#RSAC

RSAConference2017

San Francisco | February 13 – 17 | Moscone Center

SESSION ID: TECH-F02

Integrated Solutions for Trusted Clouds and SDI

Steve Orrin
Federal Chief Technologist
Intel Corp

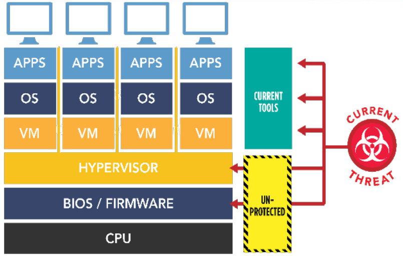
Shawn Wells
Chief Security Strategist
Red Hat Public Sector

In the next 45 minutes . . .

- *Modern* challenges for security and compliance in cloud stacks
- Building block technologies: hardware & software
- Step through reference designs
- What's coming next?
  - SDN, SDS, containers, PaaS/SaaS, Audit as a Service
- Demos!

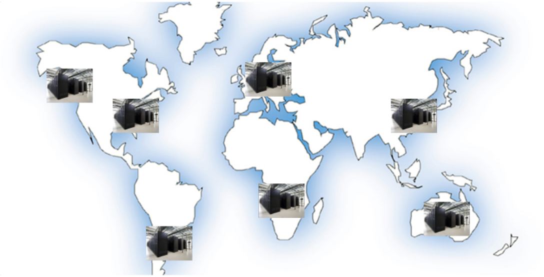
Key Security Challenges

- Attacks on the Infrastructure
- Co-tenancy Threats
- Building & Enforcing Trust



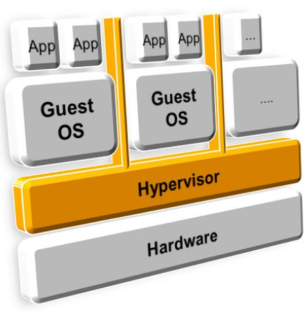
Attacks are moving down in the stack.

How do you establish root of trust in h/w?



No physical boundaries.

Do you know where you workload/data is located?

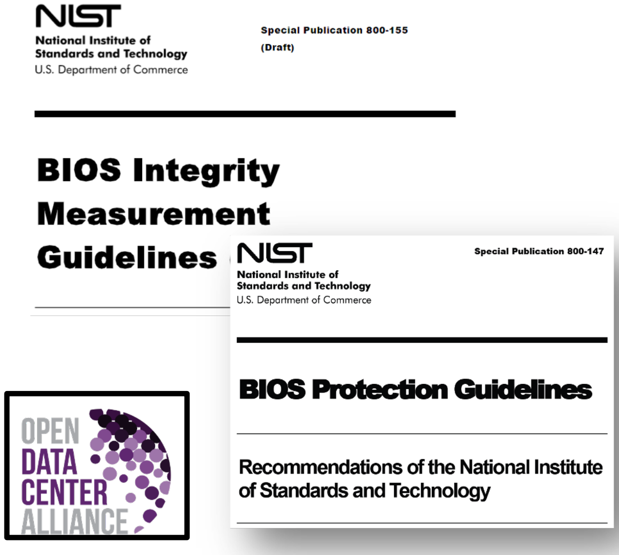


Lack of Visibility to the Integrity of Infrastructure.

How do you know your workloads are running on compliant infrastructure?

Compliance & Regulatory Challenges

- Achieving audit visibility
- Commingled regulatory environments
- Continuous monitoring
- Data use



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

Special Publication 800-155 (Draft)

BIOS Integrity Measurement Guidelines

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

Special Publication 800-147

BIOS Protection Guidelines

Recommendations of the National Institute of Standards and Technology

FedRAMP℠

FDA
21 CFR Part 11

PCI Security Standards Council™

OPEN DATA CENTER ALLIANCE

Science & Technology
Security & Trust

CYBER SECURITY
RESEARCH AND DEVELOPMENT
BROAD AGENCY ANNOUCEMENT (BAA)
BAA 11-02

Published: January 26, 2011

HIPAA
Health Insurance Portability & Accountability Act

enisa
European Network and Information Security Agency

Building Blocks of Trustworthy Clouds

- Create a chain of trust rooted in hardware that extends to include the hypervisor
- Provide visibility for compliance and audit
- Use trust as part of the Policy Management for Cloud Activity
  - Trust as part of the VM Migration and Dynamic Provisioning Policies
- Server tagging for richer policy decisions
- Leverage infrastructure capabilities/services to address data protection requirements

Building Trust & Compliance in the Cloud

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?
- Implement granular controls?
- Audit policy configuration?
- Prove compliance to industry and regulators?

RSA Conference2017

Building Blocks

Building Block Technologies

Hardware

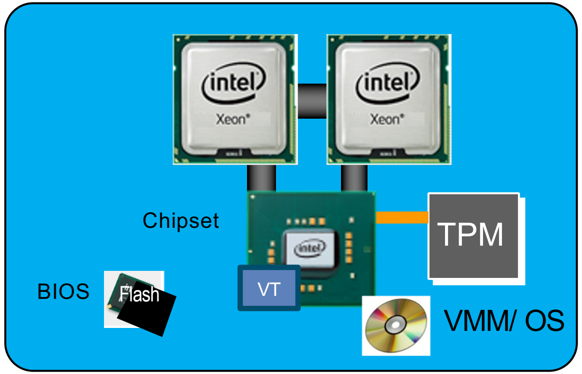
- TXT, AESNI, DRNG, CryptoNI

Software

- Linux, KVM, OpenStack, CloudForms, Ceph, VMWare (VCenter, VSphere, ESXi), OpenCIT, Hytrust, Cloud Raxak

