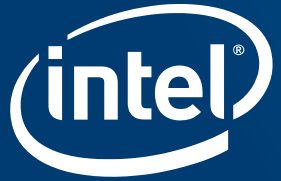


Trusted Hybrid Cloud–NIST's Trusted Cloud Building Block & Ref Architecture

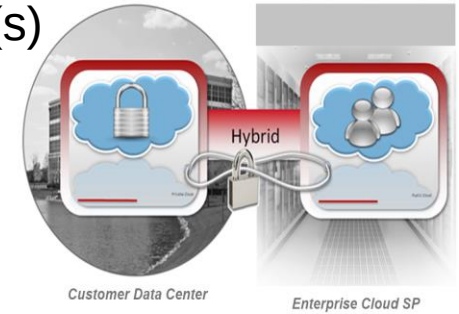
Raghu Yeluri, Intel Corporation
Michael Bartock, NIST
Harmeet Singh, IBM
Anthony Dukes, VMware
Hemma Prafullchandra, HyTrust

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

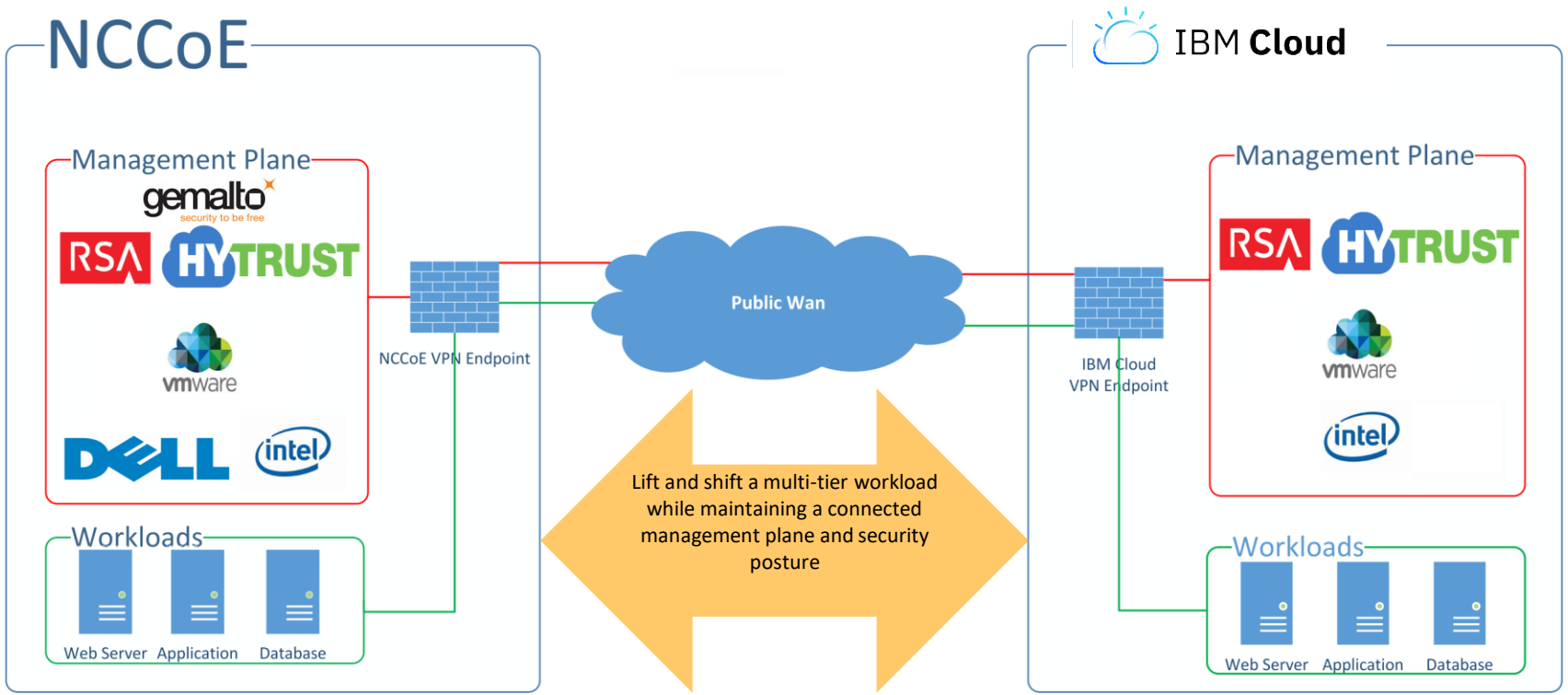
- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards

Volume C: How-To Guide

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

Trusted Cloud: Security Objectives

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



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

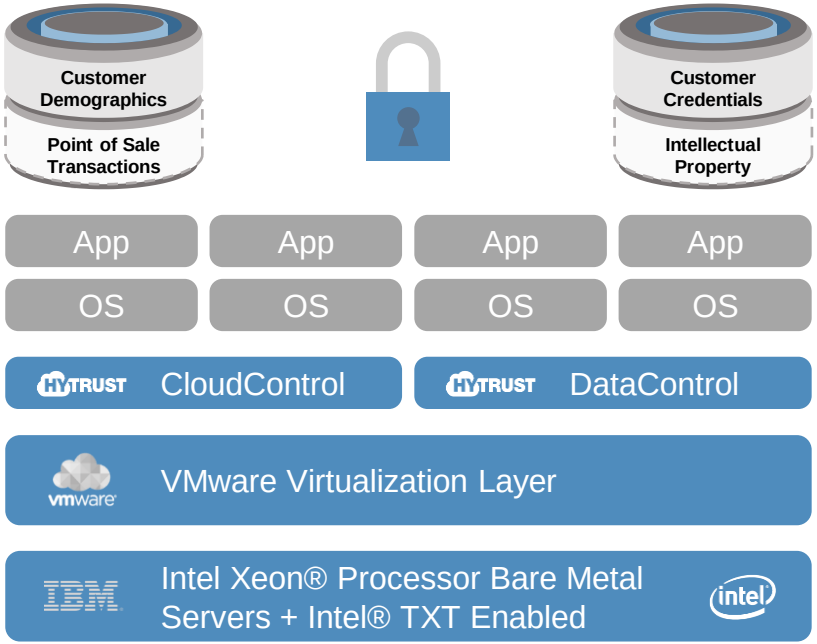
CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	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

IBM Cloud Secure Virtualization* (ICSV)

A VMware Portfolio Solution

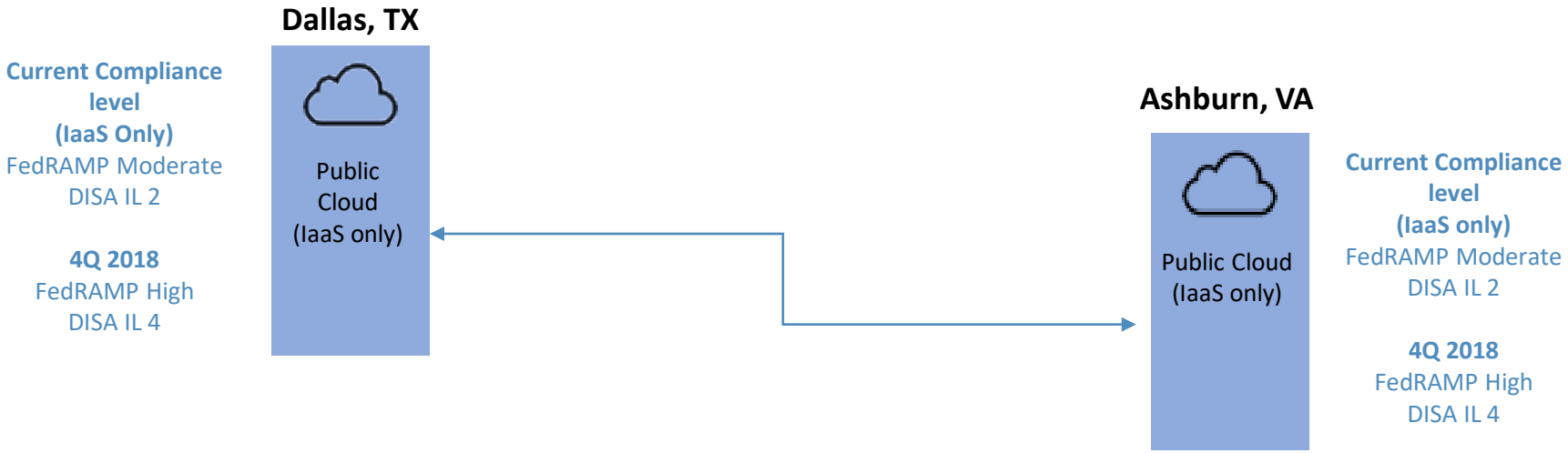
IBM Cloud is **only globally available cloud** with a solution that captures the benefits of both **HyTrust** software and **Intel®** Trusted Execution Technology to protect virtualized workloads down to the microchip* level.

