP) for virtualization-awareness
  - Fusion of views, & Reviews
    - Evaluate sufficiency, scalability & efficiency of fusion means/efforts (human-based? siloed or spanning physical & virtual? manual -vs-automatic? merged/co-located?)
    - Add any external-facing components to annual Pen Test
    - Add virtualization to Examiner/external Auditor package(s)
    - How often & How is virtualization Audited? How are findings incorporated?
  - Create a Life-cycle & Roadmap for each kind of Virtualization
    - Track the “now,” “on hold,” “tabled” and superseded (“OBE”) Milestones



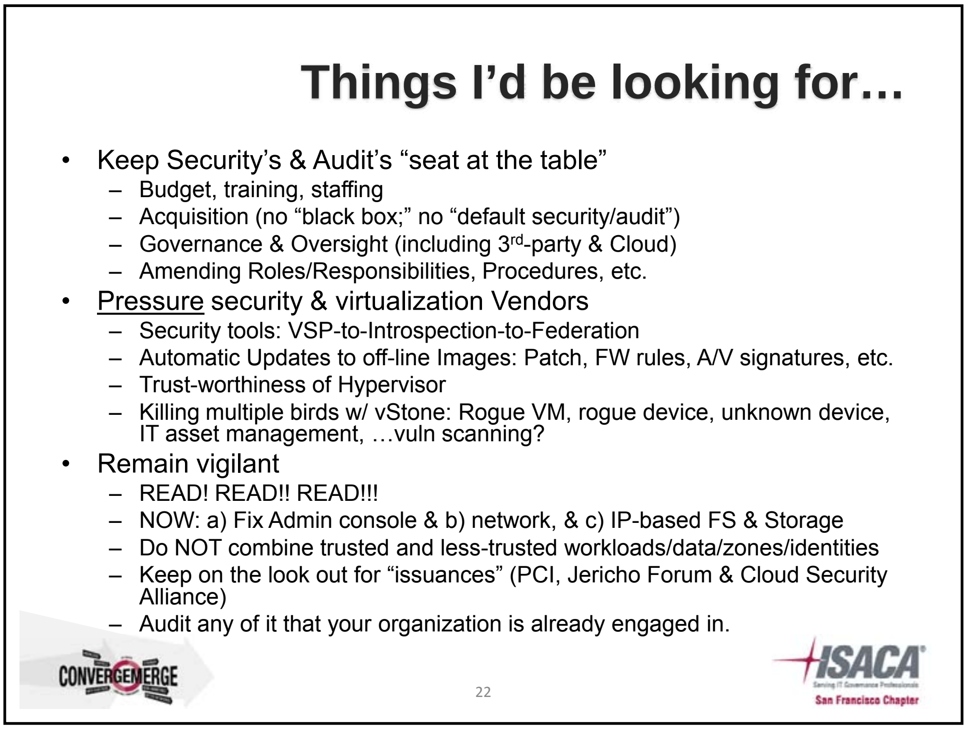
Agenda

- Top 3 things you need to know about Virtualization when you Audit it, & your IT & IT security groups.
  - What ***IS*** virtualization?
  - What are the issues?
  - What is a reasonable, “AUDIT-READY” secure Reference Architecture?
- Discuss how to Audit a virtualized IT



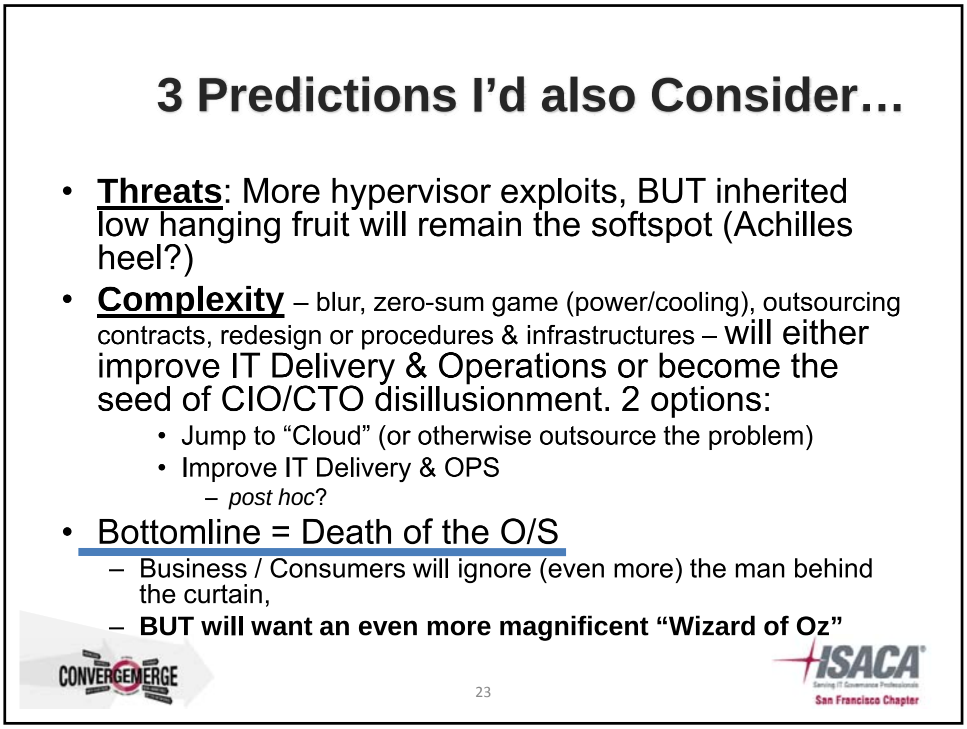
Auditing

- Priority & Scheduling
  - Drivers
  - Resources
  - Kind of Audit (Business Audit? or IT Audit? … of CIO/CTO)
- Audit Program
  - Scope
    - IT Organization
    - Applicable 3rd-Parties
    - Information Security
    - Legal/Compliance/ERM
    - Sourcing
  - Content
    - Context: Past Audits, Current Developments, Trends, & Predictions in Virtualization & the Organization/Business Unit
    - Documents & Interviews: Reference Architecture; Deliverables; Resources/Budgets; Change control of the 3 prior items; list of all virtual-aware tools; documentation of CIO/CTO decisions and risk acceptance; any security baselines, any IT governance reviews
  - Tools/Tests
    - Configuration / IT Operations Management outputs/runs
    - Security outputs/runs (Scan?)



