Defense in Depth

November 13, 2018

redhat.

@RedHatGov

IMPORTANCE OF PLATFORM SECURITY

What are Intel and Red Hat doing to help you secure your systems and infrastructure?

CYBER SECURITY DEFENSE

HOST & SYSTEM SECURITY

NETWORK

DATA & APPLICATIONS

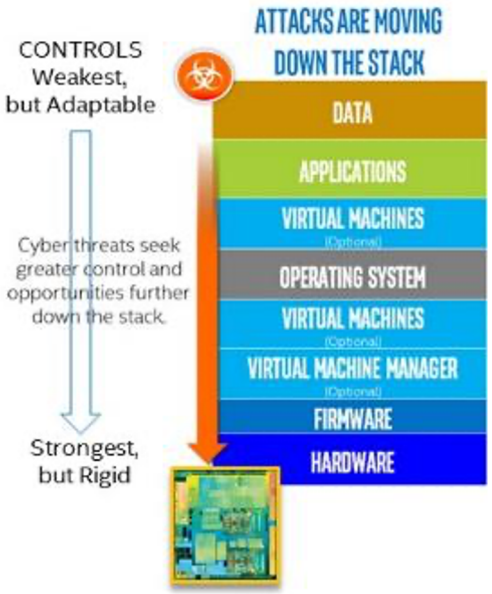
THREAT INTELLIGENCE

IDENTITY & ACCESS

EVOLVING THREAT MODEL

INTEL DRIVES INNOVATION to embed security innovations into hardware, supporting capabilities for more secure devices, operating systems, and applications.

Hardware based security is the next evolution for protection.



SECURING & PROTECTING THE PLATFORM

FIRMWARE	OPERATING SYSTEM	APPLICATIONS	DATA	SECURITY SOFTWARE
• Trusted power on • Safe updates • Secure device provisioning	• Trusted power on • Core operating system file protection • Improved virtualization and container security	• Trusted execution environments • User authentication • Secure key handling	• Faster encryption performance • Secure key storage • Data security and compartment-alization	• Hardened security Functionality • Improved performance • Deeper systems visability

Hardware-embedded controls can make fundamentals of computing more safe, private, secure

VISION FOR PLATFORM SECURITY

TRUSTED EXECUTION ENVIRONMENT	Execution environment isolating operations from manipulation or disclosure	SGX (S/W Guard Extensions)
DEVICE IDENTIFICATION	Provides unique ID for device, can serve as basis for authentication	EPID (Enhanced Privacy ID)
MANAGEMENT	Provides device management, provisioning, policy	- MeshCentral for IoT Gateways - AMT for VPro
VERIFIED BOOT	Verifies boot process, enables s/w identification. Enforces platform boot policies	Secure Boot using TXT and TPM
SECURE STORAGE	Sensitive data protected from misuse or disclosure when in use, transit, storage	- TPM: Trusted Platform Module - PTT: Platform Trust Technology

INTEL SECURITY ESSENTIALS

PLATFORM INTEGRITY

- Intel Platform Protection Technology with Boot Guard
- Intel Platform Protection Technology with OS Guard
- Intel Trusted Execution Technology (TXT)

- Verifies OEM pre-OS boot loader code executing out of reset
- Helps prevent malicious code from executing out of application memory space
- TCG Compliant Secure Boot with attestation

Framework & common root-of-trust security capabilities across Intel processors

INTEL SECURITY ESSENTIALS

TRUSTED EXECUTION

Intel Software Guard Extensions

- Enables creation and use of isolated app enclaves to protect against attacks on executing code or data stored in memory

Intel Virtualization Technology

- Creates firewall between main operating system and secure workloads running inside a secure virtual machine

Framework & common root-of-trust security capabilities across Intel processors

INTEL SECURITY ESSENTIALS

PROTECTED DATA, KEYS, IDENTITY

Intel Platform Trust Technology

- Integrated H/W TPM enables secure storage of keys/credentials, boot block measurements for remote attestation