- **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

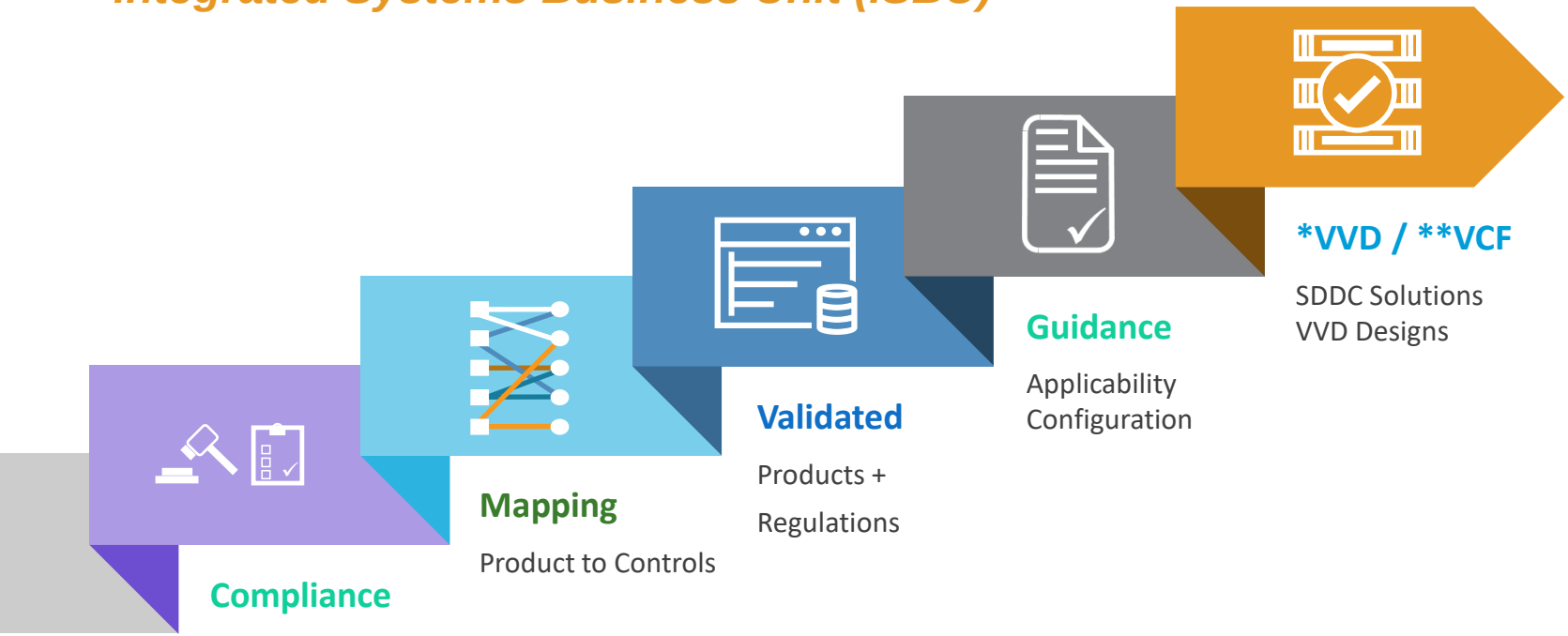


Currently IBM working on 2.0 Federal Cloud Environment

NIST and VMware* Solutions for Regulated Workloads

VMWare* Compliance Solutions

Integrated Systems Business Unit (ISBU)

