Castles in the Sky: Enabling Trust and Compliance in the Cloud

Hemma Prafullchandra, CTO & Executive VP, **HyTrust**
Evelyn de Souza, Data Privacy & Compliance Leader, **Cisco**
Pierre Fourie, Senior Manager, Advisory, **Ernst & Young**
Steve Orrin, Federal Chief Technologist, **Intel**

Governance, Risk & Compliance – G12

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

SF ISACA FALL CONFERENCE   NOVEMBER 9-11, 2015   HOTEL NIKKO-SAN FRANCISCO

Agenda

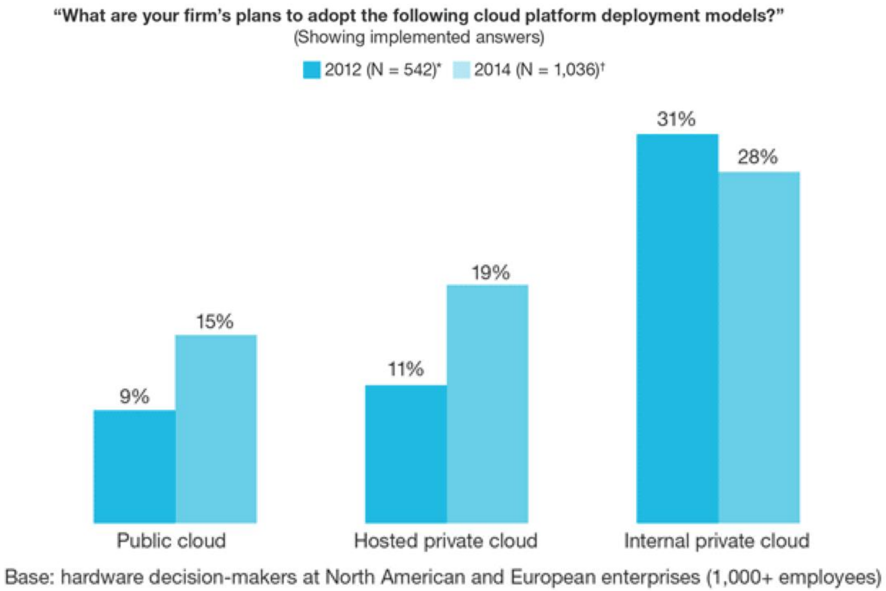
- Overview, Trends, Challenges
- Best practices, guidance & reference architectures
- Concrete example
- Closing remarks

Castles in the Sky Syndrome

Cloud Adoption Increases

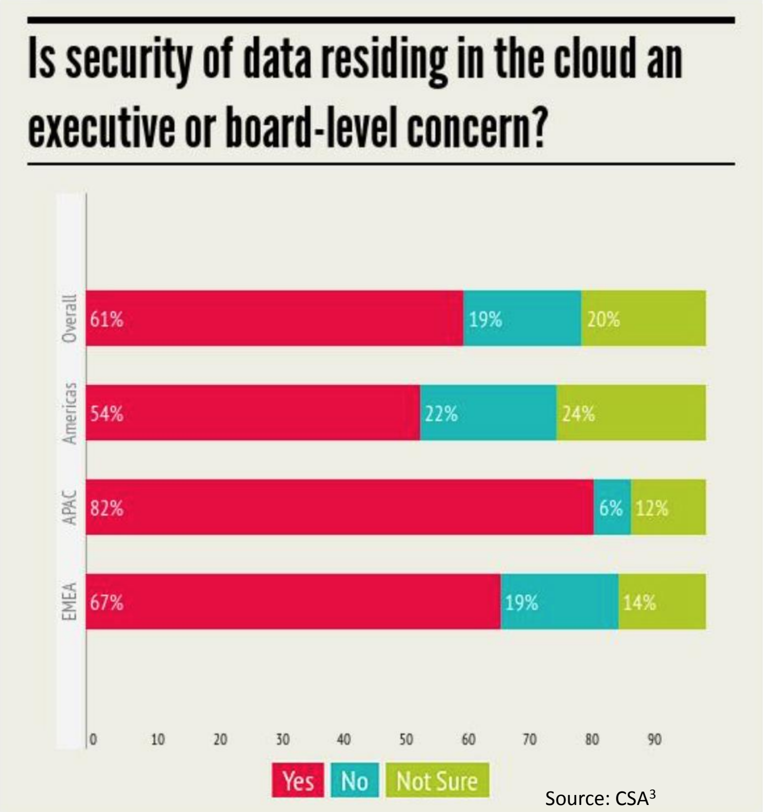
So Does the Concern

73% of CIOs will allocate budget in 2015 to private, public, or hybrid clouds[1]



Source: Forrester[4]