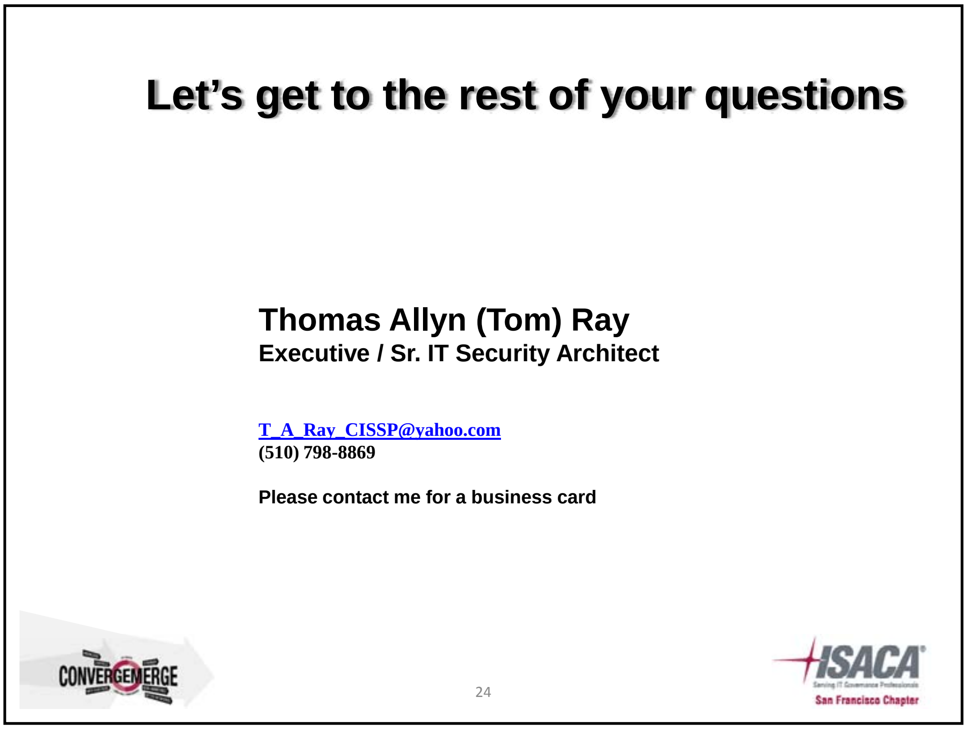
Things I'd be looking for…

- Keep Security's & Audit's "seat at the table"
  - Budget, training, staffing
  - Acquisition (no "black box;" no "default security/audit")
  - Governance & Oversight (including 3rd-party & Cloud)
  - Amending Roles/Responsibilities, Procedures, etc.
- Pressure security & virtualization Vendors
  - Security tools: VSP-to-Introspection-to-Federation
  - Automatic Updates to off-line Images: Patch, FW rules, A/V signatures, etc.
  - Trust-worthiness of Hypervisor
  - Killing multiple birds w/ vStone: Rogue VM, rogue device, unknown device, IT asset management, …vuln scanning?
- Remain vigilant
  - READ! READ!! READ!!!
  - NOW: a) Fix Admin console & b) network, & c) IP-based FS & Storage
  - Do NOT combine trusted and less-trusted workloads/data/zones/identities
  - Keep on the look out for "issuances" (PCI, Jericho Forum & Cloud Security Alliance)
  - Audit any of it that your organization is already engaged in.



3 Predictions I'd also Consider…

- **Threats**: More hypervisor exploits, BUT inherited low hanging fruit will remain the softspot (Achilles heel?)
- **Complexity** – blur, zero-sum game (power/cooling), outsourcing contracts, redesign or procedures & infrastructures – will either improve IT Delivery & Operations or become the seed of CIO/CTO disillusionment. 2 options:
  - Jump to "Cloud" (or otherwise outsource the problem)
  - Improve IT Delivery & OPS
    - *post hoc*?
- Bottomline = Death of the O/S
  - Business / Consumers will ignore (even more) the man behind the curtain,
  - **BUT will want an even more magnificent "Wizard of Oz"**