Intel Enhanced Privacy ID

- Cryptographic scheme provides direct anonymous attestation of hardware for privacy

Framework & common root-of-trust security capabilities across Intel processors

INTEL SECURITY ESSENTIALS

CRYPTO ACCELERATORS

Intel Data Protection Technology with Secure Key

- High entropy source of random numbers to generate keys

Intel Advanced Encryption Standard New Instructions

- Accelerates math calculations for AES-NI encryption

Framework & common root-of-trust security capabilities across Intel processors

WHAT IS PLATFORM SECURITY

SECURE BOOT

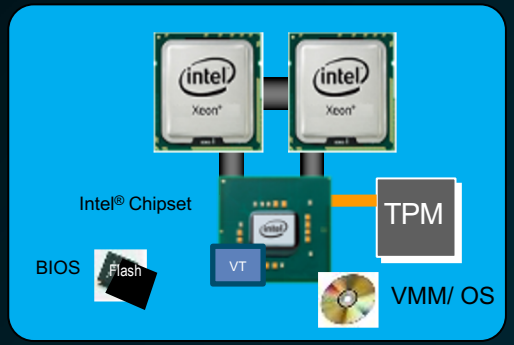
CRYPTO ACCELERATION

ATTESTATION & ASSURANCE

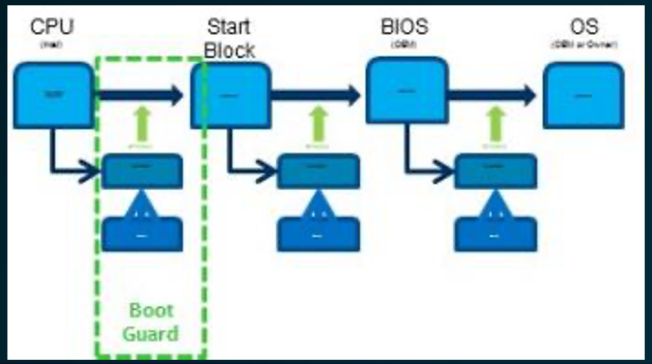
SECURE BOOT

TXT and BootGuard

Trusted Execution Technology



BootGuard



- H/W root of trust for secure boot
- Ability to program OEM root of trust into Field Programmable Fuses (FPF)
- FPF profiles for configuration and tools
- Verified boot or Verified & Measured Boot options
- Ability to use Platform Trust Technology (PTT) or TPM
- Extend chain of trust to hypervisor and VMs
- Local and Remote attestation support

HARDWARE ACCELERATED CRYPTOGRAPHY

AES-NI

UBIQUITOUS DATA PROTECTION WITH CRYPTOGRAPHIC ACCELERATION

AES-NI allows significant performance at a lower price-point with no custom hardware.

DRNG

STRONGER ENCRYPTION WITH ON-BOARD DIGITAL RANDOM NUMBER GENERATOR

High degree of entropy provides quality random numbers for encryption keys and other operations.

DRNG solves the problem of limited entropy in virtual and container platforms.

ADOX/ADX

INSTRUCTION FOR USE IN LARGE INTEGER ARITHMETIC (> 64b)

Common use is Public Key cryptography (e.g. RSA).

