Trusted Computing: Intel® Trusted Execution Technology Overview and Usages

Gideon Gerzon
Intel

Agenda

Security trends and concerns

Meeting the security challenge:

Technologies and use models to mitigate pain points

- Intel® Virtualization Technology enhances workload isolation
- Intel® Trusted Execution Technology provides visibility and enforcement point

Summary

Security Concerns Limit Adoption of Cloud

Better Security is Essential for Cloud Growth

IT Pro survey of key concerns:

57%

Avoid putting workloads with compliance mandates in cloud[1]

61%

Say lack of visibility inhibiting private cloud adoption[1]

55%

Lack of control over public cloud[1]

[1] **http://www.intel.com/content/www/us/en/cloud-computing/whats-holding-back-the-cloud-peer-research-report.html**

[1] McCann 2012 State of Cloud Security Global Survey, Feb 2012

New Attacks, Organized Attackers

New threats from:

- Social networking
- Web mash-ups
- Drive-by downloads
- Mobile devices
- Hardware and firmware attacks
- Virtualization attacks

The "bad guys" are smart and focused

Security experts consulted by GTISC believe cyberwarfare will accompany traditional military interaction more often in the years ahead. They expect it will also play a more shadowy role in **attempts by antagonist nations to subvert the U.S. economy and infrastructure**.[1]

Federal Prosecutor: Cybercrime is Funding Organized Crime

Cybercrime has been so profitable for organized crime that the mob is using it to fund its other underground exploits. And U.S. law enforcement is reaching around the world to reel it in.[2]

"We see many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises."[3]

—Tom Gillis, Vice President and General Manager, Cisco Security Products

New Pain: Threats are Getting More Sophisticated and Professional

1 http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf

2 http://cisco.com/en/US/prod/vpndevc/annual_security_report.html

3 http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=201200167

Example: Security in the Cloud

Cloud and virtualization have inherent security requirements

- Abstraction of physical hardware
- Multi-tenancy movement implicitly require audit and security

"Twitter Embeds Encryption to Foil Firesheep hackers"
—PC World

"Webhost hack wipes out data for 100,000 sites
Vaserv suspects zero-day virtualization vuln"
—The Register

"IT ops, security pros at odds over virtualization risks
IT pros upbeat about virtualization, whereas security experts harbor doubts about the security role the hypervisor can play"
—IDG News Service

Cloud and Virtualization Break Many Traditional Perimeter-oriented Security Techniques

Pain Point #1: **Isolation**

Isolating Workloads on Shared Infrastructures is Critical

A major concern of shared infrastructure

Lack traditional guarantees of physical separation

Multiple workloads may tamper or interact with each other

Homeland Security's Subcommittee Hearing: Cloud Computing: What are the Security Implications?[1]

Multi-Tenant Solutions: The Pros, the Questions and Integration Concerns[2]

Security Guidance for Critical Areas of Focus in Cloud Computing[3]

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

Source 1: http://www.outlookseries.com/A0995/Security/3817_Homeland_Security_Hearing_Cloud_Computing_Implications.htm
Source 2: http://www.itbusinessedge.com/cm/blogs/lawson/multi-tenant-solutions-the-pros-the-questions-and-integration-concerns/?cs=45181&page=2
Source 3: https://cloudsecurityalliance.org/csaguide.pdf

Pain Point #2: **Enforcement**

New Controls Needed to Enforce Protection of Infrastructure

Pre-runtime environment target of new attacks

Protections abstracted away by virtualization and cloud

Low-level attacks are hard to detect and can be difficult to recover from

Mebromi: The First BIOS Rootkit in the Wild[1]

NIST Guidelines Seek to Minimize Risk of BIOS attacks[2]

US Dept of Homeland Security Cyber Security Research & Development
Broad Agency Announcement (BAA): BAA 11-02[3]

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

Source 1: http://www.outlookseries.com/A0995/Security/3817_Homeland_Security_Hearing_Cloud_Computing_Implications.htm
Source 2: http://www.itbusinessedge.com/cm/blogs/lawson/multi-tenant-solutions-the-pros-the-questions-and-integration-concerns/?cs=45181&page=2
Source 3: https://cloudsecurityalliance.org/csaguide.pdf

Enterprise Client Security Requirements

- IT Requiring More Control of Client Systems
  - Set policy on the platform: e.g. Trusted Launch with platform policy set
    - Provides IT the ability to control the launched environment based on business segment needs
  - Preventing unauthorized s/w to run on enterprise platforms
  - Isolating/Protecting process execution and data
  - Allow full platform & network attestation
    - Prevents unauthorized access to IT networks - Provides ability for IT to control trusted networks verses guest networks