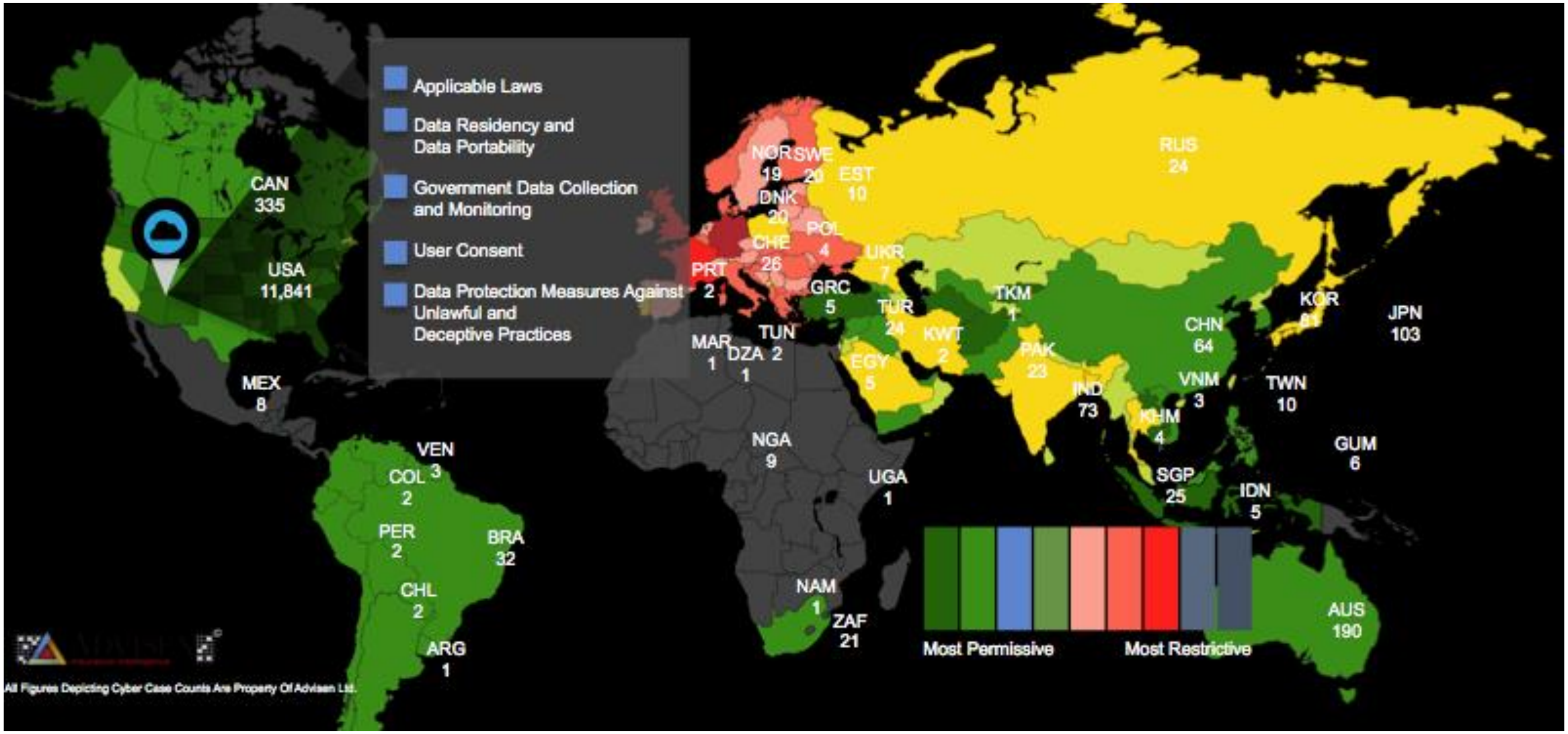
35% of companies say **security keeps them from full adoption** of public clouds[2]



Source: CSA[3]

