Trusted Compute Pools with Intel® Trusted Execution Technology (Intel® TXT)

HOST SENSITIVE WORKLOADS ON TRUSTED SERVERS IN MULTI-TENANT ENVIRONMENTS

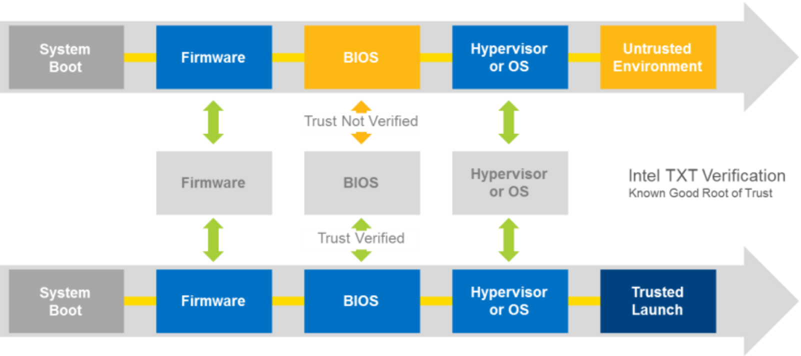
IT PRO SURVEY OF KEY CONCERNS:

61%	55%	57%
Lack of visibility[1]	Lack of control over data[1]	Compliance concerns[1]

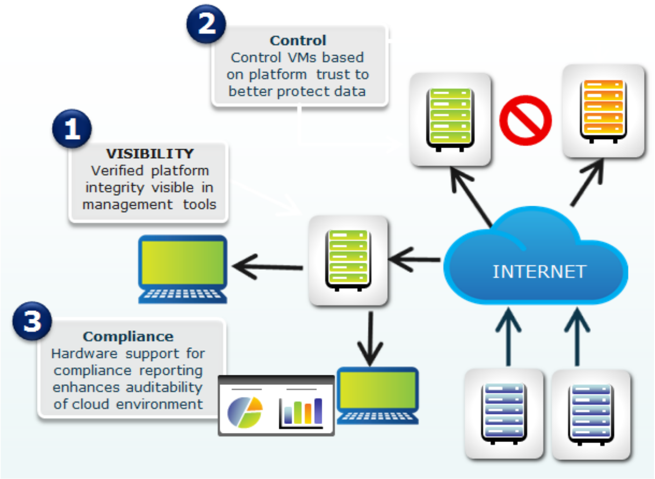
Intel® TXT with Trusted Boot (Tboot)

Intel® TXT with Trusted Boot brings servers up into a trusted launch configuration

- Measured launch environment (MLE) is stored in a Trusted Platform Module (TPM) during server setup
- The trusted boot process compares the actual launch measurement with the stored whitelist



Trusted Compute Pools



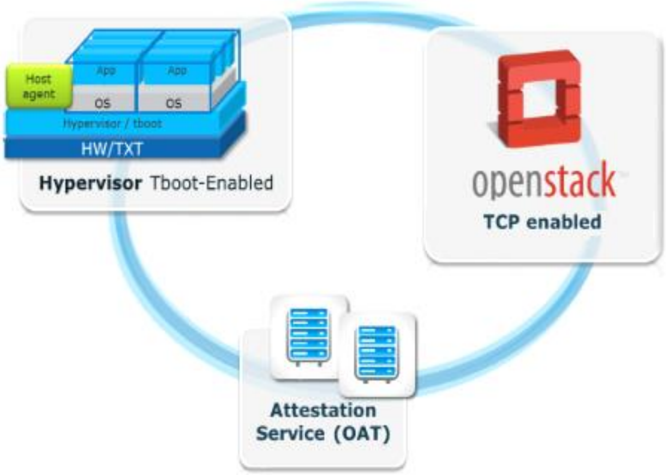
2
Control
Control VMs based on platform trust to better protect data
1
VISIBILITY
Verified platform integrity visible in management tools
3
Compliance
Hardware support for compliance reporting enhances auditability of cloud environment
INTERNET

Place workloads & VMs in trusted pools of virtualized servers

- Solution stack requirements
  - Policy Engine / Console to Manage, CPU that initiates a trusted boot, TCG Compliant Trusted Platform Module (TPM)
- Core technologies
  - Intel® Xeon® processor, Intel TXT, Intel® Virtualization Technology FlexMigration

[1] **Source**: McCann: "What's holding the cloud back?" - Cloud security global IT survey, sponsored by Intel, May 2012

OpenStack* with Trusted Compute Pools



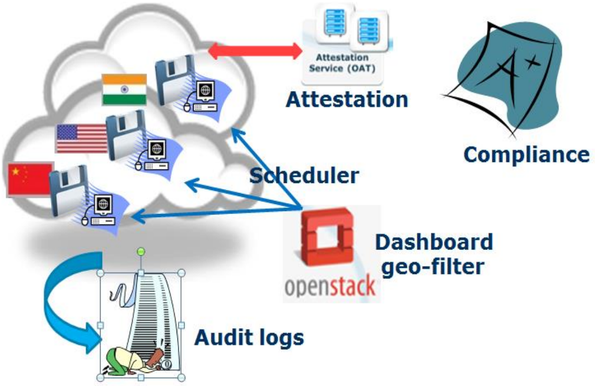
- Open Attestation (OAT) software verifies server trust status and builds a trusted compute pool for the scheduler
- The OpenStack* scheduler places workloads and VMs into the trusted servers

Trusted Compute Pools with Geo-Tagging Targeting a Future Release of OpenStack

Use asset location descriptor information to control virtual workload placement

OpenStack enhancements:

- Dashboard – display VM/storage geo
- Flavor – VM Instance and Storage geo
- Aggregate filter
- Enhance attestation service
- Contact attestation server for geo-attestation
- Provision with geo certificate for trusted machines



Links for more information:

Intel TXT: http://www.intel.com/txt
OpenStack Project: http://www.openstack.org
OpenAttestation Project: https://01.org/openattestation
White Papers and Guides: http://www.intel.com/cloud

Intel, Xeon, and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
Intel® Trusted Execution Technology (Intel® TXT): No computer system can provide absolute security under all conditions. Intel® TXT requires a computer with Intel® Virtualization Technology, an Intel TXT enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security.
Trusted Platform Module (TPM): The original equipment manufacturer must provide TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.
Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.