Let's get to the rest of your questions

Thomas Allyn (Tom) Ray
Executive / Sr. IT Security Architect

T_A_Ray_CISSP@yahoo.com
(510) 798-8869

Please contact me for a business card

Budget & Priority

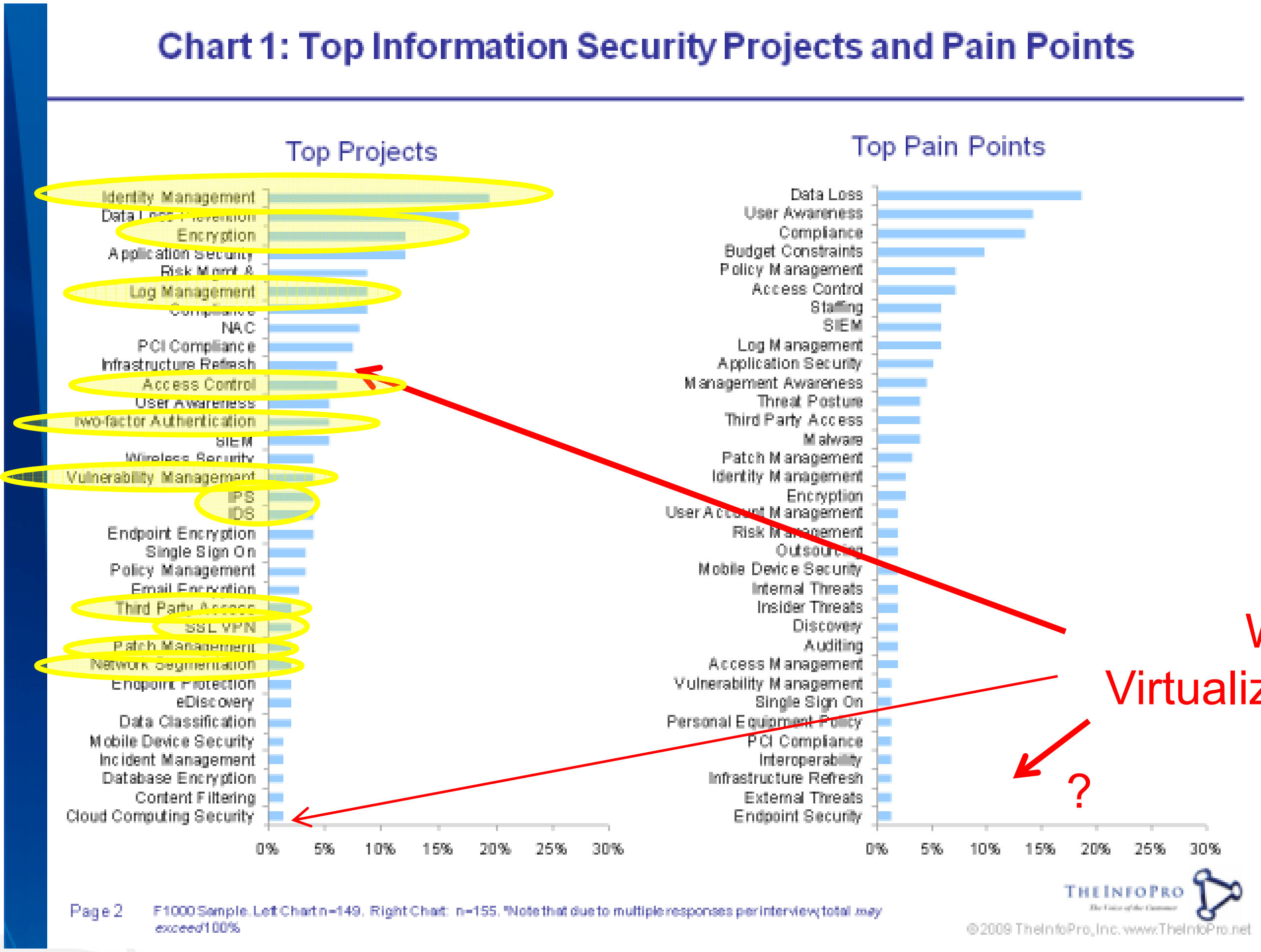


Chart 1: Top Information Security Projects and Pain Points

Page 2 F1000 Sample. Left Chart n=149. Right Chart: n=155. *Note that due to multiple responses per interview, total *may exceed 100%*

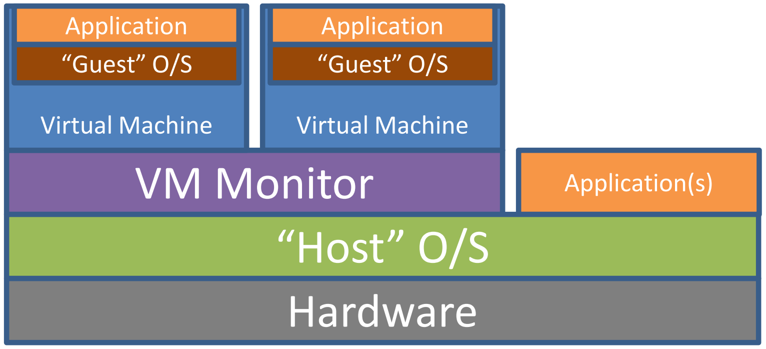
THE INFOPRO *The Voice of the Customer*

©2009 TheInfoPro, Inc. www.TheInfoPro.net

Where is Virtualization Security?

?

Balkanization of Server Virtualization



Application | Application

"Guest" O/S | "Guest" O/S

Virtual Machine | Virtual Machine

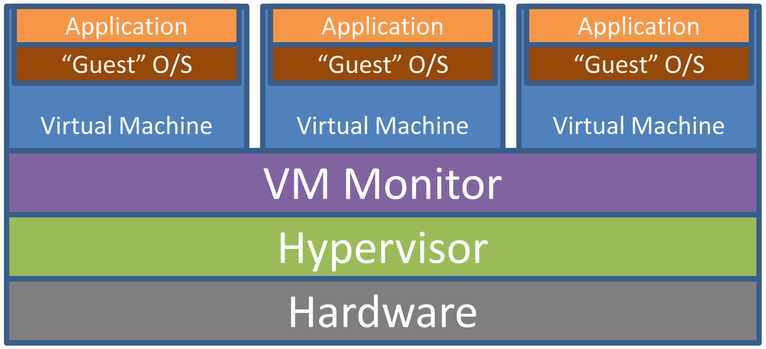
VM Monitor | Application(s)

"Host" O/S

Hardware

Hosted VM (traditional)

VMWare Workstation & GSX



Application | Application | Application

"Guest" O/S | "Guest" O/S | "Guest" O/S

Virtual Machine | Virtual Machine | Virtual Machine

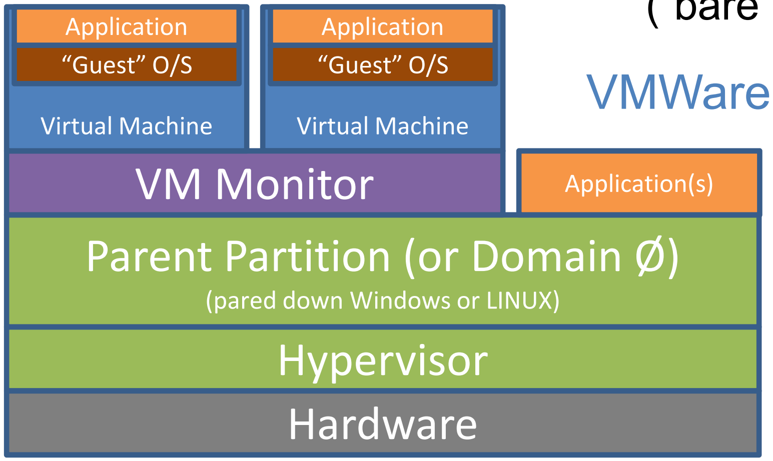
VM Monitor

Hypervisor

Hardware

Hypervisor-based VM
("bare metal")