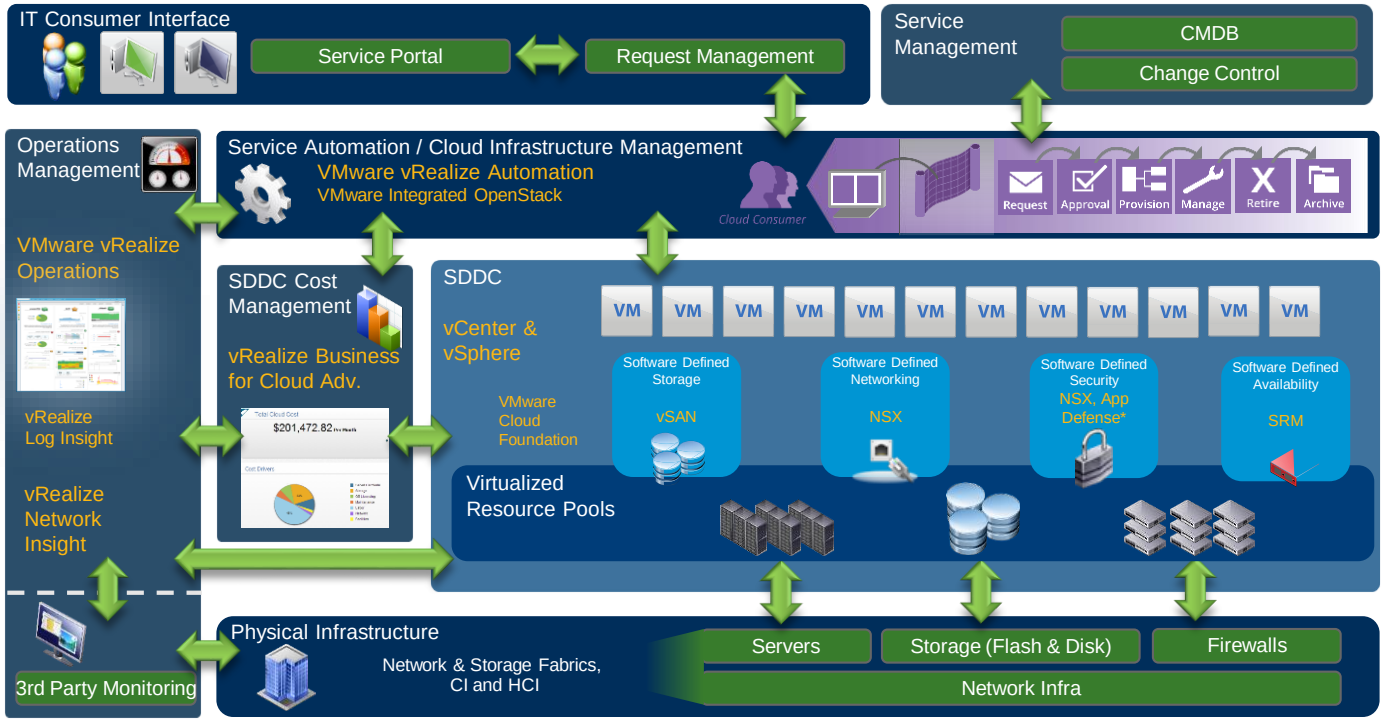


* VVD – VMware Validated Design

** VCF – VMware Cloud Foundation

Integrated Systems Business Unit

SDDC High Level Reference Architecture



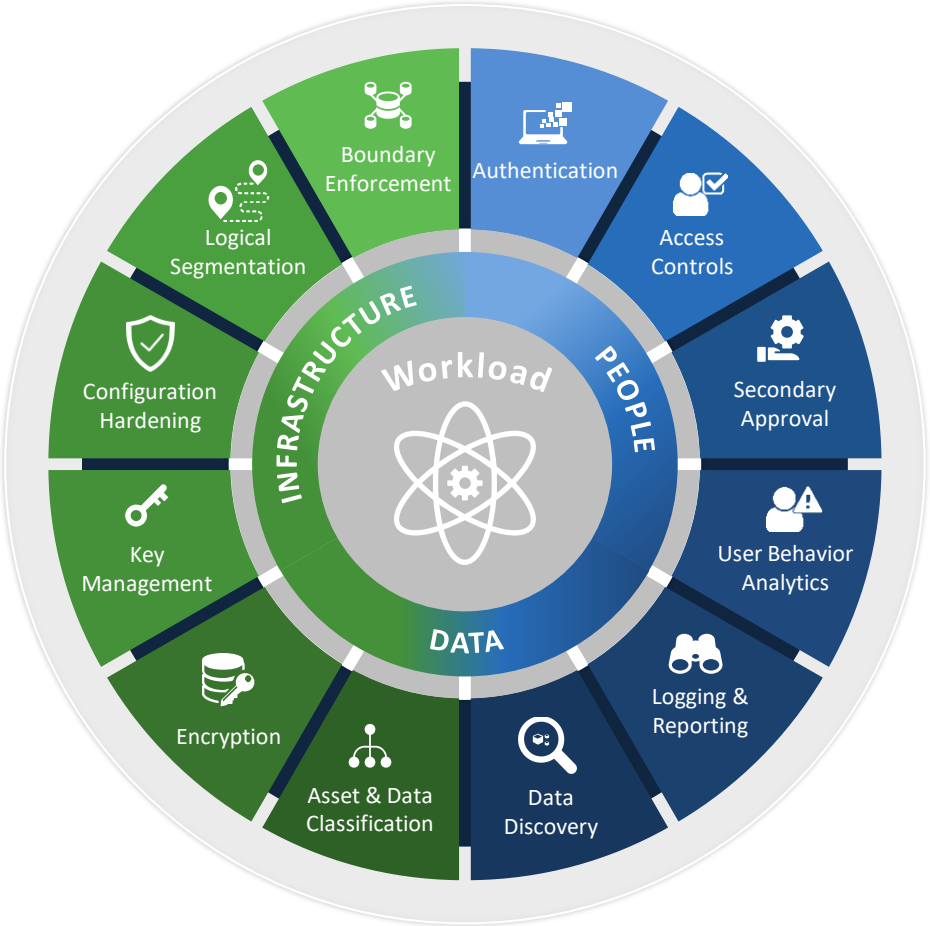
This version reflects revised vRealize