



Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.
Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org



Trusted Hybrid Cloud–NIST’s Trusted Cloud Building Block & Ref Architecture

Raghu Yeluri, Intel Corporation
Michael Bartock, NIST
Harmeet Singh, IBM
Anthony Dukes, VMware
Hemma Prafullchandra, HyTrust

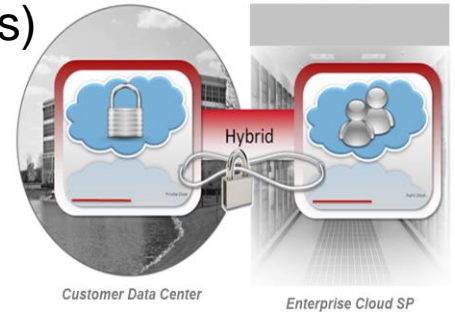


Agenda

- **Trusted Hybrid Clouds - Partnership Overview**
- **NIST 1800 Trusted Cloud Building Block* Overview**
 - Security Objectives
 - Technical Architecture
 - NIST CSF and SP 800-53 Controls* alignment for Hybrid Clouds
- Partner Summaries
 - IBM Cloud*: Physical, Technical and Operational capabilities
 - VMWare*: VVD Ref Architecture & Compliance Management
 - HyTrust*: Policy Enforcement
- Trusted Cloud Implementation Demo & Status
- Next Steps & Summary
- Q & A

Trusted Hybrid Clouds - Partnership Overview

- Collaboration between NIST* & industry partners
 - Intel, IBM* VMware*, Dell-EMC*, HyTrust*, RSA* & Gemalto*
- **Goal:** Design, engineer, and publish reference architecture(s) using COTS components & Services for Trusted Hybrid Clouds
 - Document targeted use-cases.
 - Build on NIST IR 7904 - Hardware RoT + Geo-tagging
 - Map Hybrid Cloud requirements to NIST CSF and SP 800-53
- Help organizations in regulated industries adopt Hybrid Clouds (FISMA, PCI-DSS, HIPAA, ...)
- **Output:** NIST Special Publication 1800 series for “Trusted Cloud”



NCCoE Trusted Hybrid Cloud Project

- Collaborate with industry partners
- Design, engineer, and build solutions leveraging commercial off-the shelf technology and cloud services
- Help regulated industries adopt cloud technologies and comply with applicable laws such as **FISMA, PCI, and HIPAA** as well as a voluntary framework like the **NIST Cybersecurity Framework**

Trusted Cloud security capabilities across different cloud service models

- Leverage NIST Interagency Report (IR) 7904: Trusted Geolocation in the Cloud, a trusted compute pools and isolation of workloads using hardware root of trust
- Provide data protection and key management enforcement
- Maintain persistent data flow segmentation policy
- **Enforce industry sector compliance policy for the regulated workloads (target FedRAMP and SP 800-53 moderate baseline)**

NIST Special Publication (SP)

SP 800-19 Trusted Cloud - Security Practice Guide for VMware Hybrid Cloud IaaS Environments

- Describe the security properties, architecture design decisions, and technology stack
- Compose of three volumes targeting executives, business owners, and engineers and cloud operators



SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards

Volume C: How-To Guide

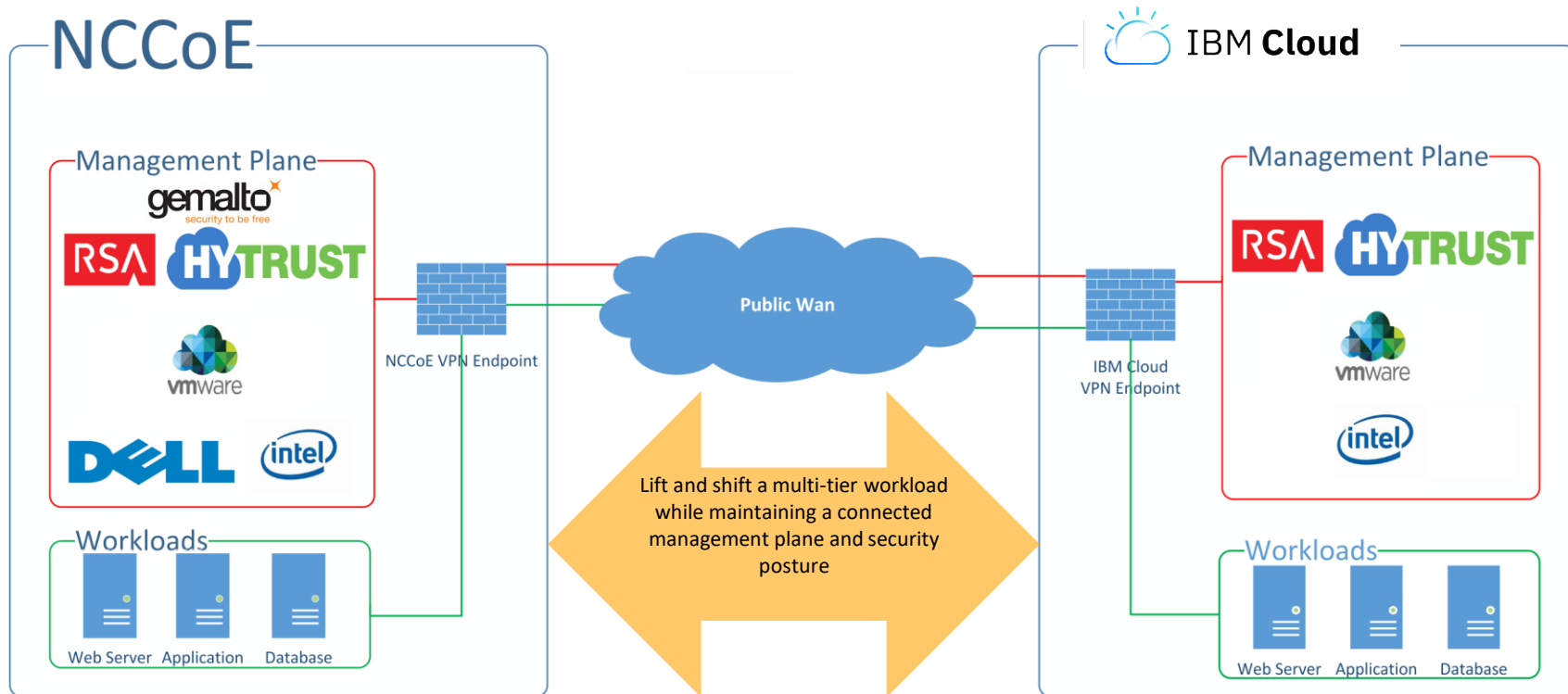
- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.

Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org

› Trusted Cloud: Security Objectives

Category	Security Outcome
Foundational	<ol style="list-style-type: none">1. Hardware Root-of-Trust based and geolocation-based asset tagging2. Deploy and migrate workloads to trusted platforms with specific tags
Building On	<ol style="list-style-type: none">3. Ensure workloads are decrypted on a server that meets the trust and boundary policies4. Ensure workloads meet the least privilege principle for network flow5. Ensure Industry sector-specific compliance6. Deploy and migrate workloads to trusted platforms across hybrid environments



Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.
 Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org

> NIST CSF & SP 800-53 Controls* alignment for Hybrid Clouds

CSF Function	CSF Subcategory	SP800-53R4 ^a	IEC/ISO 27001 ^b	CIS CSC ^c	NERC-CIP v5 ^d
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6

Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.
Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org

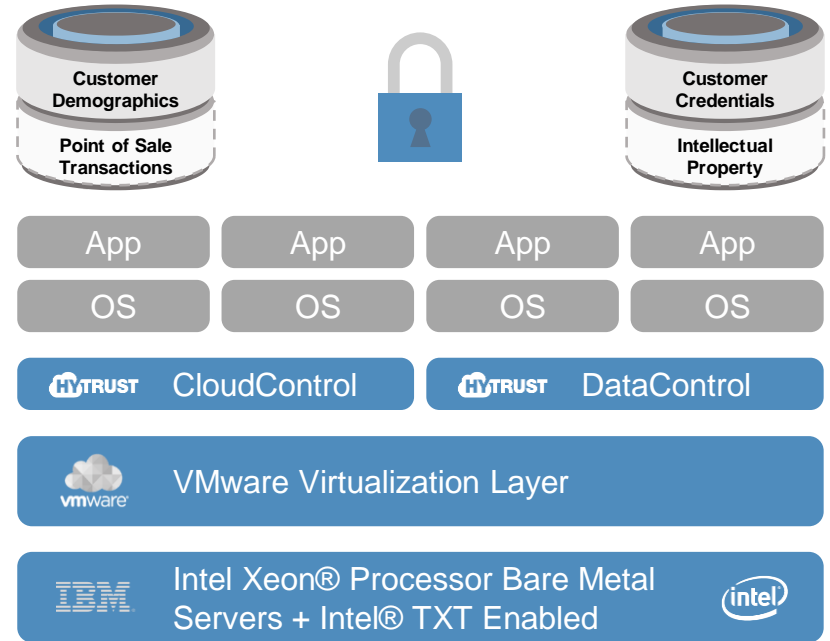
IBM Cloud Secure Virtualization* (ICSV)