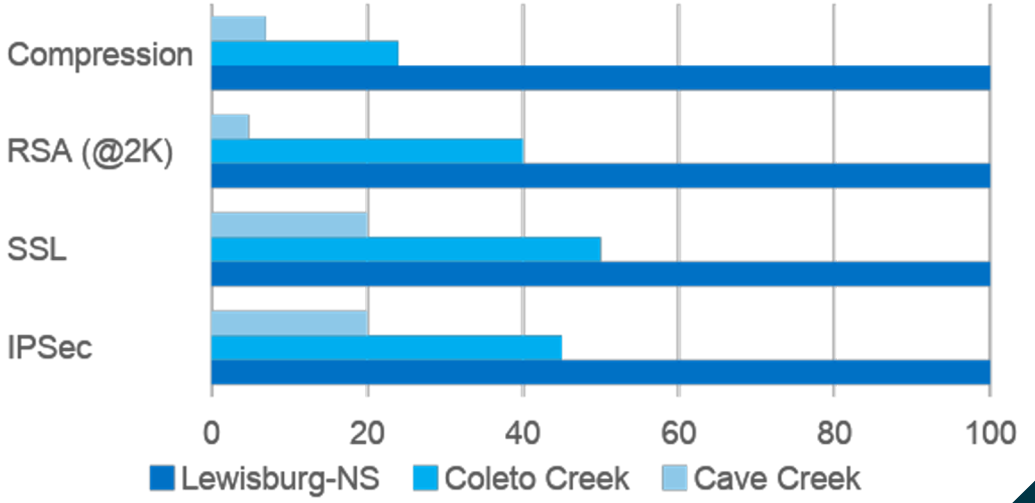
QUICK ASSIST TECHNOLOGY

LEWISBURG-NS CHIPSET

- Third generation Intel QuickAssist Technology

- First chipset offered in a common server platform

- Purely-EP platform



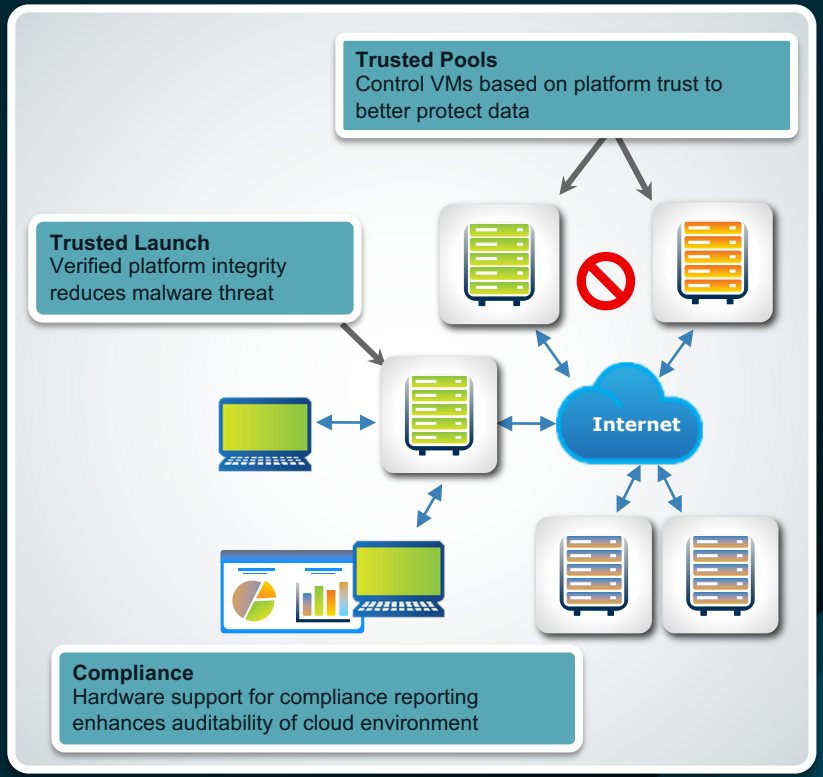
TRUSTED COMPUTE POOLS

VIRTUALIZED & CLOUD USE MODELS

- Ensure only trustable hypervisor is run on platform
- Protecting server prior to virtualization s/w boot
- Launch-time protections against run-time malware
- Compliance support

