白皮書

提升伺服器安全性並保護您在雲端的業務

使用 IBM Cloud 與 Intel® TXT[1]，在可靠的安全基礎上，建置可信賴的使用者環境

執行摘要

此份白皮書中，我們將探討 Intel® 可信賴執行技術 (TXT) 這項高擴充性架構，及其如何提供硬體型安全技術，在 IBM Cloud 建置可靠的安全基礎。

Powered by intel Cloud Technology

IBM

讓您安心的夥伴關係

保護資料與應用程式非常重要，尤其是使用雲端基礎架構的時候。在現場的資料中心環境裡，要保護硬體的實體存取與安全控管相對來說比較容易。但是，要設置內部資料中心不僅是天價，更無法像雲端供應商的資源一樣，享有相同的靈活度和可擴充性。

雲端和虛擬技術更適合現今的彈性工作負載。伴隨著全新又不斷進化的安全挑戰，需要更強大的安全工具和技術。由於對基礎架構的攻擊日益增加，手法也愈形複雜，您必須確知自己的資料安全無虞、異地硬體可通過驗證而且可以信任，而且您的雲端環境亦符合嚴格的合規要求。

IBM Cloud 與 Intel® TXT 能讓您安心。

IBM Cloud 為首屈一指的 IaaS (基礎架構即服務) 供應商，佈建了搭載 Intel® Xeon® 處理器的裸機與虛擬伺服器，為全球資料中心的安全處理樹立了業界典範。這些關鍵要素因為能解決實體與虛擬基礎架構上不斷增加的安全威脅，從而能提升合規性，並提高基礎架構的安全性與可用性。

提供硬體型驗證

Intel® TXT 與商業軟體相容，可避免 BIOS 與韌體發生異常狀況，例如不明的異動、攻擊與安裝 Rootkit 惡意程式。Intel® TXT 強大的安全基礎能確保您選擇的 IBM Cloud 伺服器可以：

- 建立**彈性的動態信任基礎測量** (DRTM)
- 啟動系統至已知的良好狀態
- 驗證重要平台元件的**完整性**
- 驗證伺服器是否實際架設在**可信賴的位置上**
- 確保您的雲端工作負載在可信賴的運算集區執行，從而建立**可見度、控管與合規**
- 確保運算集區仍然依照原始配置且值得信賴
- 在不正常關機的情況下提供**資料防護**

Intel® TXT 提供您安全無虞的防護

在軟體開機前採取行動

Intel® TXT 是一項硬體型技術，在其他啟動環境防護解決方案上，添加一層強大的防篡改層。在 IBM Cloud 裸機伺服器上啟用 Intel® TXT 後，韌體可以確保安全防護，甚至能啟動硬體。在這個層面，Intel® TXT 早在傳統軟體型的安全解決方案介入之前，就發揮作用了。

當 Intel® TXT 技術在 IBM Cloud 伺服器上啟用後，可以加強全面的資料加密、增加安全連線的使用、保護基礎架構，並建立更高的合規安全保證。

在系統啟動時建立信任基礎

透過測量和儲存已知的良好系統配置，Intel® TXT 能在啟動時，為系統的重要韌體與軟體元件，提供處理器評估。當系統在雲端啟動時，Intel® TXT 會將系統的重要平台軟體與您已知的良好配置測量結果做比較，然後判斷資訊是否相符：韌體、BIOS、作業系統以及 Hypervisor 程式碼。

驗證步驟結合信任基礎功能，套用準則來允許或拒絕工作負載在伺服器系統上執行。例如，可允許的操作包括：繼續啟動或允許啟動，但是將啟動配置標示為處於未知狀態。

建立可信任的運算集區

Intel® TXT 的測量結果，可做為建立可信任伺服器集區的新控制點。在可信任池當中，各個平台會在啟動過程之中展現出重要元件的完整性。要是平台無法通過驗證，可以退出信任池做修正。

例如，若您的 IBM Cloud 裸機伺服器搭載 Intel® TXT，就能以安全性準則在可信任集區中標示系統與工作負載。您就可以從本端或遠端監控、控管，並稽核存取、應用程式的執行與工作負載。您還可以使用地理標記，將工作負載限制在位置已核可的 IBM Cloud 伺服器上，或者使用原則工具，確保機密資料僅能在經過隱私政策、法規或適用法律核可的資料中心的伺服器上才能解密。

主機位置	地理標記	能否信賴
伺服器 202	美國華盛頓州西雅圖	✓
伺服器 241	澳洲澳大利亞雪梨	✓
伺服器 260	歐洲法國巴黎	✕
伺服器 336	亞太地區新加坡	✓
伺服器 342	美國德州達拉斯	✓
伺服器 351	美國德州達拉斯	✕

這些 Intel® TXT 型的高階安全功能，在合規要求嚴格的產業或需要處理大量機密資料的產業中特別實用。

改善稽核與合規

Intel® TXT 為啟動時間的完整性提供了嚴格的執行點。透過應用程式開發介面 (API)，Intel® TXT 還可加入至匯報機制，提供系統狀態的可見性，支援稽核與合規 [2]。

因為以 Intel® TXT 為基礎，您的 IBM Cloud 裸機環境是貴公司安全產品組合的強大元件。

採用 Intel® TXT，讓雲端提升您的工作效率

搭載 Intel® TXT 的 Intel® 雲端技術有助於啟動與保護 IBM Cloud 處理器之上的基礎架構堆疊。Intel® TXT 從信任根與測量過的啟動環境開始，能大幅增強對攻擊或未知事物的防護。提高資訊安全、改善威脅與安全漏洞管理、加強身份與存取管理、提高應用程式安全性，並改善系統的實體安全性。

如何在伺服器上取得 Intel® TXT？

這很簡單：只要在配置可使用的 IBM Cloud 裸機伺服器時，新增 Intel® TXT 支援即可。

下一步該怎麼做？

- 這裡提供幾個簡單步驟保護您的資料：**https://ibm.co/safeguard**
- 請參閱安全性文件：**http://ibm.co/securitydocs**
- 瞭解更多 Intel® TXT 相關資訊：**http://www.intel.com/txt**
- 開始在 IBM Cloud 上使用 Intel® TXT：**http://www.ibm.com/inteltxt**
- 歡迎聯絡 IBM 業務代表：**http://www-07.ibm.com/tw/InsideSales/index.html**

[1] 沒有任何電腦系統可以提供百分百的安全防護。需要已啟用的 Intel® 處理器、啟用的晶片組、韌體、軟體，也可能需向有能力的服務供應商訂購產品 (不一定每個國家皆可使用)。任何因此遺失或遭竊的資料和系統或是任何其他損失，Intel® 均毋須承擔任何責任。如需相關資訊，請造訪：http://www.intel.com/go/txt。
[2] 使用 IBM Cloud 夥伴所提供之軟體。如果要使用特定型號之全部功能，可能需要搭配其他個別軟體。

台灣國際商業機器股份有限公司 台北市 110 松仁路 7 號 3 樓 2017 年 7 月