VMWare ESX & IBM



Application | Application

"Guest" O/S | "Guest" O/S

Virtual Machine | Virtual Machine

VM Monitor | Application(s)

Parent Partition (or Domain Ø)
(pared down Windows or LINUX)

Hypervisor

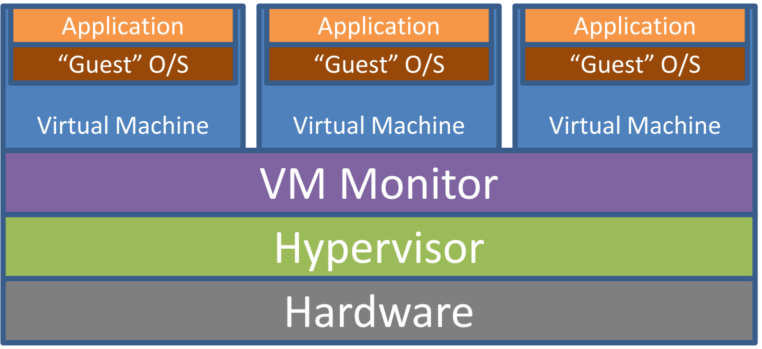
Hardware

Parent Partition VM

MS Hyper-V & CITRIX Xen

Its Impact on IT Security

- Root Hypervisor ID
- Visibility of state (introspection) & between VMs (“traffic”)
- Sensitivity of Service Partitions
  - Privilege / Unprivileged


Application | Application | Application

“Guest” O/S | “Guest” O/S | “Guest” O/S

Virtual Machine | Virtual Machine | Virtual Machine

VM Monitor

Hypervisor

Hardware

Hypervisor-based VM
(“bare metal”)

- Security of the VM Code
  - Bugs / Vulnerabilities & Exposures, & Code’s “reputation”
    - ➢ Responsiveness: How quickly and how “high touch”
  - If also Parent Partition/Dom0, then Tripwire host OS
  - Use of Hardware technologies able to support Virtualization
    - ➢ Memory (data use segregation from execution use)
    - ➢ Virtualization Technology
      - Intel: VT
      - AMD: SVM (Secure Virtual Machine)

Return

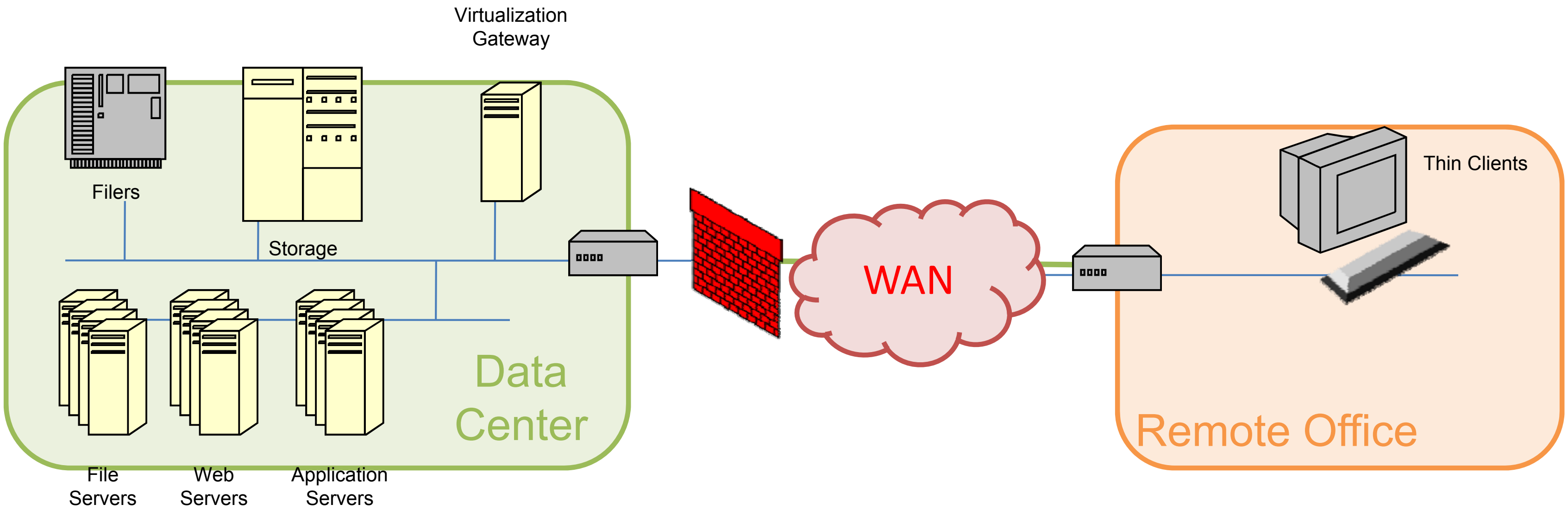
Security Tools	
IAM/Access Control	•VMWare, IBM, Microsoft, CITRIX
VPN	•CheckPoint VPN-1 Power VSX
Patch Management	•**Shavlik NetChk Protect**
BackUp/Restore	•Symantec **Backup EXEC** 12.5*
Automatic HA/Fault Tol/Rcvy	•**Marathon Technologies**
Secure management **Configuration Management &** **Integrity Checkers**	•**Reflex Systems** Virtual Management Center (VMC) + Virtual Security Appliance (VSA) •Tripwire vWire •Configuresoft (EMC) •(Symantec) **Altiris CMS** •Microsoft System Center Configuration Manager (SCCM) •BMC Software Virtualization Management (VM)
FW/H-IDS/-IPS **UTM** **NAC**	•**Apani Networks** (EpiForce: identity-based security zones/network access control as an alternative to firewall-based zoning) •**Trusted Network Technologies** (identity-based network access control) •**Astaro** Security Gateway (ASG) •**CheckPoint/Riverbed** WAN/virtual optimized Security Gateway R70 (FW, VPN, IPS,A/V, anti-spyware, URL filtering, Web security, anti-spam and policy management) •Microsoft: ISA (vsp) •Stonesoft StoneGate (FW, IPS, VPN) •Checkpoint VPN-1 VE (vsp) FW, VPN •**Montego Networks** (former Reflex employees) virtual switch (hosted N-) IDS/IPS, L2-L4 Content FW •Catbird Networks: V-gent (SNORT-based IDS/IPS, NAC and vulnerability assessment)
N-IDS/IPS	•StillSecure: Strata Guard Free (SNORT-based IDS/IPS) •SourceFire (SNORT) IPS (vsp) •Enterasys ("Dragon") Secure Networks (NAC, IPS)
Introspection-based	•**Altor Networks** (former Check Point employees) VF 3.0 •(VMWare) Determina (HIPS) & Blue Lane Technologies (in-line Patch Proxy) •**Third Brigade(TrendMicro)** FW, IPS, Integrity Monitor & Log Inspection

