vmware
vCloud Air™ Network

IBM Cloud

Sichere Cloud-Workloads

VMware auf der IBM Cloud mit Intel Trusted Execution-Technologie (Intel TXT)

Sichere Cloud-Workloads

Schützen Sie Ihre Unternehmensworkloads gegen potenzielle Sicherheitsbedrohungen in der Public Cloud. IBM Cloud Bare-Metal-Server stellen mit Intel TXT Hardware-unterstützte Sicherheitstechniken für den Aufbau einer sicheren Plattform bereit.

IBM ist der erste Cloud-Anbieter, der Intel TXT als zusätzliches Verfahren für die Sicherung Ihrer Infrastruktur anbietet. Intel TXT stellt sicher, dass sich die Hardwareplattform einschließlich Basic Input/Output System (BIOS), Firmware und Hypervisor in einem ordnungsgemäßen Zustand befinden.

Die Technologie

Intel TXT erstellt eine messbare Bereitstellungsumgebung (Measured Launch Environment; MLE), die sich aus allen kritischen Elementen einer Bereitstellungsumgebung – vom BIOS bis zum Hypervisor – zusammensetzt. Während des Boot-Prozesses werden die vom Computer generierten Schlüssel für die Verschlüsselung im Trusted Platform Module (TPM) abgelegt. Dabei handelt es sich im Wesentlichen um einen Code, der kontinuierlich Mess-, Erweiterungs-, Prüf- und Ausführungsprozesse durchführt, um ein zuverlässiges und sicheres System zu schaffen. Wenn die aktuelle Boot-Umgebung nicht mit der vorhandenen ordnungsgemäßen Konfiguration übereinstimmt, verhindert die Intel TXT-Hardware den Bereitstellungsprozess und schützt so kritische Anwendungen und Server gegen potenzielle Bedrohungen.

Erste Schritte mit Intel TXT

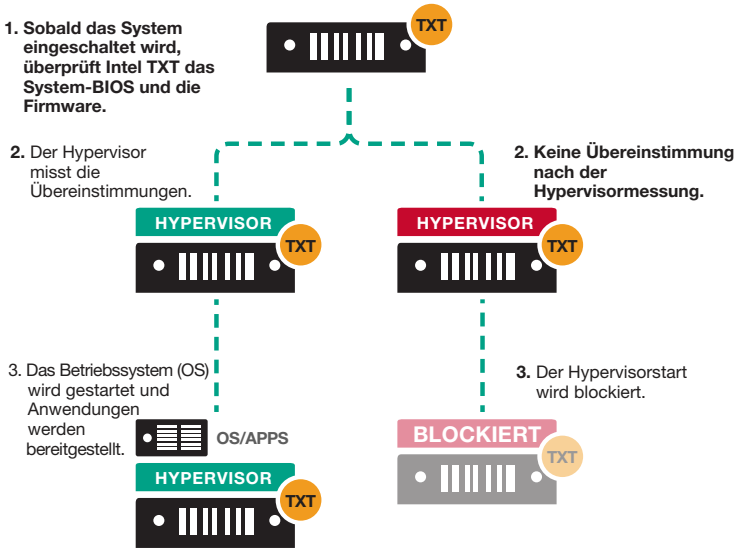
Intel TXT ist auf bestimmten Bare-Metal-Servern verfügbar, die in der IBM Cloud bereitgestellt werden. Wenn Sie einen neuen Server bestellen, wählen Sie im Store einfach die Option „Intel TXT“ aus oder kontaktieren Sie einen unserer Cloud-Experten.

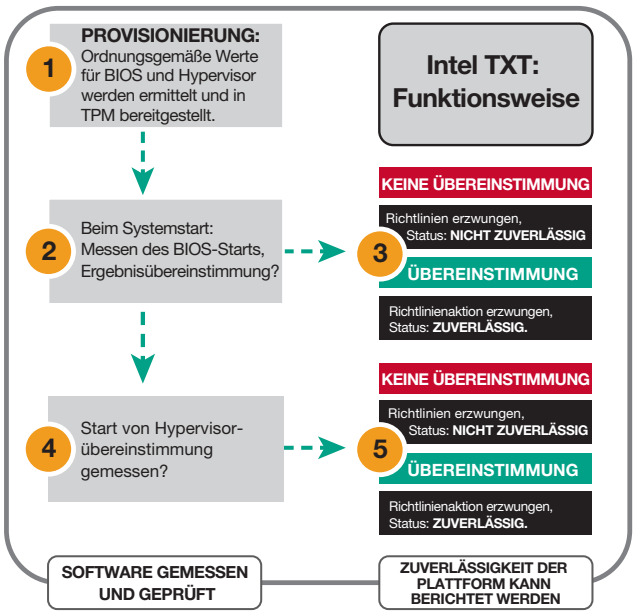
Produkteigenschaften

Eine Vertrauenskette erstellen
Während der gesamten Hardware-Bereitstellungssequenz wird eine Hardware-basierte Vertrauenskette durch den Hypervisor erweitert.

Launch Control Policy (LCP)
Die Launch Control Policy stellt sicher, dass sowohl die Hardware als auch die Software – und diese bereits vor der Bereitstellung – geprüft werden und sich in einem ordnungsgemäßen Zustand befinden.

Standortbasierte Steuerelemente bereitstellen
Zur Einhaltung der gesetzlichen Bestimmungen und Richtlinien wird eine Migration virtueller Maschinen (VMs) nur auf zugelassenen Servern, die einer speziellen Richtlinie folgen, durchgeführt.





vmware
vCloud Air™ Network

IBM Cloud