Virtualize More While Improving Your Risk Posture: The 4 “Must Haves” of Virtualization Security

- **Hemma Prafullchandra**, CTO & SVP Products, HyTrust
- **Mike Foley,** Sr Technical Manager, Platform Security, VMware
- **Evelyn de Souza,** Sr Data Center Security Strategists, Cisco
- **Steve Orrin,** Chief Security Architect, Intel

Governance, Risk & Compliance – G11

Trust in, and value from, information systems

San Francisco Chapter

CRISC

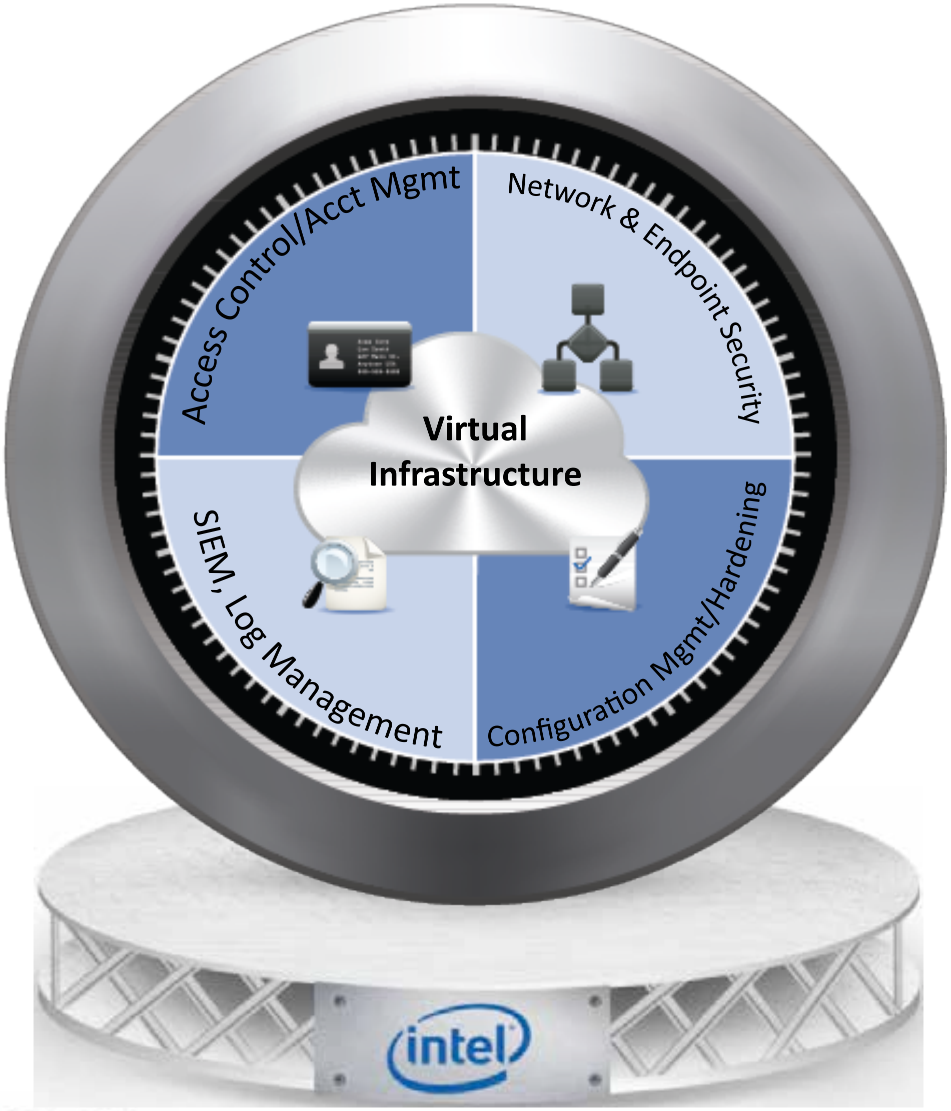
CGEIT

CISM

CISA

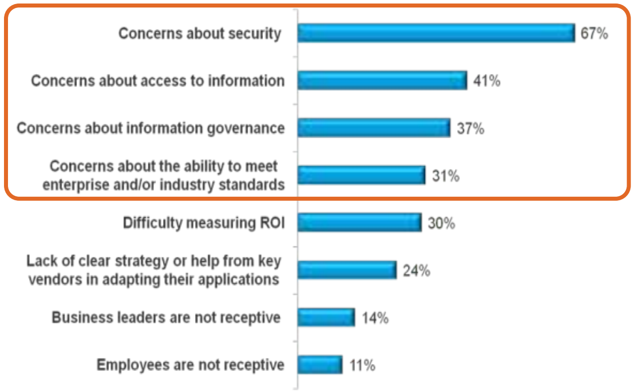
2013 Fall Conference – “Sail to Success”