A VMware Portfolio Solution

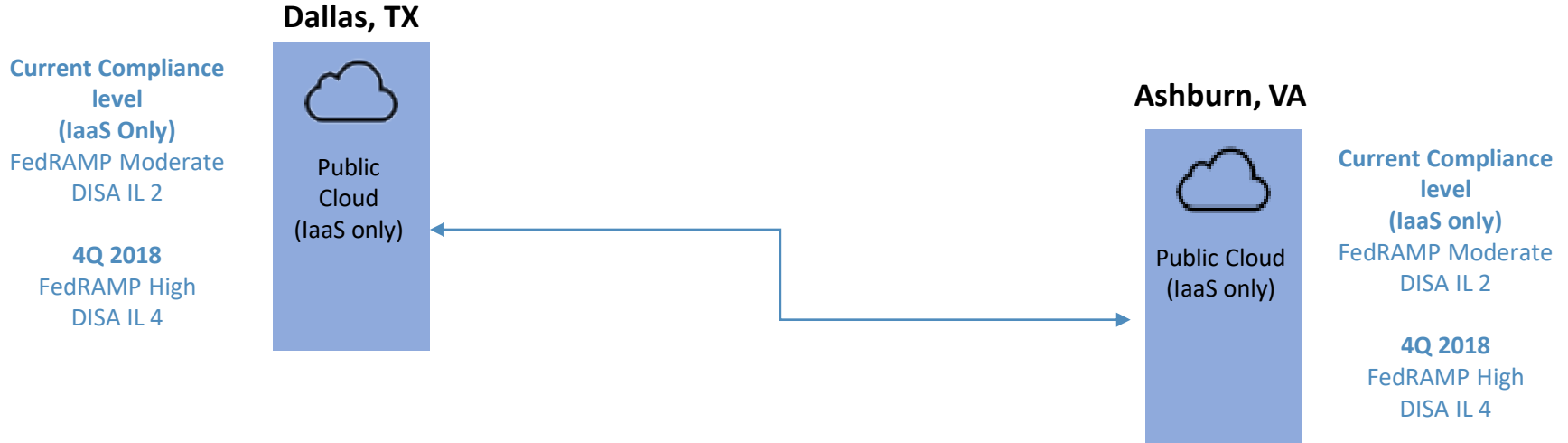
IBM Cloud is **only globally available cloud** with a solution that captures the benefits of both **HyTrust** software and **Intel® Trusted Execution Technology** to protect virtualized workloads down to the microchip* level.

- **VMware* virtualization layer options =** VMware Cloud Foundation or vCenter Server
- **HyTrust* policy tag options =** hardware and/or software
- Includes bare metal and VMware licenses