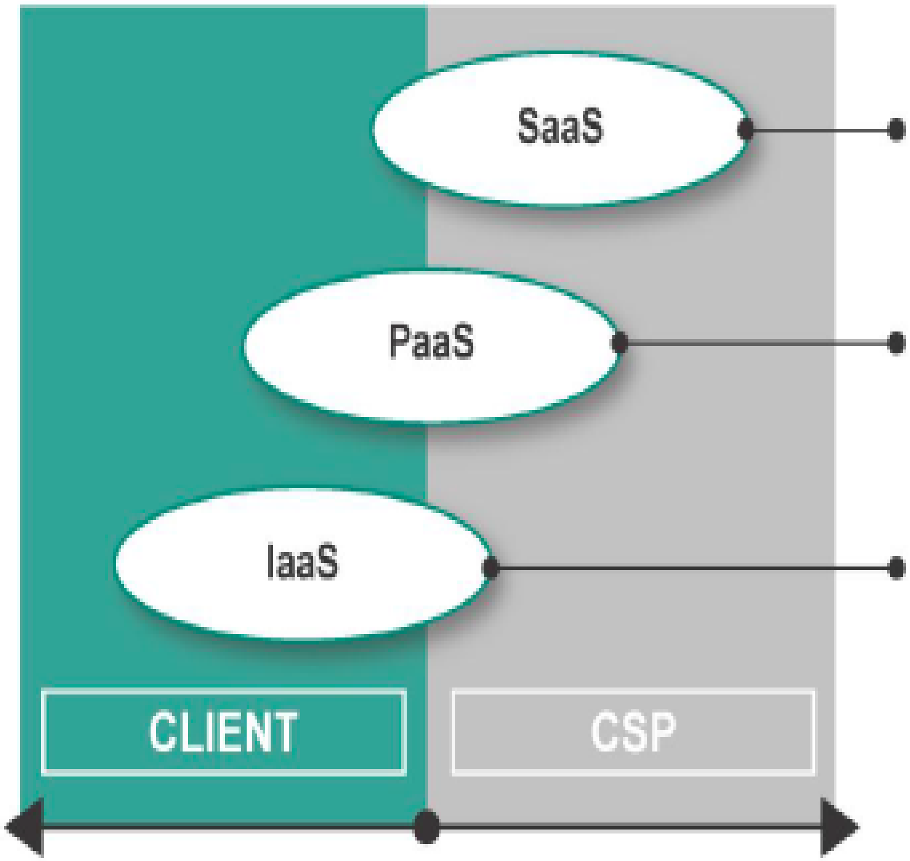
[1] Piper Jaffray CIO survey (1/15)
[2] RightScale Cloud Report (1/15)
[3] CSA Adoption Survey (1/15)
[4] Forrester (1/15) – Adoption of 2012 vs 2014

Why Data Protection is an Imperative



Shared Responsibilities…
…liability still with the Cloud Service Provider Customer

Figure 1: Level of control/responsibility for client and CSP across different service models



Saas
The client may have limited control of user-specific application configuration settings.

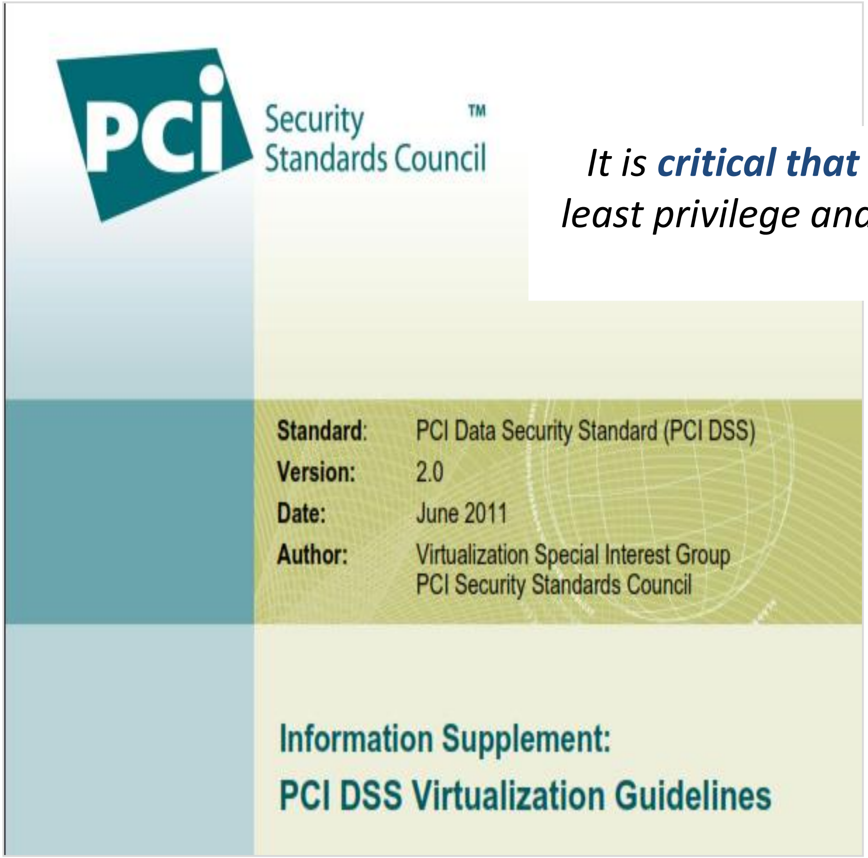
PaaS
The client has control over the deployed applications and possibly configuration settings for the application-hosting environment.