Automation interaction with service management system adjacent to vRA (i.e. ITSM, CMDB systems like ServiceNow)

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

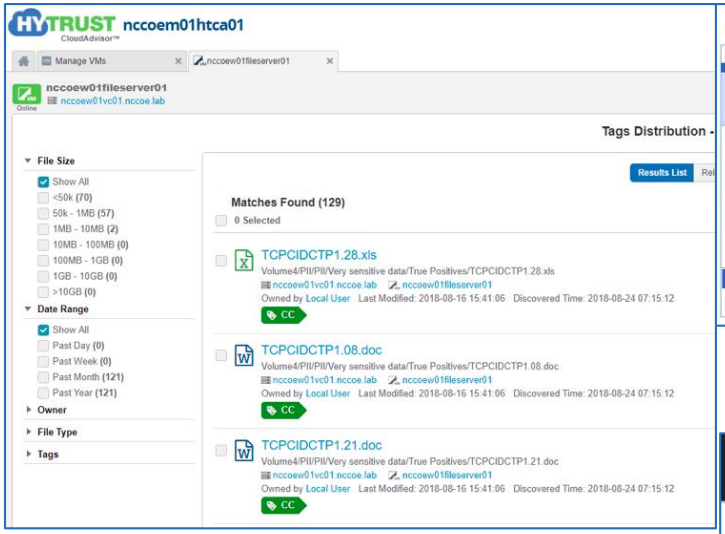
Cloud Security Policy Framework

(Discover, Analyze, Enforce)

