RED HAT SUMMIT

DELIVERING TRUSTED CLOUDS

How Intel and Red Hat integrated solutions for secure cloud computing

Steve Orrin - *Federal Chief Technologist, Intel*
Steve Forage - *Senior Director, Cloud Solutions, Red Hat*

redhat

Agenda

- The Drive to Cloud
- Key Challenges in Cloud Deployments
- Building Blocks for Trusted Cloud Architecture
    - Intel capabilities
    - Red Hat platforms
- Solutions for Trusted Clouds
    - NEC/Black Box
    - CSRA
- Summary

Why Cloud?

CLOUD BUSINESS BENEFITS

Agility & Control

Cost Savings

Rapid Innovation

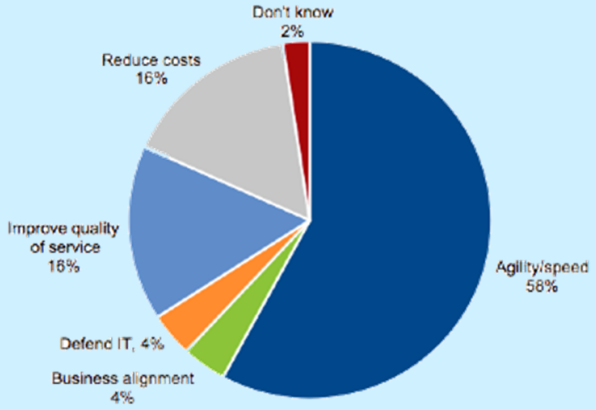


Figure 1 – Gartner Data Center Pool on Private Cloud Computing Drivers, Gartner, Private Cloud Matures, Hybrid Cloud Is Next, Thomas Bittman, September 6, 2013

TOP 5 BUSINESS DRIVERS

1. Cost Savings
2. Operational Efficiency
3. Open Platform
4. Flexibility of underlying Tech Choices
5. Ability to innovation compete

Figure 2 - "*OpenStack Foundation User Survey*", http://www.openstack.org/blog/2013/11/openstack-user-survey-october-2013/, October, 2013

Business and Networking Challenges

Increased Data Traffic

"Smart devices, video content, and cloud services are all generating double-digit growth in network traffic."
ONF, 2013

Protection of Customer Data

"Target will pay customers who suffered from a 2013 data breach up to $10,000 each in damages."
CNN Money, August 2015

Business Agility

" Business agility is at the top of every CEO's priority list…. IT agility must become an imperative too. "
ZK Research, May 2014

- Storage requirements are increasing 40% annually
- Improving Network Security
- Need More Bandwidth
- Network Virtualization
- Aligning IT and Corporate Goals
- Moving Applications to the Cloud
- Ensuring Applications Run Optimally
- BYOD Related Access and Policy Concerns

redhat. | intel

Key Security Challenges

Attacks on the infrastructure

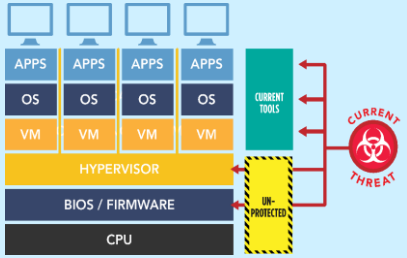
Co-tenancy threats

Regulation compliance

Visibility and Audit Challenges

Building and Enforcing Trust in the Cloud

No physical boundaries.
Do you know where you workload/data is located?



Attacks are moving down in the stack.
How do you establish root of trust in h/w?

Lack of Visibility to the Integrity of Infrastructure.
How do you know your workloads are running on compliant infrastructure?

redhat. | intel

Compliance Requirements & Regulatory Challenges

- Compliance in a cloud environment
- Achieving Audit and Visibility
- Commingled Regulatory Environments
- Continuous Monitoring
- Data Use Controls

redhat. intel

Building Trust and Compliance in the Cloud:

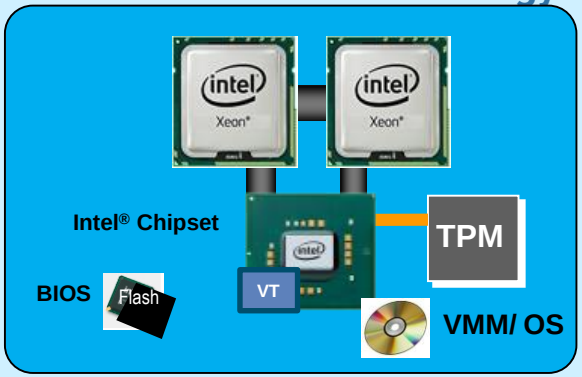
The big questions

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**

Intel provides Infrastructure Trust and Location Control

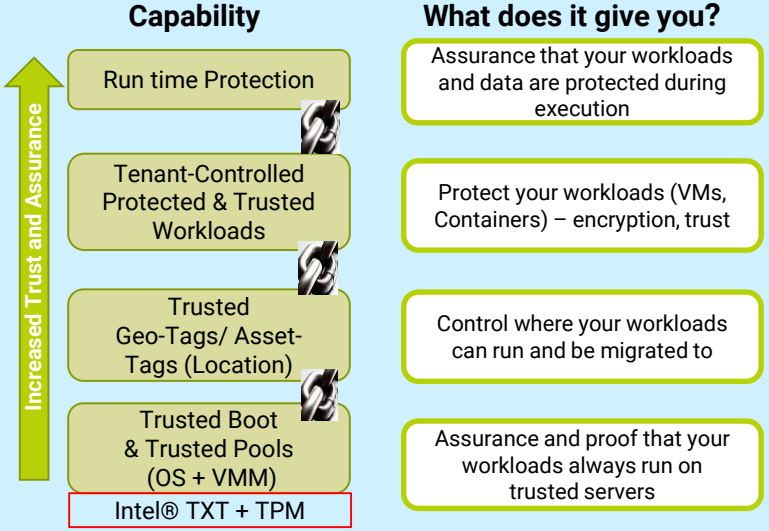
Trusted Execution Technology



Trusted Launch
Enables isolation and tamper detection at boot-time

Compliance
Hardware-based verification for compliance

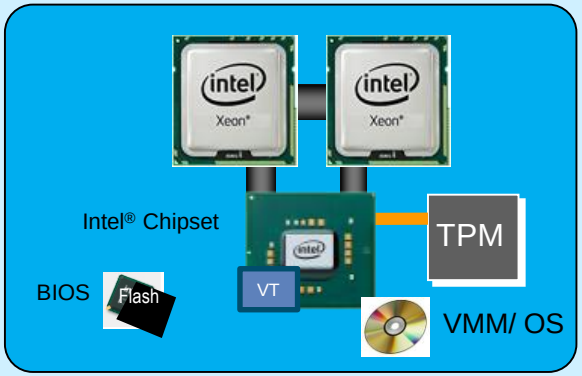
Cloud Integrity Technology – *leverages TXT*



redhat. intel

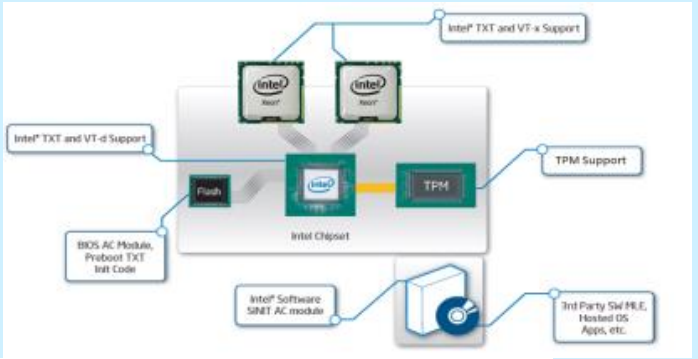
How Trust is established using Intel TXT/TPM