IaaS
The client has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Level of control/responsibility for client and CSP across different service models

Source: PCI DSS Cloud Computing Guidelines

PCI SSC Guidance on Virtualization and Cloud Computing

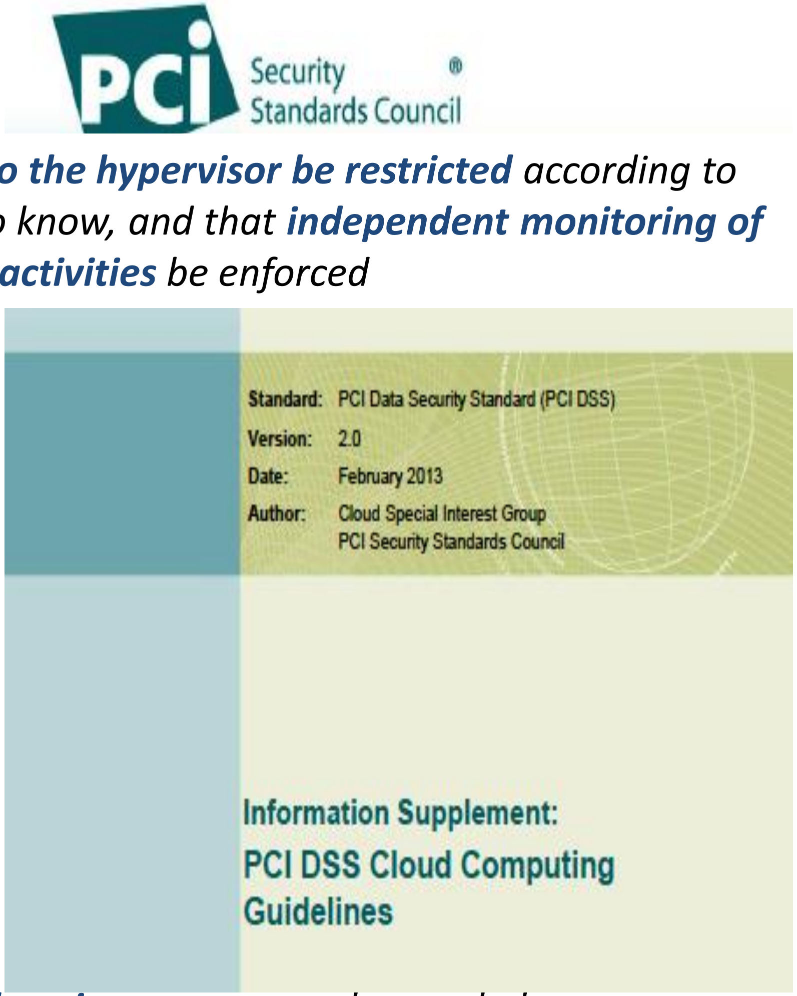


PCI Security Standards Council™

Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: June 2011
Author: Virtualization Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS Virtualization Guidelines

*It is **critical that access to the hypervisor be restricted** according to least privilege and need to know, and that **independent monitoring of all activities** be enforced*



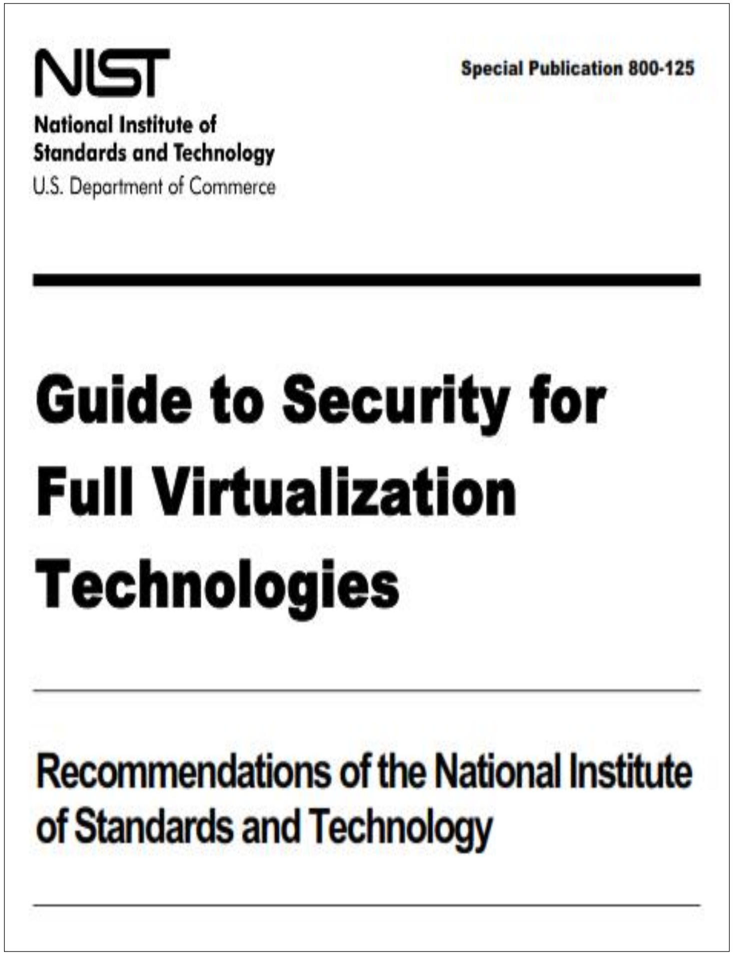
PCI Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: February 2013
Author: Cloud Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS Cloud Computing Guidelines