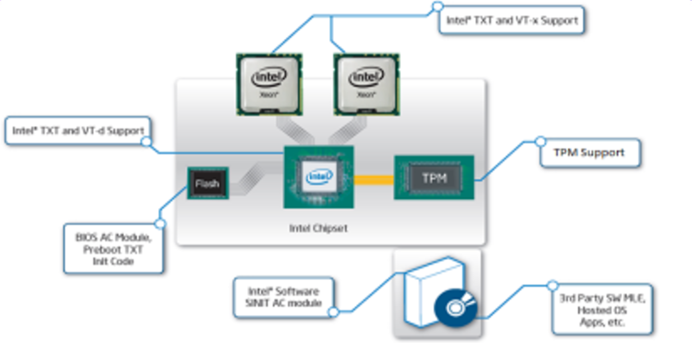
How HW Root of Trust is established

Trusted Execution Technology

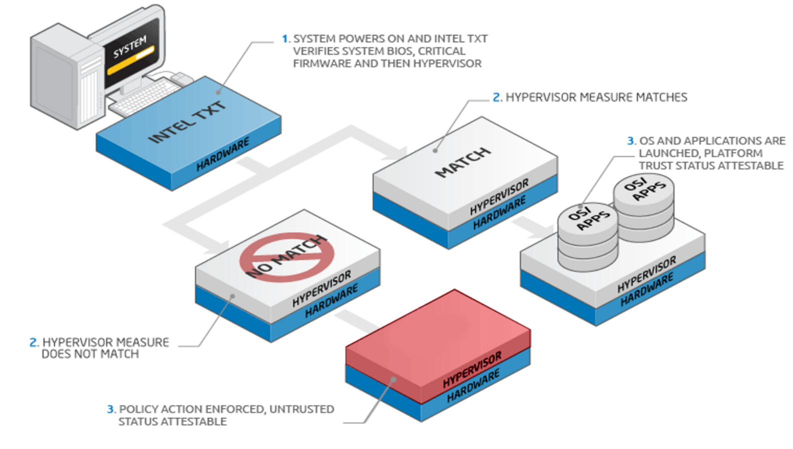


Trusted Launch
Enables isolation and tamper detection at boot-time

Compliance
Hardware-based verification for compliance



Intel® TXT and VT-x Support
Intel® TXT and VT-d Support
TPM Support
Flash
TPM
Intel Chipset
BIOS AC Module, Preboot TXT Init Code
Intel® Software SINIT AC module
3rd Party SW MLE, Hosted OS Apps, etc.



1. SYSTEM POWERS ON AND INTEL TXT VERIFIES SYSTEM BIOS, CRITICAL FIRMWARE AND THEN HYPERVISOR

2. HYPERVISOR MEASURE MATCHES

3. OS AND APPLICATIONS ARE LAUNCHED, PLATFORM TRUST STATUS ATTESTABLE

2. HYPERVISOR MEASURE DOES NOT MATCH

3. POLICY ACTION ENFORCED, UNTRUSTED STATUS ATTESTABLE

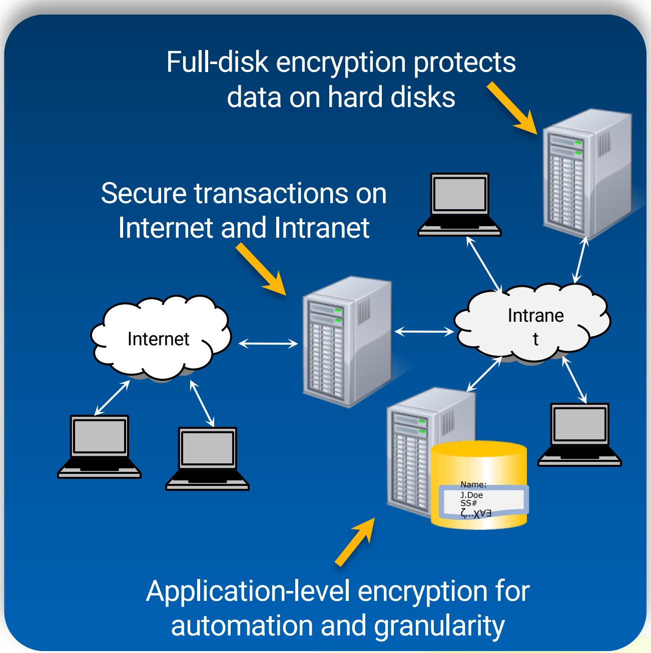
Hardware Features for Data Protection

AES HW Acceleration with AES-NI

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

HW 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



Full-disk encryption protects data on hard disks

Secure transactions on Internet and Intranet

Application-level encryption for automation and granularity

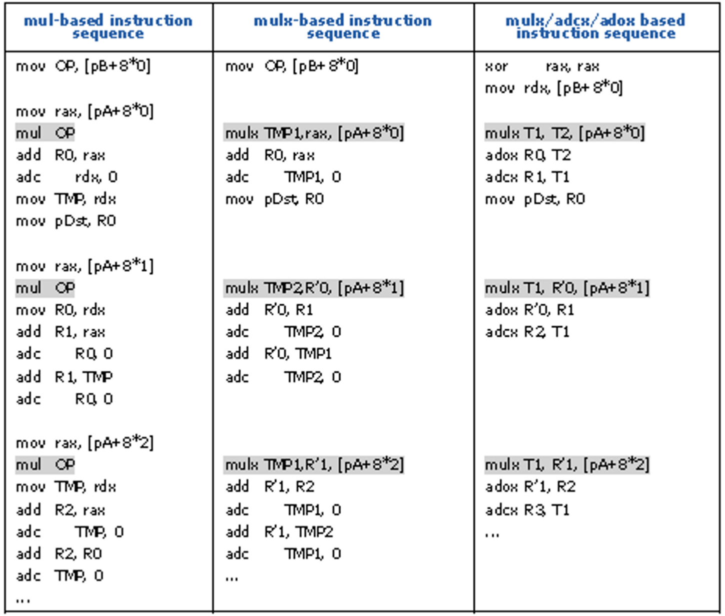
Instructions for Asymmetric Cryptography Acceleration

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



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	mulx TMP1,rax, [pA+8*0]	mulx T1, T2, [pA+8*0]
add R0, rax	add R0, rax	adox R0, T2
adc rdx, 0	adc TMP1, 0	adcx R1, T1
mov TMP, rdx	mov pDst, R0	mov pDst, R0
mov pDst, R0		
mov rax, [pA+8*1]		
mul OP	mulx TMP2,R’0, [pA+8*1]	mulx T1, R’0, [pA+8*1]
mov R0, rdx	add R’0, R1	adox R’0, R1
add R1, rax	adc TMP2, 0	adcx R2, T1
adc R0, 0	add R’0, TMP1	
add R1, TMP	adc TMP2, 0	
adc R0, 0		
mov rax, [pA+8*2]		
mul OP	mulx TMP1,R’1, [pA+8*2]	mulx T1, R’1, [pA+8*2]
mov TMP, rdx	add R’1, R2	adox R’1, R2
add R2, rax	adc TMP1, 0	adcx R3, T1
adc TMP, 0	add R’1, TMP2	…
add R2, R0	adc TMP1, 0	
adc TMP, 0	…	
…		