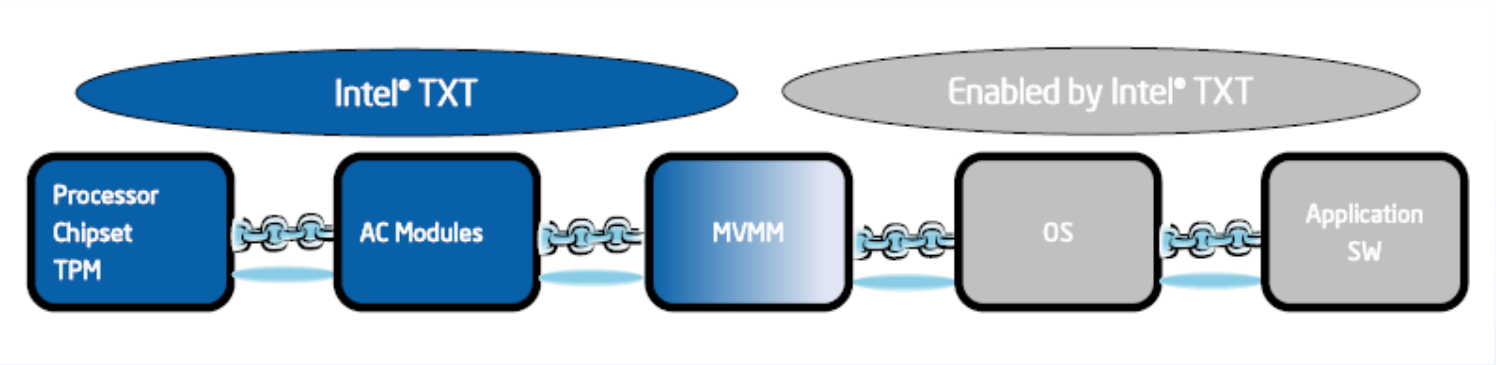
Intel® TXT Value Prop

- Provides HW root of trust and enforcement to make an auditable chain of trust more robust
  - Ensures platform integrity in support of compliance via protected, extended measurement foundation and enforcement mechanisms
  - Provide Launch Control Policy Tools: Enable end users/IT with granular management allow only approved OSes/VMMs
  - Prevents launch of untrusted software (white listing)
- Platform configuration protection
  - Memory alias checks, DMA protection, memory config locking, etc.
- Reset memory protection
  - Scrub memory on reboot when secrets flag set
- Strengthened RAS (via server extensions)
  - Enables HW-enforced protections during RAS events, such as hot-add, memory failures, etc.

Intel® TXT provides protection from SW attacks

What is Intel® Trusted Execution Technology?

- A hardware based security foundation to build and maintain a ***chain of trust***, to protect information from software based attacks

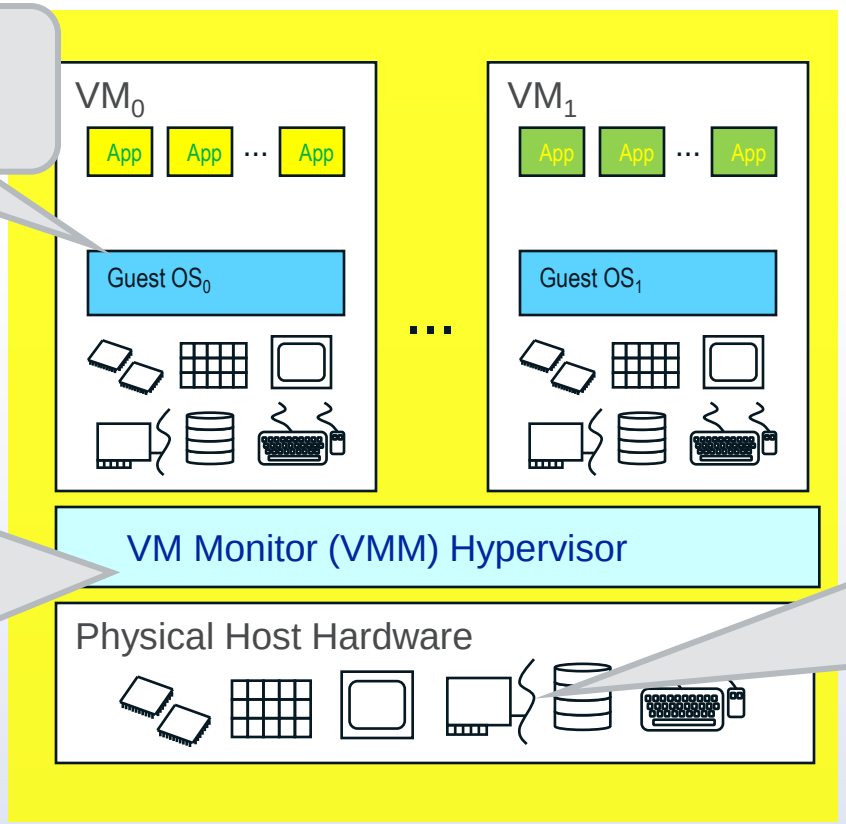


- Key definitions
- ***Trust*** means it behaves in the expected manner … uncorrupted binaries
- ***Measurement*** is a hash representation of an binary object's identity (analogy SW fingerprints)
- **MLE: M**easured **L**aunch **E**nvironment. Environment that's launched via Intel® TXT
- **MVMM** a VMM that's been launched with TXT

TXT provides measured launch into a known Platform State

Intel® Virtualization Technology (VT)

Guest OSs & Apps run in the intended ring



VMM runs in a privileged operation mode

VMM preempts guest execution via HW "transition" mechanism

VT = HW support for Processor Virtualization

- **CPU execution mode**
- **HW-based mode transitions**

Intel® VT Provides Stronger ***Isolation*** of VMs

Traditional *server* VMM-based uses

Isolation needed for:

Separation of development and production environments

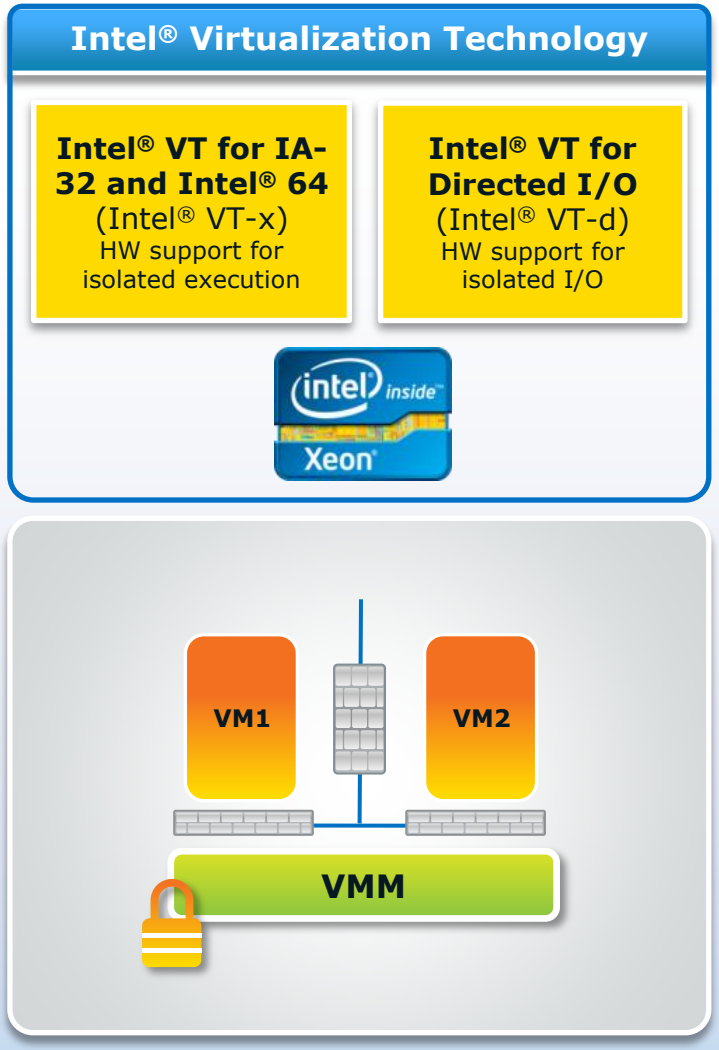
Technology demonstrations

New *cloud* security-related uses

Isolation of workloads in multi-tenant cloud

Memory monitoring for malware detection

Device isolation for protection against DMA attacks



Authenticated **C**ode **M**odules (ACMs)

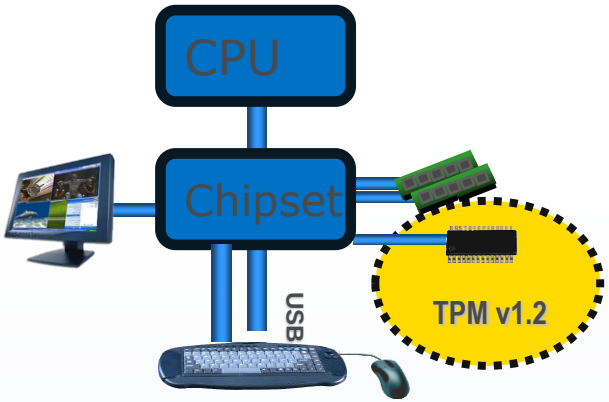
- Chipset/CPU -specific signed binary provided by Intel

- Loaded and executed into a new CPU cache area called **A**uthenticated **C**ode **E**xecution **A**rea (ACEA)

- BIOS ACM
  - Called by BIOS to unlock memory
  - Multiple processor: Invoked by CPU on reset

- SINIT ACM
- Check and lock memory config, measure MLE, etc.
- Used during MLE measurement

Trusted Platform Module (TPM)



Trusted Platform Module Capabilities

- TPM-NV Storage (Non-Volatile)
- PCR (Platform Configuration Register)
- SHA-1
- Key Generation
- Random Number Gen
- RSA Engine
- Attestation Identity Key

Intel® TXT relies on the TPM for protected storage of measurements and configurations.

Key TPM features used are:

- TPM Establishment
- TPM-NV
- PCR
- Localities

Intel® TXT Ingredients

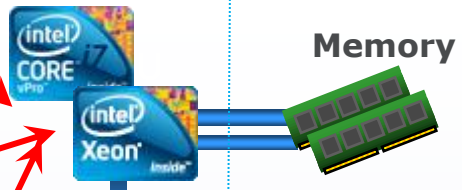
Trusted Execution Technology extensions for measured launch & memory protection (SMX)