***Specialized tools for monitoring and logging virtual environments** may be needed to capture the level of detail required from the multiple components*

NIST Guidance on Virtualization (SP 800-125)



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

Special Publication 800-125

Guide to Security for Full Virtualization Technologies

Recommendations of the National Institute of Standards and Technology

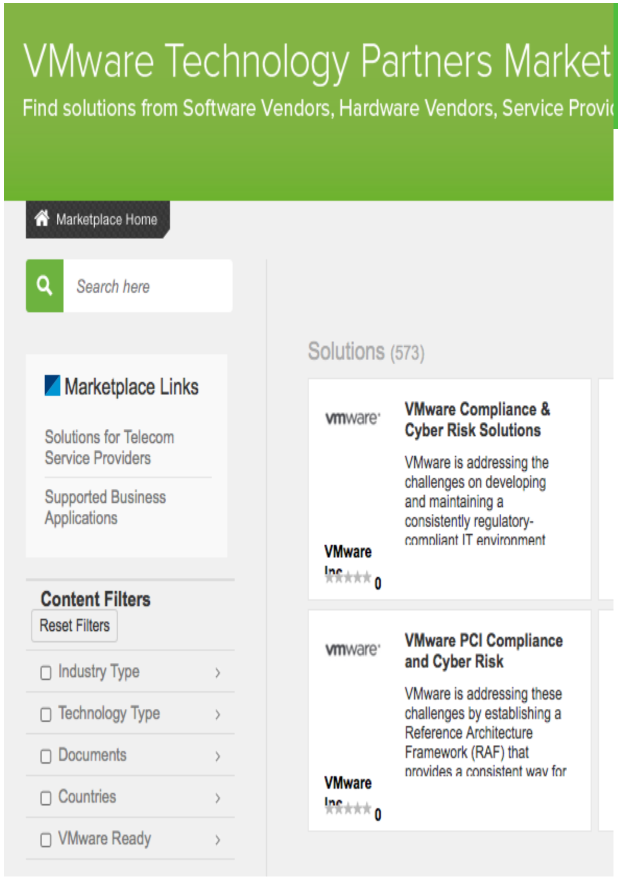
*Organizations should have the **same security controls in place for virtualized operating systems as they have for the same operating systems running directly on hardware**.*

***Ensure that the hypervisor is properly secured**.*

Restrict and protect administrator access to the virtualization solution.

The security of the entire virtual infrastructure relies on the security of the virtualization management system that controls the hypervisor and allows the operator to start guest OSs, create new guest OS images, and perform other administrative actions.

Reference Architectures



VMware Technology Partners Market

Find solutions from Software Vendors, Hardware Vendors, Service Provic

Solutions (573)

Marketplace Links

Solutions for Telecom Service Providers

Supported Business Applications

Content Filters

Reset Filters

□ Industry Type ›

□ Technology Type ›

□ Documents ›

□ Countries ›

□ VMware Ready ›

VMware Compliance & Cyber Risk Solutions

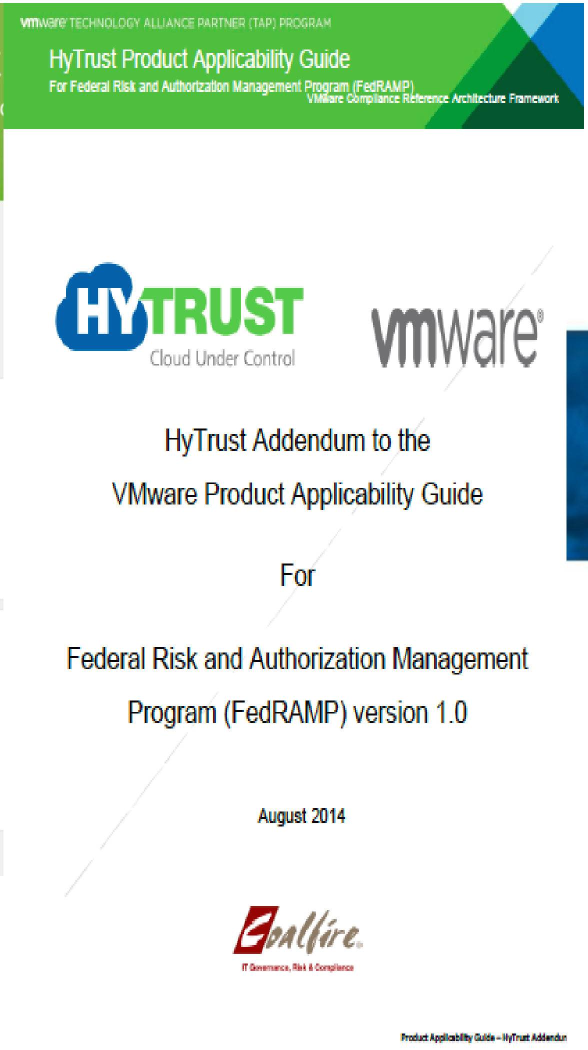
VMware is addressing the challenges on developing and maintaining a consistently regulatory-compliant IT environment