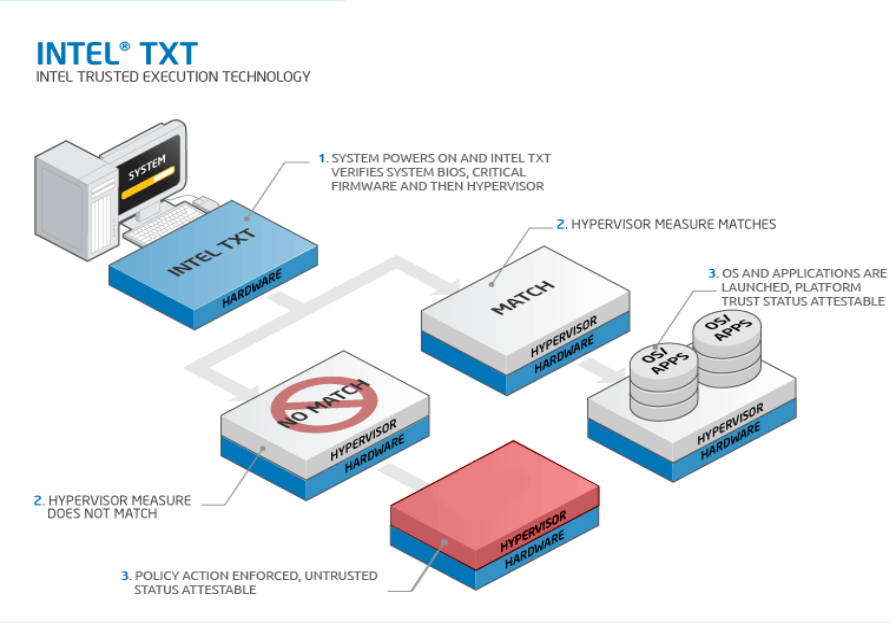
Trusted Execution Technology



Trusted Launch
Enables isolation and tamper detection at boot-time

Compliance
Hardware-based verification for compliance





redhat. intel

Trusted Compute Pools

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

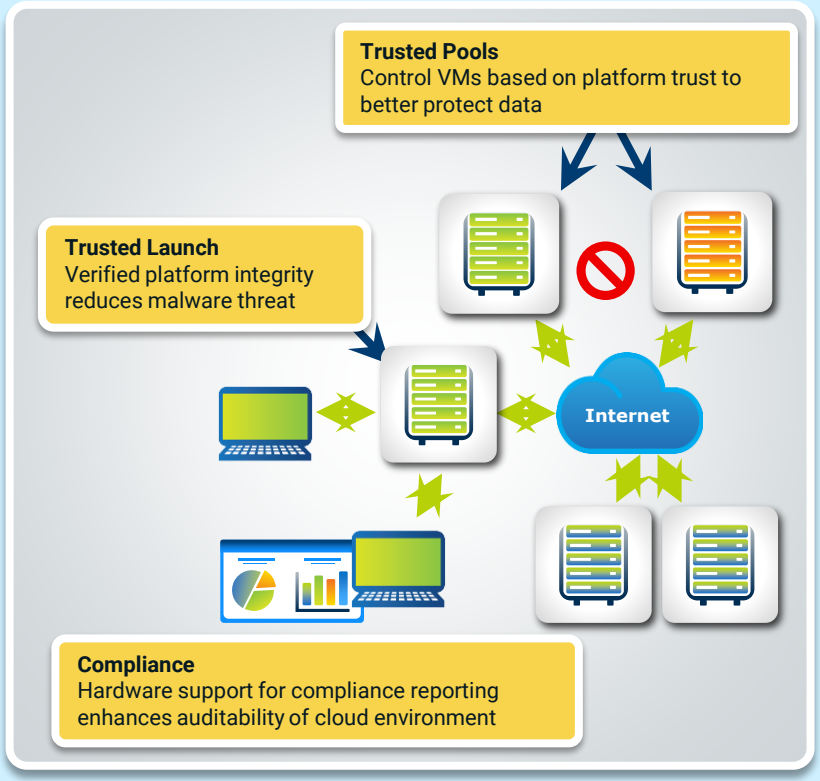
- Launch-time protections that complement run-time malware protections

- 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



redhat. intel

Cloud Integrity Technology 1.0

Platform Trust, Trusted Compute Pools

Uses Intel TXT/TPM to verify the integrity of a platform (BIOS, OS, hypervisor) against a "known good state" or "whitelist" at boot time

Helps create logical groupings (pools) of trusted systems, separates them from untrusted systems

Enables:

Visibility: Identify trusted platforms vs. untrusted

Control: Set policy that only allows workloads to run on trusted servers

Monitoring: Trust-based policies can be automatically tracked

Compliance: Trust information can be delivered to audit logs

Available as Open Source

Delivered via OpenStack or integrated into Policy & Compliance products, e.g. HyTrust Cloud Control

Use Model 1: Trusted Launch
Attestation provides information about platform trust to improve response to malware threats

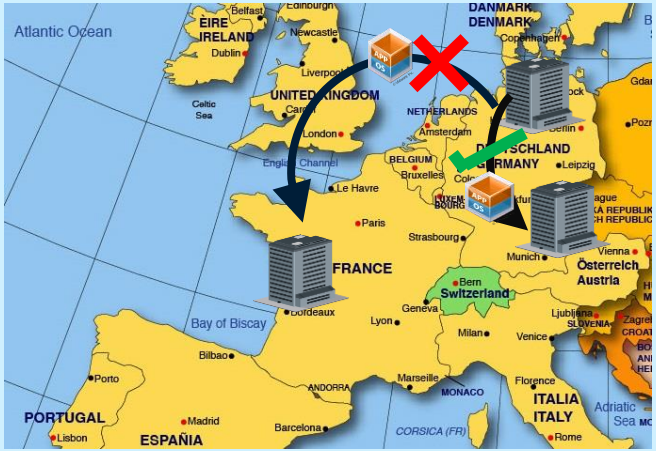
Use Model 2: Trusted Compute Pools
Attestation provides information to inform us of which systems are trustworthy for hosting our workloads

Use Model 3: Compliance
Attestation allows us to verify platform trust for comparison against policy and use in audit

redhat. intel

Cloud Integrity Technology 2.0

Trusted Location and Boundary Control



Addresses top cloud concerns:

Visibility and Control of Workload Location

Auditability and Regulatory Compliance

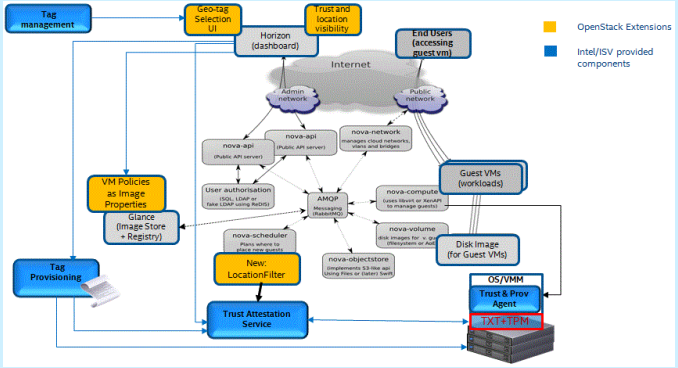
- Hardware-based Geo- and Asset Tags help control workload placement and migration
- Tags are securely stored in TPM, tag integrity is assured
- Location Boundary Control policy can be set for a workload, allowing or preventing its deployment
- This helps address and prove data sovereignty requirements
- Delivered via OpenStack or Policy & Compliance product, e.g. HyTrust Cloud Control

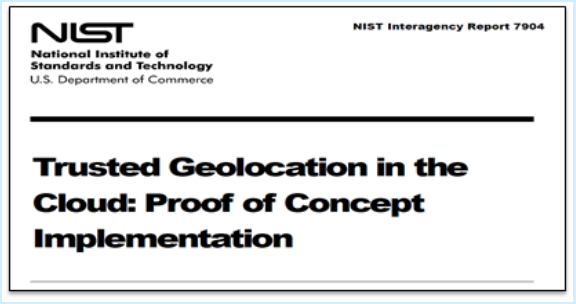
redhat. | intel

Attested Server Tagging & Trusted Geo-location in the Cloud

- Many Trusted Compute Pools Early Adopters also require:
  - GEO tagging
- Regulatory Compliance Requirements:
  - EU data protection directives (95/46/EC)
  - FISMA (geo-tag)
  - Payment Card Industry (PCI-DSS) (asset tag)
  - HIPPA (Asset Tag)