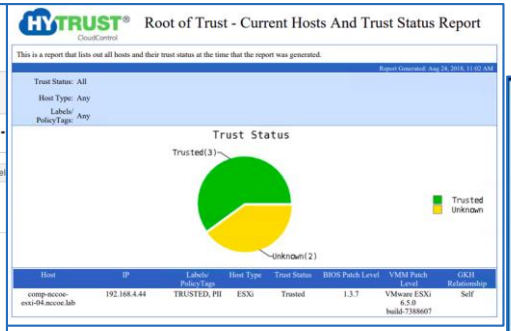


HyTrust Capabilities Enable Critical G1000 Use Cases

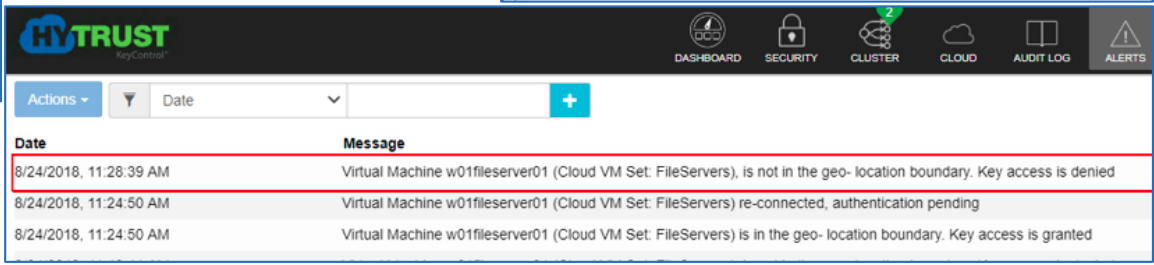
Demo - HyTrust Cloud Security Policy Framework Suite