Agenda



- Security & Compliance Challenges
- The "4 Must Haves" & Solutions
- Key Take-aways
- Resources

Security and Compliance challenges



CIO security concerns for cloud

Top CIO challenges to implementing a cloud computing strategy:

1. Security
2. Access to information
3. Information Governance
4. Ability to meet enterprise standards

Source: 2010 IDG Enterprise Cloud-based Computing Research, November 2010

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

PCI Security Standards Council™

Compliance standards

Virtualization/Cloud

- Increases impact of any compromise
- Creates a more complex environment—additional layers require new controls
- Creates a new attack surface that must be hardened
- Impacts roles and responsibilities

Shionogi & Co:

$3.2B pharmaceutical company laid off IT admin who then:

- Logged in remotely to vSphere from local McDonald's WIFI
- Deleted 88 virtual production servers
- Took down email, order entry, payroll, BlackBerry, & other services
- Caused $800K damage

Access control and management

- **87%** of companies have experienced a data breach

  — IT Compliance Institute

- **<10%** Companies with Controls to Govern Unauthorized Access

  — SANS Critical Security Controls Survey, 2013

- **>50%** Security breaches due to stolen credentials

  — Verizon report, 2013

How Virtualization Security is Impacted by Cloud?

Gartner predicts 17.9% CAGR in cloud services usage through 2016

Shift: Verify then Trust versus Trust then Verify

Where is My Workload? The USG *Example*

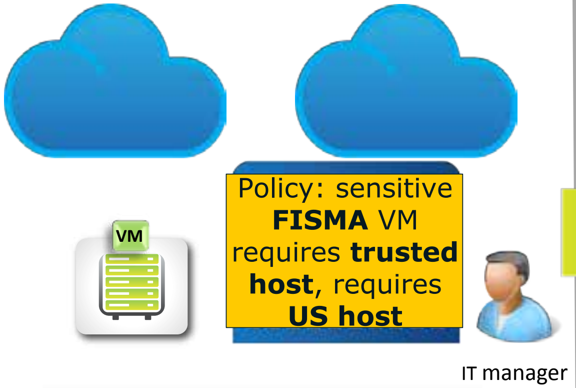
Challenge:

Where workloads run really matters. In many cases you must:

- Assure that the platform has integrity – capable to protect my data
- Make multitenancy safe – keep my workloads separate from others of different profiles
- Allow me to constrain workloads to specific geographical areas
- Provide audit capabilities to meet compliance mandates

NIST IR 7904 solution allows these capabilities for workload control, with critical steps including:

1 Identify Workloads

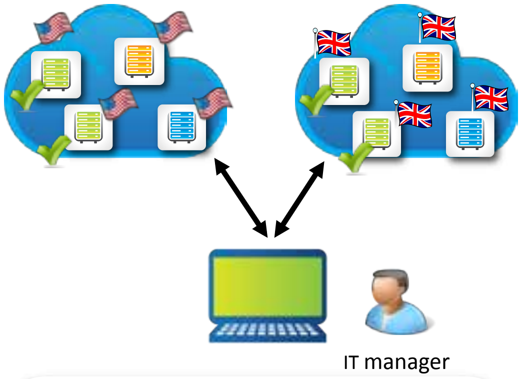


Policy: sensitive **FISMA** VM requires **trusted host**, requires **US host**

Evaluate workloads and data they contain. Use tool to label workloads' security needs, create policy requirements

Example: Label sensitive workloads: Establish policies to control migration or bursting based on required protections and placement/location conditions

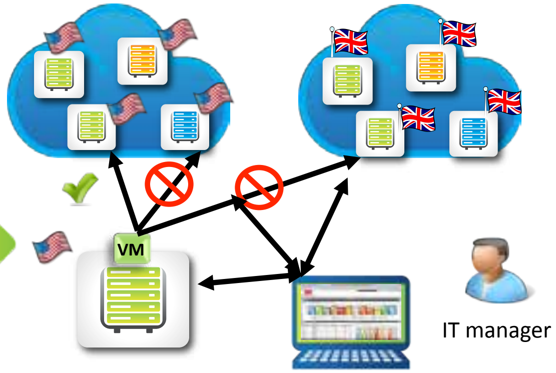
2 Establish Boundaries



Hardware based mechanism to verify platform integrity (trust) status and store/ report other asset descriptor such as location

Example: Attest to know which platforms have proven integrity, which have not. Get assurances regarding where cloud-based systems are physically located. Both provide boundaries for controlling workloads.