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

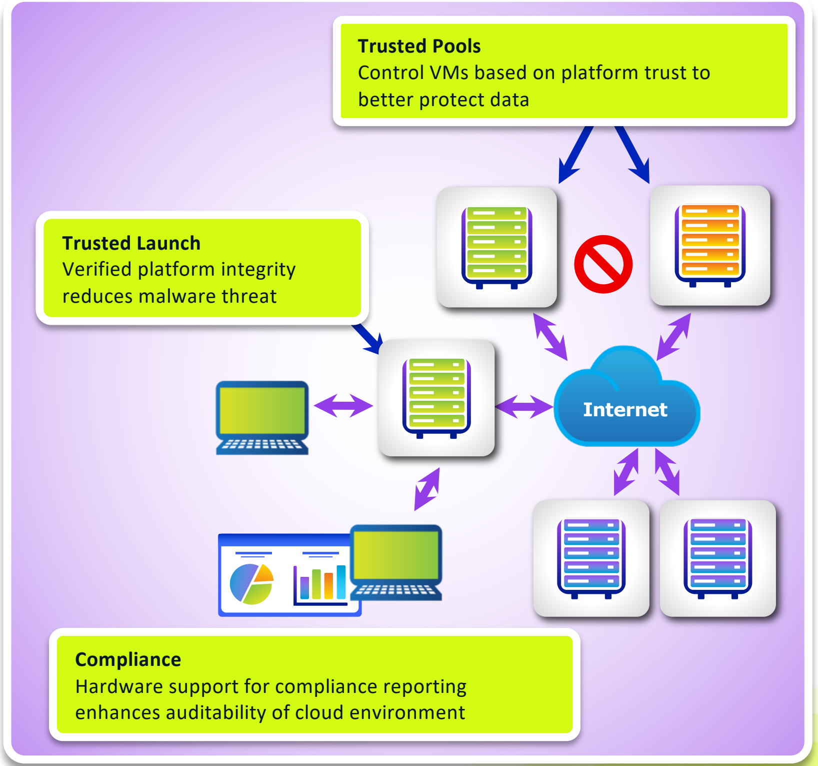
Trusted Compute Pools

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



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

OpenCIT (Open Cloud Integrity Technology)

Platform Trust, Trusted Compute Pools

- Uses Intel’s TXT and the Platform’s 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 at https://01.org/opencit
- Delivered via OpenStack or integrated into Policy & Compliance products, e.g. HyTrust Cloud Control

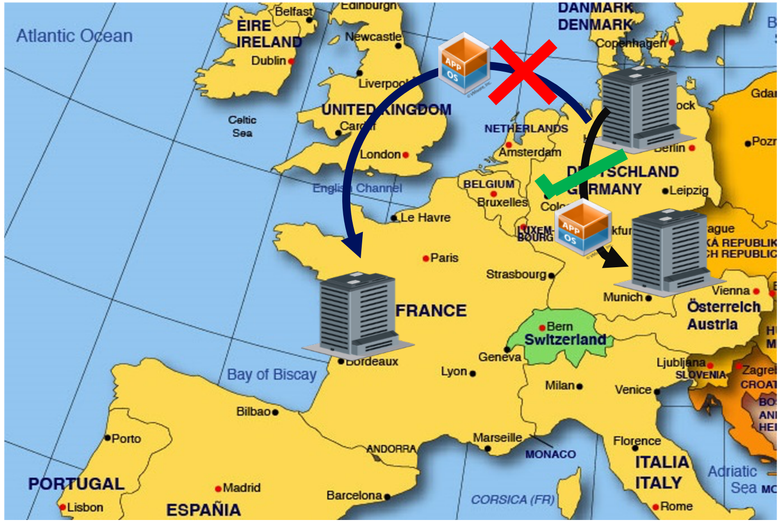
Use Model 1: Trusted Launch
Attestation provides information about platform trust to improve response to malware threats

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

OpenCIT (Open Cloud Integrity Technology)

Trusted Location and Boundary Control



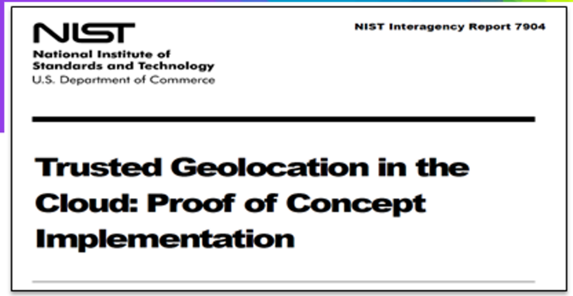
Addresses top cloud concerns:

- 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

Attested Server Tagging & Trusted Geo-location in the Cloud

- Many Trusted Compute Pools use cases 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)



NIST

National Institute of Standards and Technology

U.S. Department of Commerce

NIST Interagency Report 7904

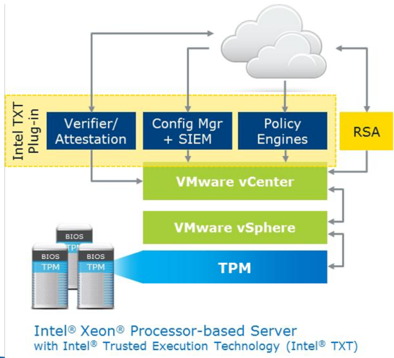
Trusted Geolocation in the Cloud: Proof of Concept Implementation

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

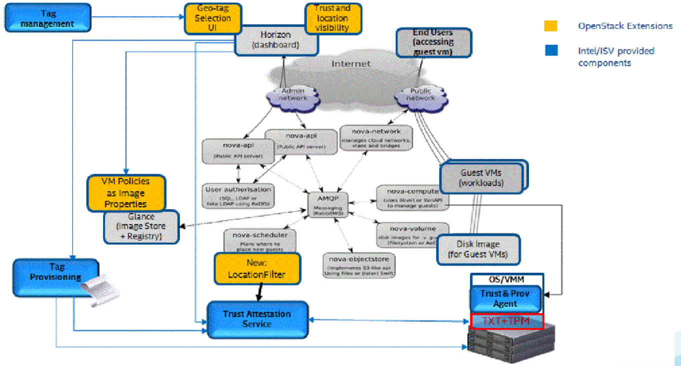
- **Trusted resource pool <u>based on hardware-based secure technical measurement capability</u>**
  - **Platform attestation and safer hypervisor launch** - Provide integrity measurement and enforcement for the compute nodes
  - **Trust-based secure migration** - Provide geolocation measurement and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