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




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

NIST IR 7904 –USG recommendation for “Trusted Geolocation in the Cloud”

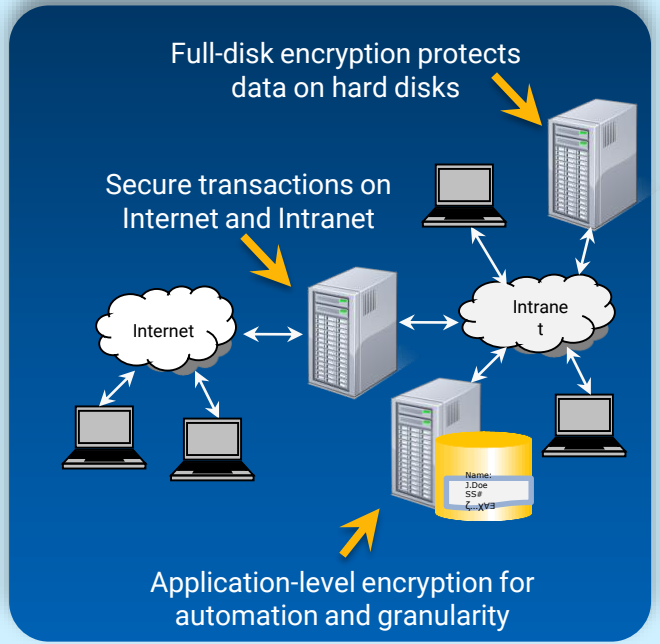
- **Trusted resource pool based on hardware-based secure technical measurement capability**
  - **Platform attestation and safer hypervisor launch** - Provide integrity measurement and enforcement for the compute nodes
  - **Trust-based secure migration** - Provide geolocation measurement and enforcement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

redhat. intel

Hardware Features for Data Protection

AES-NI
- Ubiquitous Data Protection with Cryptographic Acceleration
  - AES-NI allows significant performance at a lower price-point, no custom hardware

DRNG
- Better Keys and Simulations with On-Board Digital Random Number Generator
- Stronger encryption keys
  - High degree of entropy provides quality random numbers for encryption keys and other operations
  - DRNG solves the problem of limited entropy in virtual platforms



Introducing New Instructions for Cryptography Acceleration
ADOX/ADCX

Extension of ADC (Add with Carry) instruction for use in large integer arithmetic (integers MUCH larger than 64b); one common use is Public Key cryptography (e.g. RSA)

ADOX - Unsigned Integer Addition with carry-in/out using the Overflow Flag

ADCX - Unsigned Integer Addition with carry-in/out using the Carry Flag

Performance improvements are due to two parallel carry chains being supported at the same time

Available starting in Broadwell CPUs

mul-based instruction sequence	mulx-based instruction sequence	mulx/adcx/adox based instruction sequence
mov OP, [pB+8*0]	mov OP, [pB+8*0]	xor rax, rax mov rdx, [pB+8*0]

mov rax, [pA+8*0]
mul OP
add R0, rax
adc rdx, 0
mov TMP, rdx
mov pDst, R0
	mulx TMP1,rax, [pA+8*0]
	add R0, rax
	adc TMP1, 0
	mov pDst, R0
		mulx T1, T2, [pA+8*0]
		adox R0, T2
		adcx R1, T1
		mov pDst, R0

mov rax, [pA+8*1]
mul OP
mov R0, rdx
add R1, rax
adc R0, 0
add R1, TMP
adc R0, 0
	mulx TMP2,R'0, [pA+8*1]
	add R'0, R1
	adc TMP2, 0
	add R'0, TMP1
	adc TMP2, 0
		mulx T1, R'0, [pA+8*1]
		adox R'0, R1
		adcx R2, T1

mov rax, [pA+8*2]
mul OP
mov TMP, rdx
add R2, rax
adc TMP, 0
add R2, R0
adc TMP, 0
...
	mulx TMP1,R'1, [pA+8*2]
	add R'1, R2
	adc TMP1, 0
	add R'1, TMP2
	adc TMP1, 0
	...
		mulx T1, R'1, [pA+8*2]
		adox R'1, R2
		adcx R3, T1
		...

ADOX/ADCX Used with MULX Can Substantially Improve Public Key Encryption Code Performance

redhat. intel

Cloud Integrity Technology 3.0

Workload Integrity and Confidentiality with OpenStack

Extend trust from BIOS to workload
- Boot-time integrity of workload
- Workload can be a VM or container