IT OPS Management / Monitoring Tools
•VMWare: VirtualCenter, etc.
•CITRIX: Citrix Delivery Center
•Microsoft: SCVMM
•IBM
•CA
•HP
•BMC Software
•VKernel SearchMyVM
•Veeam FastSCP + Backup
•Akorri BalancePoint
•Embotics V-Commander(1+)
•**Reflex Systems** Virtual Management Center
•FastScale Composer with Virtual Manager
•LeftHand Networks Virtual SAN Appliance
•Ultimate Deployment Appliance+ VMWare ESX Deployment Appliance
•Vizioncore vEssentials
•Storage VMotion plug-in
•DynamicOps VResource Mgr (VRM)
•Fortisphere Virtual Essentials
•**Hyper9 Search**
•**SPLUNK> Search**
•ManageIQ Enterprise Virtualization Mgr (EVM)

Return

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Legacy Model (DC Delivery)

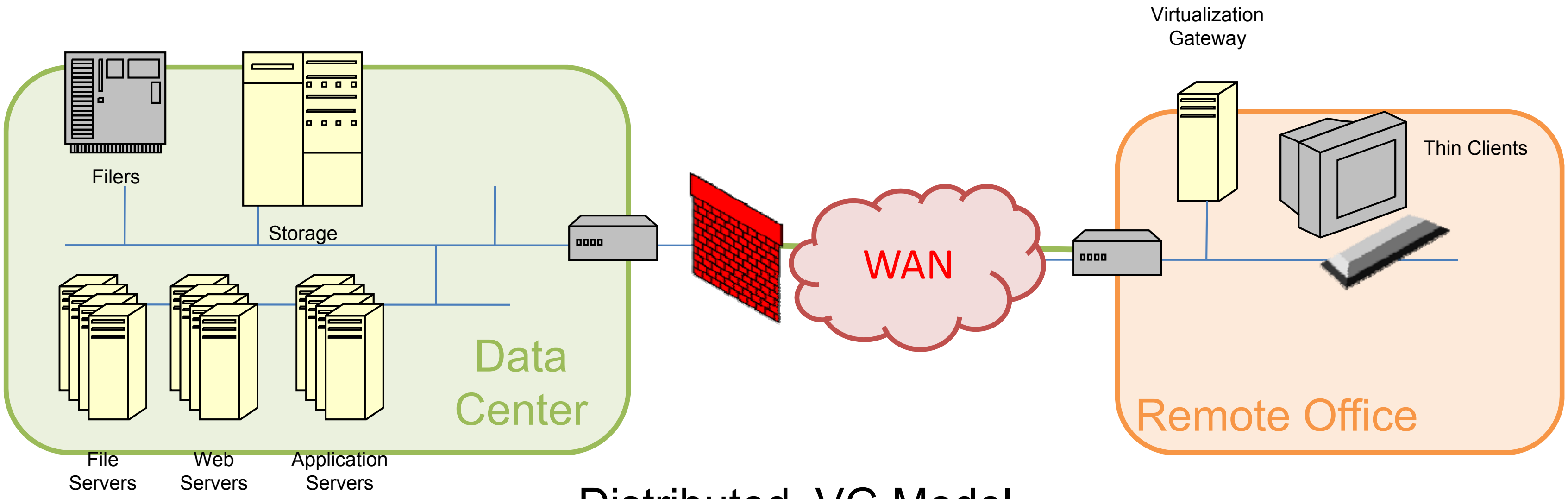


Transmit ONLY
- Visual representation of Desktop (not application data)
- Changes (e.g., mouse movements, highlights, new screens)

3 Concerns (Trade-offs?)
- How Fat is “Thin”
- BW Saturation
- Latency

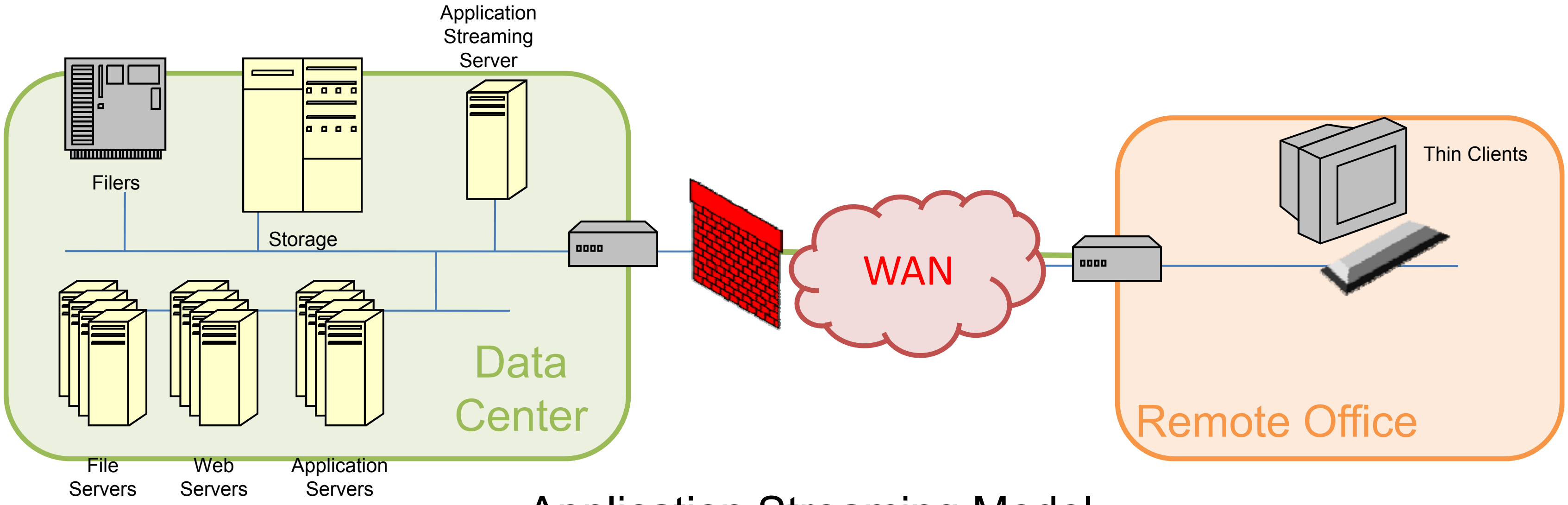
Which Network Protocol?
- TCP: But latency out-scales solution (most Term Svrs w/ RDP)
- UDP: But too thin for local applications (SunRay w/ ALP)