VMware Based



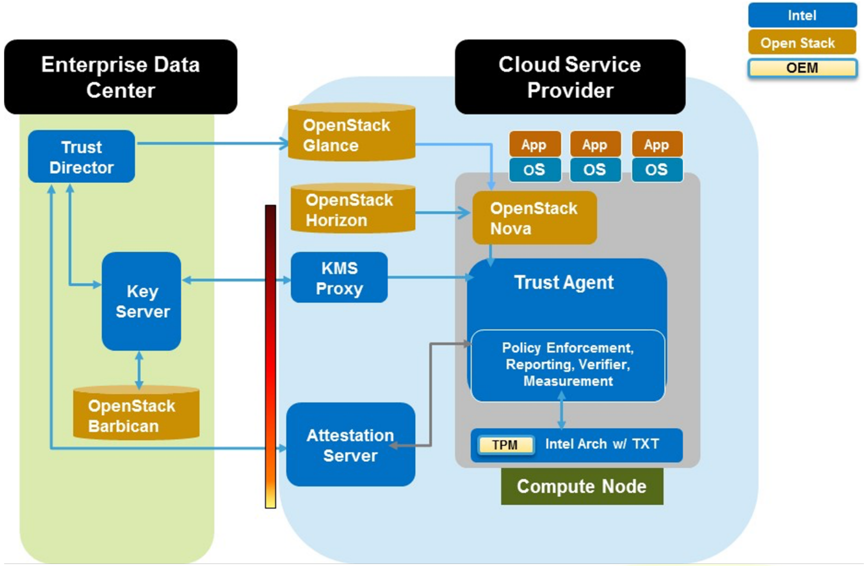
OpenStack Based


Tag management
Geo-tag Selection UI
Trust and location visibility
Horizon (dashboard)
End Users (accessing guest vm)
Internet
Admin network
Public network
nova-api (Public API server)
nova-api (Public API server)
nova-network manages cloud networks, vlans and bridges
Guest VMs (workloads)
VM Policies as Image Properties
Glance (Image Store + Registry)
User authorisation (SQL, LDAP or fake LDAP using ReDIS)
AMQP Messaging (RabbitMQ)
nova-compute (uses libvirt or XenAPI to manage guests)
nova-volume disk images for v. gu (filesystem or AoE)
nova-scheduler Plans where to place new guests
New: LocationFilter
nova-objectstore (implements S3-like api Using Files or (later) Swift
Disk Image (for Guest VMs)
Tag Provisioning
Trust Attestation Service
OS/VMM
Trust & Prov Agent
TXT+TPM
OpenStack Extensions
Intel/ISV provided components

OpenCIT (Open Cloud Integrity Technology)

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



Trusted Compute Pools Industry Support

Server Systems

CISCO · DELL · hp · HITACHI Inspire the Next · HUAWEI · IBM

inspur · lenovo · Empowered by Innovation NEC · Quanta Optimize Your Datacenter · SUPERMICRO

Software and Solutions

CITRIX · HP Helion · HYTRUST Cloud Under Control · Linux · M2Mi Machine-to-Machine Intelligence Corporation

McAfee · openstack CLOUD SOFTWARE · intel · Piston CLOUD COMPUTING · privatecore · BLACK BOX NETWORK SERVICES

redhat · RSA The Security Division of EMC · CLOUD RAXAK · ScienceLogic

SUSE · Symantec · TEAMSUN 华胜天成 · TRAPEZOID Cloud Visibility Empowered · ubuntu

UOL DIVEO muito além da infraestrutura FULL IT OUTSOURCING · VCE · virtustream · vmware · Xen Server

Products and Solution Providers

DUPONT · FLORIDA CRYSTALS · TAIWAN STOCK EXCHANGE · GOODYEAR ENGINEERED PRODUCTS · VEYANCE TECHNOLOGIES

DuPont deployed Intel TXT to ensure that the computing pools remained trusted, based on the original configurations across both Linux and Windows operating environments.

"Security in the cloud is paramount and Virtustream has adopted some of Intel technologies around security including Intel TXT." Don Whittington, VP & CIO, Florida Crystals

…address TWSE's business needs and increase the overall trust and security of its cloud infrastructure using Intel TXT and solutions from Cisco, HyTrust, McAfee and VMware.

"Hardware-enhanced security provided by Intel TXT is critical to protect our sensitive data and was key in our selection of Virtustream for cloud services." Joh F. Hill, CIO, Veyance Technologies

HP Helion · SOFTLAYER an IBM Company · virtustream

CSRA · Piston CLOUD COMPUTING · UOL DIVEO muito além da infraestrutura FULL IT OUTSOURCING

Customers

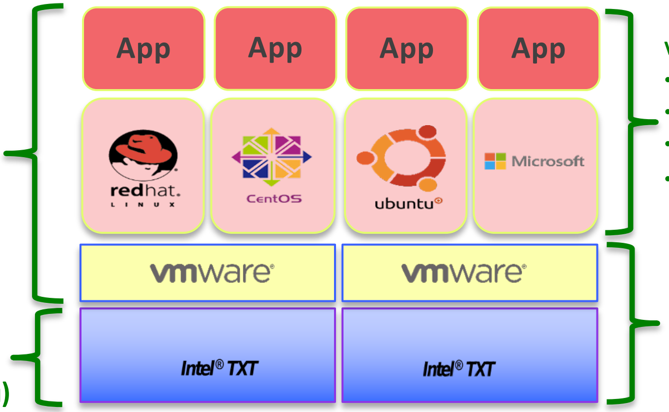
RSAConference2017

Reference Designs

Real World Solutions

- Private Cloud Implementations
  - VMWare + Intel + HyTrust
  - Intel + Red Hat (RHEL/OpenStack/CloudForms/Ceph)
- Commercial Solution Providers (CSP's)
  - IBM Softlayer (w/VMWare + Intel + HyTrust)
  - CSRA (w/Intel + Red Hat)
- Hyper Converged Secure SCI
  - BlackBox + NEC + Red Hat + Intel

Intel + Vmware + HyTrust : Secure Private/Hybrid Cloud



vmware

Hardware with:

- Root-of-Trust (TXT)
- Crypto acceleration (AES-NI)

HYTRUST DataControl™

VM and Data Encryption with:

- Fully automatic key management
- Zero-downtime encryption/rekey
- HW-speed crypto (using Intel AES-NI)
- Boundary controlled decryption (using Intel TXT)

HYTRUST CloudControl

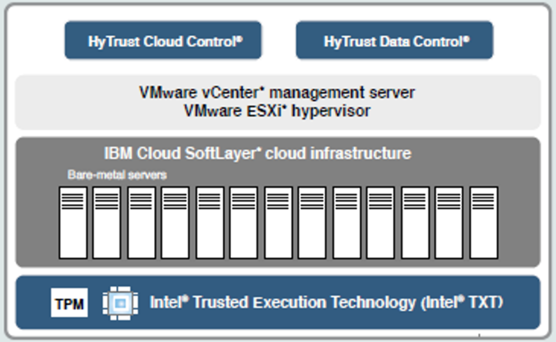
Policy-based controls with:

- Secure Governance of V-Admins
- V-Infrastructure hardening
- Compliance logging and full audit
- Physical host trust-attestation
- Geo and logical boundary enforcement (using Intel TXT)

The Road to a Secure, Compliant Cloud

A trusted infrastructure with a solution stack from Intel®, IBM Cloud SoftLayer, VMware, and HyTrust

Elements of a trusted cloud infrastructure



HyTrust Cloud Control®

HyTrust Data Control®

VMware vCenter* management server
VMware ESXi* hypervisor

IBM Cloud SoftLayer* cloud infrastructure

Bare-metal servers

TPM

Intel® Trusted Execution Technology (Intel® TXT)

Establish policies, auditing, reporting; and perform encryption

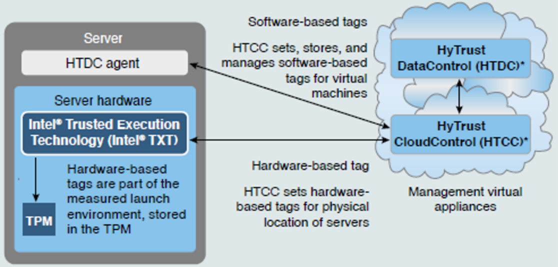
Manages virtual machines and ESXi hosts

Allows user to install their own operating systems, hypervisors, applications as needed