VMware Inc. 0

VMware PCI Compliance and Cyber Risk

VMware is addressing these challenges by establishing a Reference Architecture Framework (RAF) that provides a consistent way for

VMware Inc. 0



vmware TECHNOLOGY ALLIANCE PARTNER (TAP) PROGRAM

HyTrust Product Applicability Guide

For Federal Risk and Authorization Management Program (FedRAMP)

VMware Compliance Reference Architecture Framework

HYTRUST Cloud Under Control

vmware

HyTrust Addendum to the

VMware Product Applicability Guide

For

Federal Risk and Authorization Management Program (FedRAMP) version 1.0

August 2014

Coalfire

IT Governance, Risk & Compliance

Product Applicability Guide – HyTrust Addendum

CASE STUDY

HYTRUST Cloud Under Control

McKesson Builds Secure, Compliant Private Cloud with HyTrust

MCKESSON

Industry

Healthcare/Pharmaceutical

Snapshot

- HyTrust CloudControl™ helps enable secure administrative multi-tenancy for McKesson's private cloud initiative
- With HyTrust, McKesson simplified compliance with regulations like HIPAA and SOX for its virtualized infrastructure
- McKesson has improved visibility and control of its private cloud with strong separation of duties, granular logging and auditing of administrative actions, and hypervisor configuration hardening

About McKesson

McKesson, one of the nations largest pharmaceutical companies and is listed number 14 on the 2014 Fortune 500. Founded in 1933, McKesson supports $122B in revenue and has 43,500 employees worldwide.

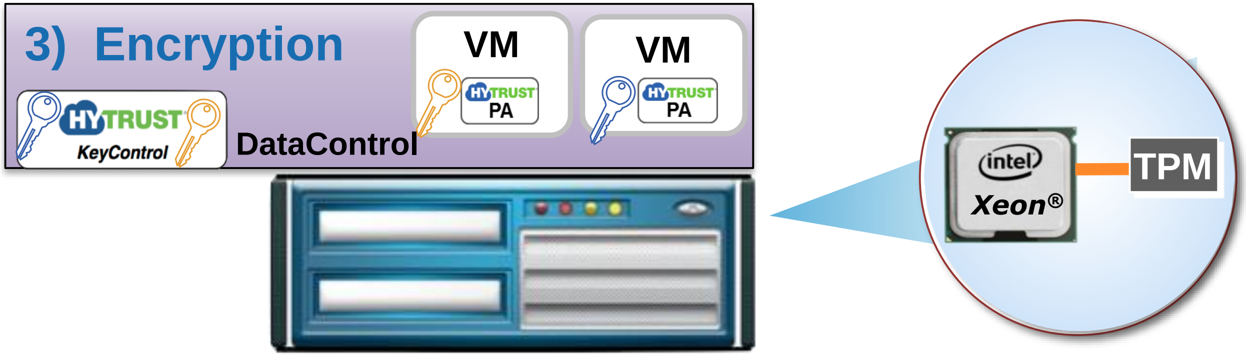
Building Trust and Compliance in the Cloud:

The big questions

When using a cloud, the tenant is not in control of their physical infrastructure. How do they:

- Verify provisioning of the infrastructure?
- Trust where servers are located?
- Control where VMs are distributed?
- Support data sovereignty requirements?
- Implement granular controls?
- Audit policy configuration of their cloud?
- Prove compliance to industry bodies & national regulations

Tech Innovations that can help…



3) Encryption

DataControl

Virtualization Host (ESXi & KVM)