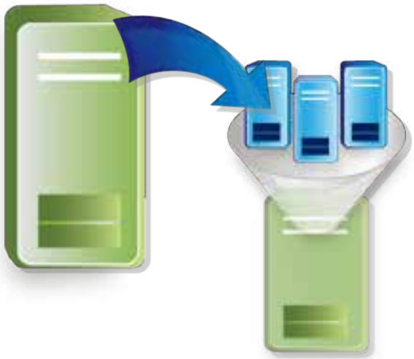
3 Enforce Policies



Security management tools can assure workloads are managed and placed within policy, enable reporting and audit of controls

Example: security and virtualization management platform can verify that platforms capabilities and enforce workload control policies, generating auditable log of events

Virtualization Platform and Security



Abstraction and Consolidation

- ↑ Capital and Operational Cost Savings
- ↓ New infrastructure layer to be secured and subject to compliance
- ↓ Greater impact of attack or misconfiguration

App
OS
ESX Server
Hardware
App
App
App
OS
OS
OS

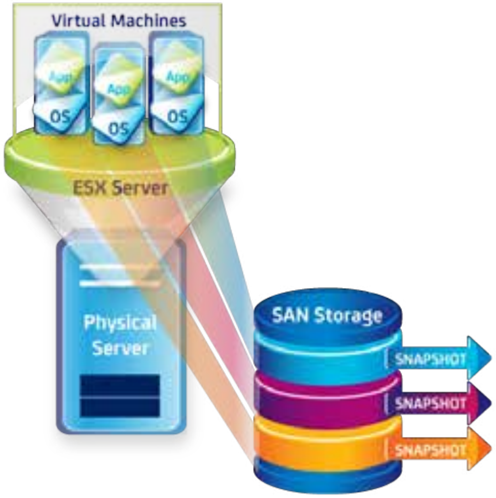
Collapse of Switches and Servers into One Device

- ↑ Flexibility
- ↑ Cost-savings
- ↓ Lack of visibility and control for virtual network and storage
- ↓ No separation of church and state (network, security, storage administration)

Faster Deployment in Shared Environment

- ↑ IT responsiveness
- ↓ Inconsistencies in configuration
- ↓ Physical change processes ineffective
- ↓ Inadequate tenant segmentation

Virtualization Containers and Security



Fuzzy Time Boundaries

- ↑ Great availability / recovery mechanism
- ↓ Security and audit events can be lost if not configured
- ↓ Changes in time are not visible from inside the virtual server