Processor contains hardware to authenticate AC Modules and perform measurements

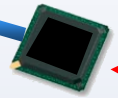
Intel® VT Provides Stronger *Isolation*

VT-d chipset feature blocks device access (e.g DMA) to protected memory pages

Intel Authenticated Software:
SINIT AC Module
BIOS AC Module



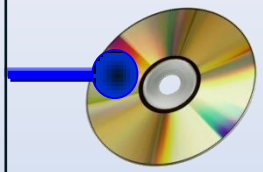
Memory



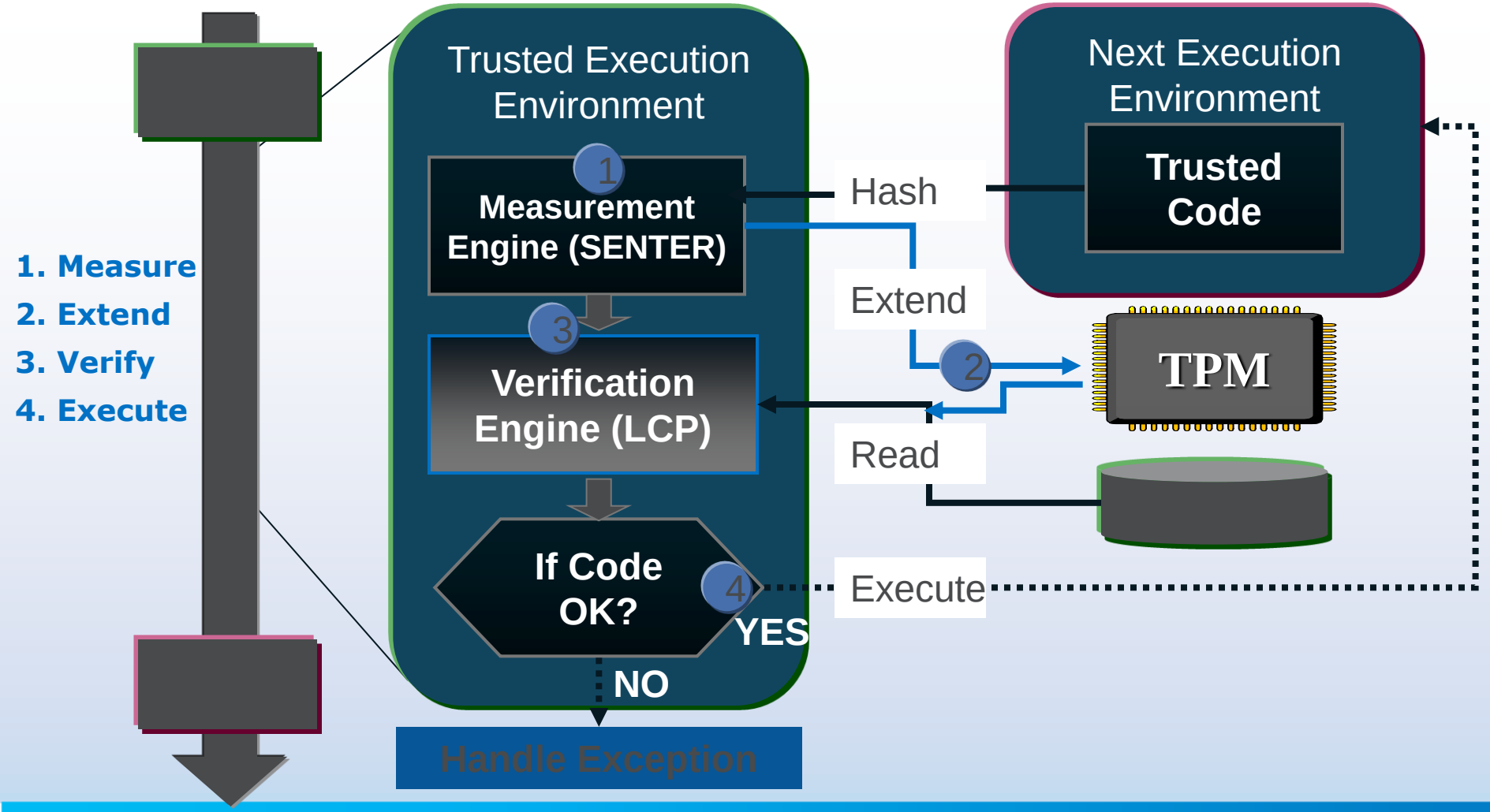
3rd party TPM (v1.2) stores and reports trusted environment measurements

BIOS / Flash
BIOS AC Module and platform initialization

3rd party Software
VMM/OS uses TXT mechanisms to establish a measured launch environment



Intel® TXT and TPM



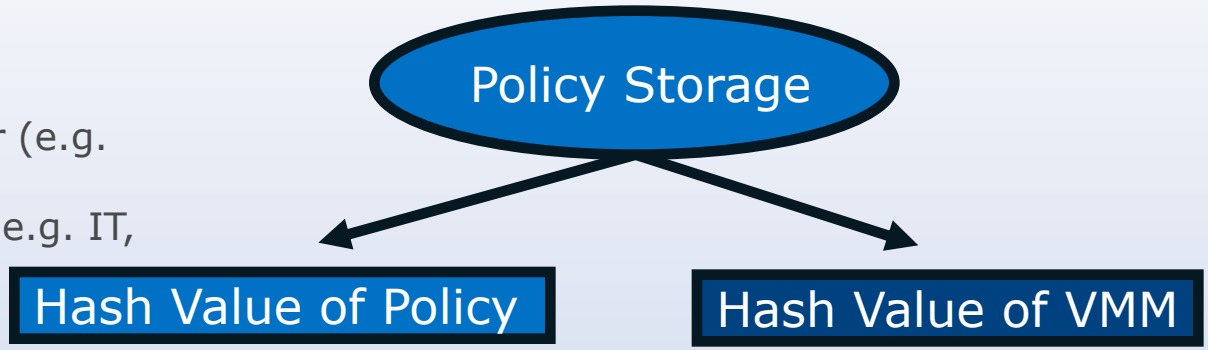
Launch Control Policy Definitions

Policy = a list of conditions you have to meet in order to launch the VMM

The policy is hashed to protect the list and then stored in two pieces

Two LCP policy authorities:

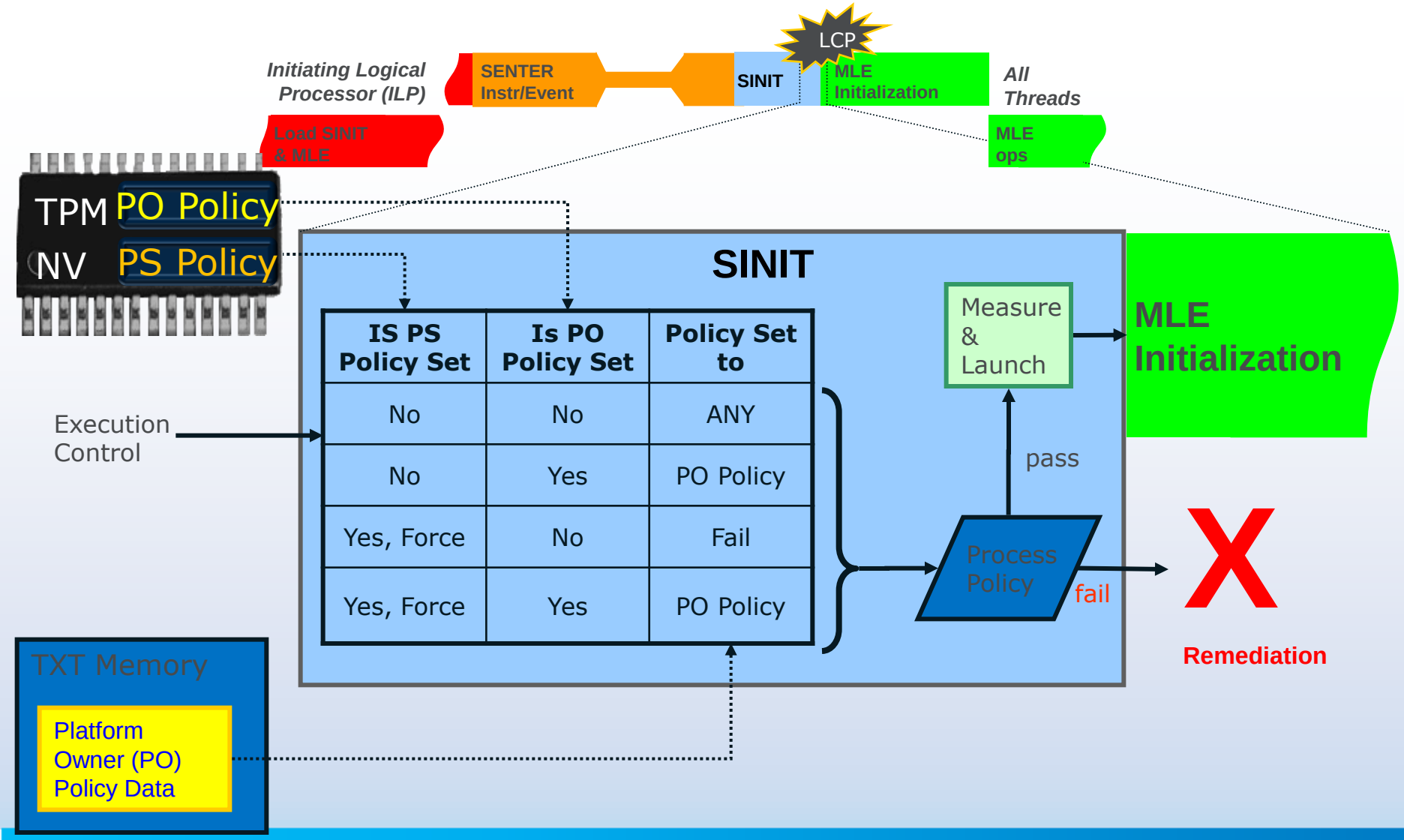
1. Platform Supplier (e.g. OEM, ODM, VAR)
2. Platform Owner (e.g. IT, end-user)



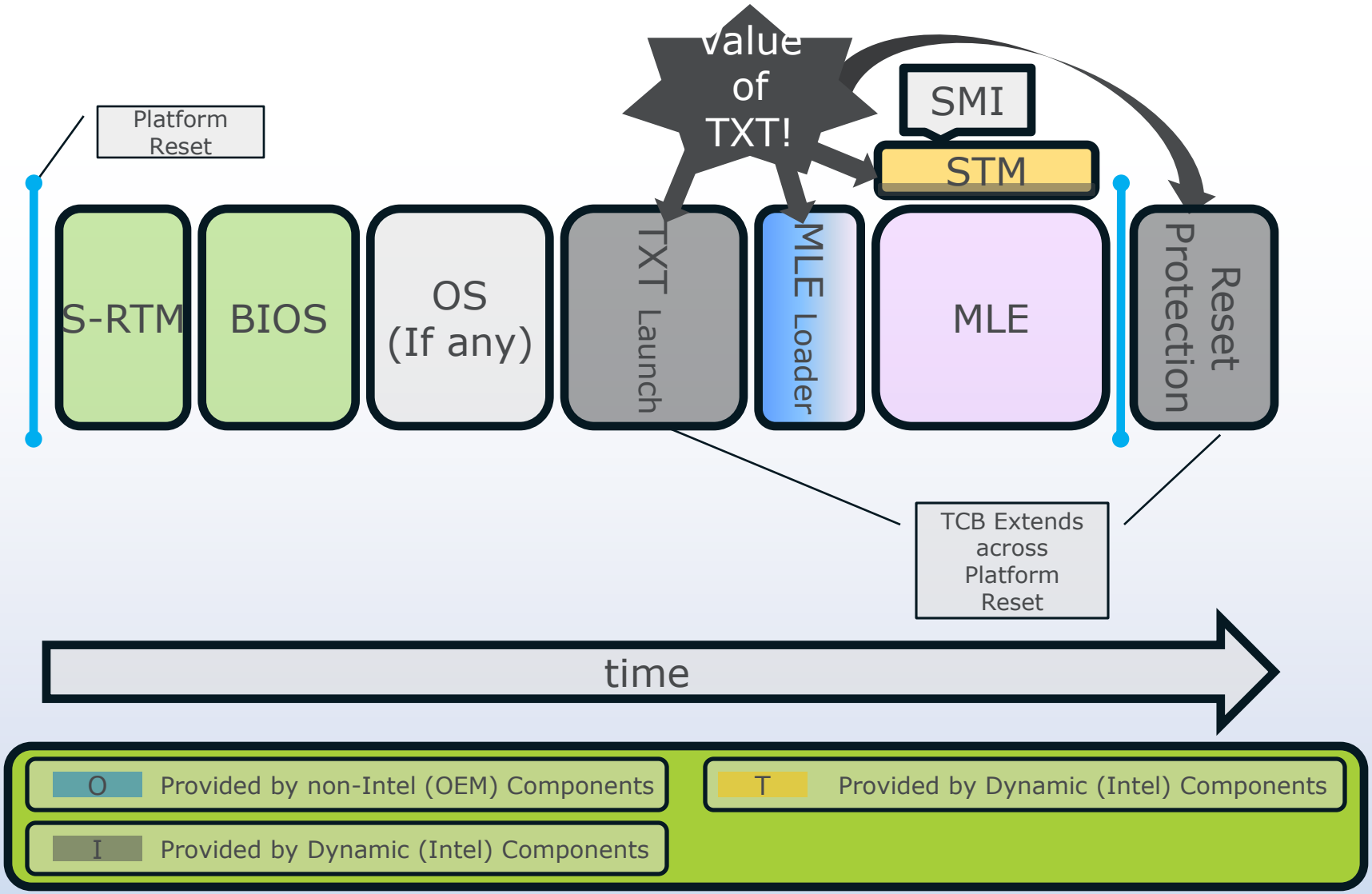
TPM NV Storage w/access control via TPM password