- Integrated with OpenStack

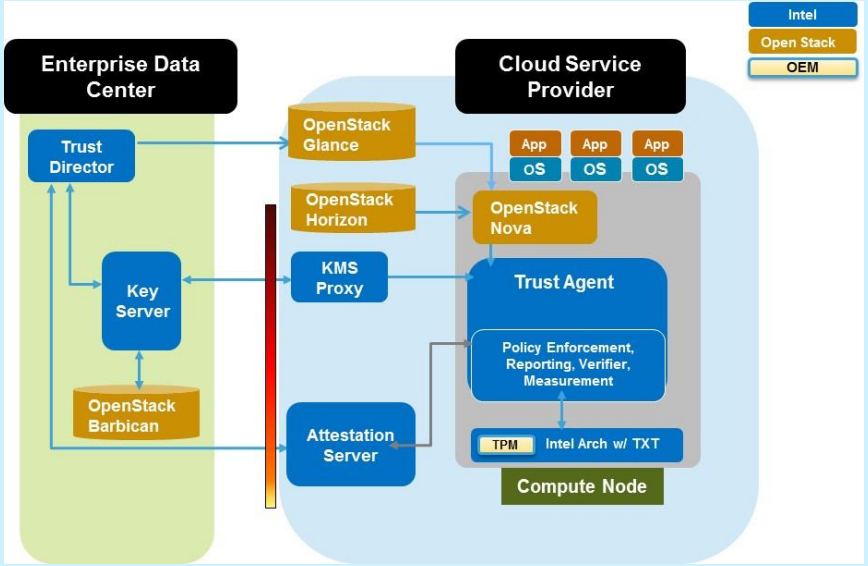
Enterprise Ownership and Control
- Encrypt workload before moving it to cloud
- Own and manage the encryption keys

- Only release keys to CSP after integrity check succeeds

- This ensures verifiable end-to-end protection

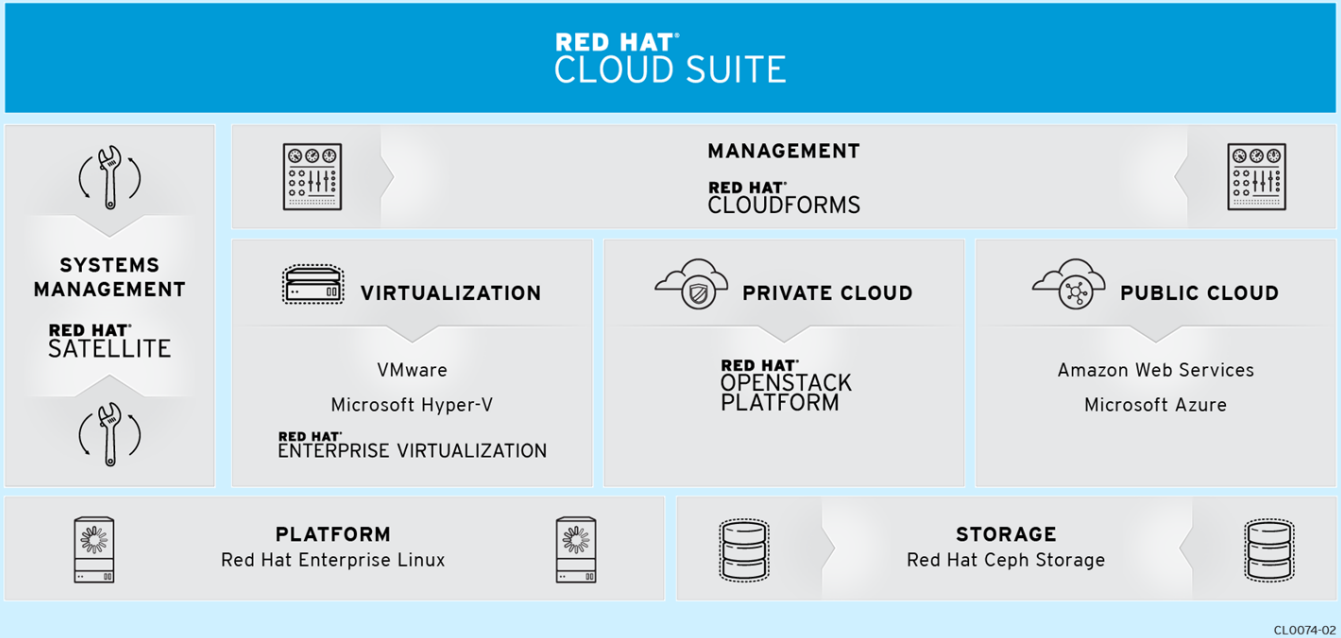
Can be applied to storage and network workloads too