CONTROL VMs BASED ON PLATFORM TRUST

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



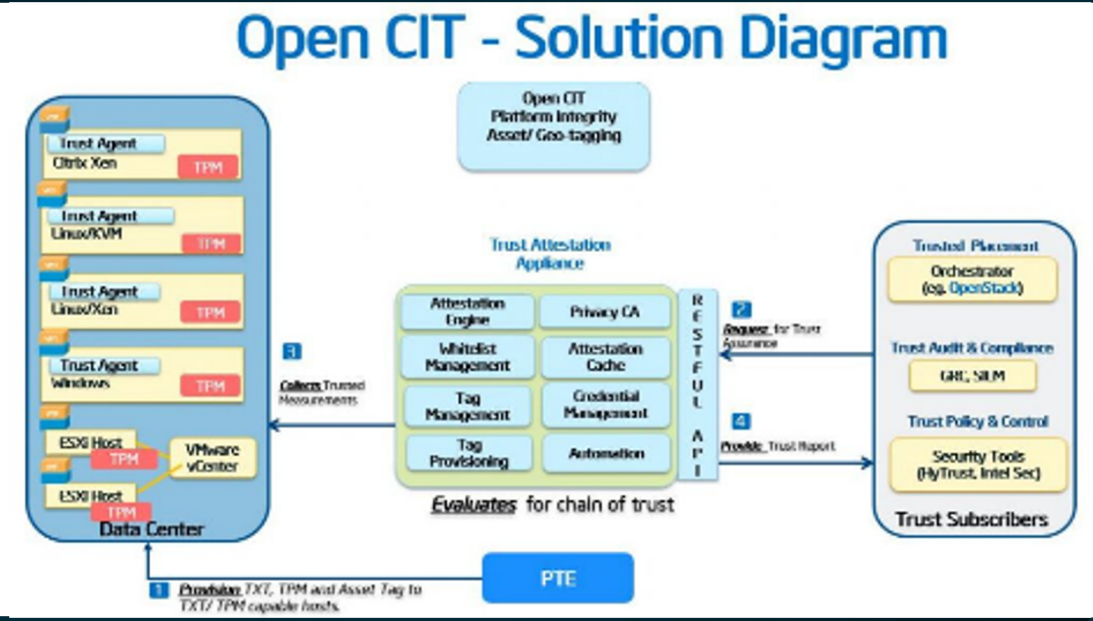
OpenCIT

- Whitelist-based chain of trust between BIOS, firmware, O/S kernel and hypervisor

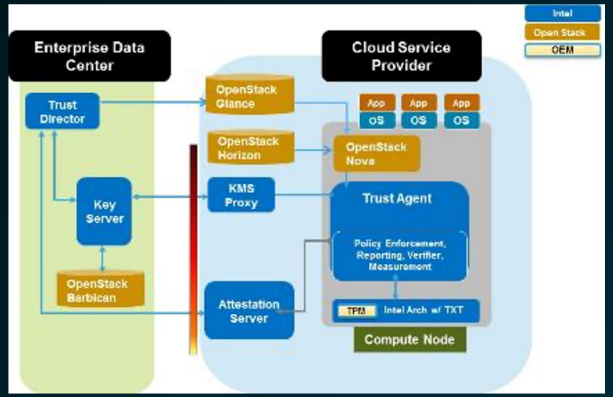
- Ability to tag/verify hosts with custom attributes stored in TPM

- OpenStack and hypervisor integration

- Mutual SSL, RESTful API, user-defined TLS policies



OpenCIT & Red Hat OpenStack Platform



TRUST FROM BIOS TO WORKLOAD

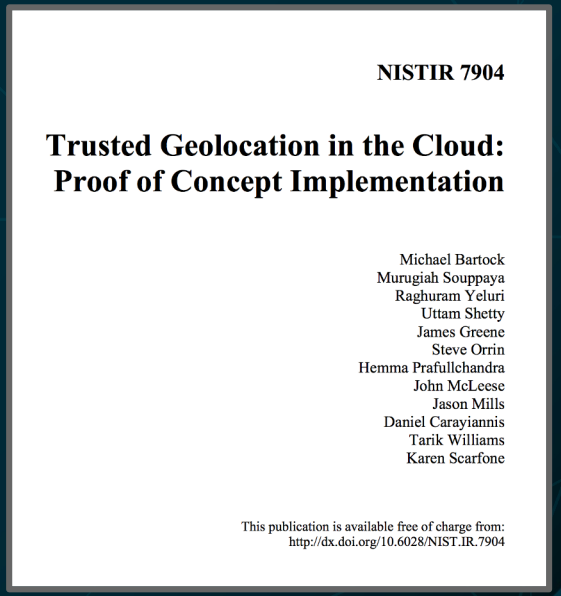
- Boot time integrity
- Workload can be container or VM
- Integrated with Red Hat OpenStack Platform