Discover sensitive data

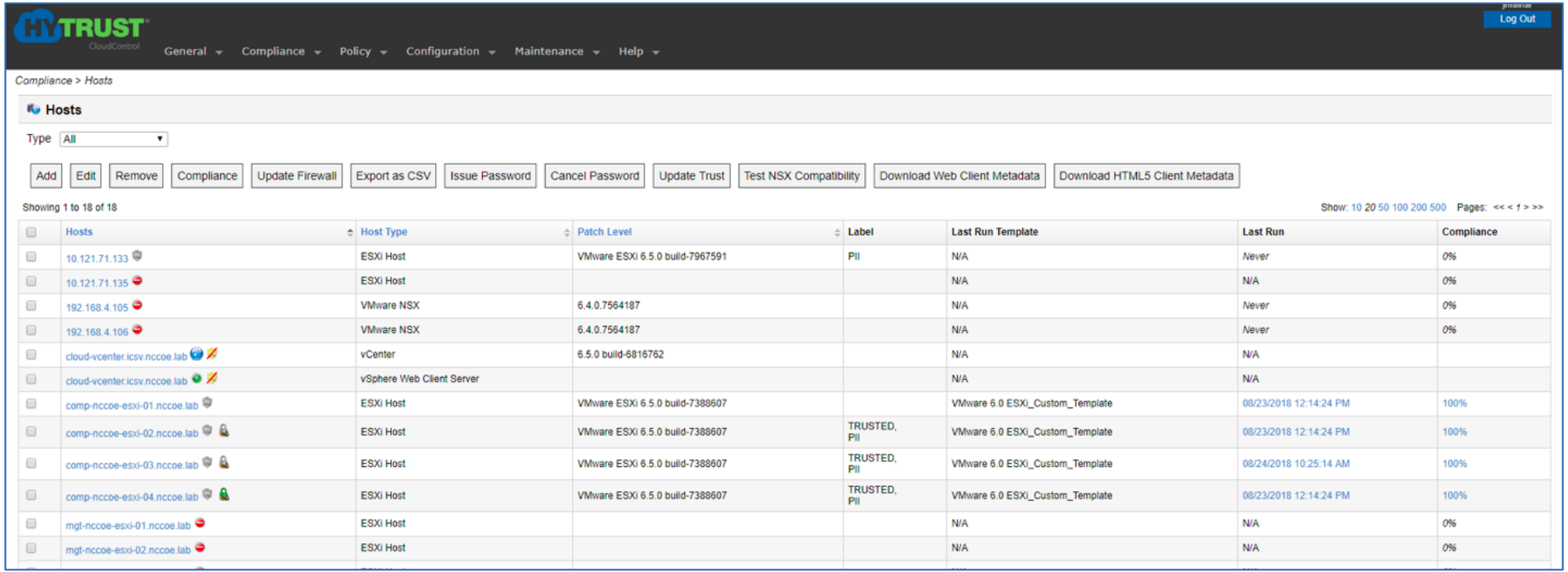


Infrastructure Integrity Status



Trust and Tag-Based Boundary Enforcement with Encryption

Demo - HyTrust Cloud Security Policy Framework Suite



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

Trusted Cloud Implementation Demo & Status

Completed	To Finish
• Dell* Hardware Installation • VMWare VVD* Implementation • Gemalto* HSM Integration • IPsec VPN connection to IBM Cloud* • HyTrust* Integration	• 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?

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

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.

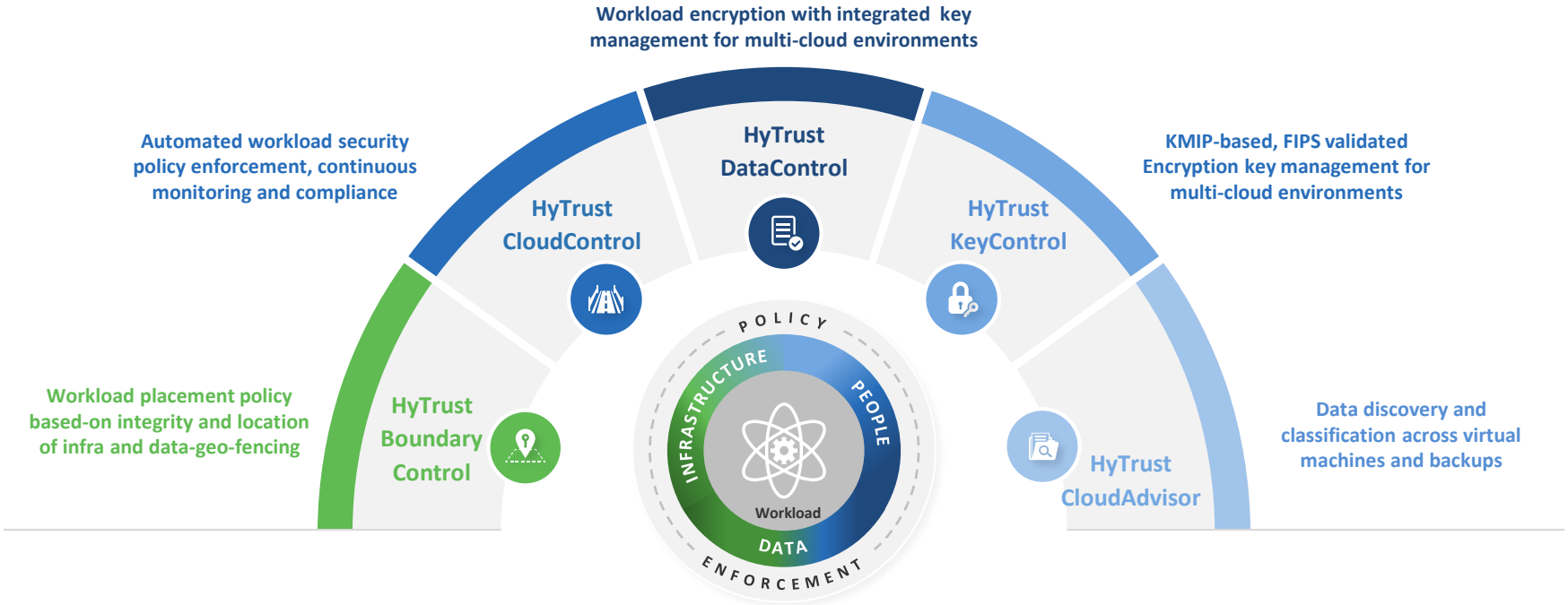
No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

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.

Backup

HyTrust Cloud Security Policy Framework – Product Portfolio



Microsoft Azure · NetApp · cisco · Pivot3 · IBM Bluemix · DELL EMC · Hewlett Packard Enterprise · NUTANIX · amazon web services · simplivity · intel · vmware

RSA Archer Dashboard from NIST IR 7904