* Requires use of hardware tags

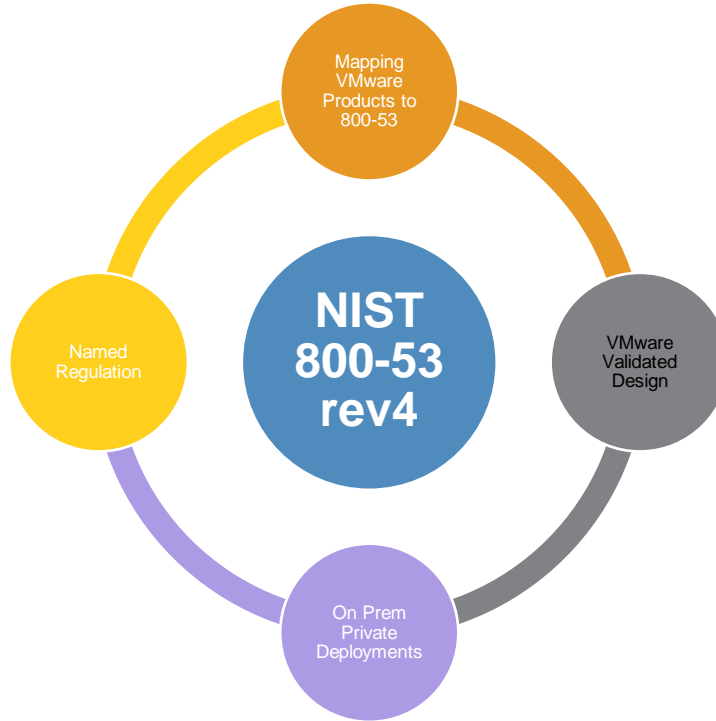


IBM IaaS FedRAMP Cloud* Environment



Currently IBM working on 2.0 Federal Cloud Environment

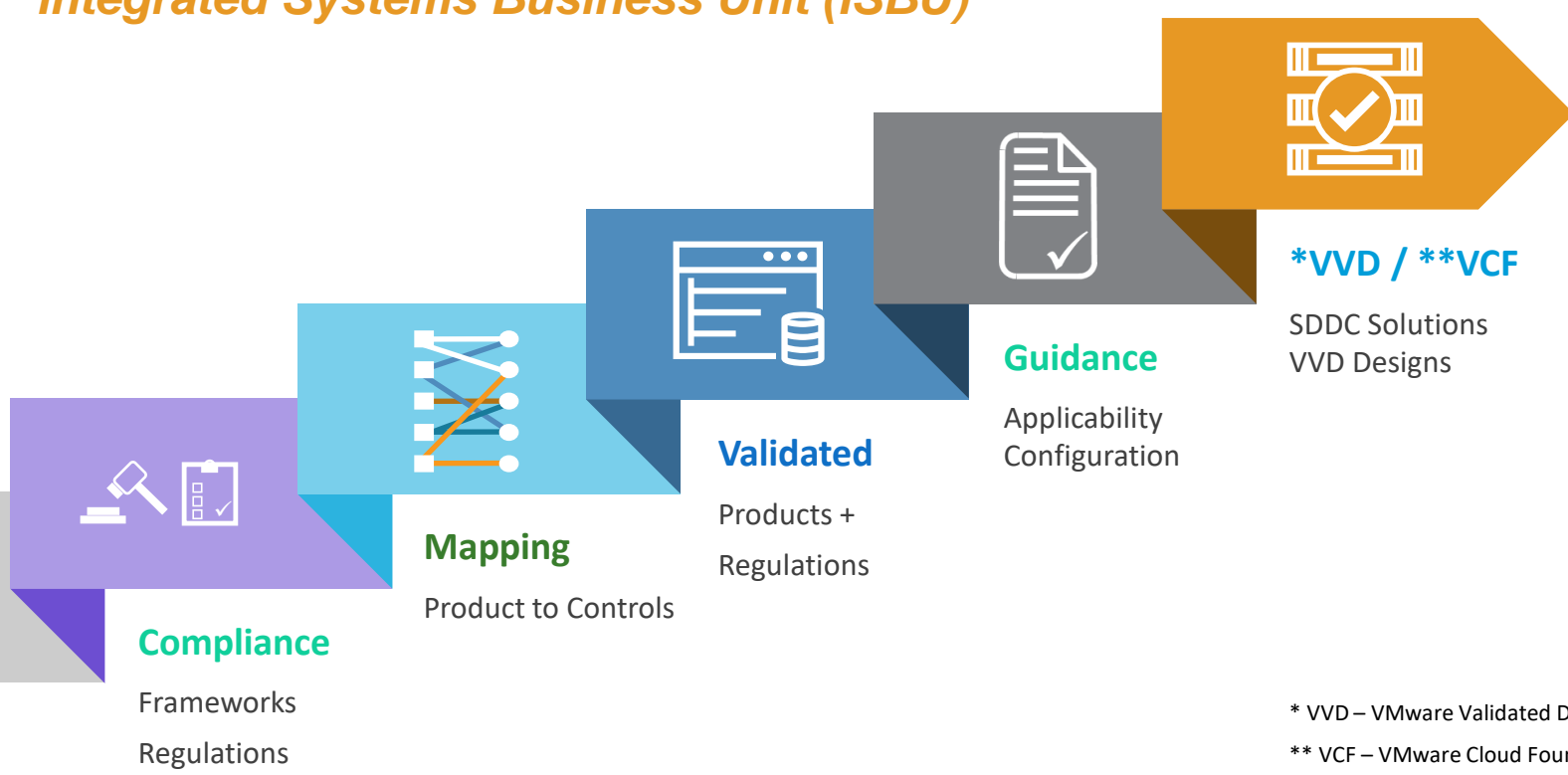
NIST and VMware* Solutions for Regulated Workloads



Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.
Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org
Confidential | ©2018 VMware, Inc.