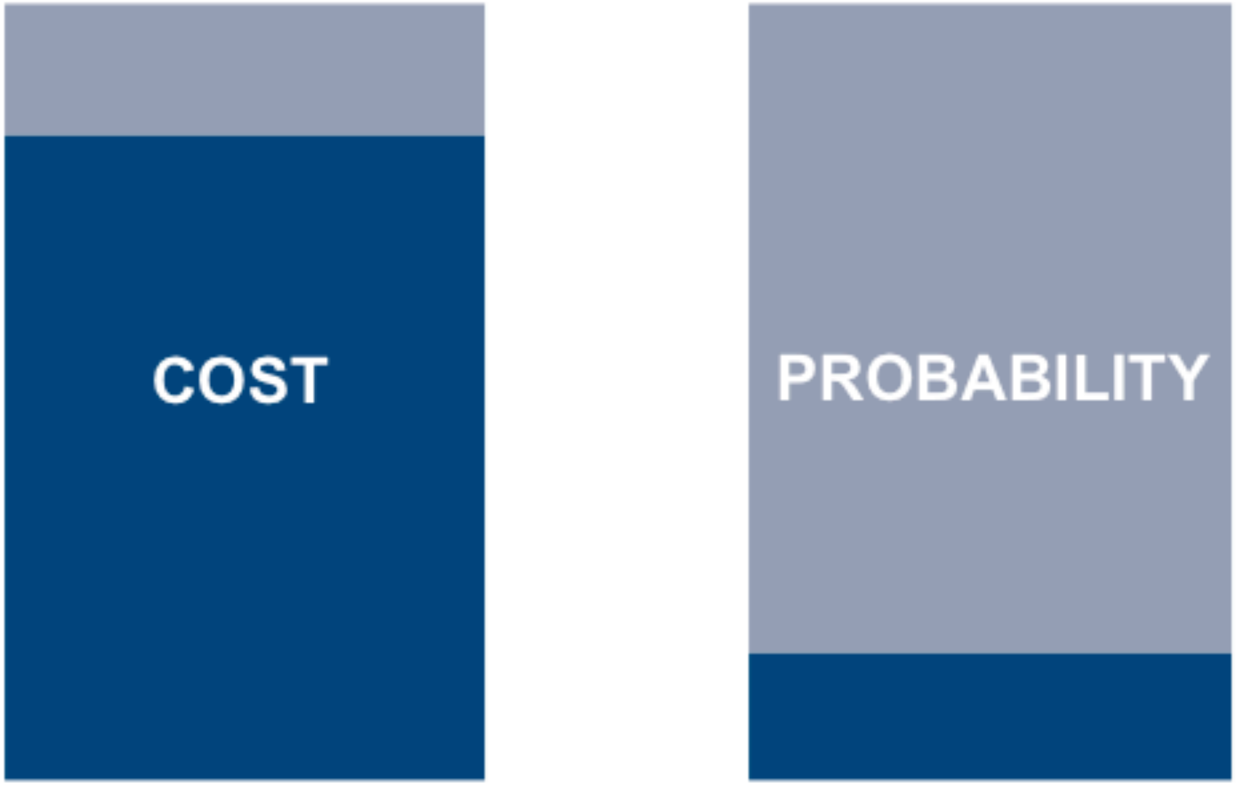
VM Mobility

- ↑ Improved Service Levels
- ↓ Identity divorced from physical location
- ↓ Policies may not follow virtual machine

VM Encapsulation

- ↑ Ease DR
- ↑ Hardware Independence
- ↓ Outdated offline systems
- ↓ Unauthorized copy
- ↓ Reconfiguring virtual hardware and console access are over in network operations