ENTERPRISE OWNERSHIP AND CONTROL

- Encrypt a workload before moving to cloud
- Own and manage encryption keys
- Release keys to CSP after integrity check succeeds

NIST IR 7904 REFERENCE ARCHITECTURE

Joint Collaboration between NIST, Intel Corporation, and Software Vendors to demonstrate the ability to control and audit workload and data provisioning based on system trust and geo-location



NISTIR 7904

Trusted Geolocation in the Cloud: Proof of Concept Implementation

Michael Bartock
Murugiah Souppaya
Raghuram Yeluri
Uttam Shetty
James Greene
Steve Orrin
Hemma Prafullchandra
John McLeese
Jason Mills
Daniel Carayiannis
Tarik Williams
Karen Scarfone

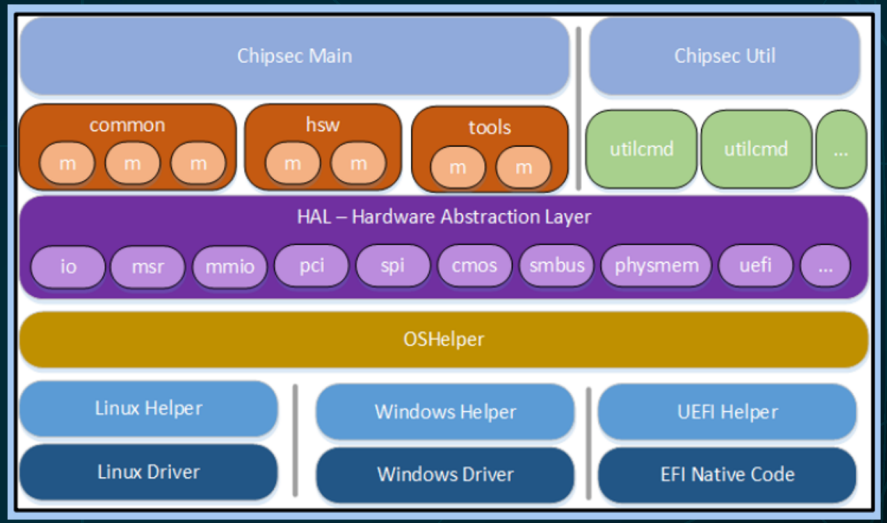
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.7904

http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7904.pdf

CHIPSEC

Collect tests for known vulnerabilities
- Continuous improvement of platform security

Capture community research as test cases
- Supports coordinated disclosure and security assessment



https://github.com/chipsec/chipsec

```
$ ./common.smrr
[+] imported chipsec.modules.common.smrr
[x][ ============================================================
[x][ Module: CPU SMM Cache Poisoning / SMM Range Registers (SMRR)
[x][ ============================================================
…
[+] OK. SMRR are supported in IA32_MTRRCAP_MSR
…
[+] OK so far. SMRR Base is programmed
…
[+] OK so far. SMRR are enabled in SMRR_MASK MSR
…
[+] OK so far. SMRR MSRs match on all CPUs
[+] PASSED: SMRR protection against cache attack seems properly
configured
```