Hardware Root-of-Trust

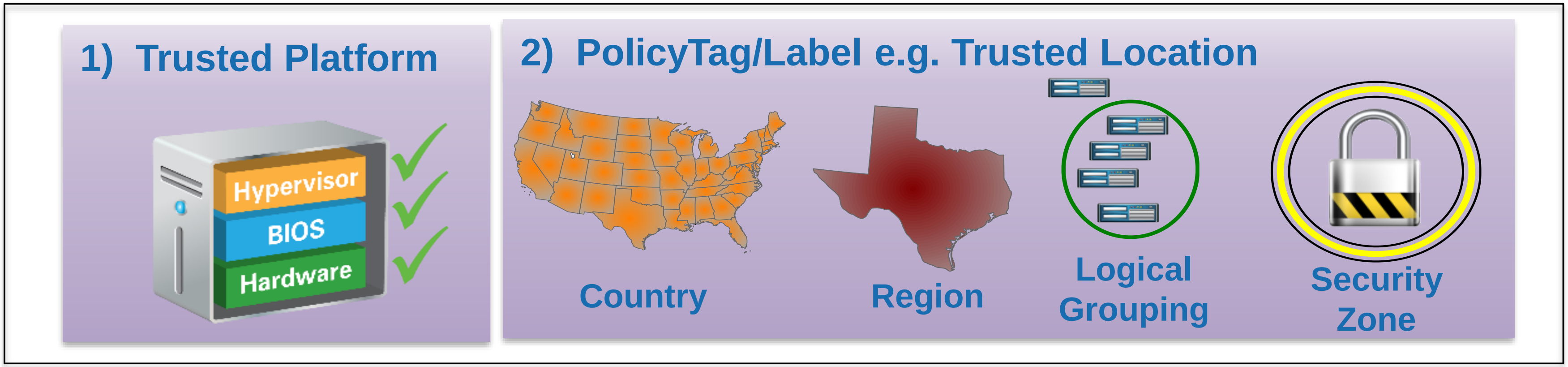
Intel® TXT

(Trusted Execution Technology)

and TPM

(Trusted Platform Module)

CloudControl



1) Trusted Platform

2) PolicyTag/Label e.g. Trusted Location

Country

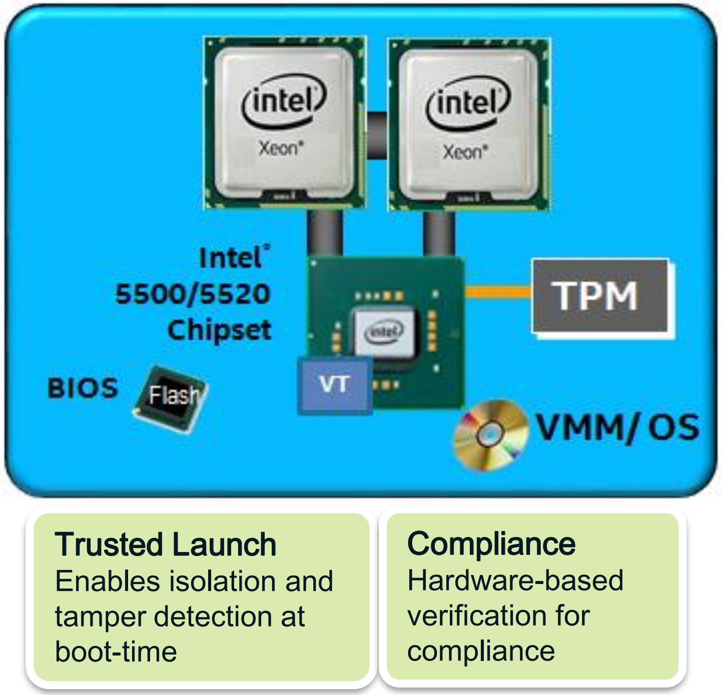
Region

Logical Grouping

Security Zone

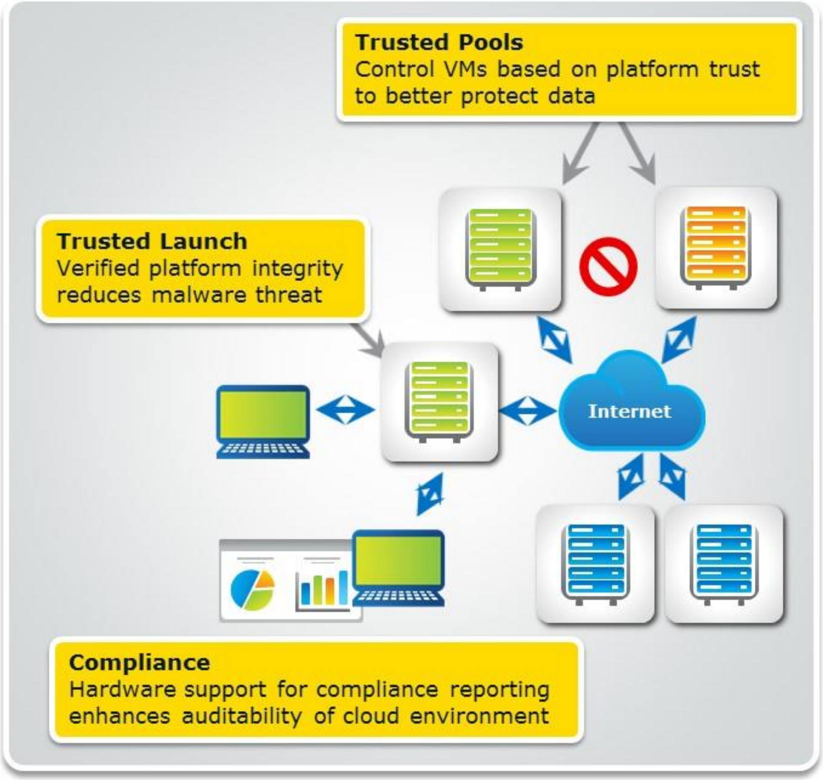
Trusted Execution Technology & Trusted Compute Pools