Distributed VG Model



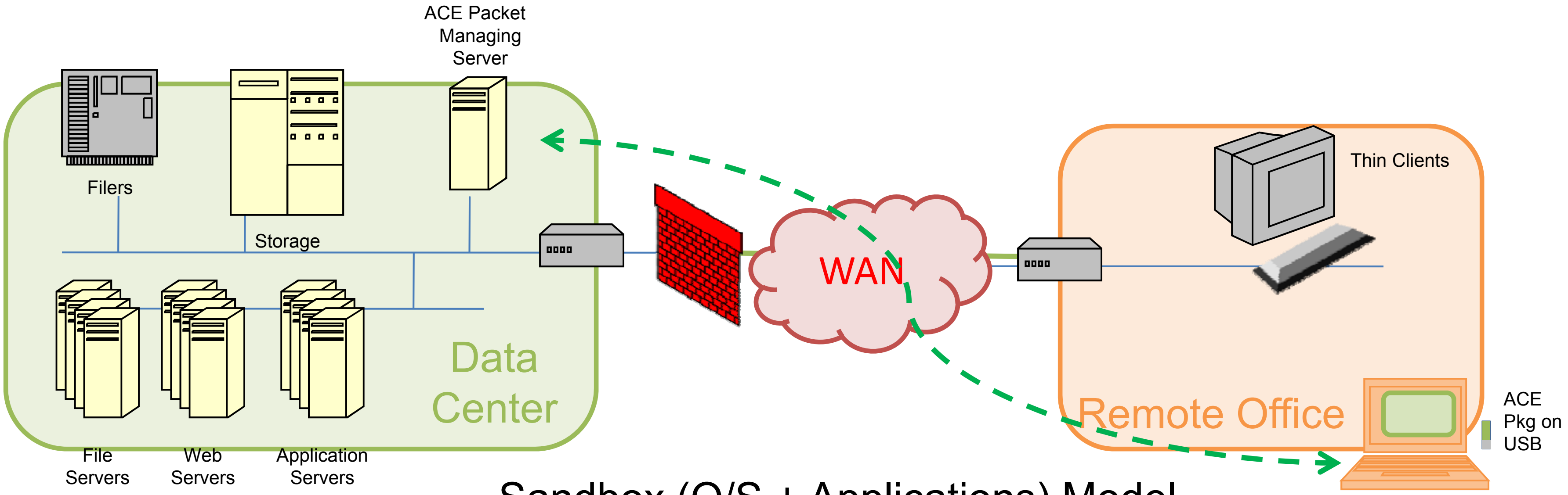
Distributed VG Model

Application Streaming Model



Application Streaming Model

Sandbox Model

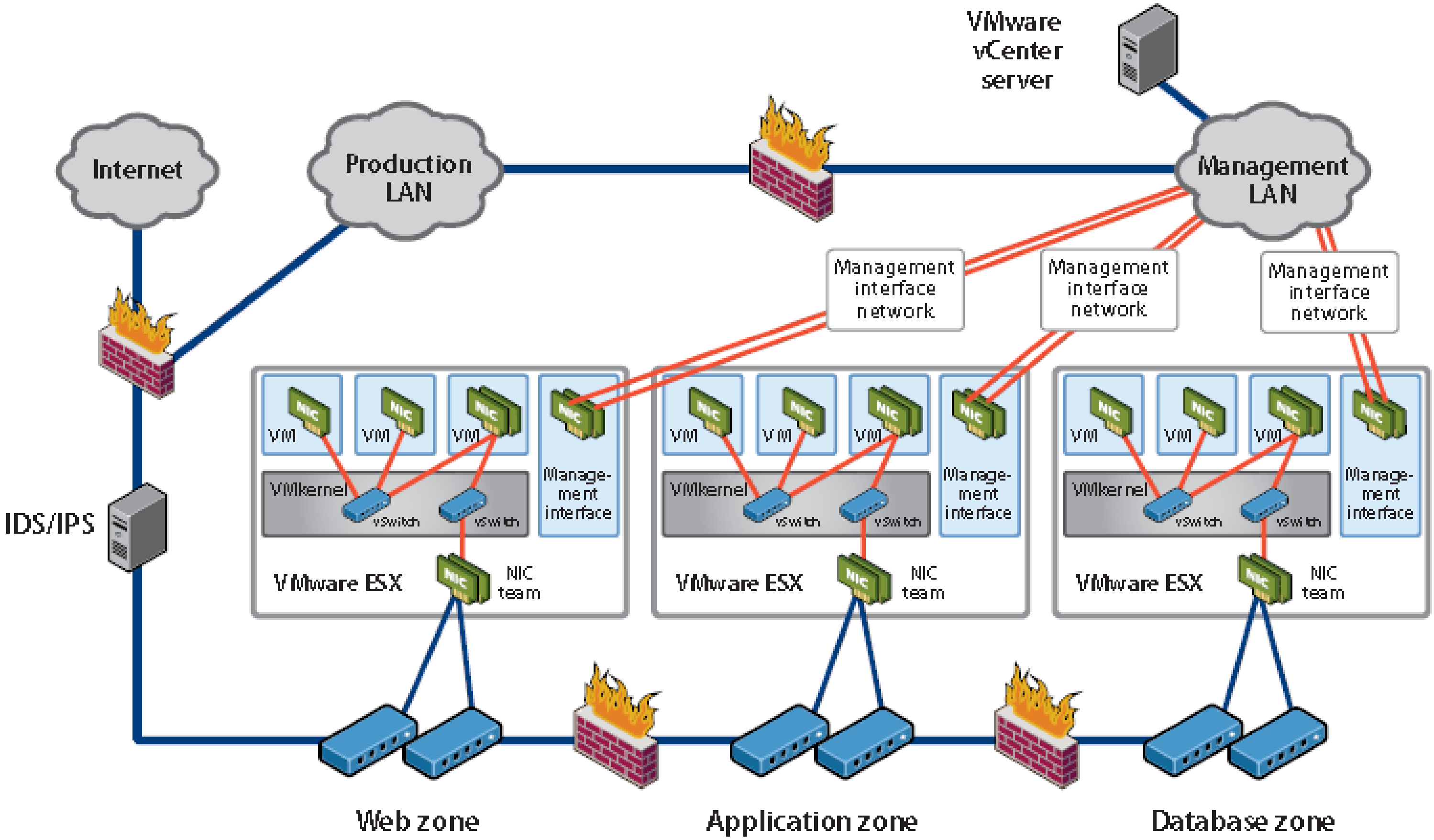


Sandbox (O/S + Applications) Model