CSPs can offer CIT 3.0 as cloud service



Red Hat Cloud Infrastructure

Cloud Management - Alternative Virtualization - OpenStack - Ceph



Why Red Hat Cloud Infrastructure Software

The Forrester Wave™: Private Cloud Software Suites, Q1 2016

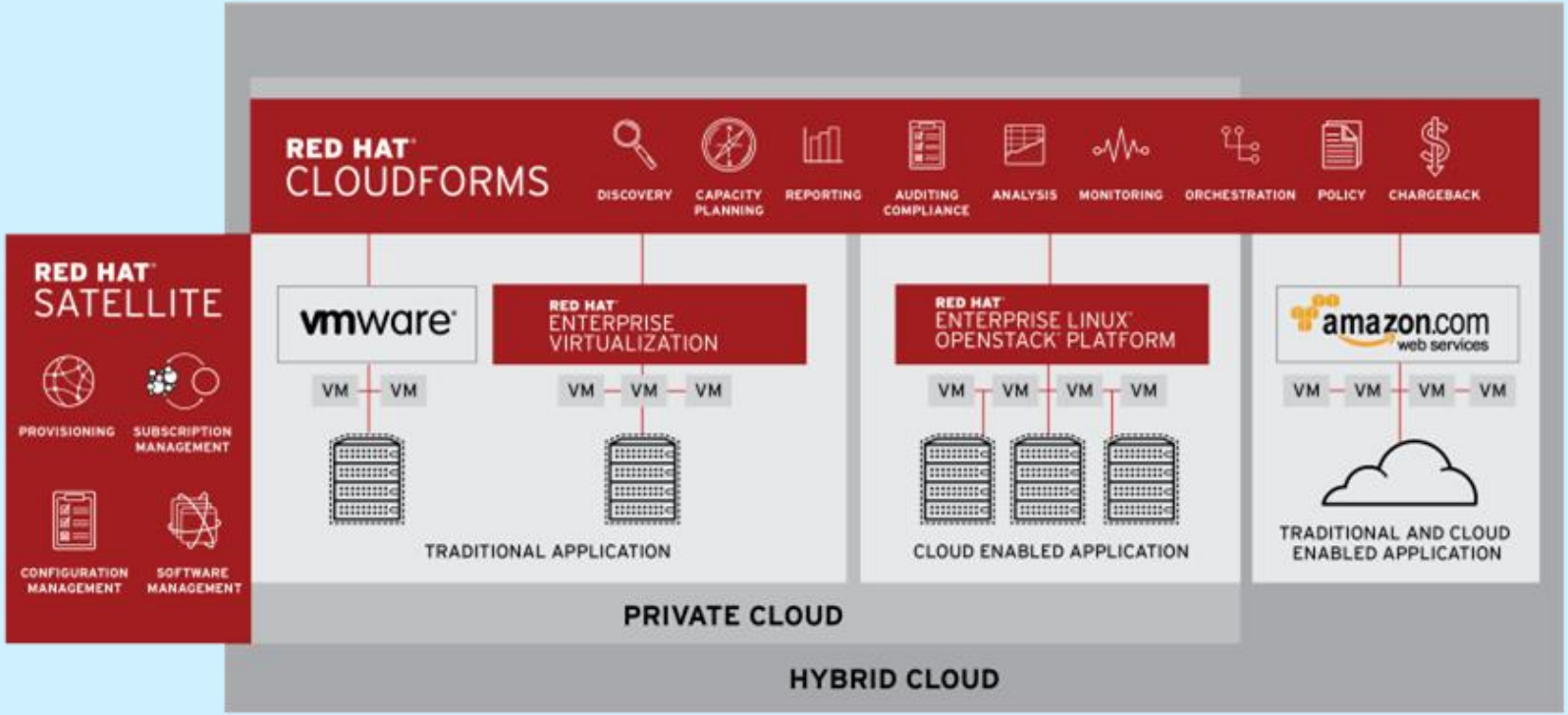
RHCI received:

+ The highest score in the "Strategy" section
+ The second-highest score in the "Current Offering" section

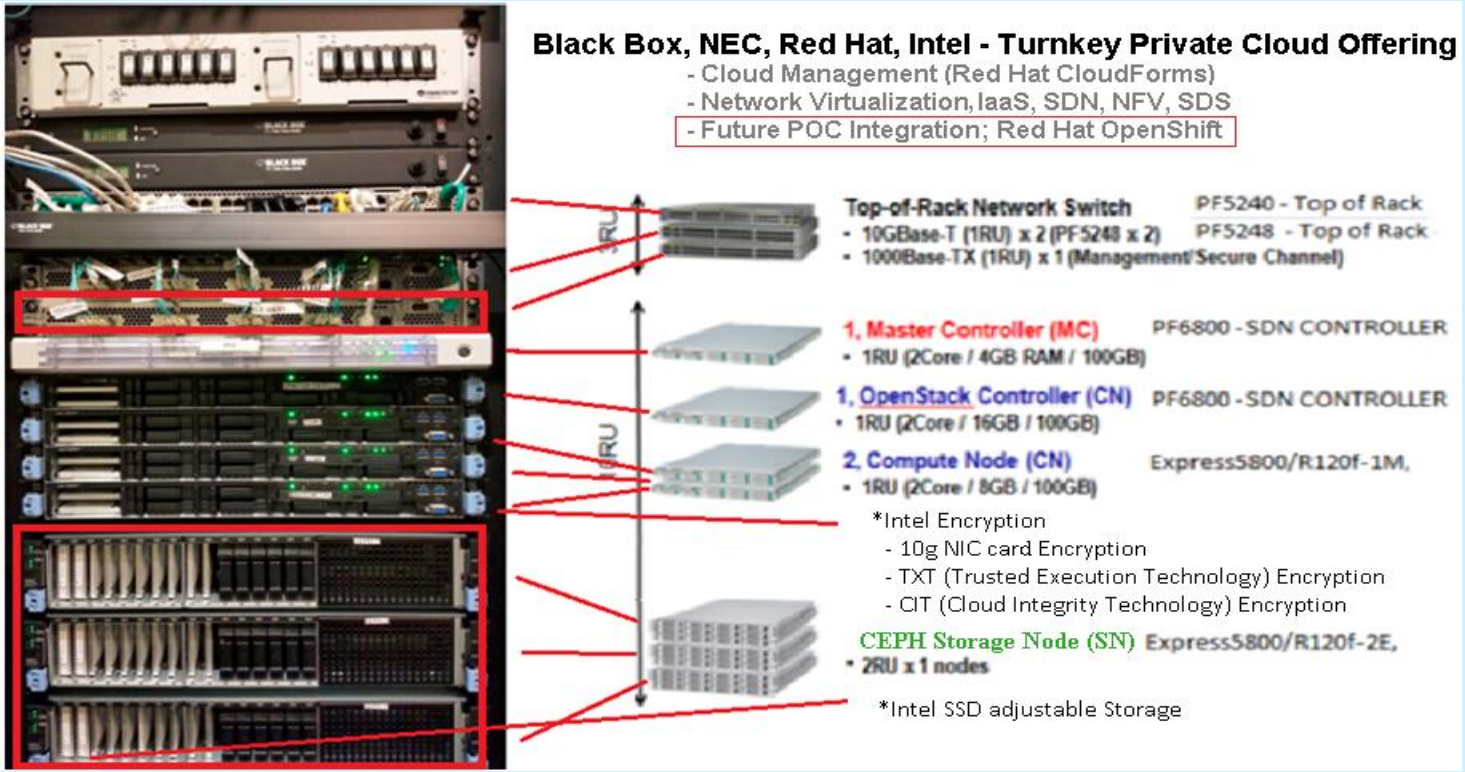
"Red Hat.. leads the evaluation with its powerful portal, top governance capabilities and a strategy built around integration, open source, and interoperability."

