IBM Cloud

SOFTLAYER®

Secure Cloud Workloads

VMware on IBM Cloud with Intel® Trusted Execution Technology

Secure Cloud Workloads

Protect your enterprise workloads in the public cloud from potential security threats. IBM Cloud bare metal servers with Intel TXT provide hardware-assisted security technologies to help you build a secure platform.

IBM Cloud is the first cloud provider to offer Intel TXT as an additional method to secure your infrastructure. Intel TXT ensures that the hardware platform including BIOS, firmware, and hypervisor are in a known good state.

The Technology

Intel TXT creates a measured launch environment (MLE) composed of all the critical elements of a launch environment ranging from BIOS to hypervisor. During the boot process, the Trusted Platform Module (TPM) holds the computer generated keys for encryption which essentially is a code that measures, extends, verifies, and executes—over and over to establish a system as trusted. If the current boot environment does not match the known good configuration, Intel TXT hardware will prevent the launch protecting critical applications and servers from potential threats.

Get Started with Intel TXT

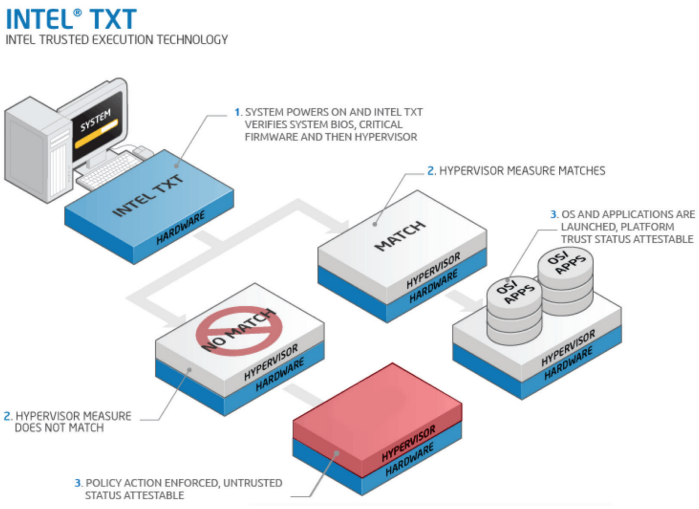
Intel TXT is available on select bare metal servers provisioned in the IBM Cloud. When ordering a new server, simply select the Intel TXT option in the store or talk with a cloud expert.

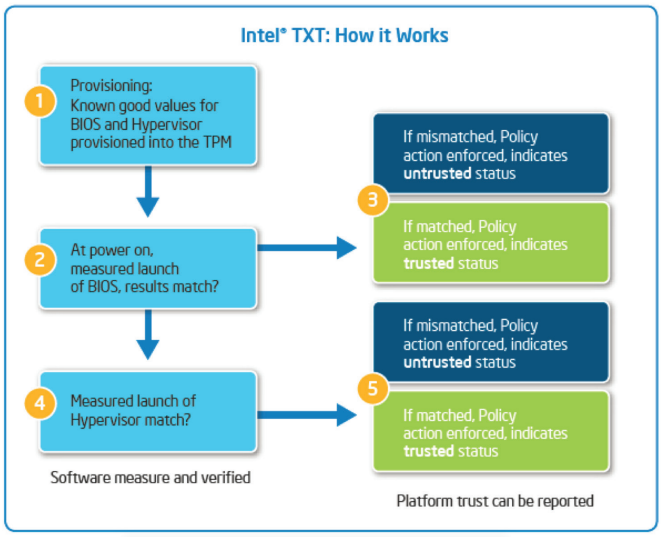
Product Features

Building a Chain of Trust
A hardware based chain of trust extends through the entire launch sequence from hardware through the hypervisor.

Launch Control Policy
Verifies hardware and pre-launch software have been vetted and are in a known good state.

Provide Controls Based on Location
To enforce regulatory compliance, limit the migration of virtual machines only to acceptable servers per specified policy.





IBM Cloud

SOFTLAYER®