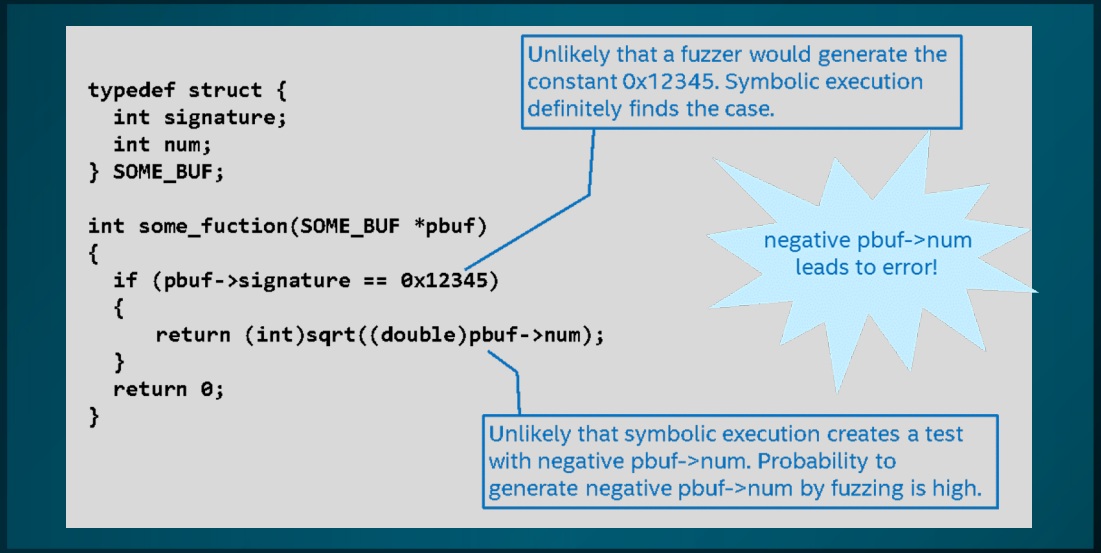
EXCITE

Fuzzing for Automated Detection of Code Security Issues in BIOS

Excite is a powerful tool for excavating BIOS security vulnerabilities in an automated mode.

Combines dynamic selective symbolic execution and guided fuzzing for test case generation.

Flow uses Simics to dump platform data and replay tests while measuring coverage.



https://software.intel.com/en-us/2017/06/06/finding-bios-vulnerabilities-with-excite

Summary

- The threats to the platform continue to evolve deeper in the stack
- Intel & Red Hat are focused on providing access to security capabilities that:
  - Enhance platform security and visibility
  - Provide efficient and performant cryptography
  - Drive scalable assurance and compliance
- Reducing the surface area of attack and providing advanced security features in hardware, firmware and software, Intel & Red hat are hardening the platform and enabling platform trust.

INNOVATION

DOES NO GOOD IF YOU CAN’T SECURE IT

J2 | Common

	A	C	F	G
1	Control ID	NIST Security Control Class	Requirement Description	Control Response
2	AC.1.a	Technical	(U) The NRO shall develop, disseminate, and review/update at least annually a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. [Source: NIST SP 800-53 AC-1]	
3	AC.1.b	Technical	(U) The NRO shall develop, disseminate, and review/update at least annually formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. [Source: NIST SP 800-53 AC-1]	
4	AC.2.a	Technical	(U) The NRO shall identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary) for each information system. [Source: NIST SP 800-53 AC-2]	
5	AC.2.b	Technical	(U) The NRO shall establish conditions for group membership. [Source: NIST SP 800-53 AC-2]	
6	AC.2.c	Technical	(U) The NRO shall identify authorized users of the information system and specify access privileges. [Source: NIST SP 800-53 AC-2]	
7	AC.2.d	Technical	(U) The NRO shall require appropriate approvals for requests to establish accounts. [Source: NIST SP 800-53 AC-2]	
8	AC.2.e	Technical	(U) The NRO shall manage the process of establishing, activating, modifying, disabling, and removing accounts. [Source: NIST SP 800-53 AC-2]	

The government created
a ***control catalog.***

Could we create
a ***response catalog***?

Can ***deployment specific*** ATO materials
be ***dynamically generated***?