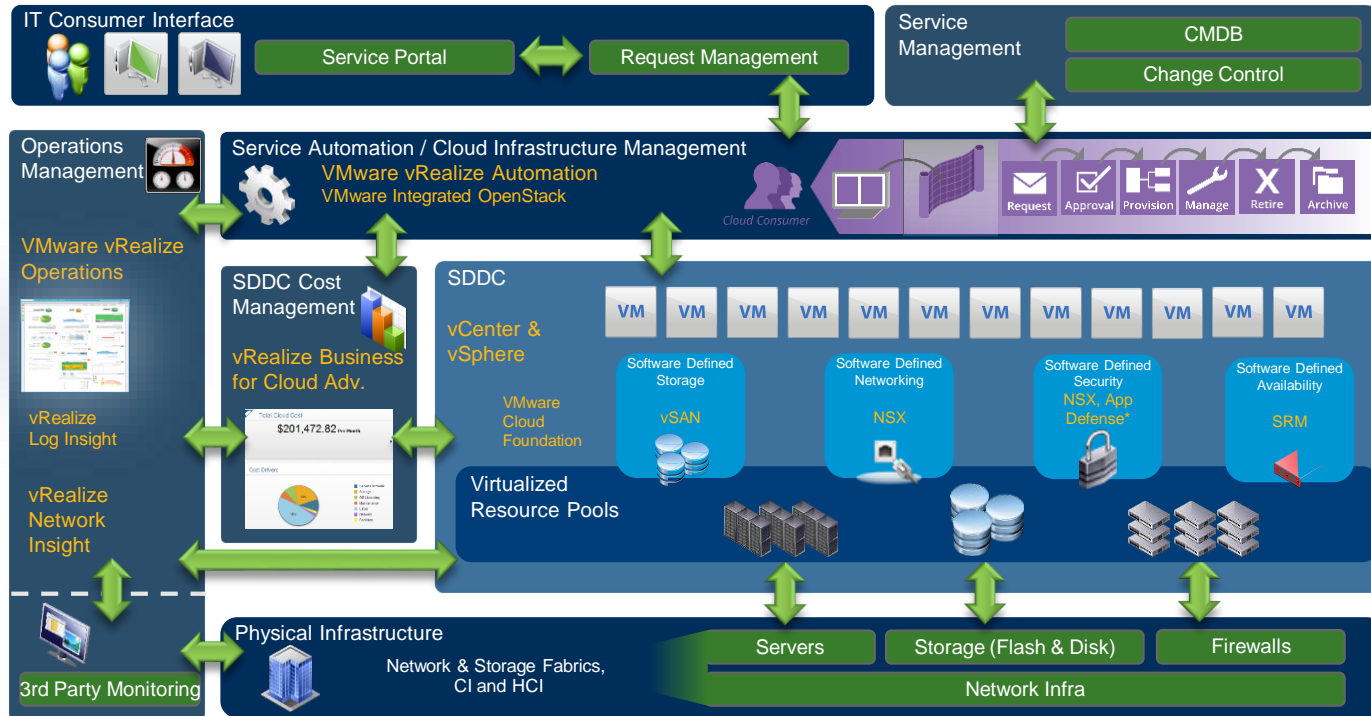
VMWare* Compliance Solutions

Integrated Systems Business Unit (ISBU)



* VVD – VMware Validated Design
** VCF – VMware Cloud Foundation

SDDC High Level Reference Architecture



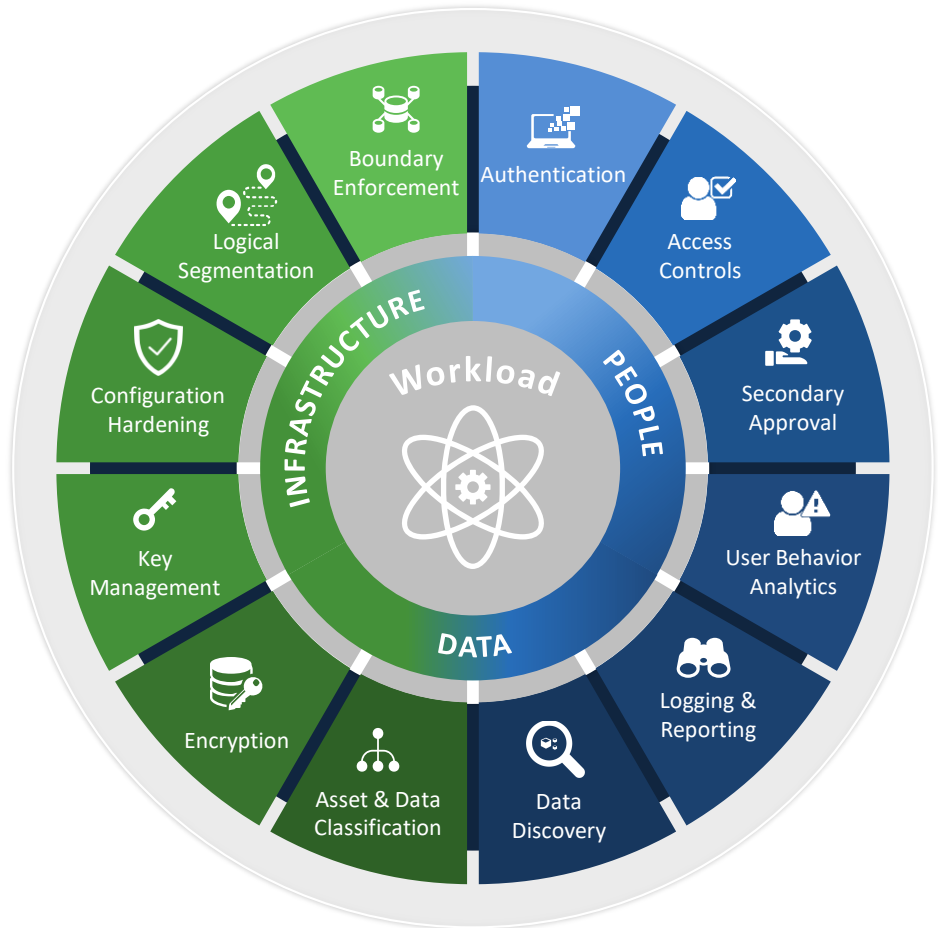
This version reflects revised vRealize Automation interaction with service management system adjacent to vRA (i.e. ITSM, CMDB systems like ServiceNow)