Red Hat Cloud Infrastructure

Cloud Management - Alternative Virtualization - OpenStack



NEC/Black Box Solution Stack



NEC/BLack Box Solution Stack - Value

Collectively we are delivering a highly performant, secure hyper-converged infrastructure appliance that is built for web-scale environments with NexGen technology in OpenSource environment.

- Provide a comprehensive cloud management tool that allows management, metering and charge-back for bi-modal (traditional mode-1 and agile, web-scale mode-2) environments; across on-premise private cloud as well as lower security public cloud offerings from Amazon and Microsoft.
- Provide agility and flexibility to the data center resources with the ability to dynamically reallocate resources with respect to compute, storage and networking.
- Ability to replace expensive legacy high-end networking and storage with cost effective infrastructure at a fraction of the price without sacrificing the intelligence and benefits.
- Support for Multi-Layer Security in a multi tenant cloud

Cloud Service Models

FedRAMP

arcp AUTONOMIC RESOURCES CLOUD PLATFORM

arcWRX

arcWRX

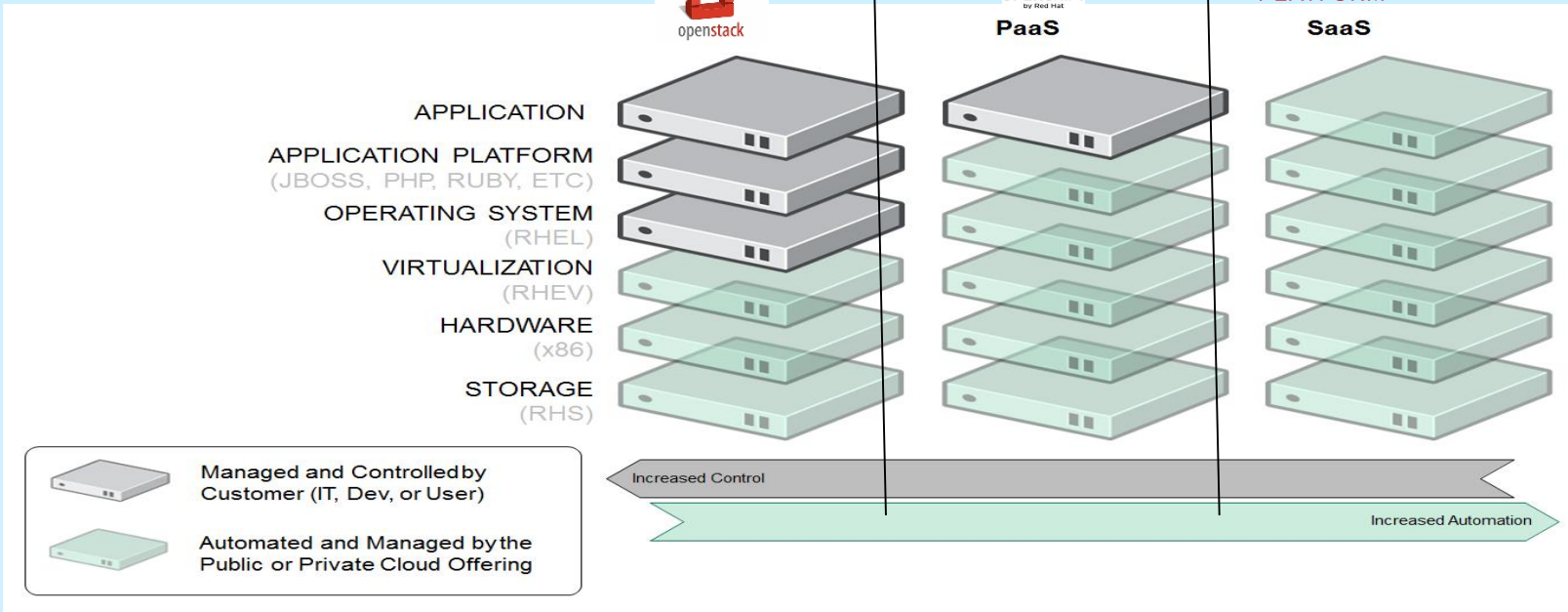
redhat openstack

OPENSHIFT by Red Hat

RED HAT MOBILE APPLICATION PLATFORM

PaaS

SaaS



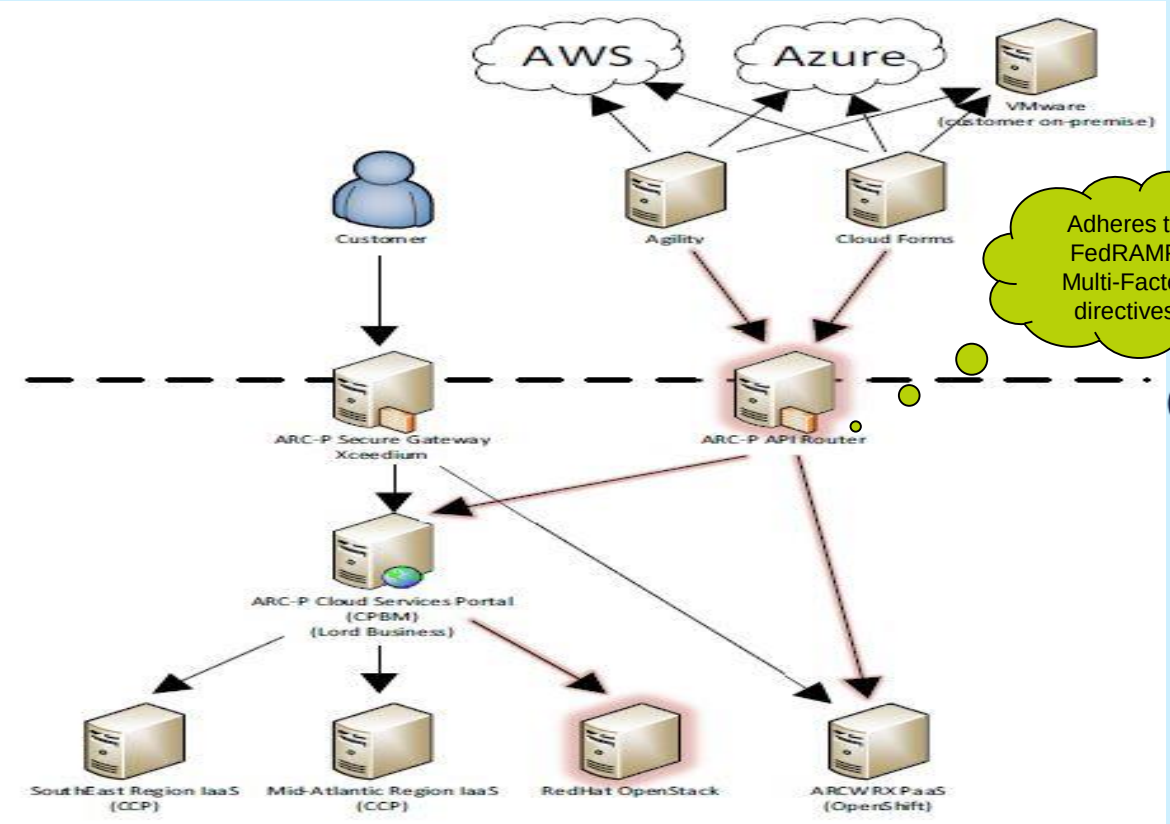
redhat intel

DoD Security Requirements Guidelines Summary

	Required		Controls that mission owners may add		
NIST Moderate	+ 260	= 260			
FedRAMP Moderate	+ 65	= 325			
DOD Impact Level 2	+ 0	= 325			
DOD Impact Level 4	+ 35	= 360	9 NIST	TBD	Privacy Overlay if required (not released)
DOD Impact Level 5	+ 9	= 369	12 NIST	TBD	Privacy Overlay if required (not released)