Structured language for ATO responses, created by 18F

```
- control_key: AC-14
  standard_key: NIST-800-53
  covered_by: []
  implementation_status: complete
  narrative:
    - text: |
        'Regardless of access mechanism, such as the Ansible
        Tower console, unauthenticated users will only be shown
        the system use notifications (as defined in AC-8) and
        login prompt. This is non-configurable behavior.'
```

```
name: DoD-STIG
standards:
 NIST-800-53:
   AC-1: {}
   AC-14: {}
   AU-2: {}
   SC-3: {}
   SI-7: {}
```

```
name: FedRAMP-mod
standards:
 NIST-800-53:
   AC-1: {}
   AC-2: {}
   AT-7: {}
   AU-11: {}
   CA-4: {}
```

```
name: DHS-4300A
standards:
 NIST-800-53:
   AC-20 (1): {}
   AC-20 (2): {}
   AC-20 (3): {}
   AC-20 (4): {}
   AC-21: {}
```

Requirements Traceability Matrix

Control	Name	Status
AC-1	Access Control Policy And Procedures	not applicable
AC-2	Account Management	not applicable
AC-2 (1)	Automated System Account Management	planned
AC-3	Access Enforcement	complete

AC-14: Permitted Actions Without Identification Or Authentication

"The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication."

AC-14 Control Response Information
Implementation Status:
complete

AC-14: What is the solution and how is it implemented?
'Regardless of access mechanism, such as the Ansible Tower console, unauthenticated users will only be shown the system use notifications (as defined in AC-8) and login prompt. This is non-configurable behavior. External service APIs also require authentication prior to granting resource access.'

SCAP SECURITY GUIDE

Automated configuration scans, co-founded with NSA Information Assurance

redhat.

NIST SP 800-53 = **CM-5(3)**		
Ensure gpgcheck Enabled For All yum Package Repositories	high	pass
Ensure gpgcheck Enabled for Local Packages	high	fail
Ensure Red Hat GPG Key Installed	high	pass
Ensure gpgcheck Enabled for Repository Metadata	high	fail
Ensure gpgcheck Enabled In Main yum Configuration	high	pass
NIST SP 800-53 = **CM-6(3)**		
Verify and Correct File Permissions with RPM	high	fail
Verify File Hashes with RPM	high	pass
NIST SP 800-53 = **CM-6(a)**		
Disable SSH Support for User Known Hosts	medium	fail
Disable SSH Support for .rhosts Files	medium	pass

ANSIBLE PLAYBOOKS AVAILABLE ON GALAXY, INCLUDING . . .

DoD STIG

- Last updated for RHEL 7.6

C2S

- Available in any RHEL image, not just highside AMIs
- Lowside development with same security settings as higher environments

FBI CJIS

- Criminal Justice Information Services (CJIS)
- Police, court systems, evidence handling systems

HIPAA

- Used by federal and commercial healthcare

https://galaxy.ansible.com/RedHatOfficial

NIST NATIONAL CHECKLIST PROGRAM

The National Checklist Program (NCP) is the U.S. Government repository of publicly available security checklists,

that provide detailed low level guidance,

on setting the security configuration of system components and applications

https://nvd.nist.gov/ncp/repository?authority=Red+Hat&startIndex=0

NIST 800-53/FISMA Applicability Guide for Red Hat OpenShift 3.x v1 Checklist Details

(Checklist Revisions)

Supporting Resources:

- Download Security Template - NIST 800-53/FISMA Control Applicability Guide for Red Hat OpenShift 3.x
  - Red Hat

Target:

Target	CPE Name	Product Category
Red Hat OpenShift Container Platform 3.5	cpe:/a:redhat:openshift_container_platform:3.5 (View CVEs)	
Red Hat OpenShift Container Platform 3.6	cpe:/a:redhat:openshift_container_platform:3.6 (View CVEs)	
Red Hat OpenShift Container Platform 3.7	cpe:/a:redhat:openshift_container_platform:3.7 (View CVEs)	
Red Hat OpenShift Container Platform 3.8	cpe:/a:redhat:openshift_container_platform:3.8 (View CVEs)	
Red Hat OpenShift Container Platform 3.9	cpe:/a:redhat:openshift_container_platform:3.9 (View CVEs)	
Red Hat OpenShift Container Platform 3.10	cpe:/a:redhat:openshift_container_platform:3.10 (View CVEs)	
Red Hat OpenShift Container Platform 3.11	cpe:/a:redhat:openshift_container_platform:3.11 (View CVEs)	