Features:

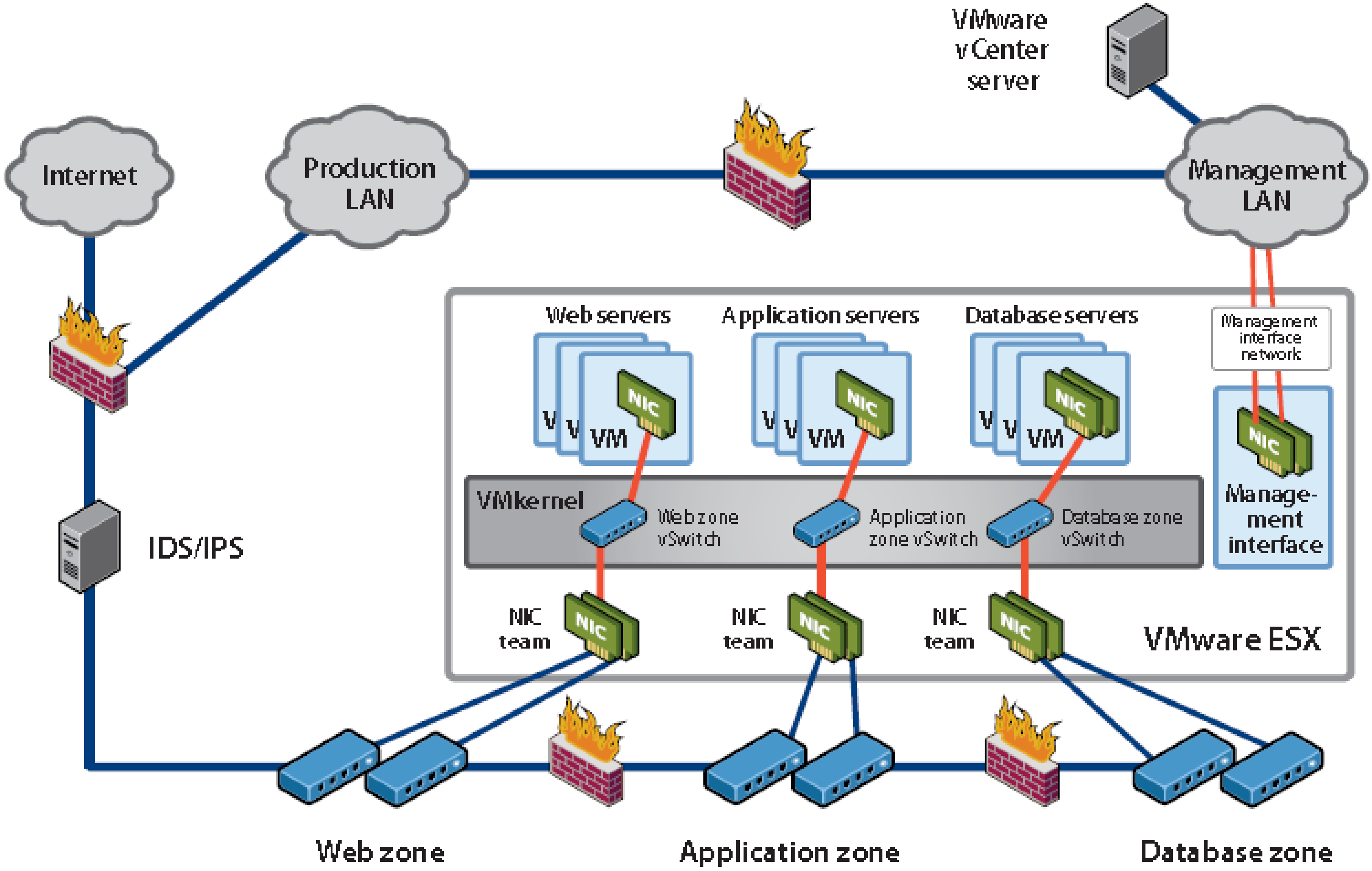
- VRM & Quarantining
  - Up to date OS
  - Up to date A/V
  - Up to date Policies
- Address: Sandbox or PC
- Remote: Backup & Kill
- AES 128 Encryption

The Collapsing Trust Zones (1 of 3)