The Real Risks of Virtualization



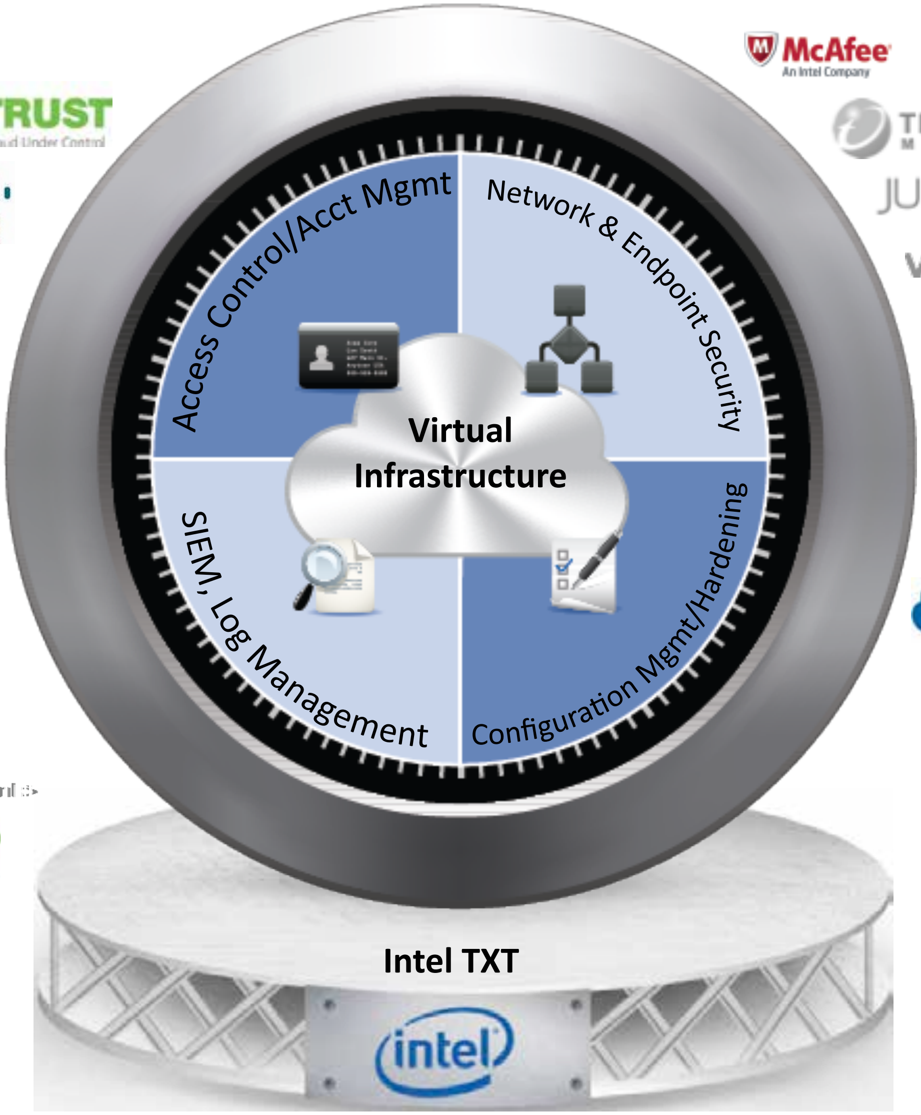
VM/VM or Hypervisor Breakout

Compromised Admin Account

4 "Must Haves" - Solutions

HYTRUST Cloud Under Control
CISCO
vmware

McAfee An Intel Company
catbird
TREND MICRO
paloalto NETWORKS
JUNIPER NETWORKS
CISCO
vmware


Access Control/Acct Mgmt

Network & Endpoint Security

Virtual Infrastructure

SIEM, Log Management

Configuration Mgmt/Hardening

Intel TXT

McAfee An Intel Company
ArcSight
RSA SECURITY
splunk
HYTRUST Cloud Under Control

vmware
HYTRUST Cloud Under Control

CObIT Objectives

PO2: Define the Information Architecture
PO4: Define the IT Processes, Organization and Relationships
PO9: Assess and Manage IT Risks
AI2: Acquire and Maintain Application Software
AI3: Acquire and Maintain Technology Infrastructure
AI4: Enable Operation and Use
DS5: Ensure Systems Security
DS9: Manage Service Desk and Incidents

Ubiquitous Security Value from Intel Xeon-based Data Center Systems

Trusted Platforms

- Minimize vulnerabilities in Hardware and Software
- Robust malware prevention and detection
- Enhanced recovery

Data Protection

- Flexible, high-performance encryption (storage, network)
- Platform trust at all layers of the stack, and through time

Cloud Security

- Enable security appliances in the virtual environment
- Deliver trusted mechanisms to expose platform security posture

Many already have a large estate of these systems!

Ubiquity & granularity to address changing scope and threats

Cisco: End user and Network

Focus on what matters most!

Business Policy

Destination ▶ ▼ Source	HR Database	Prod CRM	Storage
VD HR Users	✓	✗	✗
VPN HR User	✗	✗	✗
IT Ops	✓	✓	✓
Test Server	Test-ACL	✗	✓