Anywhere on the platform that ISV decides

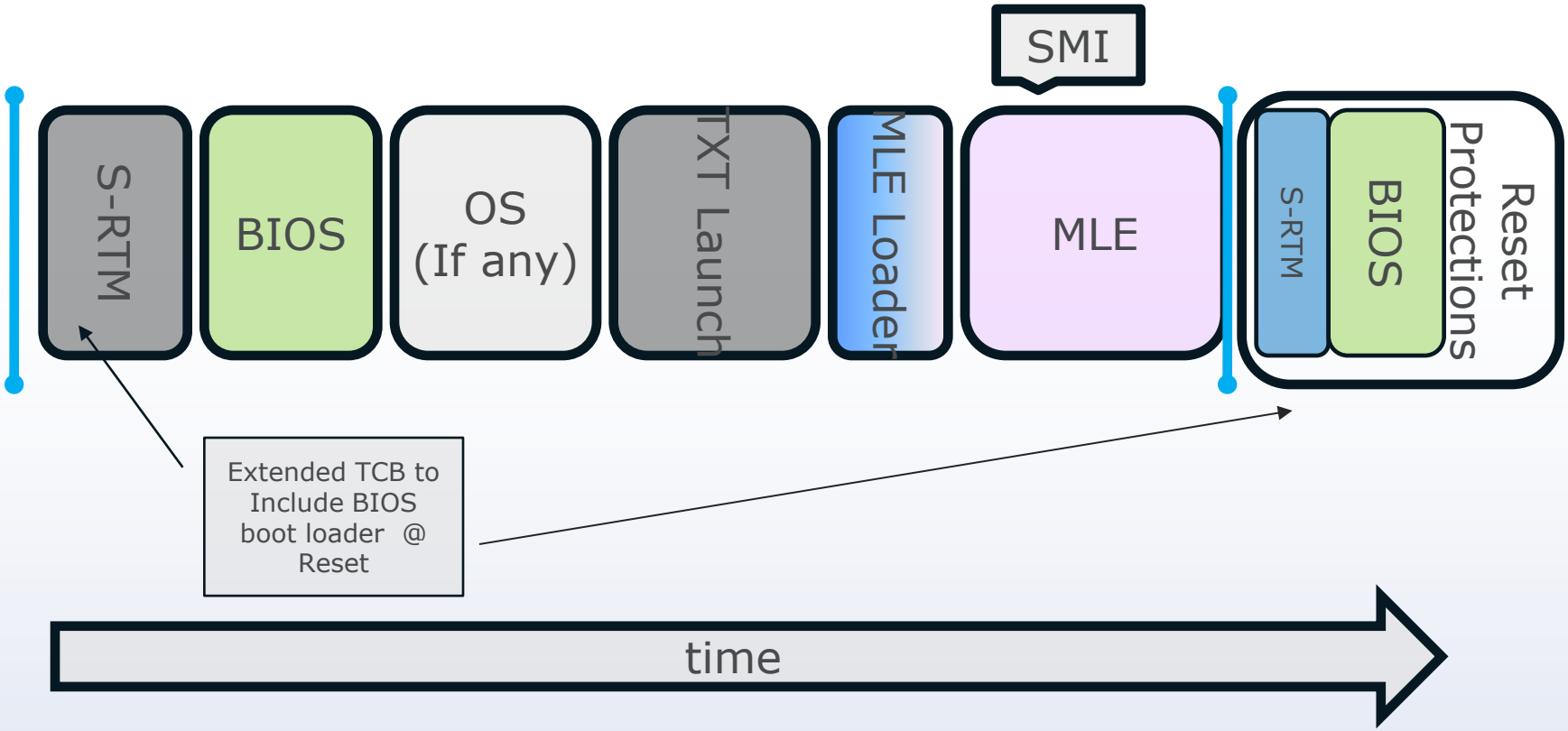
ISV Decides what policy to implement



TXT: TCB Component Timeline



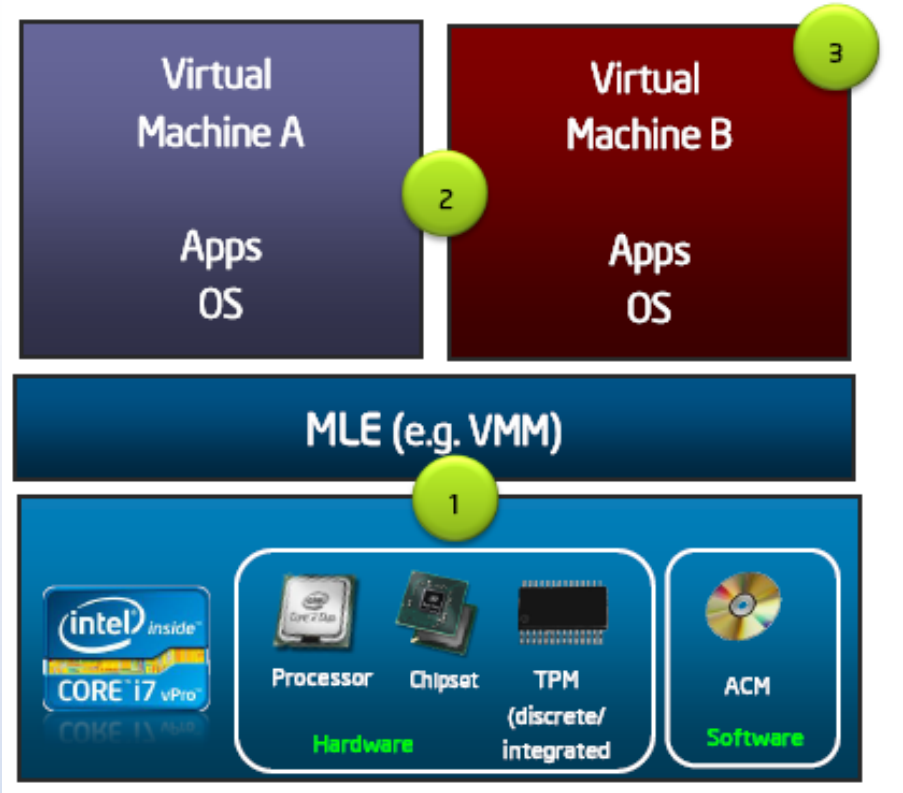
Server TXT: TCB Component Timeline



Intel® Trusted Execution Technology Advantage

- A hardware based security foundation to build and maintain a *chain of trust*, to protect the platform from software based attacks

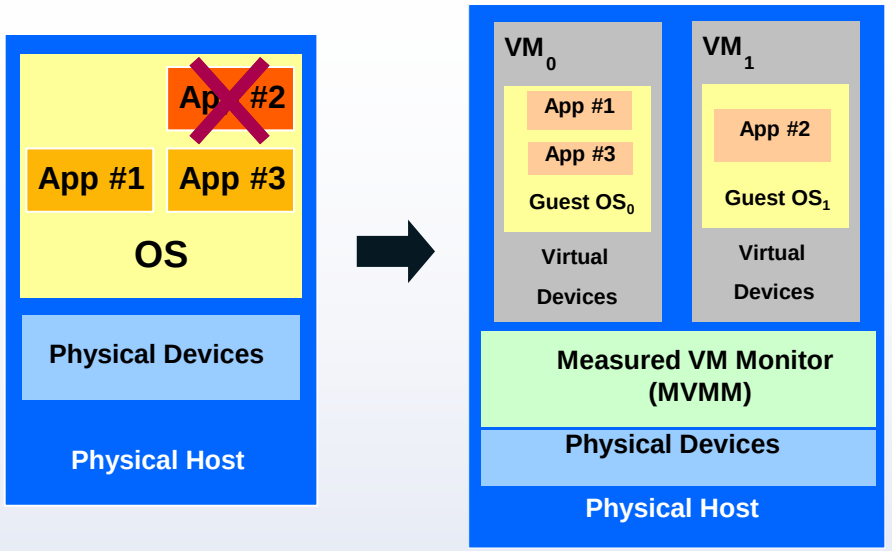