Trusted Execution Technology



Trusted Launch Enables isolation and tamper detection at boot-time

Compliance Hardware-based verification for compliance



Trusted Pools Control VMs based on platform trust to better protect data

Trusted Launch Verified platform integrity reduces malware threat

Compliance Hardware support for compliance reporting enhances auditability of cloud environment

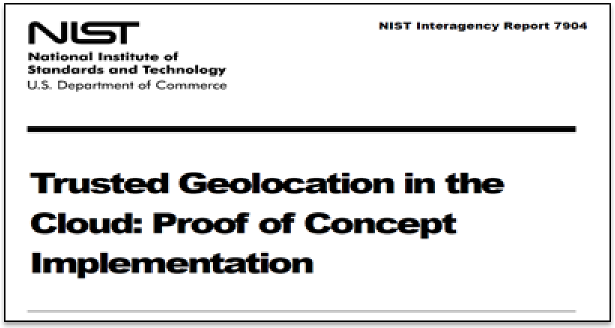
Addresses critical needs in virtualized & cloud use models

- Provides control to ensure only trustable hypervisor is run on platform
- Protecting server prior to virtualization software boot
- Launch-time protections that complement run-time malware protections
- Compliance Support

Control VMs based on platform trust

- Pools of platforms with trusted hypervisor
- VM Migration controlled across resource pools
- Similar to clearing airport checkpoint and then moving freely between gates

Attested Server Tagging & Trusted Geo-location in the Cloud



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

NIST Interagency Report 7904

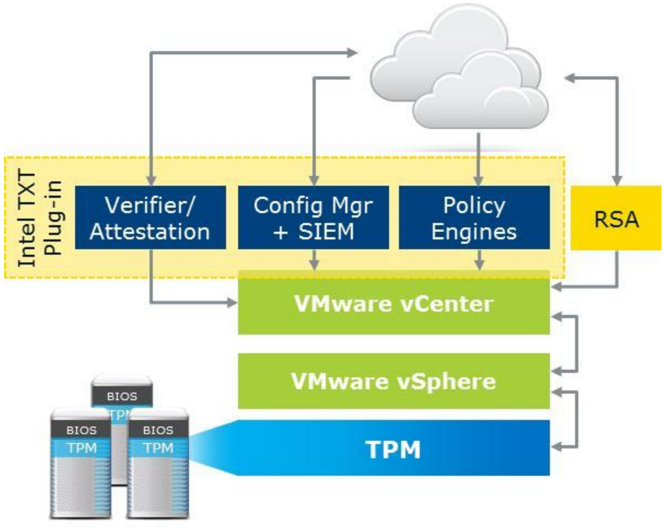
Trusted Geolocation in the Cloud: Proof of Concept Implementation

- Many Trusted Compute Pools Early Adopters also require:
  - GEO Tagging and/or Asset Tagging for workload segregation
- Regulatory Compliance Requirements:
  - EU Data Protection Directives (95/46/EC)
  - FISMA (geo-tag)
  - Payment Card Industry (PCI-DSS) (asset tag)
  - HIPPA (Asset Tag)

- NIST IR 7904 –USG recommendation for "Trusted Geolocation in the Cloud"

- Trusted resource pool based on hardware-based secure technical measurement capability
  - **Platform attestation and safer hypervisor launch** - Provide integrity measurement and enforcement for the compute nodes
  - **Trust-based secure migration** - Provide geolocation measurement and enforcement for the compute nodes

A PoC of the NIST IR 7904 solution is at the NIST National Cyber Center of Excellence (NCCOE) in Rockville, MD



Intel® Xeon® Processor-based Server with Intel® Trusted Execution Technology (Intel® TXT)

Standards, Best Practices, Training, …

- ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757

- ISO/IEC 27018:2014 – Code of practice for protection of (PII) across public cloud

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

- CSA Cloud Controls Matrix – for harmonizing cloud security across different cloud models

https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_downloads

- FedRAMP – government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

https://www.fedramp.gov/

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
  - http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Security-Considerations-for-Cloud-Computing.aspx
- CSA/Safecode: https://downloads.cloudsecurityalliance.org/initiatives/collaborate/safecode/SAFECode-CSA-Cloud-White-Paper.pdf
- NIST: http://csrc.nist.gov/publications/drafts/ir7904/nistir_7904_second_draft.pdf
- HyTrust: http://www.hytrust.com
- Cisco: *www.**cisco**.com/en/US/netsol/ns340/ns394/ns224/ns376/index.html*
- Ernst & Young:

- Intel: http://www.intel.com/txt

THANK YOU!