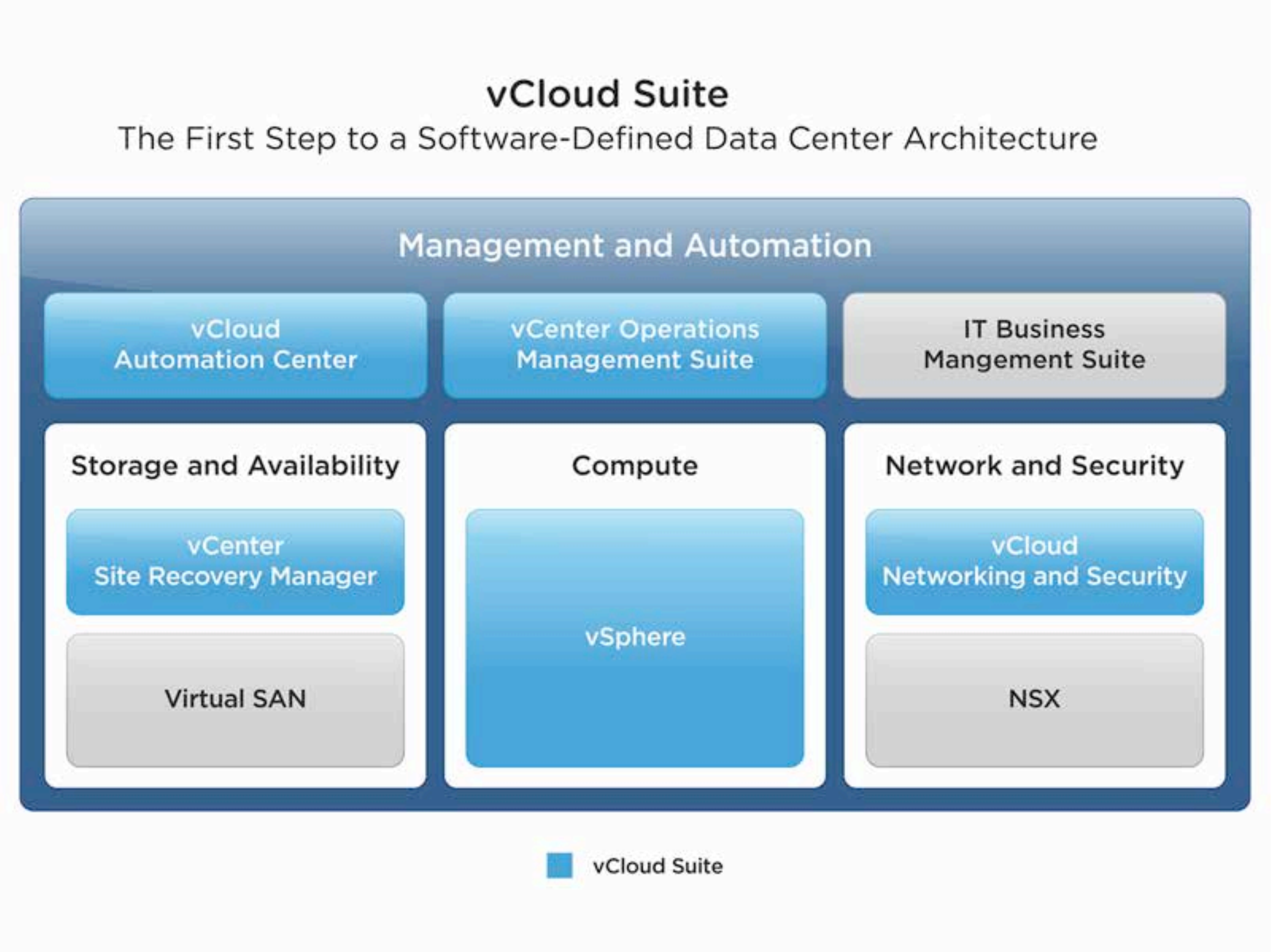
Dynamic Context

User and Devices

Resources and Demands

APP
in
g+
skype
box

VMWare Solutions



vCloud Suite

The First Step to a Software-Defined Data Center Architecture

Management and Automation

vCloud Automation Center

vCenter Operations Management Suite

IT Business Mangement Suite

Storage and Availability