Enables trust from the hardware level up

- Intel® Xeon® processors
- Intel® Trusted Execution Technology (Intel® TXT)
- Trusted Platform Module (TPM) 1.2
- Intel® Advanced Encryption Standard - New Instructions (Intel® AES-NI)
- IBM Cloud SoftLayer (SoftLayer)* bare-metal servers
- VMware vCenter* management server
- VMware ESXi* hypervisor (the virtualization OS)
- HyTrust CloudControl (HTCC)*
- HyTrust DataControl (HTDC)*

Measurements of launch environment are stored in hardware



Server

HTDC agent

Server hardware

Intel® Trusted Execution Technology (Intel® TXT)

TPM

Hardware-based tags are part of the measured launch environment, stored in the TPM

Software-based tags

HTCC sets, stores, and manages software-based tags for virtual machines

Hardware-based tag

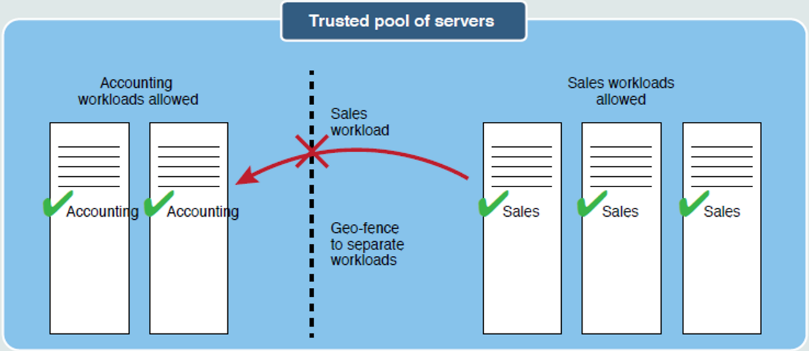
HTCC sets hardware-based tags for physical location of servers

HyTrust DataControl (HTDC)*

HyTrust CloudControl (HTCC)*

Management virtual appliances

Geo-fencing: Restrict workloads to specific servers within a trusted pool



Trusted pool of servers

Accounting workloads allowed

✓ Accounting

✓ Accounting

Sales workload

Geo-fence to separate workloads

Sales workloads allowed

✓ Sales

✓ Sales

✓ Sales

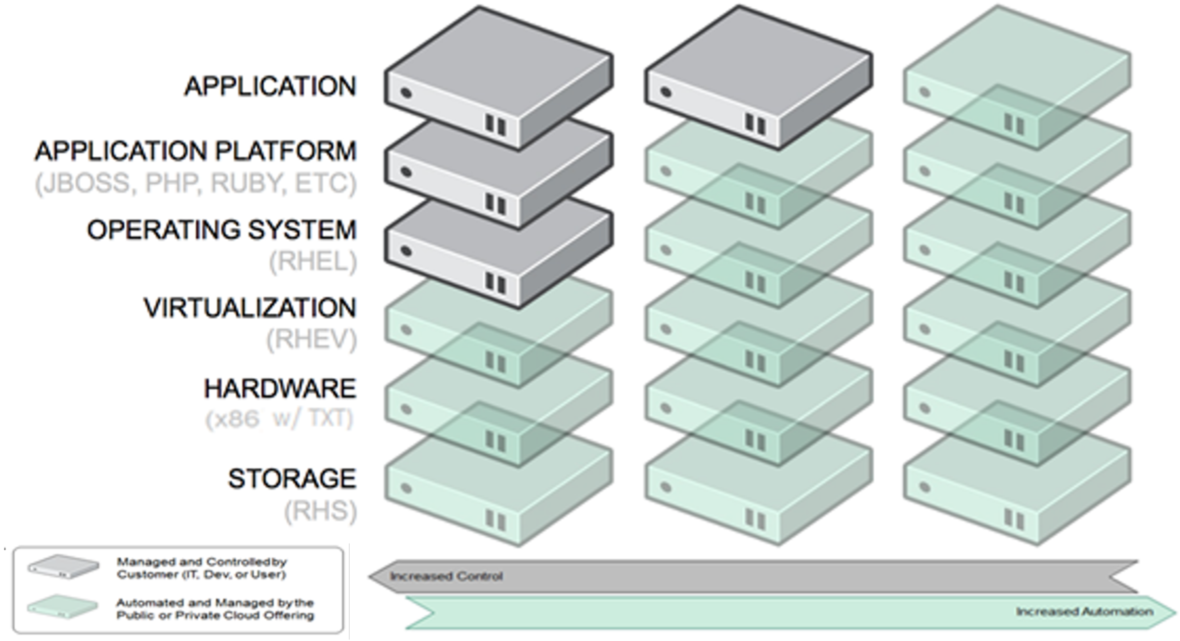
Trusted Cloud as a Service (Public Cloud)

FedRAMP

IaaS

PaaS

SaaS



APPLICATION

APPLICATION PLATFORM
(JBOSS, PHP, RUBY, ETC)

OPERATING SYSTEM
(RHEL)

VIRTUALIZATION
(RHEV)

HARDWARE
(x86 w/ TXT)

STORAGE
(RHS)

Managed and Controlledby Customer (IT, Dev, or User)

Automated and Managed bythe Public or Private Cloud Offering

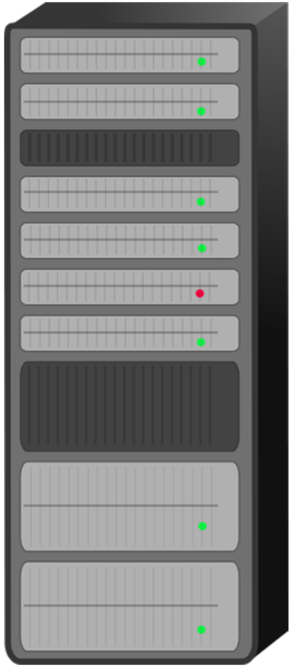
Increased Control

Increased Automation

Hyper-Converged Secure Private Cloud Stack

Collectively 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



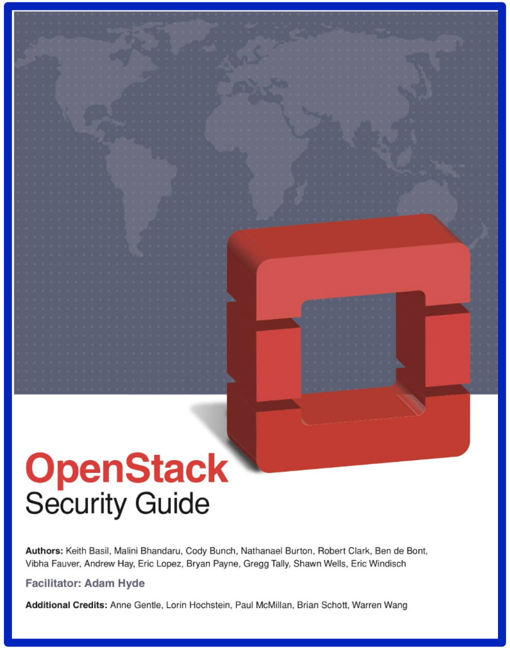
- ToR Switch and Networking
- SDN Controller

- Red Hat CloudForms
- RHEL OpenStack Controller
- Intel CIT
- Compute Nodes
  - 10 Gig NIC
  - Intel TXT w/TPM
  - Intel AESNI & CryptoNI

- CEPH Storage
  - Intel SSDs

Demos!