1	**Verified Launch** Intel TXT hardware-based chain of trust enables launch of MLE into a known, expected state. Changes to MLE can be detected via hash-based measurements
2	**Protected Configuration** Intel TXT hardware protects the launched configurations from malicious SW. Maintaining integrity of the measured launched environment identity
3	**Secret Protection** Intel TXT hardware removes residual data at improper MLE shut down, protecting data from memory snooping software.



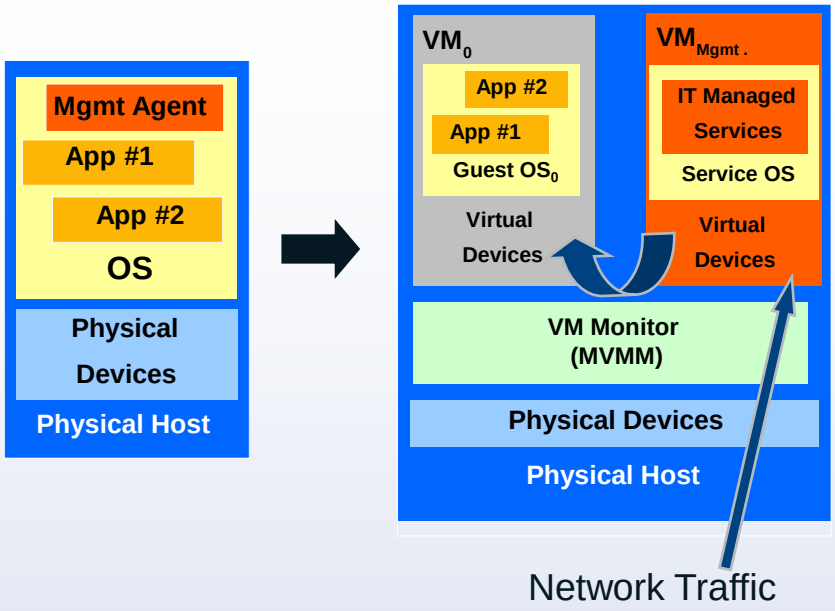
Enterprise Client Security Intel® TXT Based Security Solutions: Example Usage