vCenter Site Recovery Manager

Virtual SAN

Compute

vSphere

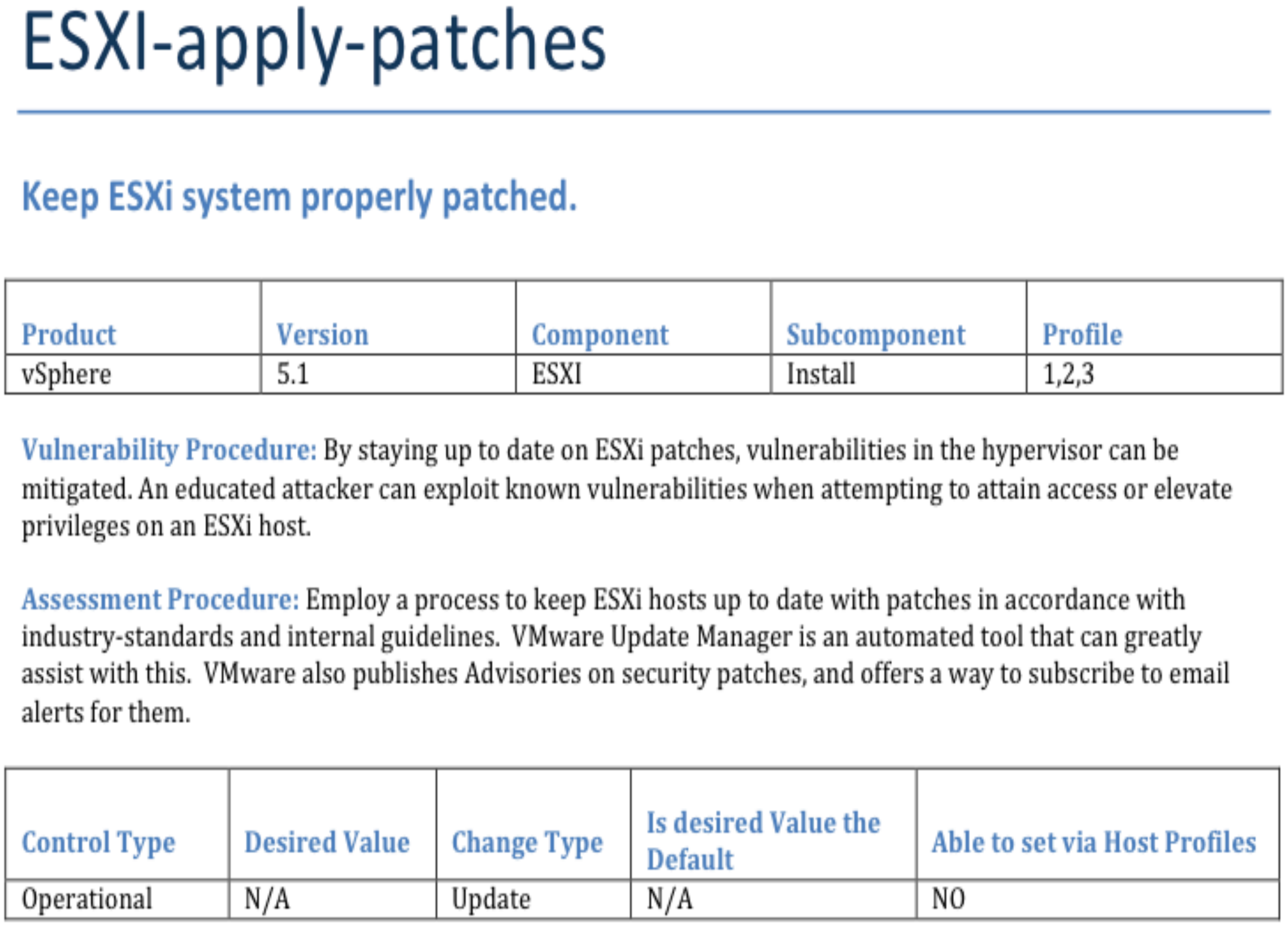
Network and Security

vCloud Networking and Security

NSX

🟦 vCloud Suite

vSphere 5.x Hardening Guide



ESXI-apply-patches

Keep ESXi system properly patched.

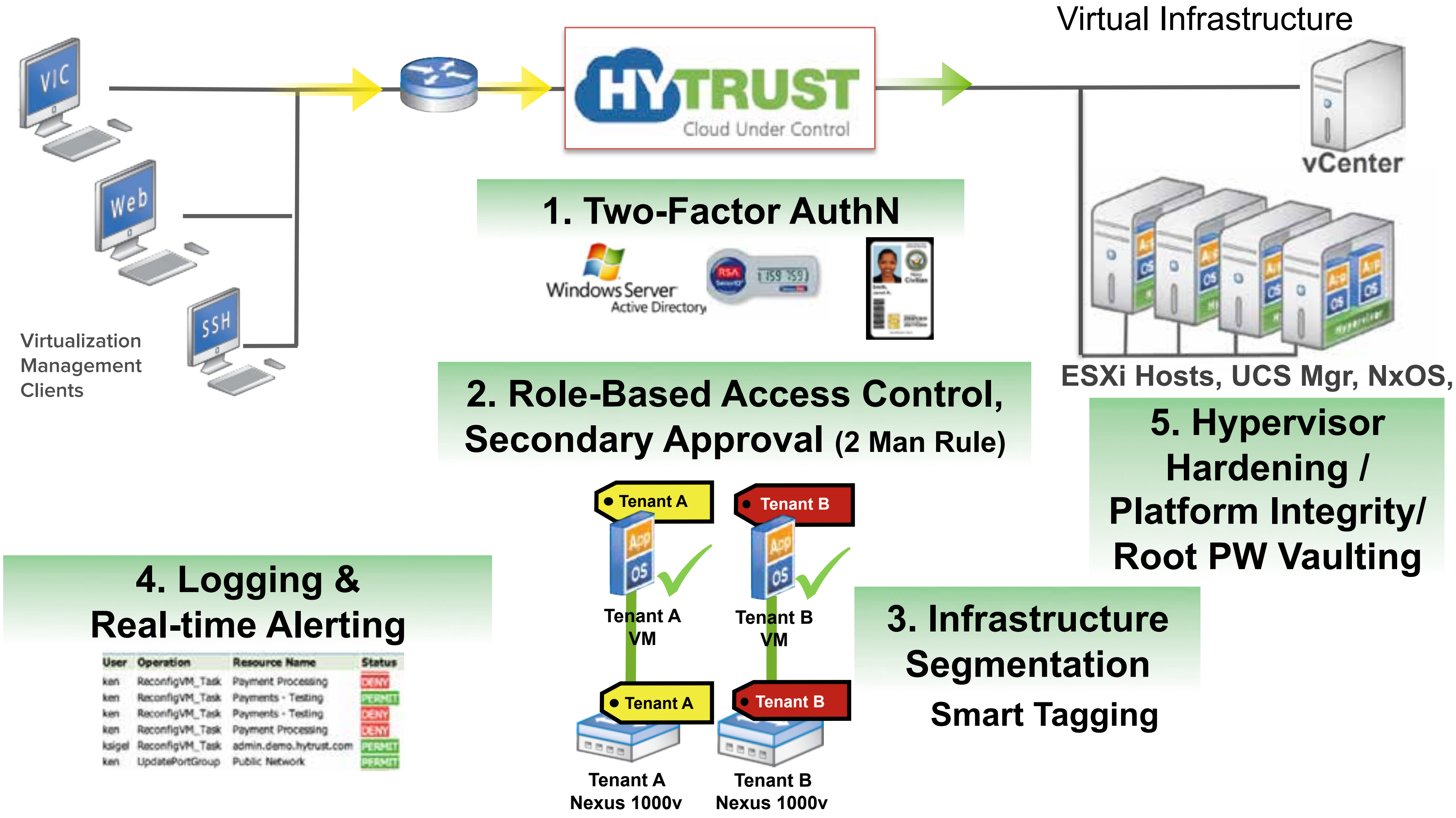
Product	Version	Component	Subcomponent	Profile
vSphere	5.1	ESXI	Install	1,2,3