Demo #1: Automated Security Scanning



OpenStack
Security Guide

Authors: Keith Basil, Malini Bhandaru, Cody Bunch, Nathanael Burton, Robert Clark, Ben de Bont, Vibha Fauver, Andrew Hay, Eric Lopez, Bryan Payne, Gregg Tally, Shawn Wells, Eric Windisch

Facilitator: Adam Hyde

Additional Credits: Anne Gentle, Lorin Hochstein, Paul McMillan, Brian Schott, Warren Wang

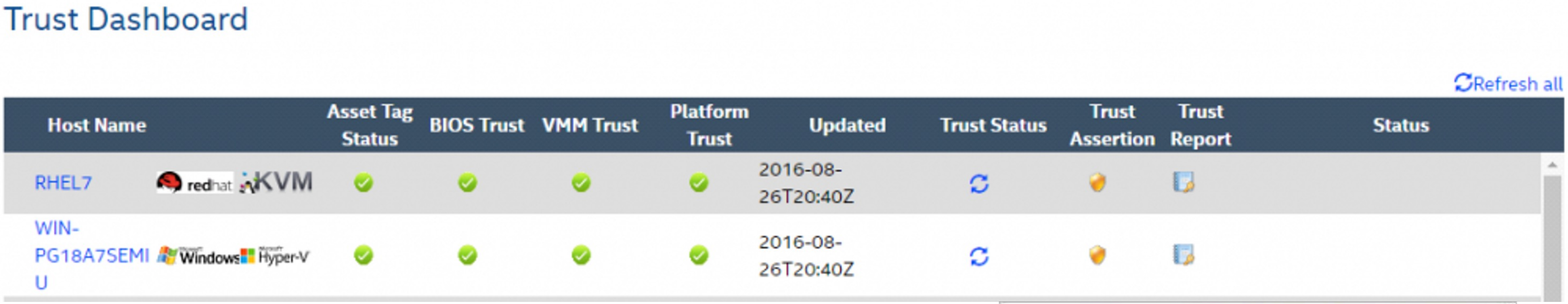
http://docs.openstack.org/sec/

→

OpenSCAP

https://www.open-scap.org/

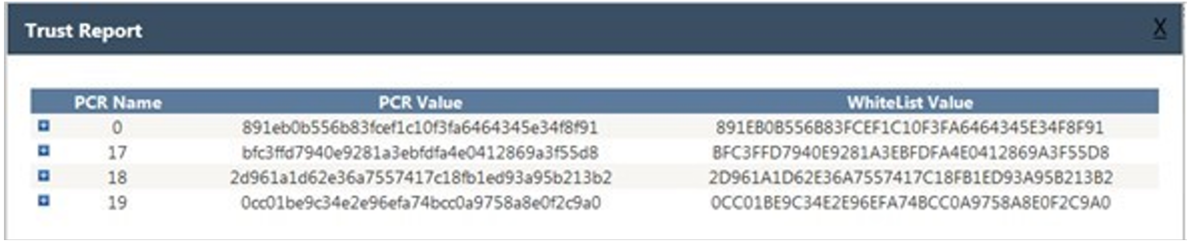
Demo #2: OpenCIT (1 / 2)



Trust Dashboard

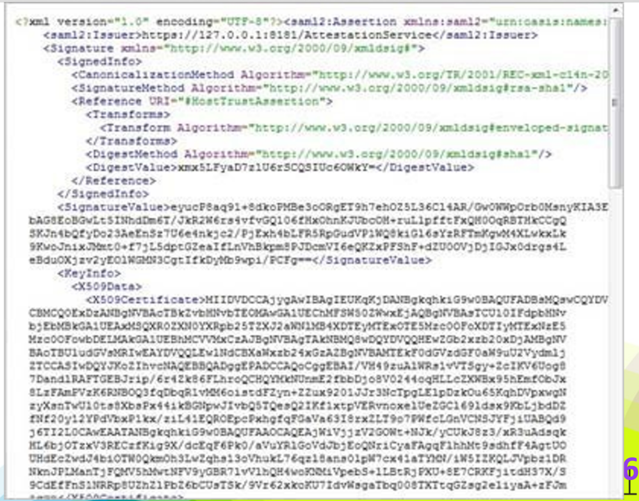
Refresh all

Host Name		Asset Tag Status	BIOS Trust	VMM Trust	Platform Trust	Updated	Trust Status	Trust Assertion	Trust Report	Status
RHEL7	redhat KVM	✓	✓	✓	✓	2016-08-26T20:40Z				
WIN-PG18A7SEMIU	Windows Hyper-V	✓	✓	✓	✓	2016-08-26T20:40Z				



