Intel® Trusted Execution Technology (Intel® TXT) Platform Guidelines

Intel® Trusted Execution Technology (Intel® TXT) Platform Guidelines

Executive Summary

Intel® Trusted Execution Technology (Intel® TXT) is a powerful component of enterprise data protection. In fact Intel® believes that every server should have Intel® TXT activated. Intel® TXT creates a hardware root of trust and measured launch environment, which assure you're server is running "known good" configurations of your critical software components (firmware, BIOs, Operating System and Hypervisors). A hardware root of trust adds an additional level of protection for Intel® servers.

Some added capabilities introduced with the TPM 2.0 specification include the following:

- Support for additional cryptographic algorithms
- Enhancements to the availability of the TPM to applications
- Enhanced authorization mechanisms
- Simplified TPM management
- Additional capabilities to enhance the security of platform services

For more information on how Intel® TXT is used as part of cloud security solutions, please visit the Intel® Cloud Builder reference architectures site: https://www.intel.com/content/www/us/en/cloud-computing/enterprise-cloud.html

In order to enable Intel® TXT the platform must include a Trusted Platform Module (TPM), Intel® TXT supported CPU, Chipset and OS/Hypervisor. Fortunately, Intel® TXT is supported by every Intel® Xeon processor and corresponding Intel® chipset. Finally, Intel® TXT is supported by many operating system and hypervisor vendors, including Red Hat Enterprise Linux, VMware VSphere*, SuSe Linux Enterprise Server* and many others.

Additional Helpful Intel® TXT Links

TCG TPM 1.0 and 2.0 specifications can be found here: http://www.trustedcomputinggroup.org/resources/tpm_library_specification

More information on Cloud Usage Models: http://www.Intelcloudbuilders.com/cloud-usage-models/index.html

General Intel® TXT Information: http://www.Intel.com/txt

Customer and partner software solutions that can extend your Intel® TXT architecture can be referenced here: https://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/where-to-buy-isv-txt.html