IBM Cloud

SOFTLAYER

安全無虞的雲端工作負載

VMware on IBM Cloud 整合
Intel® 可信賴執行技術

安全無虞的雲端工作負載

保護公有雲的企業工作負載，避免潛在的安全性威脅。IBM Cloud 裸機伺服器整合 Intel TXT，提供硬體輔助安全性技術，協助您打造安全無虞的平台。

IBM Cloud 是第一個採用 Intel TXT 確保基礎架構安全的雲端服務供應商。Intel TXT 能確保 BIOS、韌體與 Hypervisor 等硬體平台正常運作。

導入技術

Intel TXT 打造一個已衡量執行環境 (*Measured Launch Environment,* MLE)，其包含從 BIOS 到 Hypervisor 的環境執行關鍵要素。在開機的過程中，信任平台模組 (TPM) 會保留電腦產生的加密金鑰，此編碼會不斷測量、展延、驗證與執行，直到建立一個可信任的系統。如果目前的開機環境不符合明定的完善配置，Intel TXT 硬體會避免啟動系統來保護關鍵應用程式與伺服器免於潛在威脅。

開始使用 Intel TXT

IBM Cloud 上所佈建的部分裸機伺服器搭載了 Intel TXT。當您訂購全新伺服器時，僅需要勾選 Intel TXT 選項或聯繫雲端專家。

產品特色

打造可信賴的流程
硬體保障的可靠的流程貫穿了整個執行過程，從硬體延伸到 Hypervisor。

啟動控制原則
驗證硬體與預先啟動軟體是否經過審查且保持最佳狀況。

依據地點提供監控服務
為了確保合規標準，系統會根據特定原則限制虛擬機器僅能遷移到認可的伺服器。