CHECKLIST HIGHLIGHTS

Checklist Name: NIST 800-53/FISMA Applicability Guide for Red Hat OpenShift 3.x
Checklist ID: 866
Version: v1
Type: Compliance
Review Status: Final
Authority: Software Vendor: Red Hat
Original Publication Date: 08/29/2018
Checklist Group: View

TEASER

Title	Severity	Result
Guide to the Secure Configuration of Red Hat Enterprise OpenShift Container Platform 3 39x fail 1x error		
OpenShift Settings 39x fail 1x error		
OpenShift etcd Settings 8x fail		
Configure etcd Log Storage	medium	fail
Enable The Client Certificate Authentication	medium	pass
Ensure That The etcd Peer Key File Is Correctly Set	medium	fail
Ensure That The etcd Peer Client Certificate Is Correctly Set	medium	fail
Disable etcd Peer Self-Signed Certificates	medium	fail
Configure A Unique CA Certificate for etcd	medium	pass
Disable etcd Auto Log Rotation	medium	fail
Enable The Peer Client Certificate Authentication	medium	pass
Ensure That The etcd Client Certificate Is Correctly Set	medium	fail
Disable etcd Self-Signed Certificates	medium	fail
Ensure That The etcd Key File Is Correctly Set	medium	fail
OpenShift Controller Settings 1x fail		
Ensure that the --use-service-account-credentials argument is set	medium	pass

SECURITY POLICY

Done

RHVH 4.2 INSTALLATION

us

Help!

Change content | Apply security policy: ON

Choose profile below:

Standard System Security Profile
This profile contains rules to ensure standard security baseline
of Red Hat Enterprise Linux 7 system. Regardless of your system's workload
all of these checks should pass.

PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
This is a *draft* profile for PCI-DSS v3.

C2S for Red Hat Enterprise Linux 7
This profile demonstrates compliance against the
U.S. Government Commercial Cloud Services (C2S) baseline.

This baseline was inspired by the Center for Internet Security
(CIS) Red Hat Enterprise Linux 7 Benchmark, v2.1.1 - 01-31-2017.

For the SCAP Security Guide project to remain in compliance with
CIS' terms and conditions, specifically Restrictions(8), note
there is no representation or claim that the C2S profile will
ensure a system is in compliance or consistency with the CIS
baseline.

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
This is a *draft* SCAP profile for Red Hat Certified Cloud Providers.

Common Profile for General-Purpose Systems
This profile contains items common to general-purpose desktop and server installations.

DISA STIG for Red Hat Enterprise Linux 7
This profile contains configuration checks that align to the
DISA STIG for Red Hat Enterprise Linux V1R1.

In addition to being applicable to RHEL7, DISA recognizes this
configuration baseline as applicable to the operating system
tier of Red Hat technologies that are based off RHEL7, such as RHEL
Server, RHV-H, RHEL for HPC, RHEL Workstation, and Red Hat
Storage deployments.

STIG for Red Hat Virtualization Hypervisor
This is a *draft* profile for STIG. This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

Where is the RHV-H STIG?

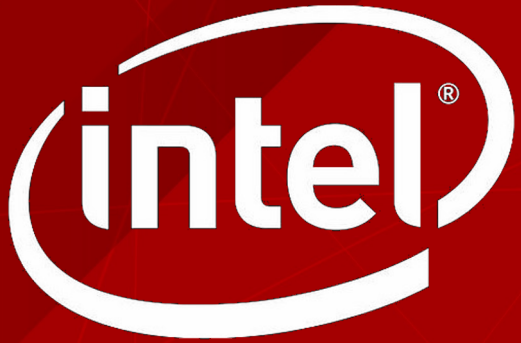
Question: May I deploy a product if no STIG exists?
Answer: Yes, based on mission need and with DAA approval.

Select profile

redhat.

Step-by-Step Configuration Guide: Trusted Compute Pools in Red Hat Enterprise Linux* OpenStack* Platform

Table of Contents



redhat

THANK YOU