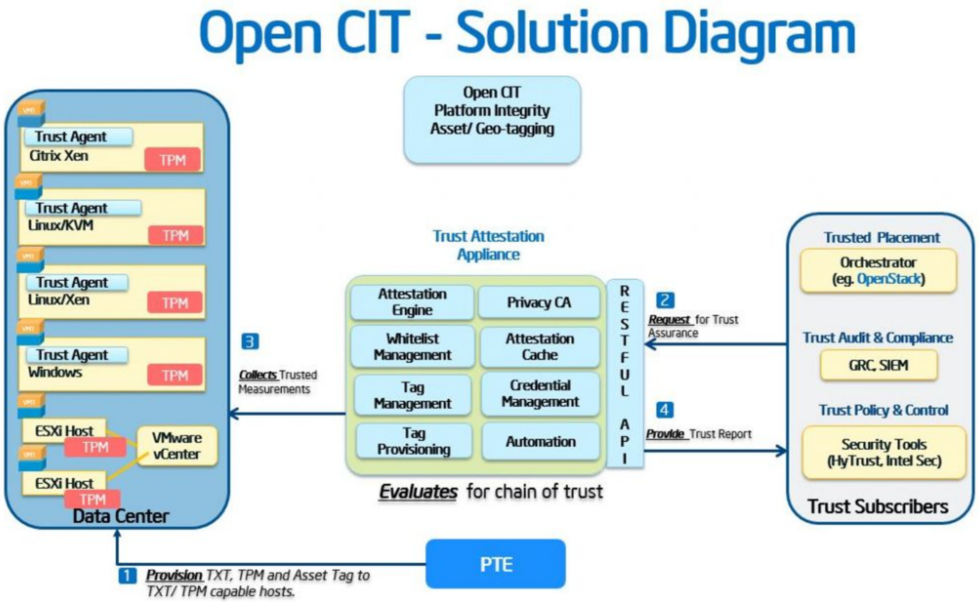
Trust Report X

	PCR Name	PCR Value	WhiteList Value
⊞	0	891eb0b556b83fcef1c10f3fa6464345e34f8f91	891EB0B556B83FCEF1C10F3FA6464345E34F8F91
⊞	17	bfc3ffd7940e9281a3ebfdfa4e0412869a3f55d8	BFC3FFD7940E9281A3EBFDFA4E0412869A3F55D8
⊞	18	2d961a1d62e36a7557417c18fb1ed93a95b213b2	2D961A1D62E36A7557417C18FB1ED93A95B213B2
⊞	19	0cc01be9c34e2e96efa74bcc0a9758a8e0f2c9a0	0CC01BE9C34E2E96EFA74BCC0A9758A8E0F2C9A0



```
<?xml version="1.0" encoding="UTF-8"?><saml2:Assertion xmlns:saml2="urn:oasis:names:
    <saml2:Issuer>https://127.0.0.1:8181/AttestationService</saml2:Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <Reference URI="#HostTrustAssertion">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <DigestValue>xmx5LFyaD7z1U6rSCQSIUc6OWkY=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>eyucP8aq91+8dkoPMBe3oORgET9h7ehOZ5L36C14AR/GwOWWpOrb0ManyKIA3E
  bAG8EoBGwLt5INhdDm6T/JkR2W6rs4vfvGQ106fMxOhnKJUboOM+ruLlpfftFxQM0OqRBTMkCCgQ
  SKJn4bQfyDo23AeEnSz7U6e4nkjc2/PjExh4bLFR5RpGudVP1WQ8kiGl6sYzRFTmKgwM4XLwkxLk
  9KwoJnixJMmt0+f7jL5dptGZeaIfLnVhBkpm8PJDcmVI6eQKZxPFShF+dZU0OVjDjIGJx0drgs4L
  eBduOXjzv2yEO1WGMN3CgtIfkDyMb9wpi/PCFg==</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509Certificate>MIIDVDCCAjygAwIBAgIEUKqKjDANBgkqhkiG9w0BAQUFADBaMQswCQYDV
  CBMCQ0ExDzANBgNVBAcTBkZvbHNvbTEOMAwGA1UEChMFSW50ZWwxEjAQBgNVBAsTCU10IFdpbHNv
  bjEbMBkGA1UEAxMSQXR0ZXN0YXRpb25TZXJ2aWNlMB4XDTEyMTExOTE5Mzc0OFoXDTIyMTExNzE5
  Mzc0OFowbDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQ8wDQYDVQQHEwZGb2xzb20xDjAMBgNV
  BAoTBU1udGVsMRIwEAYDVQQLEw1NdCBXaWxzb24xGzAZBgNVBAMTEkF0dGVzdGF0aW9uU2Vydmlj
  ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI/VH49zuA1WRs1vVT5gy+ZcIKV6Uog8
  7Dand1RAFTGEBJrip/6r4Zk86FLhroQCHQYMkNUnmE2fbbDjo8V0244oqHLLcZXWBx95hEmfObJx
  8LzFAmPVzK6RNBOQ3fqDbqR1vMM6oistdFZyn+ZZux9201JJr3NcTpgLElpDzkOu65KqhDVpxwgN
  zyXsnTwU10ts8XbsPx44ikBGNpwJIvbQ5TQesQ2IKf1xtpVERvnoxelUeZGCl691dsx9KbLjbdDZ
  fNf20y12YPdVbxP1kx/ziL41EQROEpcPxhgfqFGaVa63I8rxZLT9o7PWfcLGnVCNSJYFjiUABQd9
  j6TI2L0CAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAjWiVjjzV2GOWt+NJk/yCUkJ8z3/xR3uAdsqk
  HL6bjOTzxV3RECzfKig9X/dcEqF6Pk0/aVuYR1GoVdJbjEoQNriCyaFAgqF1hhMt9sdhfF4AgtUO
  UHdEcZwdJ4biOTW0QkmOh3LwZqhs13oVhukL76qzl8ans0lpW7cx41aTYMN/iW5IZKQLJVpbz1DR
  NknJPLManTjFQMV5hMwtNFV9yGBR71vVlhQH4woKNMiVpebS+lLBtRjPXU+8E7CRKFjitdH37X/S
  9CdEfFnS1NRRp8UZhZ1PbZ6bCUsTSk/9Vr62xkoKU7IdvWsgaTbq008TXTtqGZsg2eliyaA+zFJm
```

Demo #2: OpenCIT (2 / 2)

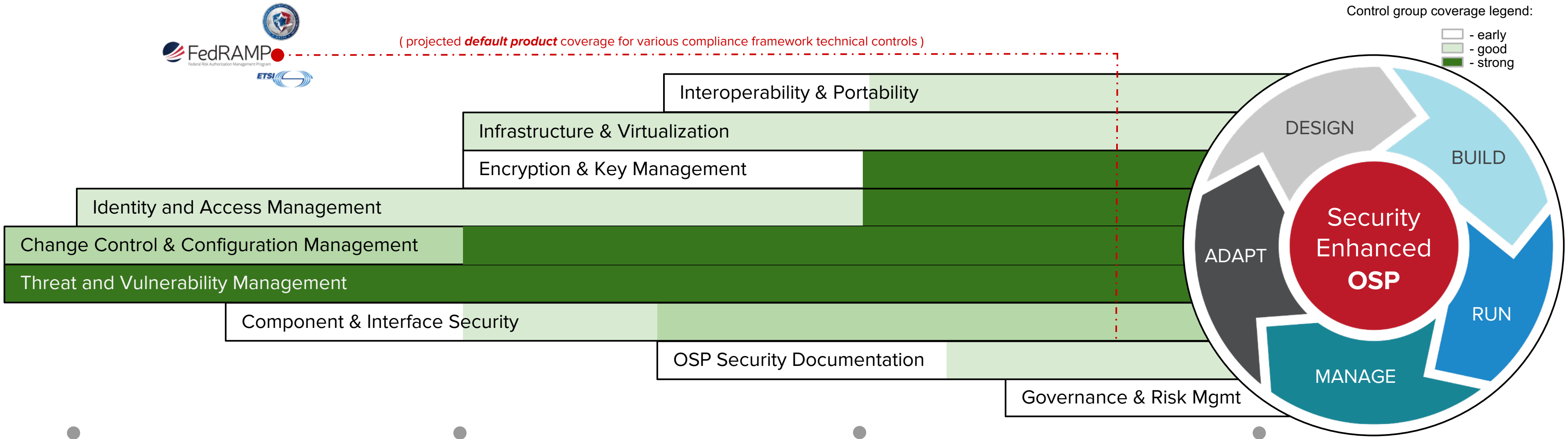


Key Features

- Establish chain of trust of BIOS, firmware, OS kernel & hypervisor by verifying against configured good values (whitelists)
- Ability to tag/verify hosts with custom attributes stored in TPM
- OpenStack & VMWare integration
- Mutual SSL authentication
- RESTful API
- User defined TLS policies