DOD Impact Level 6	+ 0	= 369	11 NIST	98	Controls from the Classified Privacy Overlay if required

ARC-P runs at FISMA High with 412 Security Controls in place

Solution Stack - ARC-P Cloud Brokering Options



redhat. intel

Solution Stack Highlights

- Adding Red Hat OpenStack to ARC-P FedRAMP FISMA High Baseline ATO (with reciprocity to DoD Impact Level 4 or 5)
- Utilizing Intel TXT Technology
- Utilizing CEPH, OSP Director, and Red Hat Linux 7
- To be added to cloud service offerings of CSRA on all contracts/bids
- To be in Private IaaS mode, each customer sets up the way they need
- Possible Ansible as a Service add-on
- Deployed in Government Private (off premise) Cloud or ARC-P on Premise

Summary

Cloud Security begins with trust and visibility enabled by hardware and delivered by the infrastructure
- Intel is driving hardware assisted security into the ecosystem of OEMs, ISVs, and CSPs
- Red Hat delivers platform and solutions for private, hybrid, and public cloud

The risks and threats to the Cloud can be mitigated and managed
- But it takes an ecosystem of software, hardware, and service providers

Call to Action

Work with your vendors and CSPs
- Require security and trust for your workloads and data
- Require visibility and the necessary feeds and monitoring to achieve compliance
- For Private and Hybrid use cases, implement your policies for workload and data protection/control and then enforce them via orchestration
- Make platform/HW trust a requirement on your service providers and supply chain

Verify, then Trust, then Verify again
- Validate that controls are configured correctly and generating the necessary ‘evidence’ (logs, reports, attestation of trust, ...)
- Continuously validate trust level and residency

Q & A