Trusted Cloud: Security Objectives Supported by Partners

Category	Security Outcome	Partner Supported Outcome
Foundational	1. Hardware Root-of-Trust based and geolocation-based asset tagging	Intel, Dell-EMC*, VMware* & HyTrust*
	2. Deploy and migrate workloads to trusted platforms with specific tags	VMware & HyTrust
Building On	3. Ensure workloads are decrypted on a server that meets the trust and boundary policies	Gemalto*, VMware, HyTrust & RSA*
	4. Ensure workloads meet the least privilege principle for network flow	VMware, HyTrust
	5. Ensure Industry sector-specific compliance	VMware, HyTrust & RSA
	6. Deploy and migrate workloads to trusted platforms across hybrid environments	VMware, IBM* & HyTrust

Cloud Security Policy Framework

(Discover, Analyze, Enforce)



HyTrust Capabilities Enable Critical G1000 Use Cases

Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.

Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org

Demo - HyTrust Cloud Security Policy Framework Suite

The screenshot shows the HyTrust CloudAdvisor interface with a search for sensitive data. The search criteria include File Size (Show All) and Date Range (Show All). The results list three files:

- TCPCIDCTP1.28.xls**: Volume4[P]I[P]Very sensitive data/True Positives/TCPCIDCTP1.28.xls. Owned by Local User. Last Modified: 2018-08-16 15:41:06. Discovered Time: 2018-08-24 07:15:12.
- TCPCIDCTP1.08.doc**: Volume4[P]I[P]Very sensitive data/True Positives/TCPCIDCTP1.08.doc. Owned by Local User. Last Modified: 2018-08-16 15:41:06. Discovered Time: 2018-08-24 07:15:12.
- TCPCIDCTP1.21.doc**: Volume4[P]I[P]Very sensitive data/True Positives/TCPCIDCTP1.21.doc. Owned by Local User. Last Modified: 2018-08-16 15:41:06. Discovered Time: 2018-08-24 07:15:12.

Discover sensitive data

The screenshot shows the 'Root of Trust - Current Hosts And Trust Status Report'. It includes a pie chart for 'Trust Status' and a table of host details.

Trust Status

- Trusted (3)
- Unknown (2)

Host	IP	Labels	Host Type	Trust Status	BIOS Patch Level	VM Patch Level	GKCI Relationship
comp-ncoo-ent-01.ncoo.lab	192.168.4.44	TRUSTED, PII	ESX	Trusted	1.3.7	VMware ESX 4.2.0 build-7386607	Self

Infrastructure Integrity Status

The screenshot shows the HyTrust GUI with the following information:

- HyTrust Agent Version: 4.2 (b13635)**
- KeyControl**: 192.168.4.145:443
- KeyControl List**: 192.168.4.145:443, 192.168.4.146:443
- Status**: Reauth needed (HTCC authorization failed)
- Last Heartbeat**: Fri Aug 24 11:28:38 2018 (failed)

Drive	Disk	Part	Cipher	Status	GUID
C:	0	2	none	Avail-Sys	N/A
E:	1	1	AES-XTS-512	Detached	B945DE72-3D08-42E7-942D-DE8C9F81B1

The screenshot shows the HyTrust Alerts section with a table of messages:

Date	Message
8/24/2018, 11:28:39 AM	Virtual Machine w01fileserv01 (Cloud VM Set: FileServers), is not in the geo- location boundary. Key access is denied
8/24/2018, 11:24:50 AM	Virtual Machine w01fileserv01 (Cloud VM Set: FileServers) re-connected, authentication pending
8/24/2018, 11:24:50 AM	Virtual Machine w01fileserv01 (Cloud VM Set: FileServers) is in the geo- location boundary. Key access is granted

Trust and Tag-Based Boundary Enforcement with Encryption

Demo - HyTrust Cloud Security Policy Framework Suite

The screenshot displays the HyTrust CloudControl interface. At the top, there is a navigation menu with options: General, Compliance, Policy, Configuration, Maintenance, and Help. The main content area is titled "Compliance > Hosts" and shows a list of hosts. The list has columns for Hosts, Host Type, Patch Level, Label, Last Run Template, Last Run, and Compliance. The hosts are sorted by Last Run date, with the most recent runs at the top. The compliance status is shown as a percentage for each host.

Hosts	Host Type	Patch Level	Label	Last Run Template	Last Run	Compliance
10.121.71.133	ESXi Host	VMware ESXi 6.5.0 build-7967591	PII	N/A	Never	0%
10.121.71.135	ESXi Host			N/A	N/A	0%
192.168.4.105	VMware NSX	6.4.0.7564187		N/A	Never	0%
192.168.4.106	VMware NSX	6.4.0.7564187		N/A	Never	0%
cloud-vcenter.icsv.nccoe.lab	vCenter	6.5.0 build-6816762		N/A	N/A	
cloud-vcenter.icsv.nccoe.lab	vSphere Web Client Server			N/A	N/A	
comp-nccoe-esxi-01.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607		VMware 6.0 ESXi_Custom_Template	08/23/2018 12:14:24 PM	100%
comp-nccoe-esxi-02.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII	VMware 6.0 ESXi_Custom_Template	08/23/2018 12:14:24 PM	100%
comp-nccoe-esxi-03.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII	VMware 6.0 ESXi_Custom_Template	08/24/2018 10:25:14 AM	100%
comp-nccoe-esxi-04.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII	VMware 6.0 ESXi_Custom_Template	08/23/2018 12:14:24 PM	100%
mgt-nccoe-esxi-01.nccoe.lab	ESXi Host			N/A	N/A	0%
mgt-nccoe-esxi-02.nccoe.lab	ESXi Host			N/A	N/A	0%

vSphere and NSX Infrastructure Inventory, Trust Status and Configuration Hardening Compliance Status

Trusted Cloud Implementation Demo & Status

Completed	To Finish
<ul style="list-style-type: none">• Dell* Hardware Installation• VMWare VVD* Implementation• Gemalto* HSM Integration• IPsec VPN connection to IBM Cloud*• HyTrust* Integration	<ul style="list-style-type: none">• RSA SecurID* and Archer integration• IBM Cloud Integration• Documentation

Deliverables

- SP 1800-19A published for comment on 8/24/2018
- SP 1800-19B published for comment (Date TBD)
- SP 1800-19C published for comment (Date TBD)

<https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud/hybrid>

Additional Special Thanks to Project Participants

NIST	Murugiah S, Donna D, Matt S, Kevin S
Intel	Tim K, Uttam S, Gene Q, Irena R
IBM	Andras Z, Dieter P, Rajeev G, Laura S, Andrew G
VMware	Carlos P, Jeff L, Brenda S, Jerry B, John Mc, Kevin S, Rob T
Dell-EMC	Daniel C, Sean S, Aaron M, Dan C, Clinton J, Jeremy B
HyTrust	Jason M, Mike B, Mike T, Dave S
RSA	Tarik W, Steve S, Tim S, Dan C, Mike D
Gemalto	Gina S, Paul M

Summary

- **Unique partnership between NIST* & Private Industry**
- **Goal: Design, engineer, and publish reference architecture (s) using COTS components & Services for Trusted Hybrid Clouds**
- **First Reference Implementation: Migrate multi-tier workload between NCCoE datacenter and the IBM Cloud whilst meeting security & compliance requirements**
- **Deliverable: NIST SP-1800-19A series publication**
- **Timelines: Q3 2018 Public Draft; Q4 final version**
- **Future additions to architecture : Multi-Cloud, Container Workloads**

Questions?

2
2

Visit the Intel Booth #1212 for a demo and Q & A with NIST* and the Industry partners

Visit the Intel VMWare site at
<https://www.intel.com/content/www/us/en/cloud-computing/intel-and-vmware-partnership.html>

References

- <https://nccoe.nist.gov/projects/building-blocks/trusted-geolocation-in-the-cloud>
- **NIST** Cybersecurity Framework: <https://www.nist.gov/cyberframework>
- <https://www.hytrust.com/hytrust-cloud-security-policy-framework/>
- www.vmware.com
- www.dell.com
- www.rsa.com
- www.ibm.com/cloud/secure-virtualization
- www.intel.com
- www.gemalto.com

Q & A

Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.

Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org

Legal Notices and Disclaimers

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration.

No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

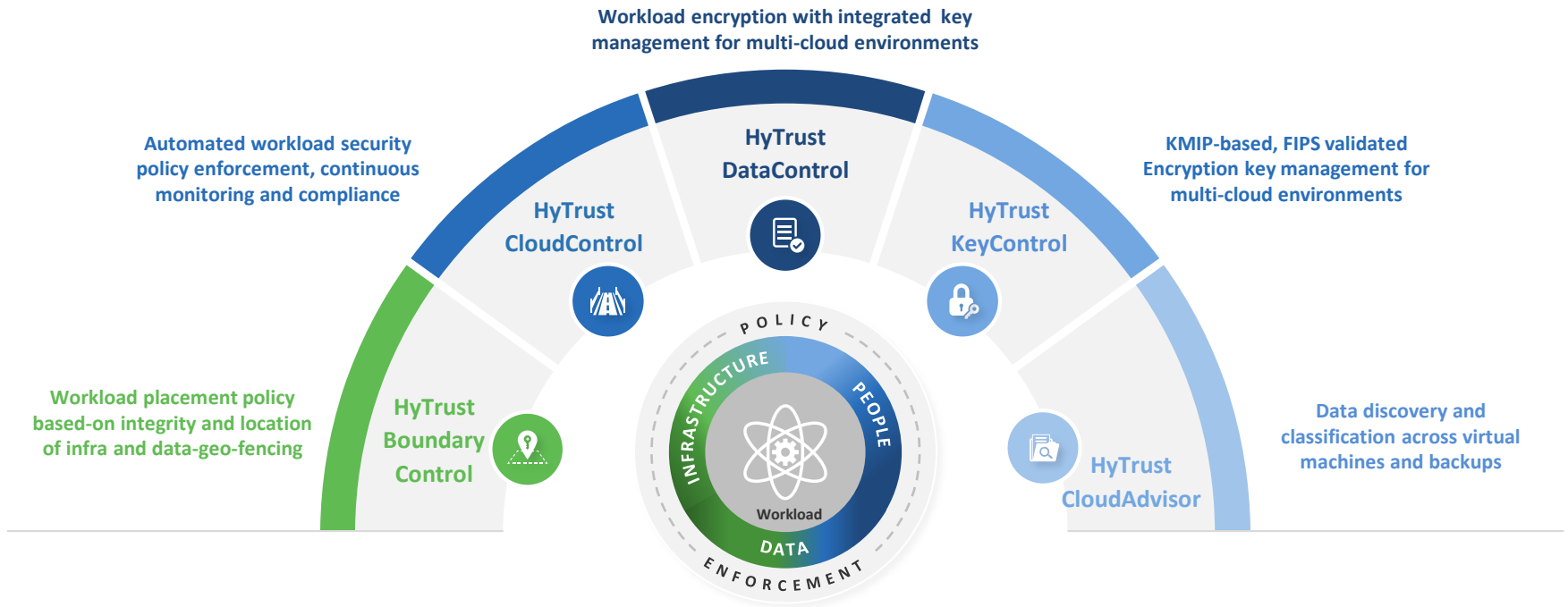
Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2018 Intel Corporation. All rights reserved

Backup

HyTrust Cloud Security Policy Framework – Product Portfolio



Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.
Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org

RSA Archer Dashboard from NIST IR

7904

RSA Archer GRC

Preferences Reports Help Logout

Search: NIST PCR POC

Enterprise Governance, Risk and Compliance

Policy Center Policy Management Vendor Management Threat Management Task Management Administration **NIST PCR POC**

Navigation Menu

Administration

NIST PCR POC

pcr

Search Records

New Record

Records

Data Import

Reports

Dashboard: Intel PoC Dashboard

Welcome, System Administrator

Options

Overview

Total Compliance View

VMWare Host	Trusted Boot Validation	Geo-Location Validation	System Validation	Last PCR Pull
hypervisor1.nccoe.lab				9/23/2015 1:55 PM
hypervisor2.nccoe.lab				9/23/2015 1:55 PM
hypervisor3.nccoe.lab				9/23/2015 1:55 PM

Page 1 of 1 (3 records)



Disclaimer: These slides are originally presented in CSA APAC Congress 2018, Manila, Philippines.
Do not distribute or recreate copies. For more information please email: membership@csaphilippines.org