Roadmap

Roadmap: Security Enhanced OpenStack



FedRAMP

ETSI

(projected ***default product*** coverage for various compliance framework technical controls)

Control group coverage legend:

- ☐ - early
- 🟩 - good
- ■ - strong

Interoperability & Portability

Infrastructure & Virtualization

Encryption & Key Management

Identity and Access Management

Change Control & Configuration Management

Threat and Vulnerability Management

Component & Interface Security

OSP Security Documentation

Governance & Risk Mgmt

10 Newton

- TLS/SSL for external services
- Fernet token support
- Maturing Single Sign On
- Domain focused & implied roles

11 Ocata

- More coverage of TLS/SSL for internal services
- Maturing Federation services

12 Pike

- Barbican [fully supported]
- Custodia [TP[1]]
- Cinder encrypted volumes
- Infrastructure & virtualization hardened images

13 Queen

- CloudForms based Governance and Risk Management
- Attestation/TXT [TP[1]]

Roadmap: Security Enhanced OpenStack

Encryption and Key Management

Barbican - secure storage, provisioning and management of secrets

Foundational for enhanced security

Unblocks security for other components

Will include HSM support long term

Secrets Management

- As a service used by many components, Barbican stores, provisions and manages secrets such as:
  - private keys
  - certificates
  - passwords
  - SSH keys

Secrets Storage

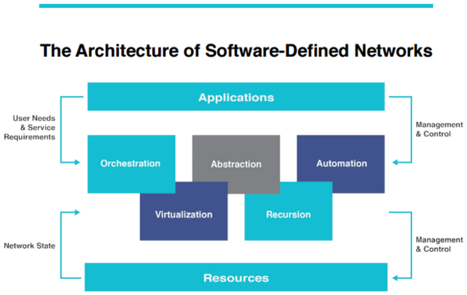
Encryption mechanisms and backends

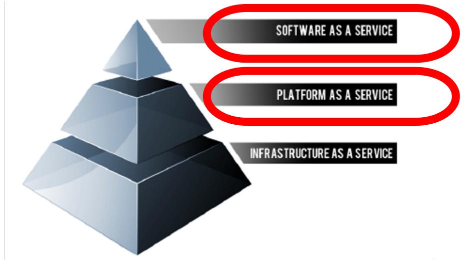
- Network Security Services (NSS) support via Dogtag.
- Network Hardware Security Modules (SafeNet) and Key Management Interoperability Protocol (KMIP) support

What’s coming next

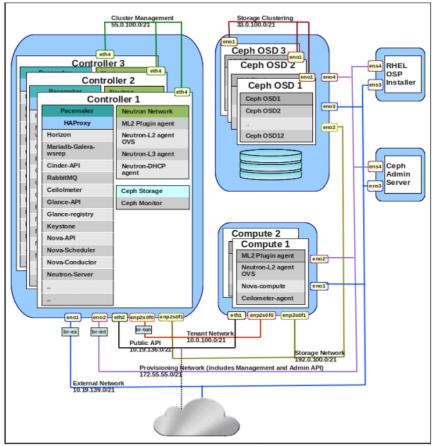
- SDN, SDS, Containers, PaaS/SaaS, Audit as a Service

OPEN NETWORKING FOUNDATION


The Architecture of Software-Defined Networks

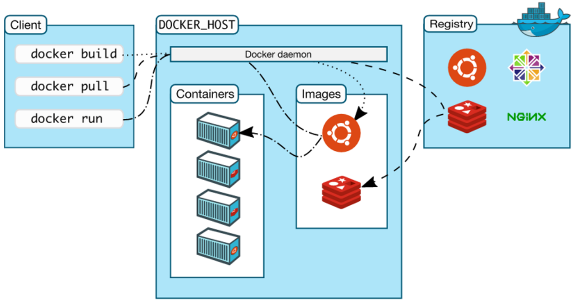


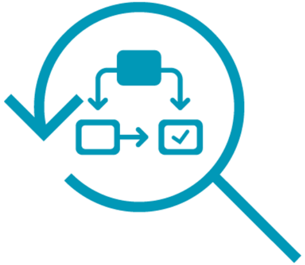
ceph



OpenStack-Ceph Environment

docker





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 enables the technologies in Linux and OpenStack 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

What should be Next?

- What architectures and configurations should Industry tackle next?
- Where else is trust and secure orchestration needed?

Q & A

Contact Us

Steve Orrin
Federal Chief Technologist, Intel Corp
steve.orrin@intel.com

Shawn Wells [LinkedIn]
Chief Security Strategist, Red Hat Public Sector
shawn@redhat.com

Legal Disclaimers

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.
  A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.
- Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.
- The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.
- Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm

Intel, the Intel logo, Intel Xeon, Xeon logo, and the Look Inside. logo 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 © 2017 Intel Corporation. All rights reserved.

Legal Disclaimers - Continued

- Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Go to: Learn About Intel® Processor Numbers http://www.intel.com/products/processor_number
- Some results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- Intel does not control or audit the design or implementation of third party benchmarks or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmarks are reported and confirm whether the referenced benchmarks are accurate and reflect performance of systems available for purchase.
- Relative performance is calculated by assigning a baseline value of 1.0 to one benchmark result, and then dividing the actual benchmark result for the baseline platform into each of the specific benchmark results of each of the other platforms, and assigning them a relative performance number that correlates with the performance improvements reported.
- SPEC, SPECint, SPECfp, SPECrate, SPECpower, SPECjbb, SPECompG, SPEC MPI, and SPECjEnterprise* are trademarks of the Standard Performance Evaluation Corporation. See http://www.spec.org for more information.
- TPC Benchmark, TPC-C, TPC-H, and TPC-E are trademarks of the Transaction Processing Council. See http://www.tpc.org for more information.
- Intel® Advanced Vector Extensions (Intel® AVX)* are designed to achieve higher throughput to certain integer and floating point operations. Due to varying processor power characteristics, utilizing AVX instructions may cause a) some parts to operate at less than the rated frequency and b) some parts with Intel® Turbo Boost Technology 2.0 to not achieve any or maximum turbo frequencies. Performance varies depending on hardware, software, and system configuration and you should consult your system manufacturer for more information.
- No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware and/or software optimized to use the technologies. Consult your system manufacturer and/or software vendor for more information

*Intel® Advanced Vector Extensions refers to Intel® AVX, Intel® AVX2 or Intel® AVX-512. For more information on Intel® Turbo Boost Technology 2.0, visit http://www.intel.com/go/turbo