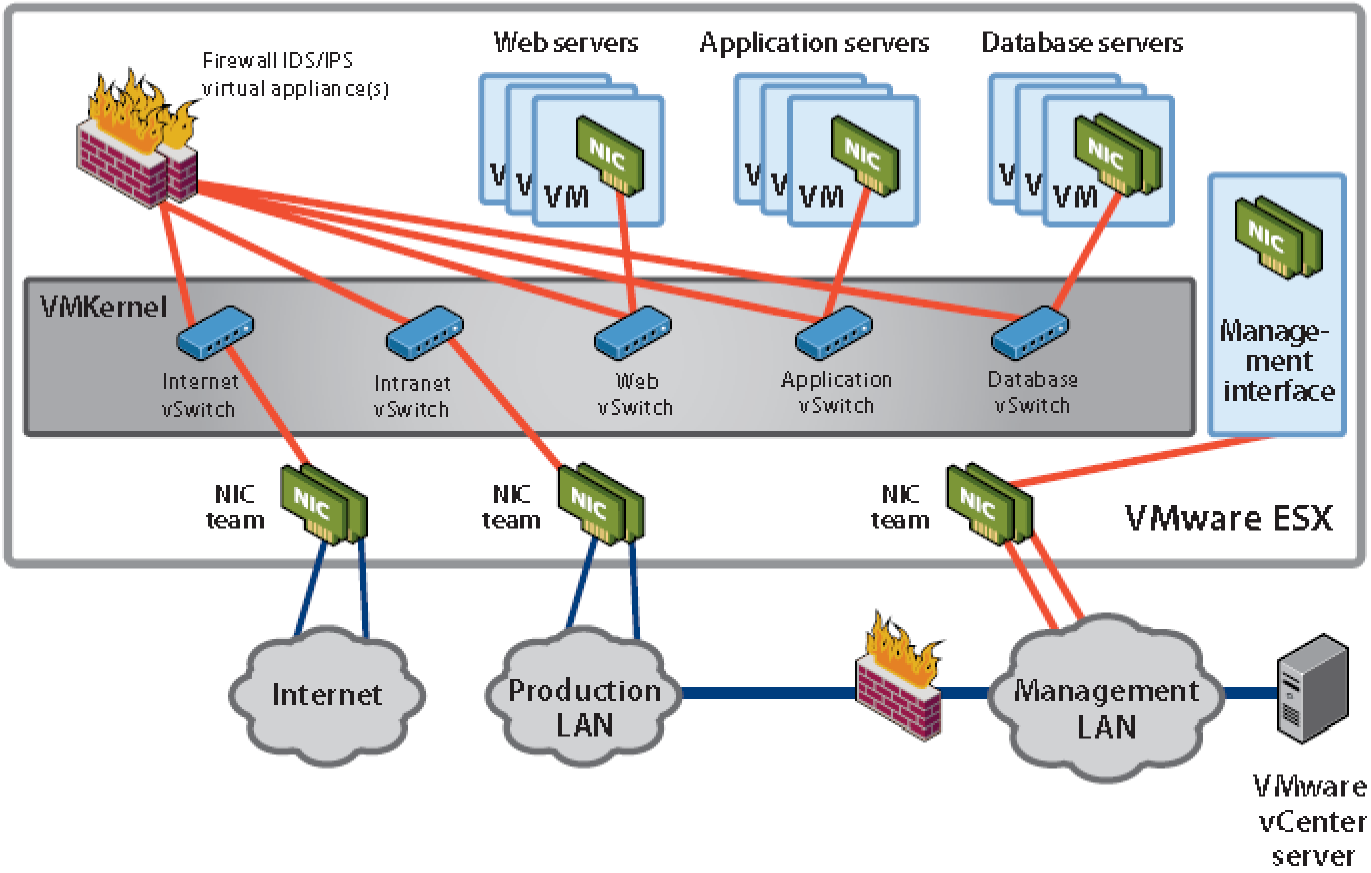
Partially Collapsed with Separate Physical Trust Zones

The Collapsing Trust Zones (2 of 3)



Partially Collapsed with Virtual Separation of Trust Zones

The Collapsing Trust Zones (3 of 3)



Fully Collapsed Trust Zones

Return

Roles & Responsibilities “Buckets"

Policy & Business Requirements	Virtualization Delivery Teams	Security Teams	IT Operations
Definition (Scope of • Demands • Dependencies • Impacts	Own	Contribute	Review
Development	Own	Review	Contribute
Promotion	Request	Test/Approve	Own/Test
Changes	Request	Test/Approve	Own/Test

- 3 Keys to Success:
  - **Workflow based & vetted** (assess, plan, build, configure, certify, provision, populate, monitor, maintain, back-up, troubleshoot); not RACI
  - **Experiment/pilot & frequently assess** (post mortem, scheduled periodic, issue triggered)
  - **Segregation of duties with clear hand-offs or by-consensus**

Return

Security Configuration Standard

- Check out: Center for Internet Security (CIS), NSA, DISA, & each of Specific VM Vendors
  - Context
    - Enterprise Architecture (minimum: In-Scope/Out-of-Scope, and Triggers for Update/Review)
    - Other Applicable Standards & Documents
  - IT Operations Requirements
    - Resources (HD, logical partitions, memory, etc.)
    - Management & Monitoring (backup, consoles, etc.)
  - Security Requirements

(Next Slide)

- Technical-Trust Enablement
  - Services on the host & between hosts/networks or segments (MAC address filtering; Promiscuous mode)
    - Encryption (SSH,SSL for web console, SSL mutual authentication, VPN, etc.)
  - Services in the virtual machine (TCP/IP, SMTP, NTPD, xinetd, etc.)
  - Access Controls & Authentication (accounts , access, & permissions/privileges)
  - Disaster Recovery (FW/VPN & Secure gateways, & how do DR site replication, & keep it up-to-date)
  - Server & Hypervisor Build, Configuration Control, Patching, IT Asset Management, Snapshots & Automatic Migration
  - Configuration Integrity Checking, Logging/Logs
  - Hypervisor/VMM specific (prohibited software packages, core dump file)
- Threat Mitigation
  - Security / Trust Zones (&/or vShield)
  - Vulnerability Scanning, FW, H-IDS, N-IDS/IPS monitoring, Filtering (DoS) & Incident Handling
- Compliance
  - Governance: Authorization (& legal banners),
  - Fusion & Reviews: Timeliness and types of Certification & Validation (e.g., of configuration, patching, changes, vulnerability scan results, accounts, etc.)
  - Life-cycle &/or Roadmap, and log/record retention

Return