Environment Isolation

(Based on user, application, security, activity)



Embedded IT



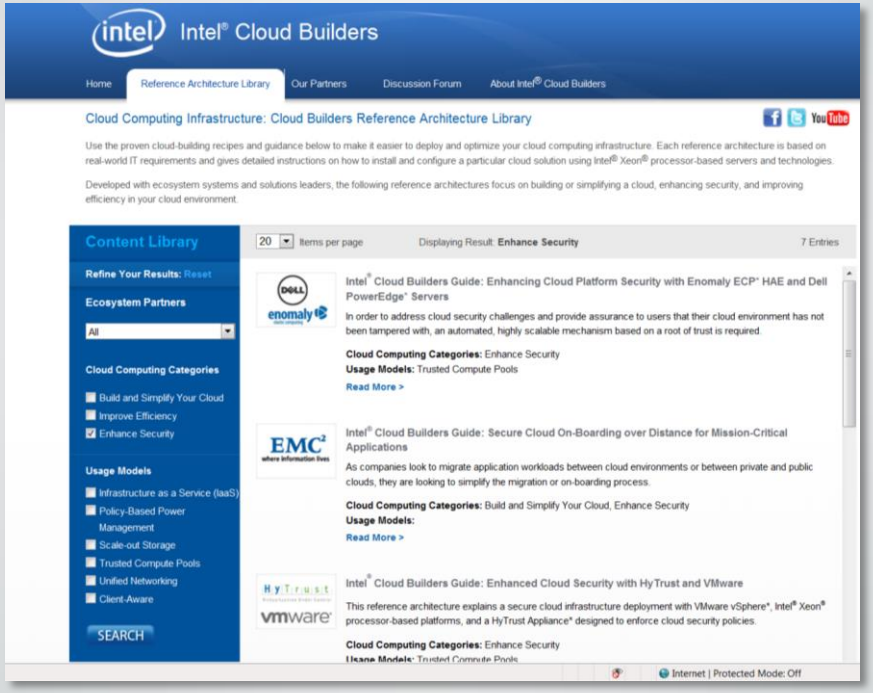
Intel® Cloud Builder

Security Reference Architectures Provide the "How To"

Support and/ or Reference Architectures Featuring:

vmware
DELL
enomaly elastic computing
EMC²
HyTrust Virtualization Under Control
Parallels
openstack CLOUD SOFTWARE
Platform Computing

Accelerate your ability to deploy key technologies that enhance cloud security



For the latest Intel® Cloud Builder Security Reference Architectures, go to:
Cloud Builder: Enhance Cloud Security

Support and/or Implementation White Papers Featuring:

Microsoft
ORACLE
McAfee
redhat
OpenSSL
Check Point SOFTWARE TECHNOLOGIES LTD.
vmware

† Not all features and capabilities will be supported by all listed providers
***Other names and brands may be claimed as the property of others**

Intel® TXT Based Open Source Projects

Trusted Boot (tboot) project

- Uses Intel TXT to perform verified launch of OS kernel/VMM
- Open source, pre-kernel/VMM module
- Project also contains tools for policy creation and provisioning
  - Intel TXT Launch Control Policy (LCP)
  - Tboot Verified Launch policy
- Available from **http://sourceforge.net/projects/tboot**
- **http://tboot.hg.sourceforge.net:8000/hgroot/tboot/tboot**

OpenAttestation Project

- Development Kit, to add cloud management tools with capability of establishing hosts integrity information by remotely retrieving and verifying Hosts' integrity
- Targeted at cloud and enterprise management tools

https://github.com/OpenAttestation/OpenAttestation.git

Summary

- **Organizations need more tools to deal with growing threats against data and infrastructures**
- **Security is essential to usable cloud deployments**
- **Intel® TXT adds value to Trusted Platforms:**
- Solutions for current and emerging attacks and pain points
- Enhanced ability to *Isolate*, *Enforce*
- Hardware building blocks to facilitate compliance with policies, regulations and standards
  - Integrity Measurements, Attestation, Protected Capabilities
  - Protected Execution
  - Launch Control Policy (LCP) enforcement
- Enabled by a growing ecosystem, documented in deployment guides & Cloud Builder Reference Architectures

Legal Information

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. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.

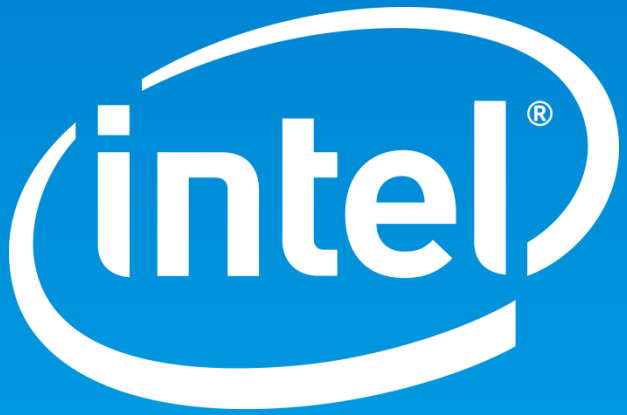
Intel may make changes to specifications and product descriptions at any time, without notice.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards 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.

Intel, and Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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


intel