Vulnerability Procedure: By staying up to date on ESXi patches, vulnerabilities in the hypervisor can be mitigated. An educated attacker can exploit known vulnerabilities when attempting to attain access or elevate privileges on an ESXi host.

Assessment Procedure: Employ a process to keep ESXi hosts up to date with patches in accordance with industry-standards and internal guidelines. VMware Update Manager is an automated tool that can greatly assist with this. VMware also publishes Advisories on security patches, and offers a way to subscribe to email alerts for them.

Control Type	Desired Value	Change Type	Is desired Value the Default	Able to set via Host Profiles
Operational	N/A	Update	N/A	NO

HyTrust Appliance Capabilities



1. Two-Factor AuthN

2. Role-Based Access Control, Secondary Approval (2 Man Rule)

3. Infrastructure Segmentation

Smart Tagging

4. Logging & Real-time Alerting

User	Operation	Resource Name	Status
ken	ReconfigVM_Task	Payment Processing	DENY
ken	ReconfigVM_Task	Payments - Testing	PERMIT
ken	ReconfigVM_Task	Payments - Testing	DENY
ken	ReconfigVM_Task	Payment Processing	DENY
ksigel	ReconfigVM_Task	admin.demo.hytrust.com	PERMIT
ken	UpdatePortGroup	Public Network	PERMIT

5. Hypervisor Hardening / Platform Integrity/ Root PW Vaulting

Key Takeaways

- Understand security and compliance implications of virtualizing your Data Center or moving to the cloud
- Review and update existing processes and technologies
  - An ecosystem of technologies will be required to address even the minimum MUST HAVES
  - Look to vendors that are working together and have developed technologies that are virtualization-aware
- Verify, then Trust, then Verify Again
  - Validate that controls are configured correctly and generating the necessary 'evidence' (logs, reports, …)
  - Continuously validate the ability to reproduce/trouble-shoot if an incident does occur

Resources

- ISACA Virtualization Checklist - http://www.isaca.org/Knowledge-Center/Research/Documents/Virtualization-Security-Checklist-26Oct2010-Research.pdf
- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Virtualization-Benefits-and-Challenges.aspx
- NIST: 800-53, 7904, 144, 145, 146
- HyTrust: http://www.hytrust.com/resources/main
- Cisco: *www.**cisco**.com/en/US/netsol/ns340/ns394/ns224/ns376/index.html*
- VMWare: https://www.vmware.com/solutions/datacenter/cloud-security-compliance/protect-critical-applications.html
- Intel: http://www.intel.com/content/www/us/en/enterprise-security/multi-level-enterprise-security.html